A Bibliography of Pseudorandom Number Generation, Sampling, Selection, Distribution, and Testing

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254

E-mail: `beebe@math.utah.edu`, `beebe@acm.org`, `beebe@computer.org` (Internet)
WWW URL: `https://www.math.utah.edu/~beebe/`

14 June 2025
Version 1.410

Title word cross-reference

#14 [2327]. **#15949** [896]. **#4059** [1273]. **#8373** [2149].

$(0,1)$ [1082]. $(0,s)$ [2592, 3010]. $(a^n-1)/(a-1)$ [943]. (j,ϵ) [749]. $(n^2\alpha)$ [2543]. $(n^k\alpha)$ [2544]. $(n\alpha)$ [2543]. (t,m,s) [2091, 2965, 2097, 2400]. (t,s) [2691, 2091, 2391, 2965, 2097]. (X,Y) [3754]. $(X^2-Y^2)^{1/2}$ [500]. $0.1(0\times 1)0\times 9$ [141]. 1 [756, 900, 2913, 173, 306, 731, 3046, 3048]. $1,2,3$ [3600]. $1.13198824\ldots$ [2567]. $10,000$ [285]. **$10.00** [170]. 10^{2857} [2538]. 10^{435} [2088]. 1200μ [3223]. 128 [3249]. 13 [273]. 16 [273]. 2 [2913, 2168, 955, 3183, 2552, 2890, 3050, 397]. 2,000 [87]. **$24.95** [2136]. $2^{-31}-1$ [859, 956]. 2^{15} [2186]. $2^{31}-1$ [3652, 823, 1000, 1033, 1225, 1226]. $2^{31}-69$ [3488]. $2^{32}-1$ [1115]. 2^{α} [1510, 2287]. 2^{β} [1348, 1517, 1769]. 2^k [2672]. 2^{k-1} [2672]. 2^p [3344]. 2^p-1 [2320]. 2^t [4001]. 3 [1825, 3801]. 32 [3743]. 4 [273]. 48 [248]. 5 [273]. **$52.95** [3707]. 64 [3940]. $[0,1]$ [219, 871]. $^{-1}$

[3744]. ^{2} [3223]. $_\tau$ [2422, 2000]. a [369]. $a = \pm 2^q \pm 2^r$ [2455, 2530]. a_n [667]. $\alpha \geq 1$ [3747]. $\alpha\lambda$ [733, 734]. b [2183, 3439]. $b = 2, 3, 5, 6, 7, 10, 11, 12$ [1062, 1333, 2679]. $b^n \pm 1$ [1062, 1333, 2679]. $\beta = 32$ [1348]. $\beta = 48$ [1348]. $\beta \simeq 32$ [1517]. $\beta \simeq 48$ [1517]. $\left\{\frac{a}{m}j^2\right\}, \left\{\frac{a}{m}(j+\tau)^2\right\}$ [328]. mod1 [301, 302, 408, 659, 742, 664]. mod$n$ [2253]. C^∞ [1292]. $C\exp(-\lambda|x|^\nu)$ [1498]. χ^2 [349, 951, 1112, 1113, 1114, 6, 7]. D [2426, 1845, 3058, 2127]. d^2 [93]. e [81, 1536, 87, 372]. ϵ [1950]. F_2 [3094, 3105, 3330, 3940]. F_{2^w} [2891]. G [453, 454]. Γ [1247, 1220]. j [2052]. K [2240, 3959, 1486, 3928, 3961, 1803, 2160, 1067, 1350, 1957, 3800, 3835, 1133, 1389, 2008]. $k > 1$ [1378]. L^2 [2076, 2004]. L_2 [2178]. L_p [2452]. λ [2880]. M [1465, 1230, 1196, 852, 470, 1069, 1038, 447, 250, 1382, 2203, 2386, 2120, 2228, 2230, 2317, 1144, 231]. $\mathbf{F}_2$ [3186, 3563]. $\mathbf{F}_{2^w}$ [3049]. $\mathbf{F}_q$ [3307, 3621]. $\mathbf{F}_{q^m}$ [3307, 3621]. $\mathbf{R}^d$ [4068]. $\mathbf{F_2}$ [3564]. GF(2^{m}) [1595]. μ [3286]. N [1162, 919, 270, 1338, 1714, 1715, 2274, 730, 3797, 205, 623, 196, 2852, 201, 1552, 3917, 804, 207, 430, 807]. O(3) [1597]. $O(n(1+\log(N/n)))$ [1967]. P [6, 728, 3980, 4057, 3228, 2474, 2221, 3441, 2234, 2418]. $\partial^2 u/\partial x^2 + \partial^2 u/\partial y^2 + (K/y)(\partial u/\partial y) = 0$ [197]. π [2928, 81, 1536, 87, 285, 288, 2985]. ± 1 [667]. $\pm 2^{k_1} \pm 2^{k_2}$ [2320]. $\pm 2^{p_1} \pm 2^{p_2}$ [2664]. q [2556]. S [1032, 1908]. σ [1597]. $\sqrt{2}$ [411, 442]. $\sum a_n/n$ [667]. T [2625, 2908, 1898, 853, 1908, 1336, 3099, 870, 965, 970, 40]. $U(0,1)$ [2780]. $X(I+1) = AX(I) \bmod 2^{31}1$ [785]. X/Z [3754]. $x^2 \bmod N$ [2035]. $X_{n+1} = a_n X_n + b_n \pmod p$ [1830]. $X_t = X_{t-3p} \oplus X_{t-3q}$ [1520]. Y/Z [3754]. $y = [(a+x)\sin(bx)] \bmod 1$ [2398]. Z [3754]. Z/nZ [1941]. Z_p [1420].

good [2723].

-adic [3439, 454, 453, 2418]. **-biased** [1950]. **-Bit** [3249, 3940, 248]. **-concave** [2625]. **-D** [3183]. **-deformed** [2556]. **-dependent** [1950]. **-Detection** [3917]. **-digit** [273]. **-Dimensional** [270, 196, 201, 919, 1552, 2008, 1803, 807, 205, 1338, 3058]. **-discrepancy** [2076]. **-distributed** [1350]. **-Distribution** [970, 1898, 1067]. **-distributions** [1845, 2127]. **-échantillon** [804]. **-estimates** [1465]. **-Fock** [2556]. **-function** [2052, 2880]. **-functions** [1292]. **-homomorphism** [2426]. **-Linear** [3094, 3186, 3940, 3105, 3330, 3563, 3564]. **-model** [1597]. **-net** [2091]. **-Nets** [2965, 2097, 2400]. **-nm** [3743]. **-observation** [1714, 1715]. **-quanta** [1220]. **-Random** [2234]. **-sample** [804]. **-sequence** [1038, 1382, 2386, 2091, 1230, 1196]. **-Sequences** [852, 2592, 3010, 447, 2391, 2965, 2097, 2691, 1069, 2203, 2120, 2228, 2230, 2317]. **-sphere** [1144, 430]. **-step** [1133, 1389]. **-System** [2240]. **-Values** [728, 3228]. **-Vector** [3961, 3928, 3800, 3835]. **-wise** [3959, 1486, 2160, 1957].

/dev/random [2762, 3724, 2820, 2915]. **/dev/urandom** [2820].

0.57pJ [3358]. **0.57pJ/bit** [3358]. **'05** [4239, 4243]. **'07** [4249]. **'08** [4254].

1 [766, 1071, 1963, 1964, 3470, 3373]. **1.04** [3286]. **1.1** [3827]. **1.6** [3744]. **'10** [4268, 912]. **1013** [4006]. **106** [1114, 845]. **10th** [4096, 4244]. **11** [1342]. **111** [818]. **11th** [4093, 4264, 4175]. **12** [896]. **120** [2910]. **128-bit** [2508, 3242]. **12th** [4243]. **'13** [4290]. **133** [268, 269, 308, 314]. **134** [900]. **13th** [4211]. **14th** [4250, 4178]. **153** [954, 1113, 1114]. **155** [951, 1114]. **157** [1003]. **16** [2926, 1508, 3057, 937]. **16-Bit** [1295, 1906, 762, 1508, 2224]. **16-bit-PC** [1508]. **160** [2526]. **16th** [4161]. **1750** [1921]. **17th** [4268]. **181** [1869]. **183** [1187, 1053, 1147, 1262]. **193** [1173, 1072]. **1949** [4085]. **1953** [4088]. **1954** [4089]. **1957** [4090]. **1960** [4091]. **1962** [4095]. **1965** [4096]. **1967** [4098]. **1970** [507]. **1971** [4101]. **1974** [4103]. **1976** [4107, 4104]. **1978** [4108]. **1981** [4113]. **1983** [4116, 4119]. **1984** [4123, 4121]. **1986** [4127, 4131]. **1987** [4132]. **1988** [4138, 4137, 4139, 4141, 4142]. **1989** [4147]. **1990** [4148, 4149, 4163]. **1991** [4155, 4156, 4161]. **1992** [4159, 4166, 4167]. **1994** [4177, 4179, 4187, 4180, 4181]. **1995** [4182, 4193, 4184]. **1996** [4207, 4195]. **1997** [4196, 4200]. **1998** [4213, 4206, 4214]. **1999** [4209, 4210]. **1a** [3474].

2 [196, 221, 2305, 3471]. **2.4GHz** [3483]. **20** [2136, 2475]. **200** [303, 364]. **2000** [4231, 4220, 3197]. **2001** [4226, 4228]. **2002** [4229, 2678, 4236]. **2003** [2963]. **2004** [4234, 2678, 4246]. **2005** [4239, 4248]. **2006** [4257]. **2007** [4249, 3224, 4253]. **2008** [4254, 4256, 4265]. **2009** [4266]. **2010** [4268, 4273]. **2011** [4280]. **2014** [3842, 3883]. **2018** [3954]. **204** [1112]. **205** [1414, 1123]. **20MHz** [2598]. **20th** [4295, 4141, 4142]. **21st** [4206, 2845]. **22** [2940, 3029, 3693]. **22nd** [4210]. **235** [321]. **23rd** [4114]. **247** [324]. **24th** [4117]. **25** [2149]. **256** [2909]. **25th** [4120]. **266** [361, 362, 630]. **267** [363]. **27th** [4252]. **28th** [4135]. **29** [505, 809]. **294** [426]. **29th** [4156, 4140]. **2nd** [4113, 4126].

3 [3645, 3188, 3837, 1986, 3472, 3844]. **3-Key** [2946]. **3.0** [2693]. **3.x** [2326]. **30** [3611]. **30th** [4146, 4167]. **31** [2612]. **31-bit** [774]. **31st** [4152]. **32-Bit** [1242, 2964, 2989, 3030, 3104, 1777, 3487]. **32-bit-word** [546]. **334** [435, 480]. **33rd** [4162]. **342** [460, 462]. **360** [816, 680, 479, 484, 493, 463]. **360/370** [724]. **369** [530]. **36th** [4234, 4185]. **370** [502, 620]. **37th** [4239, 4194]. **3800** [2132]. **381** [517, 625]. **38th** [4198]. **39th** [4249].

4 [466, 675, 3473]. **4086** [2929]. **40th** [4254]. **41st** [4219]. **42** [695, 696]. **4217th** [3488]. **4217th-order** [3488]. **425** [598, 700]. **42nd** [4223]. **440** [3149]. **440-nA** [3149]. **441** [647]. **45nm** [3358, 3483]. **46** [2149]. **48** [498]. **48-Bit** [1048, 933]. **488** [677]. **4Gbps** [3358].

5.0 [1676]. **5.2** [2820]. **500** [3411, 322]. **51st** [4274]. **52** [896]. **52nd** [4289]. **5th** [4255].

6 [3742]. **60th** [4291]. **61** [1262]. **623-dimensionally** [2385]. **64-bit** [2258, 763, 2723, 2878, 2550, 3608, 3613]. **647** [1228]. **659** [1331, 2791]. **668** [1366]. **678** [1445]. **6th** [4218].

701 [155]. **71** [1273]. **712** [1743]. **738** [1901]. **76** [1039]. **780** [2355]. **79** [2182]. **7mW** [3483].

8-bit [2598]. **8.8/11.2** [4272]. **800** [3079, 3881]. **800-22** [3474]. **800-90** [3079]. **800-90B** [3881]. **802** [2516]. **806** [2541, 2542]. **8088/8086** [1275]. **80f** [937]. **82** [4115]. **82g** [1071]. **82h** [1039]. **84** [4125]. **85** [2058]. **'86** [4136]. **'87** [4133]. **'88** [4151]. **8th** [4284, 4139].

'90 [4153, 3079, 2064]. **90/150** [2821]. **90/95** [2690]. **90B** [3881]. **'91** [4161]. **92** [719]. **'93** [4168, 4171]. **'94** [4178, 4179, 4180]. **947** [3794]. **'95** [4184, 4186, 2023]. **958** [3870]. **'96** [4190, 4195]. **'97** [4200, 2464]. **970** [3921]. **978** [3742]. **978-0-521-17561-6** [3742]. **978-0-88385-043-5** [3707]. **97j** [2305]. **'98** [4213, 771, 865]. **9th** [4272].

= [4090, 4101].

A.2.4 [2946]. **AAECC** [4211]. **AAECC-13** [4211]. **AbBT** [1630]. **Absolute** [401, 371]. **Absorption** [290]. **Abstract** [2428, 1167, 1524, 2613, 1641, 1646, 1561, 1201, 3666, 1444, 2521, 1837, 3575, 1248, 2487, 2490]. **abstracts** [4161]. **abuses** [1396]. **AC** [2001]. **Accelerated** [3333, 1887, 3717, 3772, 3727, 3208]. **Accelerating** [2332, 3420, 3805]. **Acceleration** [3933, 2275, 3783, 3976, 1960]. **Accelerator** [4002]. **Acceptance** [1518, 3666, 1125, 979, 3853, 2917, 1011, 1039]. **Acceptance-Complement** [1125]. **Acceptance-Rejection** [1518, 3666, 3853, 2917, 1011, 1039]. **Acceptance/rejection** [979]. **Access** [1799, 2037, 4009, 2206, 1701, 1702, 3191, 2087, 2759]. **according** [11, 697]. **Accumulated** [338, 1996]. **Accuracy** [212, 2769, 1344, 1455, 654, 1188, 2570, 3142, 3588, 2464, 2729, 2963, 3224, 3339, 565, 3808, 575, 631, 2207, 3072]. **Accurate** [3072, 854, 3831, 3141, 602, 3746]. **Achieve** [3967]. **achieving** [441]. **Acknowledgement** [695, 696]. **ACM** [4176, 4127, 4132, 4138, 4148, 4159, 4168, 4177, 4182, 4209, 4216, 4229, 4239, 4249, 4254, 4267, 4276, 4283, 4290, 4156, 4243, 4266, 4180, 677, 502, 598, 517, 647, 361, 620, 3596, 530]. **ACM-SIAM** [4176]. **ACORN** [1483, 1791]. **acquisition** [2283]. **acquisition-processing** [2283]. **ACR** [1529]. **Actel** [3176]. **actions** [2065]. **Active** [3635, 3129]. **Actuarial** [4238]. **Acyclic** [1410]. **Ada** [1411, 2023, 1212, 1729, 1362]. **Adams** [2255]. **Adaptive** [3077, 2055, 2273, 3188, 919, 735, 3813, 3433, 2289, 3800, 3601, 807]. **Add** [1785, 2672, 1933, 1883]. **Add-with-Carry** [1785, 1883]. **Addendum** [1335]. **addition** [2207]. **Additional** [3219, 806]. **additions** [2071]. **Additive** [2134, 2673, 909, 2255, 200, 185, 2082, 2083, 2883, 456, 634, 471, 556, 600, 601,

1977, 842, 2316, 3620, 3266, 3498]. **adic** [3439, 453, 454, 2418]. **Adjoint** [2099]. **Adjustable** [4079, 3283]. **Administration** [4189]. **Admissible** [3116]. **Advance** [4081]. **Advanced**
[1487, 1959, 4103, 4272, 4221, 2482, 2561]. **Advances** [4115, 4133, 4151, 1096, 4201, 4213, 2716, 4172, 2738, 4123, 4125, 4178, 4252, 4136]. **Advancing** [4262]. **Adventures** [4026, 4197]. **adversaries** [3706]. **advised** [3889]. **aegis** [4096]. **AES** [2785, 2521, 2609, 2946]. **Affairs** [4096]. **Affects** [4014, 3541]. **Affine** [3871, 3973, 2557]. **Against**
[2923, 4070, 3396, 3900, 1361, 3236, 3706, 3500, 3889, 3989]. **Age** [2769]. **Agricultural** [24, 299, 47, 73, 114, 115, 171, 172]. **Ahead**
[3094, 3186, 3187, 3381]. **Ahrens** [896]. **AI** [4076]. **aid** [2111]. **Aimed** [3062]. **Air** [4098, 1917]. **AIS** [2612, 2475]. **AIX** [2820]. **Akima** [776]. **al.** [921]. **Alabama** [4156]. **Alamos** [3786]. **Alberta** [4103]. **Alea** [3518]. **aléatoire** [1900, 322, 804]. **aléatoires** [4082, 2844, 762, 2196, 284, 343, 2552, 1588]. **aleatorios** [134]. **Alexandria** [4243]. **Alfred** [3318]. **Algebra**
[2029, 3288, 1866, 3708, 4157, 3864, 4211, 425, 4157]. **Algebraic**
[436, 4169, 2768, 3785, 1537, 4186, 2390, 2391, 527, 3500, 4050, 3970, 4211, 1368, 121, 665, 99, 286, 3957]. **Algebraic-Geometry** [2390]. **Algorithm**
[4006, 756, 817, 2499, 2999, 903, 677, 1797, 545, 502, 760, 3645, 681, 1912, 1280, 2438, 2439, 2440, 2593, 105, 3187, 512, 1173, 2788, 1072, 598, 919, 1294, 4071, 3791, 517, 647, 27, 651, 2955, 3214, 3592, 1300, 1384, 1652, 1568, 2098, 838, 361, 2646, 620, 367, 530, 1998, 1999, 3482, 1881, 2005, 3921, 2902, 1051, 1589, 2231, 1052, 2668, 1887, 1678, 2987, 3853, 1894, 1896, 3395, 3151, 3076, 3720, 853, 1269, 1498, 759, 2424, 2501, 2921, 1108, 3902, 504, 4030, 553, 1160, 3302, 1285, 2171, 2776, 2600, 2938, 3563, 1171, 1124, 3204, 2949, 1457, 3999, 4036, 1746, 3878]. **algorithm** [2886, 796, 2633, 1191, 1305, 2889, 3756, 3916, 2393, 1085, 3918, 1090, 704, 931, 623, 3843, 1578, 1875, 3601, 2116, 3486, 1787, 1788, 1315, 2410, 2411, 1674, 2131, 2988, 2908, 4045, 753, 3710, 807, 2761, 4006, 900, 818, 268, 269, 435, 1331, 1901, 719, 951, 505, 321, 954, 1112, 1228, 303, 771, 1003, 324, 2355, 380, 1173, 865, 1072, 2516, 2791, 1366, 1445, 480, 3794, 308, 3870, 1743, 2541, 2542, 1187, 700, 362, 363, 364, 391, 314, 625, 845, 460, 462, 426, 630, 3921, 809, 1053, 1147, 3384, 3507, 1262]. **Algorithmic**
[3414, 3969, 4003, 1755, 570, 1591, 4202]. **algorithmische** [570]. **algorithmischer** [1755]. **Algorithms**
[4176, 898, 900, 3894, 818, 1796, 2243, 1270, 2152, 719, 3171, 951, 1614, 505, 1111, 954, 1112, 1113, 1114, 3304, 1034, 771, 772, 1003, 1935, 3021, 4212, 1172, 2607, 2702, 1173, 865, 646, 690, 1072, 1835, 1840, 2946, 2368, 2527, 2190, 1371, 2192, 1967, 2798, 487, 1187, 4002, 2208, 1309, 2219, 2222, 1778, 845, 2482, 4228, 4165, 4106, 809, 1053, 1147, 1262, 1682, 896, 3772, 2580, 1692, 3077, 2150, 1220, 2930, 2173, 2270, 4211, 1169, 3661, 2178, 1732, 1369, 1839, 1541, 1542, 4055, 2626, 1747, 3746, 1758, 3689, 3046, 1307, 1872, 2473, 4061, 3805, 2001]. **algorithms** [2002, 4212]. **Alias** [2220, 2978, 1404, 1005, 922]. **alignments** [1894]. **All-Digital** [3358, 3483]. **All-Optical** [3681]. **alla** [470]. **Alleged** [2596]. **Alley** [1998, 1881, 2005]. **Allocation** [646, 690, 732, 2680, 3433].

Almost [3008, 3664, 1486, 4020]. **Along** [3946]. **Alternating** [1359, 3119]. **Alternative** [3549, 826, 1946, 2626, 2813]. **Alternatives** [2466, 1229, 164, 50]. **Alto** [4290, 4204]. **always** [3754]. **AMD** [3963]. **Amer** [1273, 1039]. **America** [3707]. **American** [4093, 4160, 4088]. **Amiel** [319]. **Among** [2434, 1537, 285, 847, 1908, 2084, 2085, 2462, 2493]. **Amplification** [2634, 2808]. **Amplified** [3499, 3650]. **amplifier** [3513, 3514]. **Amsterdam** [4133, 4295]. **Anal** [937]. **analiz** [351]. **Analog** [354]. **Analog-Digital** [354]. **Analogue** [197, 1125, 553]. **analyse** [4101]. **Analyses** [1821, 3066]. **Analysis** [3143, 4251, 3146, 3894, 3148, 2326, 4065, 2144, 947, 948, 992, 3964, 759, 3536, 993, 1212, 3857, 1911, 404, 4088, 1615, 1159, 2049, 3091, 1115, 1517, 2596, 3309, 2599, 3019, 2604, 3185, 3662, 777, 2861, 960, 1954, 3791, 963, 921, 2527, 2192, 3998, 968, 3869, 2370, 4280, 787, 447, 969, 3439, 3219, 873, 1980, 1469, 4038, 3341, 1568, 3838, 838, 1985, 4015, 4163, 842, 55, 57, 976, 3478, 493, 1999, 2978, 4094, 1479, 1785, 291, 265, 3268, 3380, 3500, 753, 1203, 4101, 1682, 1025, 2424, 2501, 3079, 402, 2156, 4026, 1805, 3724, 3415, 2166, 1164, 1225, 1226, 1348]. **analysis** [2351, 2054, 1628, 3562, 2277, 2357, 1364, 3191, 1237, 2186, 3573, 2526, 1843, 1040, 1638, 2528, 3032, 3036, 2955, 3581, 4036, 788, 1747, 2797, 2960, 3443, 2725, 1014, 1083, 3449, 3343, 1759, 1248, 1304, 2637, 3882, 3349, 1987, 665, 459, 2111, 746, 264, 2116, 2657, 2663, 3065, 3130, 209, 1587, 2410, 2411, 3373, 3617, 20, 236]. **Analytic** [2037, 3571, 1086]. **Analytical** [2594, 356, 4291]. **analyze** [4024, 3970]. **Analyzing** [2242, 2266, 1370, 2190]. **anaylsis** [499, 618]. **Andersen** [238]. **Anderson** [1042, 2537]. **Android** [3725]. **Angeles** [4086, 4135, 91]. **angenäherten** [278]. **Angle** [517, 625]. **animals** [1899]. **Ann** [695, 696]. **Annealing** [3790, 3058]. **Annual** [4229, 4234, 4239, 4249, 4254, 4290, 4268, 4156, 4117, 4152, 4162, 4185, 4194, 4198, 4219, 4274, 4289, 4126, 4252, 4228, 4215, 4167, 4108, 4176, 4122, 4127, 4132, 4138, 4143, 4148, 4159, 4177, 4182, 4191, 4209, 4216, 4178, 4218, 4114, 4120, 4135, 4140, 4146]. **Anosov** [3884]. **ANSI** [2946, 2620, 2718, 3035, 3107]. **Anthanasios** [389]. **Antithetic** [725, 732, 2077]. **Antonio** [4208]. **Antony** [4217]. **ANTS** [4202]. **ANTS-III** [4202]. **any** [349, 2448, 76, 617]. **Aperiodic** [3855, 2783, 3735, 3240, 1600]. **APG** [1869]. **apparent** [839]. **Appearing** [1545]. **Appears** [1354]. **Appendix** [2946]. **Appl** [2305, 3708]. **Apple** [1149, 1265]. **Applesoft** [1353]. **applicability** [1157]. **Application** [3510, 852, 3148, 4123, 906, 2847, 4133, 304, 2779, 2702, 3190, 4256, 1630, 2288, 2529, 2370, 44, 3223, 3752, 2468, 3698, 3062, 888, 290, 3253, 3370, 3991, 3281, 2921, 2027, 3539, 2851, 4272, 3425, 2786, 3569, 3570, 3435, 1127, 3683, 2101, 1194, 2895, 706, 978, 746, 1255, 2478, 137, 3257, 1595, 3269, 4045, 2759, 7, 4046]. **Application-based** [1630, 3683]. **Application-Specific** [4256]. **Applications** [1151, 3768, 4144, 2915, 3394, 180, 819, 2246, 3160, 2429, 2036, 2683, 3083, 4109, 1922, 3009, 1167, 3021, 3095, 513, 2861, 2943, 3430, 156, 1836, 2452, 518, 1848, 2297, 3213, 1243, 1968, 3589, 2086, 805, 2649, 3474, 2822, 4247, 2655, 3984, 537, 2407, 2231, 4101, 4201, 3157, 3, 2767, 3859, 4193, 1711, 635, 4230, 1809, 2257, 2170, 2173, 2270, 1069, 1431, 1627, 4255, 3312, 3313, 3906, 4242, 2787, 3322,

4213, 2068, 2185, 3739, 2629, 3583, 2198, 3444, 2801, 3230, 1562, 802, 1654, 2549, 2396, 2553, 1587, 1588, 2666, 1099, 3264, 2235, 1261, 1054, 3742, 4101, 2136]. **Applied** [4098, 4093, 4088, 3301, 4271, 1169, 4292, 2300, 4163, 2222, 498, 320, 42, 242, 482, 4108, 4211]. **Applying** [3521, 2100, 3772]. **Approach** [1492, 3649, 72, 2049, 3553, 4052, 777, 3108, 525, 3451, 2390, 4293, 290, 2575, 4024, 1811, 3970, 2437, 3215, 3835, 1563, 2973, 569, 1050, 1584, 3953, 2669, 2568]. **approaches** [2756]. **Approximate** [902, 2036, 4051, 1635, 2379, 1987, 621, 705, 4076, 573, 952, 278, 423, 750, 1784, 2829]. **Approximately** [510, 1839]. **Approximating** [2509, 4051, 3576]. **Approximation** [2252, 2432, 2451, 1455, 1544, 2906, 2570, 1896, 3177, 1288, 1129, 3835, 1255, 751]. **Approximations** [145, 2864, 1078, 485, 1029, 3101, 1256, 3067, 3133]. **April** [4123, 4093, 4133, 4156, 4272, 4104, 4221, 4106, 4167, 4141, 4142]. **Arbitrary** [2248, 834, 1569, 3137, 990, 3934, 3965, 3080, 199, 1733, 3606, 3252, 1316, 714, 3653]. **Archimedean** [3390]. **Architecture** [2915, 2859, 3975, 3476, 2122, 3381, 3660, 3916, 1588]. **Architectures** [1487, 4256, 3875, 3763]. **arcsine** [4000]. **Area** [241, 1932, 3848, 3143, 2242]. **Area-Efficient** [3848, 3143]. **areas** [4250, 4218, 2795]. **ARENA** [4251]. **Argument** [687]. **arguments** [431]. **Arisen** [1]. **Arising** [1276, 1558, 3623, 3708]. **Arithmetic** [2331, 2423, 2160, 769, 3793, 2796, 739, 3840, 228, 369, 4175, 3630, 3, 1627, 1435, 1252, 1571, 2225, 1876, 1480, 1596]. **arithmetical** [297]. **arithmétiques** [3]. **Arizona** [4117, 4158]. **Arlington** [4176, 4210, 4225, 4119, 4166]. **ARM7** [3176]. **Arnold** [2997]. **arranged** [22]. **arrangements** [59]. **Array** [1413, 3400, 2632, 1399]. **Arrays** [1514, 941, 3801, 810]. **arrival** [3666, 2614, 3618, 3377]. **arrivals** [2776]. **Art** [1751, 1773, 3844, 347, 4110]. **Artefacts** [1606]. **Arthur** [3122]. **article** [896, 2305]. **Artifacts** [2775]. **Artificial** [147, 65, 74]. **ARX** [3752]. **Ascending** [2797]. **aSHIIP** [3493]. **ASIC** [2855]. **Aspects** [4098, 4126]. **Asperger** [3053]. **ASR** [1262]. **Assembler** [2276]. **assembly** [3899]. **assess** [1953]. **Assessing** [2190, 2463]. **Assessment** [1402, 2144, 2847, 2689, 1322, 1485, 2356]. **Assignment** [863, 869, 872, 885, 886, 887]. **Assoc** [1273, 1039]. **Associated** [1279, 2817, 3267, 2913, 1032, 22, 256, 425]. **Association** [1847, 4102, 167, 3707, 978, 7]. **associées** [1032]. **Assumption** [3643]. **assumptions** [1527]. **Astronomical** [1437]. **Asymmetric** [705, 3862]. **Asymptotic** [579, 102, 3811, 687, 4036, 1568, 804, 2315, 1597, 56, 2318, 405, 3292, 2510, 2614, 1788]. **Asymptotical** [2934]. **Asymptotically** [296, 3433, 1465, 2389, 669, 3116]. **Asymptotics** [3100]. **asymptotiques** [804]. **Atari** [1466]. **ATI** [3544]. **Atlanta** [4209, 4196, 4124]. **Atomic** [2574]. **atoms** [1194]. **Attachment** [4009]. **Attack** [3140, 3512, 3892, 3635, 2923, 3182, 2631, 2972, 2406, 3532, 3338]. **Attacking** [4033]. **Attacks** [3396, 2768, 2523, 2366, 3761, 3129, 3500, 3989, 3856, 4026, 3900, 3585, 1468, 166]. **Attraction** [1575, 371, 748]. **Attractor** [1703]. **Auburn** [4156]. **auctions** [3309]. **Audio** [3539]. **Auditorium** [4204]. **August**

[4250, 4160, 4088, 4178, 4218, 4204, 4213, 4224, 4252, 4103, 4163, 2678]. **Austria** [4113, 4171, 4207, 4163, 4199]. **Authentication** [2025, 3920, 3952, 3367, 3368, 3332]. **autism** [3053]. **Autocorrelated** [1650, 1012, 1888]. **Autocorrelation** [1618, 328, 653, 797, 798, 1717, 306, 439, 472]. **Autocorrelations** [329, 991]. **Autocorrelazioni** [991]. **Autokcorrelation** [472]. **Autokorrelation** [439]. **Automata** [2335, 3183, 3196, 3119, 1997, 4094, 4065, 1278, 3299, 2857, 1440, 1441, 1530, 1751, 2386, 3449, 2821, 2652, 2745, 2478, 2405, 2009, 1588, 2488, 2566, 1671, 1260, 1261, 2016]. **automata-based** [1440]. **automated** [3915, 1869]. **Automates** [1588]. **Automatic** [170, 1217, 2853, 2517, 2863, 2535, 789, 163, 2516, 3944, 4037, 137, 176, 4087, 3004, 3082]. **Automatically** [2423]. **Automation** [3317, 4279]. **automaton** [2912, 3949]. **automorphisms** [3785]. **Autonomous** [3493]. **Autoregressive** [1740]. **available** [3241]. **Avalanche** [3363]. **Average** [1804, 2165, 2259, 2260, 2688, 3011, 2736, 2166, 2854, 3671, 2454, 3604]. **average-case** [2166, 3671]. **Averages** [864]. **Averaging** [3790, 284]. **avoid** [1405, 1624]. **Avoided** [1197]. **Avoiding** [3733, 2600, 1825]. **AVX** [3865]. **award** [3596]. **Awarded** [3954]. **Aware** [1676]. **AWC** [1915]. **AWC/SWB** [1915]. **AWGN** [2673, 3587].

B [400, 2149, 70]. **Babington** [70]. **Babington-Smith** [70]. **Background** [1791, 665]. **backpropagation** [2949]. **backward** [3103, 3066, 3486]. **bacteriophage** [3627]. **Bad** [2269, 2346, 2931, 4113, 4035, 2290, 2619, 3356, 4044, 3469]. **BadRandom** [4011]. **bag** [1736]. **Bailey** [3720, 3721]. **Baillie** [3728]. **balancing** [1364]. **Ball** [4068]. **ballistic** [2339]. **Baltimore** [4148, 4239]. **Banach** [825, 689]. **Band** [628]. **Banff** [4090]. **Baptist** [4231]. **Barbara** [4178, 4252]. **Base** [1912, 787, 1025, 470, 3728, 2399, 3503]. **Based** [3523, 3635, 3638, 2423, 3962, 2847, 4048, 4025, 4066, 2428, 2769, 1706, 3087, 998, 2040, 2687, 637, 2775, 3551, 4031, 4079, 3419, 2511, 2697, 2933, 4053, 3790, 3026, 3324, 3200, 2946, 3740, 2451, 3869, 3214, 3744, 4056, 3442, 3829, 3038, 3223, 3837, 2098, 929, 3460, 4015, 3917, 3352, 1997, 934, 3354, 4076, 2655, 3125, 3247, 3064, 3363, 1786, 3256, 3367, 3368, 1052, 3376, 428, 3268, 3765, 3271, 3412, 3389, 3960, 3274, 3142, 3513, 3514, 102, 2912, 3145, 3991, 3855, 3992, 3633, 3856, 3152, 2917, 3721, 2843, 3158, 2767, 3536, 3283, 3284, 3404, 3407, 4049, 1704, 3542, 3176, 3089, 3970]. **based** [3783, 3552, 3784, 1069, 1230, 2598, 2699, 1070, 2446, 2857, 776, 3313, 1358, 3183, 3423, 3424, 3660, 3315, 1361, 3562, 3566, 3735, 2944, 1440, 3323, 3736, 1630, 3572, 1293, 1447, 3198, 3201, 3976, 4054, 1373, 2291, 2293, 2294, 2714, 2951, 3909, 2873, 2874, 3037, 3332, 3580, 3678, 1849, 3440, 3585, 3873, 4000, 4074, 2721, 3338, 3682, 3683, 2203, 2733, 796, 3836, 3342, 1252, 1388, 3453, 3454, 3755, 4059, 2890, 2891, 3050, 3349, 3693, 1659, 3236, 2396, 2553, 2471, 3466, 704, 2648, 2743, 3598, 99, 189, 3121, 1196, 2557, 3601, 3602, 4041, 3480, 1256, 3126, 3246, 1258, 2827, 2657, 2658]. **based** [4003, 3610, 3360, 3490,

1480, 3253, 3364, 1143, 1671, 2832, 3370, 3496, 3374, 3618, 51, 3850, 3957, 2669, 3379, 2910, 2759, 4063, 3626, 3506, 2990, 3386, 3766, 3077]. **basée** [2890]. **Bases** [3006, 2704, 1148, 583, 1171, 1172, 1018]. **basic** [1626, 1238, 925, 1030]. **Basics** [3417, 3371]. **Basis** [2835, 465, 496, 3943]. **Batteries** [4005, 2641, 3915]. **Battery** [2079, 2201, 4057, 4044]. **Battin** [170]. **Bay** [4268]. **Bayes** [1213]. **Bayesian** [584, 3933, 2036, 3972, 3192, 1014, 2969]. **BBC** [1168]. **BCH** [488]. **Be** [1496, 2607, 3597, 1197, 3768, 3650, 469, 607, 3754, 1, 1676]. **Beach** [4198, 4219]. **Beam** [2687, 3360]. **Beat** [3869]. **been** [3768]. **Beginner** [3909, 2635, 2636]. **Begrenzung** [1755]. **Begründung** [570]. **Behavior** [267, 2633, 874, 3357, 2835, 1326, 3896, 2934, 3092, 1730, 3191, 1253, 463]. **behavioral** [4227]. **behaviors** [3789]. **Behaviour** [2165]. **Belgium** [4256]. **Belong** [3887]. **Benchmark** [1630]. **Benchmarks** [2132]. **Benford** [3525, 3397, 3177, 2774, 3308, 3192, 3043, 3226, 2399]. **Berechnung** [278]. **Bergen** [4248]. **Berichtigung** [221]. **Berkeley** [4127]. **Berlekamp** [2999, 3921]. **Bernoulli** [3540]. **Berry** [659]. **beschränkter** [246]. **Best** [2148, 2584, 783, 1863, 838, 1484, 3596, 3760]. **Bestimmung** [1755]. **Beta** [673, 755, 756, 898, 900, 844, 980, 535, 896, 1268, 318, 853, 855, 3778, 331, 3034, 788, 2096, 1094, 979, 716, 1891]. **beta-** [331]. **beta-verteilten** [1891]. **betaverteilten** [331]. **Bets** [3786]. **Better** [3659, 3193, 3027, 3219, 3608, 634, 4020]. **Between** [3740, 2302, 1794, 1493, 2335, 1431, 2858, 2061, 329, 1950, 1951, 2872, 1553, 927, 928, 34, 1200, 4108]. **Beware** [2455]. **Beyer** [1512]. **Beyerm** [2149]. **Beyond** [3018, 3465]. **bezüglich** [741]. **bialgebras** [2623]. **Bias** [3073, 1798, 3567, 3995, 258, 3378, 3622, 1465, 1562, 3618]. **Bias-Free** [3378, 3622]. **Biased** [1102, 2151, 3986, 1207, 1950, 3234, 2312, 2408]. **Biases** [3887]. **Bibliography** [610, 490, 629, 889, 1257, 935, 977]. **bicompositional** [3639]. **Biennial** [4102]. **billion** [1934]. **billion-record** [1934]. **Billions** [4014]. **Biltmore** [4158]. **bimodal** [3862]. **bin** [1476]. **Binary** [375, 468, 1705, 549, 327, 1847, 3582, 3681, 523, 2543, 2544, 2883, 832, 929, 3695, 2400, 1999, 628, 1782, 538, 539, 2575, 1687, 2913, 1691, 3157, 3158, 3281, 3282, 1154, 759, 2424, 2501, 3536, 3965, 1907, 3163, 1611, 3299, 552, 1714, 1817, 92, 726, 116, 411, 442, 2856, 3312, 3313, 3560, 1842, 3941, 3217, 3584, 3980, 1745, 602, 561, 695, 696, 1081, 3880, 1191, 162, 568, 1047, 843, 2410, 2411, 575, 631, 671, 80, 1890]. **Binomial** [673, 2579, 2274, 1367, 1445, 1545, 3693, 1192, 945, 896, 1831, 1244, 623]. **Binomial-Truncated** [1545]. **Bioinformatics** [3430]. **Biological** [24, 299, 3541, 47, 73, 114, 115, 171, 172]. **Biometric** [2901]. **biomolecular** [3393, 3508]. **biomolecules** [3356]. **biostatistics** [4240]. **Birds** [4060]. **Birger** [515, 483]. **Birnbaum** [3210, 2819]. **Birthday** [4291, 388, 2616]. **Bit** [1326, 3515, 2998, 3160, 3535, 1419, 3861, 3824, 1838, 2711, 1242, 1295, 3681, 1648, 3691, 3881, 1561, 1653, 2964, 1475, 1048, 3599, 1665, 2655, 3249, 3250, 3251, 3135, 3258, 1885, 3374, 2757, 2989, 1681, 4046, 3960, 3143, 3074, 3634, 3532, 1906, 546, 3168, 762, 547, 3542, 3902, 1508, 3415, 2258, 2508, 763, 2598,

1822, 2937, 774, 3940, 3189, 2363, 3572, 1293, 3325, 3199, 3326, 4013, 248, 3030, 3104, 2534, 3873, 4056, 2723, 2878, 1753, 2733, 3449, 3450, 2550, 3463, 2396, 933, 3242, 1777, 2224, 4041, 2312, 3608, 2827, 3487, 3613, 3955, 3370, 3264, 3626, 2012, 3358]. **Bit-level** [1838]. **Bit-parallel** [2757]. **bit-serial** [1822]. **Bit-wise** [1326]. **bit-XOR** [4041]. **Bitcoin** [3725]. **bitrate** [3612]. **Bits** [3510, 1027, 1101, 854, 1918, 3994, 1770, 3137, 3521, 3929, 1417, 1334, 762, 1068, 3093, 1443, 1368, 3792]. **Bivalent** [1658]. **Bivar** [2388]. **Bivariate** [1494, 1903, 857, 330, 3669, 868, 1049, 3482, 676, 2516, 1244, 2096, 4043, 3886]. **Black** [2925]. **Black-Box** [2925]. **Block** [2611, 1298, 2546, 2972, 3315, 2786, 1637, 3236]. **Blockcipher** [2698]. **blocking** [1229]. **Blood** [338]. **Blum** [2977, 2977]. **bodies** [33]. **body** [2890, 1310]. **Bonferroni** [1214, 783]. **BonGCL** [1375]. **bons** [1375]. **Book** [294, 895, 2136, 542, 400, 2500, 319, 2154, 3082, 3004, 170, 596, 1525, 640, 1004, 3318, 515, 1539, 1540, 559, 3202, 483, 3742, 2884, 389, 1756, 1084, 1862, 2635, 2894, 3059, 1878, 1311, 3707]. **Boolean** [3893, 3816, 3695]. **Bootstrap** [1980]. **Bootstrapping** [3009]. **borehole** [1591]. **Borrow** [1785, 3919, 1883]. **Borwein** [4291, 3720, 3721]. **both** [1784, 2829]. **Bound** [2098, 2044]. **Boundary** [197, 1951]. **Bounded** [2239, 1141, 945, 2576, 1809, 246, 305, 1567, 1765, 3606, 3618]. **Bounding** [2331, 3643, 2017]. **Bounds** [1922, 2043, 595, 731, 783, 2302, 2210, 3234, 2307, 1192, 3357, 811, 1809, 3177, 1512, 1720, 1928, 2340, 2341, 1933, 2286, 1450, 1635, 659, 1564, 3122, 2750, 1596]. **Box** [2925, 4022, 721, 770, 3036, 3587, 3746, 657]. **BPP** [2443, 1551, 2314]. **Bracket** [2904]. **Braid** [2697, 2621, 3038]. **Branch** [2098]. **Branching** [3401, 3775, 3402, 3994, 4070, 3945, 2893, 1712, 1438, 2065]. **Break** [639]. **breakdown** [3586]. **Breaking** [1052, 3887, 2701]. **Bridge** [3662]. **Brilliant** [3868]. **British** [4159, 4254]. **BRL** [118, 129]. **Broadband** [3148]. **Broadcast** [2631]. **Broken** [3140, 3963]. **Brownian** [1617, 3595]. **Browser** [2174]. **Bruijn** [3274, 2238, 2426, 3965, 1359, 518, 3877]. **Brunswick** [4289]. **Bryan** [262]. **BSAFE** [2140, 2326]. **BSDCon** [4232]. **BSTJ** [498]. **BTPEC** [1445]. **Buena** [4181]. **Buffer** [2037]. **buffering** [1670]. **Bug** [3244]. **build** [2959]. **Builder** [3870]. **Building** [1319]. **Built** [3182, 3914, 3129, 1440, 1530, 2386, 3754, 2009]. **Built-In** [3129, 3182, 1440, 1530, 2386, 2009]. **Bulgaria** [4213]. **bulk** [3320]. **Bureau** [91]. **Burlington** [4194]. **Butterfly** [3985]. **Butterfly-patterned** [3985].

C [498, 135, 1602, 1684, 3413, 1822, 2181, 2620, 2718, 3035, 3106, 3107, 2299, 2460, 2725, 3884, 3885, 2222, 1778, 3762]. **C-systems** [3884, 3885]. **C.** [3159, 446]. **C.449** [2416]. **C21** [879]. **C364** [1493]. **C52** [913]. **C77** [958]. **CA** [4276, 4252, 4189, 4183, 4144, 4232, 2492, 3138]. **CAB** [322]. **Cache** [3951]. **Cache-Efficient** [3951]. **Caesar** [2682]. **Calcul** [284]. **Calculate** [722]. **calculated** [87]. **Calculating** [4085, 1010, 1164, 1596]. **Calculation** [1148, 6, 288, 290, 1882, 1800, 278, 573, 2133]. **Calculations** [2574, 348, 119, 346, 503, 1310, 2491]. **Calculator** [131, 2109, 1098]. **Calgary**

[4103]. **California** [4127, 4249, 4290, 4268, 4192, 4178, 4135, 4204, 4214, 4215, 4108, 4137, 4086, 4219, 4228]. **Calls** [3664]. **Cambridge** [4267, 4284, 3742]. **Can** [1496, 2607, 1534, 3650, 607, 1]. **Canada** [4159, 4177, 4229, 4254, 4250, 4218, 4103, 4186]. **Canadian** [4090]. **canadien** [4090]. **Cancellation** [3188]. **cancer** [3361]. **Candidate** [4221, 4060, 2482]. **Candidates** [2561]. **Cannot** [3597]. **Can't** [1496]. **Capacitor** [3087]. **capacity** [3617]. **Capital** [4147]. **Captured** [2245]. **caractéristique** [2890]. **Carbon** [3914]. **Card** [3223, 2767, 4272]. **CARDIS** [4272]. **cards** [36]. **Carlo** [4098, 178, 2500, 112, 4270, 4231, 4086, 4257, 4265, 2884, 4187, 4207, 4214, 4236, 4246, 2305, 189, 3059, 4226, 1878, 1789, 1205, 432, 2138, 3150, 348, 2144, 178, 2580, 179, 3075, 212, 3637, 1605, 2244, 1606, 1330, 1693, 2246, 2247, 2676, 3398, 234, 1415, 905, 2152, 1155, 90, 195, 503, 3541, 1911, 152, 2039, 3544, 3175, 1281, 4285, 1220, 3656, 197, 3416, 2266, 2347, 2436, 2509, 591, 1285, 3417, 1725, 2173, 2270, 1117, 727, 2353, 2777, 3905, 1231, 198, 351, 220, 1825, 3786, 511, 128, 223, 326, 914, 1828, 513, 2358, 2515, 3567, 3427]. **Carlo** [1174, 1531, 1630, 961, 2709, 156, 157, 1239, 3195, 2185, 1454, 1372, 648, 1010, 2716, 2871, 3207, 3436, 3208, 1181, 3827, 2533, 2622, 3108, 3942, 1970, 2877, 159, 3683, 146, 656, 78, 4089, 3799, 2089, 2090, 3947, 876, 1764, 132, 2890, 491, 1135, 663, 1771, 1988, 1307, 744, 703, 2217, 2106, 2397, 99, 261, 2472, 133, 4112, 4294, 1577, 1666, 2112, 1310, 1875, 3702, 2310, 393, 1141, 712, 1583, 3806, 290, 2828, 2900, 2407, 138, 2904, 1589, 1787, 2489, 2906, 1591, 265, 464, 465, 496, 2018]. **Carmichael** [2880]. **Carnegie** [4106]. **Carnegie-Mellon** [4106]. **Carolina** [4146, 4167]. **carried** [234]. **Carry** [1785, 1885, 2034, 2251, 2781, 2070, 3999, 1090, 1883]. **carry-free** [1090]. **Carus** [3707]. **cascade** [2146]. **Case** [2243, 3993, 520, 1, 2918, 3292, 1804, 2166, 2347, 3671, 3037, 51, 3266]. **cases** [2885, 2896, 3057]. **Casinos** [3868]. **Casuali** [991, 491]. **cat** [2997]. **Cathedral** [4232, 4286]. **Cauchy** [1324, 3649, 2594]. **Cautionary** [1771]. **Cautions** [1265]. **CC0** [3441]. **CCS** [4243]. **CDC** [1123]. **Cdfs** [3616]. **CDROM** [2079]. **Cebysev** [1726, 1235]. **Cell** [3148, 3767, 1360]. **Cells** [3982, 2571, 3730]. **cellulaires** [1588]. **Cellular** [2335, 3183, 1440, 1530, 3196, 3119, 1588, 2016, 4065, 1278, 3299, 2857, 1441, 1751, 2386, 3449, 3949, 2821, 2652, 2745, 2227, 2478, 2405, 2009, 2488, 2566, 1671, 1260, 1261]. **Censored** [866]. **Centenary** [4284]. **Center** [4153]. **Central** [1113, 3043, 3429, 3588, 3831, 2807, 1272, 2594, 2898]. **Centre** [4101]. **centro** [3623, 3708]. **centro-invertible** [3623, 3708]. **centroids** [438]. **Century** [2505, 4206, 2845]. **Certain** [42, 506, 687, 25, 431, 1325, 102, 1915, 2257, 173, 301, 302, 408, 221, 222, 1536, 2616, 1745, 1468, 1558, 708, 1588]. **certains** [1588]. **Certifiable** [3706]. **Certification** [3511, 364, 314, 630]. **Certified** [4080, 3829, 3387, 3723, 4021]. **Cesàro** [48]. **CFTP** [3547]. **ChaCha** [3146, 3155, 3860, 3861, 3571, 3830, 3761]. **ChaCha20** [3825, 3948]. **Chain** [1102, 2580, 1207]. **Chains** [2252, 513, 3192, 663, 2011, 212, 3416, 712]. **Challenges** [4035]. **Chance** [2421, 3597, 469, 247]. **Change** [1912, 3553, 3479, 584, 1014]. **Changes** [2594]. **Changing** [2763, 1872].

Channel [993, 3405, 1836, 2504, 2855, 3236, 3617]. **Chaos** [1685, 1703, 3087, 2610, 3200, 2792, 3580, 4237, 2892, 2657, 2658, 3271, 2759, 3991, 3152, 3000, 3542, 3201, 1849, 2804, 3235, 1571, 3349, 3466, 3490, 3257, 2418, 2910, 3506, 3766]. **Chaos-Based** [3087, 3580, 2657, 2658, 2759, 3152, 3542, 3349, 2910, 3766]. **chaos-type** [3257]. **Chaotic** [3520, 1495, 3551, 2066, 2627, 2387, 3229, 3460, 3352, 2655, 3250, 3251, 3258, 2835, 3376, 1678, 3389, 4064, 3960, 3158, 3295, 3550, 2932, 3783, 2598, 2446, 3313, 3425, 3820, 3562, 1439, 3323, 3736, 2872, 3584, 3454, 3755, 1194, 4041, 3359, 3370, 3956, 3374, 3264, 3383, 4046]. **Chapman** [2352]. **Chapter** [3005, 3033]. **Character** [2577, 2737]. **characterisation** [2065]. **Characteristic** [1217, 1301, 1592, 3812, 3934, 3965, 996, 1106, 781, 2890, 2007, 2120]. **Characteristics** [3752, 198]. **Characterization** [2037, 888, 3496, 3151]. **characterizations** [1711]. **Characterizing** [3705]. **Characters** [2883]. **Cheat** [3868]. **Chebyshev** [1447, 3873]. **check** [912]. **Checks** [2707]. **Chen** [3736, 3755]. **Chernoff** [2302, 2307]. **CHES** [4264, 4224]. **Chi** [826, 44, 1300, 1384, 3451, 88, 1360, 1178, 14]. **Chi-Square** [826, 3451, 88, 14]. **chi-squared** [1360, 1178]. **Chicago** [4138, 4234, 4114]. **children** [3053]. **China** [4231, 4279]. **Chinese** [106, 2749]. **Chip** [3176, 1490, 3167, 4013, 3366]. **chip-scale** [4013]. **chips** [4204]. **chisel** [351]. **Choice** [497, 694, 44, 628, 88, 2615, 2668]. **Cholesky** [978]. **Choose** [838]. **Choosing** [829, 604, 1855, 2801, 972]. **Choquet** [3601, 3602]. **Chosen** [3091, 3830]. **chromatic** [2052]. **Chronological** [629]. **CI** [3519]. **CiE** [4284]. **Cipher** [2911, 3154, 2765, 3641, 1914, 3097, 2611, 3825, 1978, 3111, 3222, 3594, 4259, 2108, 934, 2655, 2909, 2989, 1681, 2786, 3197, 3236, 3802, 2557, 3264]. **Ciphers** [1488, 3147, 3156, 2682, 2768, 3091, 639, 2546, 3753, 2972, 3500, 3305, 3941, 3585, 1468, 1754, 3448, 1662, 2979]. **Circuit** [2775, 4060, 2974, 3122, 3158, 3270]. **Circuits** [2573, 3893, 1495, 4273, 3137, 3382, 1530, 2722, 2006]. **Circular** [341, 342]. **Circulation** [3791]. **Cirencester** [4244]. **City** [4132, 4210, 4088, 4188]. **claims** [3039]. **Claremont** [4214]. **Class** [1488, 852, 2916, 2531, 3795, 3211, 44, 2200, 1650, 2640, 2108, 2400, 536, 3249, 3625, 1686, 2842, 1338, 1505, 1816, 1828, 3320, 2181, 967, 1849, 1644, 1981, 2393, 1987, 3958, 3384]. **Classes** [2612, 1545, 97, 2475, 88, 1178, 1837, 1640, 3122]. **Classical** [3894, 3397, 3936, 1931, 816, 680, 1734]. **Classification** [1930]. **Classified** [629, 889, 1257]. **classifiers** [3384]. **Classroom** [399, 582, 298, 516, 388, 365, 368, 2983]. **Clearer** [3317]. **Cleve** [2088, 2633]. **client** [1987]. **client-server** [1987]. **Clipped** [628]. **Clipper** [2086]. **Clipper-like** [2086]. **Clock** [2024]. **Clock-controlled** [2024]. **Close** [2529, 1176, 2712]. **Close-Point** [2529]. **Closed** [709]. **Closer** [3658]. **Cloudier** [3857]. **clubs** [1321]. **Cluster** [1875, 2310]. **Cluster-flipping** [1875]. **clustered** [256]. **clustered-rocket** [256]. **Clustering** [3314, 913, 3311]. **cm** [170]. **CMOS** [3411, 3188, 3460, 3358, 3483]. **Co**

[170, 2226]. **Co-evolving** [2226]. **Code** [3277, 2843, 2159, 3301, 1010, 3442, 2222, 3709, 2764, 999, 3319, 1970, 2106, 4084, 1084]. **Code-based** [2843]. **Coded** [3231, 3892]. **Codes** [3408, 2682, 1298, 4211, 273, 607, 3836]. **Coding** [2627, 492, 4244, 4248, 4145, 436, 920, 4172]. **Coefficient** [3314, 3292, 40]. **Coefficients** [3173, 1041, 837, 2664]. **Coherent** [1419, 3553, 4015, 3612]. **Coin** [3894, 1102, 2151, 3402, 1798, 2597, 3431, 1463, 163, 1207]. **Coin-Tossing** [1798]. **Coins** [2841, 2524]. **Collatz** [4069]. **Collected** [4094, 2016]. **collecting** [140]. **collection** [4098, 2267]. **Collector** [144]. **College** [4088]. **Collision** [3642, 2831, 2905, 4049]. **collision-based** [4049]. **Collision-Resistant** [3642]. **collisions** [4010]. **colorectal** [3361]. **Coloring** [2307]. **Columbia** [4159, 4254]. **column** [3136]. **Combination** [951, 2254, 1112, 1113, 1114, 3115, 2110, 428, 2422, 3313, 2293, 1662, 1255, 2908]. **Combinations** [399, 516, 485, 368, 1809, 1121, 2866, 448, 449, 62]. **Combinatorial** [636, 3729, 203, 2378, 1563, 2139, 238, 3558, 773]. **Combinatorics** [4150, 2782]. **Combined** [3316, 3824, 2191, 2456, 2530, 2793, 2749, 1479, 2008, 3619, 3502, 1803, 1937, 1376, 1640, 2193, 2194, 2372, 2459, 2721, 1478, 1669, 2664]. **Combiner** [2406]. **combiners** [1754]. **combinés** [2664]. **Combining** [907, 908, 1612, 3301, 2601, 3175, 3789]. **Coming** [3769]. **Comment** [295, 1609, 170, 2593, 863, 1071, 960, 1037, 1633, 963, 869, 968, 2954, 969, 872, 2646, 976, 887, 879]. **Commentary** [2192]. **Comments** [2842, 3159, 1155, 724, 789, 603, 1779]. **Commitment** [1561, 1653]. **Commodore** [1149]. **Common** [1214, 3972, 512, 1294, 1735, 3110, 1759, 1575, 811, 2183, 1124, 3689, 1864, 1090, 753, 3646, 2584, 2252, 1119, 1728, 915, 777, 732, 921, 1370, 2451, 1863, 2092, 944, 1484, 1680]. **Commonly** [2850]. **Commun** [2058, 2182]. **Communicating** [1317]. **Communication** [586, 4247, 1317, 4067, 1334, 2504, 2855, 3569]. **Communications** [506, 2711, 4243, 4172, 2759]. **Comp** [2149]. **Compact** [2021, 2832, 3071, 3141, 1421, 2522, 3107, 602]. **Companion** [4292]. **Comparative** [1344, 402, 503, 3303, 2123]. **Comparing** [1229, 915, 1835, 2190, 3384]. **Comparison** [672, 580, 1059, 3289, 3905, 3738, 1735, 3207, 2089, 204, 2302, 612, 1086, 703, 2217, 2819, 1680, 1493, 1692, 1501, 593, 594, 1729, 2951, 2533, 3361, 2756, 463, 812]. **Comparisons** [1863, 2092, 1484, 1405, 1759, 1864]. **compatibility** [3718]. **Compatible** [1522, 1552, 3665]. **Competing** [186]. **Competition** [3645]. **compiled** [70]. **Complement** [1125, 739, 479]. **Complete** [1298, 1020, 3151, 939, 2410, 2844, 2844]. **Completed** [957]. **Completely** [510]. **Complex** [3733, 3992, 684, 4197, 3789, 3849]. **Complexity** [2837, 2994, 1496, 1799, 4025, 3414, 1817, 2941, 3976, 2613, 1848, 1967, 2297, 3213, 3833, 2654, 4106, 1317, 2496, 2145, 1908, 1334, 3902, 3654, 1164, 2937, 2784, 3671, 782, 2950, 3584, 2805, 3112, 1757, 3880, 1563, 2984, 2016, 1890]. **complicated** [2564]. **Component** [1914, 2713, 3047, 3046, 3048]. **Component-by-Component** [2713, 3047, 3046, 3048]. **components** [2793]. **Composite**

[3290, 30, 2713, 874, 1582, 2114, 3247, 2158, 1708, 1451, 2113, 1877]. **Composited** [3877]. **Composition** [1942, 2220, 3768, 1245, 849]. **Composition-Alias** [2220]. **Compound** [1277, 2432, 1923, 2049, 2165, 2166, 2259, 2261, 2344, 2979, 3530, 1811, 2048, 2260, 2169, 2170, 2624, 2955, 2638, 80, 2235]. **compressed** [2087]. **compression** [4150]. **Compromise** [3140, 3040]. **Compromised** [3780, 3903]. **COMPSTAT** [4139]. **Comptes** [4090]. **Compton** [377]. **Comput** [2058, 1071, 2182]. **Computability** [4284, 2467, 3345]. **Computable** [3895]. **Computation** [4085, 3897, 4241, 4169, 2153, 2925, 1707, 857, 30, 142, 4279, 330, 1954, 4186, 4074, 4171, 2096, 2099, 3917, 4228, 3272, 945, 4087, 3927, 1269, 2425, 1908, 2606, 2520, 3025, 4057, 1860, 1765, 2000, 894, 4253]. **Computational** [4291, 4263, 2587, 952, 4287, 2466, 2726, 4154, 344, 3983, 4253, 425, 3854, 2921, 1064, 4139, 3970, 4235, 1523, 558, 1746, 4295]. **Computationally** [4163, 4042, 4142]. **Computations** [1155, 414, 1174, 3793, 703, 2560, 2145, 2422, 2503, 727, 1438, 1379, 159, 1567]. **compute** [2795]. **Computer** [578, 673, 990, 1022, 896, 755, 897, 898, 899, 543, 4124, 2769, 1336, 3651, 1159, 4111, 506, 1521, 244, 414, 4104, 4114, 4117, 4120, 4135, 4140, 4146, 4152, 4162, 4185, 4194, 4198, 4219, 4223, 4274, 4289, 1176, 1177, 868, 779, 828, 870, 1543, 732, 1959, 830, 1381, 603, 337, 359, 1042, 4243, 4126, 1084, 4097, 3690, 4293, 1571, 1086, 4118, 4173, 1475, 1091, 3844, 2558, 1667, 4175, 891, 892, 4106, 1144, 715, 429, 540, 1268, 1690, 853, 1270, 762, 1028, 4217, 3174, 995, 996, 473, 999, 764, 765, 767, 2442, 4205, 1011, 1039, 2075, 1244, 1970, 311]. **computer** [385, 1129, 455, 833, 1248, 617, 227, 1045, 4105, 1195, 1995, 3699, 1779, 374, 1316, 849, 2442, 4116]. **Computer-Zufallszahlen** [2442]. **Computers** [2237, 4144, 267, 2334, 1798, 2337, 1504, 1030, 1342, 272, 145, 245, 1295, 2958, 282, 187, 204, 739, 206, 1577, 2480, 4094, 1142, 1683, 234, 403, 546, 2249, 1423, 1503, 218, 1066, 1826, 1827, 2059, 1734, 3826, 1457, 203, 1550, 1972, 340, 147, 662, 4092, 122, 137, 1792, 176, 2058]. **Computes** [4284]. **Computing** [4122, 4127, 4132, 4138, 4143, 4148, 4159, 4177, 4182, 4191, 4209, 4216, 4229, 4234, 4239, 4249, 4254, 4267, 4276, 4283, 4290, 2838, 896, 3072, 3001, 375, 468, 3409, 681, 152, 1808, 1820, 957, 2441, 2512, 1294, 964, 4280, 3216, 119, 1043, 1773, 2821, 4247, 3605, 4174, 3616, 4142, 2572, 212, 3287, 2776, 2178, 4278, 4288, 118, 1124, 96, 129, 3439, 2875, 3798, 3227, 4172, 4187, 1595, 139, 4141]. **con** [470]. **Concave** [2067, 1108, 1947, 2516, 2625]. **Concavity** [2349]. **Concentration** [3899]. **Concept** [384, 386, 37]. **conception** [1588]. **Concepts** [638, 4287, 599, 402, 2173, 2270, 4235, 2063]. **Conceptual** [3512, 4055]. **Concerning** [355, 80, 2785, 188]. **concert** [3051]. **Conclusion** [3317, 2462]. **Concrete** [2029, 3288, 2977, 2146]. **Concurrent** [4144]. **Conditional** [2084, 2085, 2462, 3231]. **conditionally** [3620]. **conditions** [2033]. **cone** [2562]. **Conference** [4190, 4137, 4183, 4196, 4091, 4144, 4210, 4149, 4241, 4192, 4284, 4156, 4272, 4130, 4256, 4279, 4220, 4295, 4280, 4147, 4243, 4206, 4252, 4221, 4158, 4110, 4225, 4119, 4226, 4121, 4253, 4174, 4244,

4180, 4228, 4166, 4181, 4189, 4215, 4167, 4131, 4128, 4193, 4109, 4178, 4157, 4231, 4255, 4242, 4096, 4204, 4213, 4095, 4187, 4207, 4214, 4236, 4208]. **Confidence** [1735, 39, 86, 1635]. **Configurable** [4015, 2571]. **configuration** [1194]. **Confusion** [1663]. **Congrès** [4090]. **Congress** [4090]. **Congruence** [2022, 1088, 1375, 1046, 193]. **congruences** [1349, 189]. **congruent** [2205]. **Congruential** [293, 2994, 267, 544, 2030, 2923, 1618, 1619, 1620, 1623, 1719, 2043, 2165, 2261, 2263, 3008, 3179, 823, 1000, 1033, 1115, 1517, 3554, 1118, 861, 771, 772, 2447, 2860, 2057, 2607, 2941, 865, 327, 2189, 1546, 1377, 1378, 2455, 1740, 2957, 605, 657, 797, 615, 877, 2469, 2966, 661, 2110, 428, 1055, 1204, 1403, 3891, 2149, 1497, 1060, 1417, 2425, 634, 1699, 3284, 1608, 721, 2031, 320, 1915, 1707, 1341, 587, 407, 1425, 2508, 1428, 1511, 1512, 1621, 1622, 1624, 1625, 1717, 1718, 1720, 1721]. **congruential**
[1722, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1923, 1925, 1926, 1927, 1928, 1929, 2044, 2045, 2047, 2166, 2167, 2168, 2260, 2262, 2264, 2340, 2341, 2342, 1223, 1283, 1284, 1346, 1347, 2265, 2346, 2347, 2436, 859, 956, 1225, 1226, 1348, 1819, 768, 2934, 3092, 556, 2701, 1358, 2514, 3093, 3184, 4033, 2606, 778, 867, 3322, 356, 2186, 2187, 2287, 3199, 966, 1179, 1738, 3030, 829, 1375, 2193, 2458, 1180, 2296, 2955, 3439, 2199, 2721, 486, 522, 2383, 2632, 2881, 3112, 4001]. **congruential**
[456, 3116, 698, 800, 801, 878, 1190, 1386, 1387, 1470, 1564, 2548, 2638, 2639, 2967, 2889, 1393, 1768, 1769, 839, 972, 931, 2896, 2897, 3057, 2309, 2223, 2899, 3760, 987, 4042, 1312, 2979, 2981, 3130, 3362, 3487, 3613, 2984, 3260, 3261, 3262, 3497, 494, 2130, 2413, 2015, 3266, 3498, 2320, 3070, 3958, 233, 2321]. **conjecture** [717, 501]. **conjoint** [4043]. **connected** [3854, 2897]. **connection** [297, 100]. **Connoisseurs** [2610]. **connues** [804]. **Consecutive** [3740]. **Consequences** [1302, 1266, 1408]. **Conserved** [3384]. **consideration** [289]. **Considerations** [468, 2282, 1900, 1002, 1900]. **consisting** [2913]. **Constant** [2573, 2577, 2925, 3137, 3987, 2470]. **Constant-Depth** [3137]. **Constant-Error** [3987]. **Constant-Round** [2925]. **Constantine** [2498]. **constants** [3898]. **Constrained** [3967, 3097, 2117, 3853, 3817, 3977, 3624]. **Constraints** [3787, 1837, 3351]. **Construct**
[4008, 1232, 3603, 4023, 1171, 1172, 1380]. **Constructed** [1514, 3163, 3560]. **Constructing** [3003, 3732, 3664, 3193, 3870, 3833, 3426, 74]. **Construction** [1620, 1718, 2779, 2856, 2604, 3185, 3026, 2189, 357, 2713, 2883, 2468, 3047, 2890, 1658, 1665, 3246, 2490, 2758, 1486, 2146, 15, 588, 65, 1957, 2073, 3941, 3046, 3048, 3801, 881, 3606, 712, 2890]. **Constructions**
[2698, 2714, 1760, 2965, 1562, 2301, 1761, 3705, 3851, 3509]. **Contactless** [3635]. **Contemporary** [4164]. **Content** [2769]. **Contents** [49]. **Context** [3984, 2156, 3889]. **Context-Driven** [3984]. **context-free** [2156, 3889]. **contiguous** [2069]. **contingencies** [455]. **Contingency** [6, 7]. **Continued** [286, 2928]. **Continuous** [2019, 4006, 3525, 2789, 514, 1952, 1078, 565, 676, 3416, 1288, 776, 2625, 2626, 1247, 3235, 702, 1316, 3506]. **continuous-time** [3235, 3506]. **Contour** [241]. **contrôle** [762]. **Contributions** [52, 4157]. **Control** [170, 1863, 3984, 3256, 1484, 1680, 1203, 762, 3018, 455, 170].

Control-variate [1863]. **Controllability** [861]. **controllable** [2857]. **Controlled** [1359, 2024]. **Controlling** [2039, 2661]. **Controls** [3166, 918]. **Convenient** [3029, 335, 3102]. **conventional** [3145]. **Convergence** [2252, 1962, 1964, 2236, 2038, 381, 1528, 3498]. **Convergent** [315]. **Conversion** [3084]. **Converting** [3792]. **Convex** [857, 2614, 3570, 33, 614, 741]. **Convolution** [1545, 2319, 3620]. **convolutional** [3836]. **Convolutions** [687, 2623, 1596]. **Cooperation** [3687]. **Cope** [2492]. **Copenhagen** [4139]. **Coprocessor** [2608, 3737]. **copula** [3139]. **copulae** [3953]. **Copulas** [3139]. **Copyright** [2329]. **CORDIC** [3746, 3805]. **Core** [3176, 4040, 2673]. **Corfu** [4253]. **Corner** [830, 2088, 2633]. **Coronado** [4192]. **corps** [2890]. **Corput** [911]. **Correcting** [4044, 4211]. **Correction** [1273, 3081, 1543, 2414, 1147, 221]. **Corrections** [270, 2865, 927]. **correctly** [1933]. **Correctness** [3924, 1789]. **Correlated** [2836, 2145, 1102, 141, 643, 3787, 598, 923, 2379, 700, 1, 2575, 432, 349, 1207, 1246, 3221, 2388, 227, 2393, 1993, 2824, 1892]. **Correlation** [3512, 2248, 216, 52, 1000, 2599, 244, 2523, 1754, 738, 843, 816, 1794, 498, 680, 1805, 956, 2277, 2357, 558, 482, 2872, 2720, 1131, 1468, 40, 658, 3232, 1768, 666, 1578, 51]. **Correlational** [816, 680, 463]. **Correlations** [758, 2583, 679, 2434, 2061, 2898, 1611, 1339, 1506, 2039, 550, 1428, 2437, 141, 1824, 2282, 1838, 1393, 1875, 2311, 3248, 2313, 2493]. **Correspondence** [675, 2066, 1855, 2109]. **corresponding** [711, 1140]. **Corrigenda** [2149]. **Corrigendum** [2273, 1039, 2542, 1384, 538, 631, 3708]. **Corroboration** [2769]. **Cosmological** [3742, 3589]. **Cost** [3351, 3272, 1013, 3750, 3591, 2473, 3361]. **cost-effectiveness** [3361]. **Costruzione** [470]. **Countable** [3]. **Counter** [3179]. **Counter-Dependent** [3179]. **Counting** [2852, 1842, 1745, 2219, 3128, 1896, 1839]. **Counts** [3363, 1360]. **Couple** [2655]. **Coupled** [3551, 3251, 3550, 3199, 3454, 3250]. **Coupling** [3436]. **Coupon** [144, 140]. **courbe** [35]. **course** [4160, 4103]. **Courses** [3301, 265]. **Covariance** [422, 53]. **covariates** [3890]. **covering** [3801]. **coverings** [430]. **covers** [3682]. **Cox** [3890]. **CPU** [3938]. **CPUs** [3963, 3772, 1777]. **crack** [2860]. **cracked** [607]. **Cracking** [931, 3470, 3471, 3472, 3473, 841]. **Cramér** [294, 559]. **Crash** [3995]. **CRAY** [2433, 1394]. **CRAY-System** [2433]. **Create** [2769, 1766]. **created** [2308]. **Creates** [2892]. **creation** [2384]. **Criteria** [1402, 1485, 3010, 521, 1469, 2822, 102, 2374, 2622, 3360]. **Criterion** [1]. **Critical** [2769, 1708, 4014, 3081, 1707]. **Crofton** [2795]. **Cross** [1794, 3551, 3250, 3251, 3550, 558]. **Cross-correlation** [1794, 558]. **Cross-Coupled** [3551, 3251, 3250, 3550]. **cryogenic** [1490]. **Cryptanalysis** [2761, 2918, 3638, 3641, 1332, 1697, 3860, 2924, 3085, 3086, 3300, 3012, 2693, 2697, 2702, 2862, 3830, 1978, 2734, 2989, 2922]. **Cryptanalytic** [2366]. **CryptMT3** [3222]. **CRYPTO** [4125, 4178, 4252, 4136, 3140, 3024, 2608, 4040, 4026, 4084, 4115, 4151]. **Cryptoanalysis** [2703]. **Cryptographic** [1264, 1323, 4005, 3394, 2243, 4123, 3160, 3857, 3645, 4133, 3293, 1917, 3176, 2343, 1167, 2859, 3021, 3737, 3205,

2957, 1971, 2387, 2642, 1663, 2649, 3474, 2822, 3603, 3062, 3359, 3253, 1052, 4064, 2136, 3991, 3157, 3281, 2767, 3722, 3313, 1170, 3906, 2786, 1442, 2495, 2526, 3435, 1745, 1245, 2198, 3349, 2471, 2895, 4061, 4063, 3509, 4264, 4224]. **Cryptographically** [3275, 3391, 3520, 1027, 1101, 1373, 3463, 3055, 1097, 2760, 4027, 3820, 4054, 1312, 1900]. **cryptographically-secure** [4054, 1900]. **cryptographiquement** [1900]. **Cryptography** [4145, 2332, 906, 1703, 2683, 3083, 3015, 916, 2518, 2627, 3038, 3446, 1649, 2300, 2555, 2218, 2222, 4247, 2655, 4248, 1681, 2430, 4282, 4250, 2444, 4218, 3323, 1732, 1547, 1983, 2396, 2553, 3469, 2478, 3609, 2657, 3370, 3264, 4244]. **Cryptology** [1151, 4125, 4115, 4133, 4134, 4154, 1136, 4164, 4123, 4178, 4151, 4252, 4136]. **CryptoQNRG** [4061]. **Cryptosystem** [3364, 1373, 3836]. **Cryptosystems** [880, 2453, 1388, 3257]. **Crystal** [4210, 54, 4225, 4119, 4166]. **crystallography** [3322]. **CSD** [2114]. **Cuba** [2939]. **cube** [423, 1587, 807]. **Cubic** [1619, 2261, 1871]. **CUDA** [3631, 3190, 3328, 3700, 4003]. **Cumulant** [1706]. **Cumulative** [3968, 4051, 3669, 3670, 2796, 2018, 577]. **CURAND** [3631, 3700]. **Current** [3200, 1184, 3201]. **Current-Mode** [3200, 3201]. **curve** [3079, 2874, 3123, 35]. **Curves** [3529, 2057, 2941, 2654, 3093, 4033, 1632, 1296, 34, 4022]. **Customer** [2769]. **Cusum** [1203]. **Cusum-Shewhart** [1203]. **cut** [2601, 3739]. **Cyber** [1123, 1414]. **CYBER-205** [1414]. **Cycle** [1034, 1859, 1319, 3162, 3934, 2685, 2770, 799]. **cycles** [224, 2880]. **Cyclic** [917, 805, 1730, 3337, 4046].

D [895, 1825, 3183, 3920, 3952]. **D-PUF** [3920, 3952]. **D.** [3560, 249, 3217, 1747]. **D.C** [4241]. **d.f** [247]. **Daemon** [2674]. **Dagpunar** [1539, 1525, 1540]. **DAGs** [2069]. **Dallas** [4121]. **Dana** [4268]. **Dances** [3146, 3571]. **dangers** [1422]. **dans** [2890]. **DAP** [1199]. **d'après** [697, 736]. **Dark** [3363, 4026]. **Darling** [2537, 1042]. **Data** [947, 948, 992, 586, 2431, 639, 3565, 960, 866, 2943, 1836, 963, 1456, 968, 787, 969, 790, 3451, 3452, 840, 1016, 976, 1667, 4180, 1482, 3768, 4091, 1025, 3817, 438, 42, 1822, 3421, 3311, 3425, 3566, 2283, 2520, 3025, 1837, 2190, 796, 1662]. **Data-Oriented** [3451, 3452]. **data-parallel** [1822]. **Database** [4168, 2037, 4266]. **databases** [2054, 1934]. **datasets** [2087]. **Day** [4044]. **dbC** [1822]. **DC** [4098, 4179, 4206, 3707, 4168, 4147, 4131]. **DDH** [3481]. **Deák** [1756, 1862]. **Dear** [2114]. **Debian** [3140, 3244, 3850]. **Debiasing** [3986]. **Decay** [2898, 2907]. **December** [4137, 4183, 4196, 4149, 4192, 4231, 4220, 4147, 4206, 4158, 4110, 4225, 4119, 4244, 4166, 4181, 4131]. **decentralized** [3918]. **Decimal** [293, 1636, 2962, 131, 81, 87, 79]. **Decimals** [288, 15, 749]. **Deciphering** [966, 1179]. **decision** [1213, 4095, 1315, 3379]. **Deco** [2142]. **Decoding** [2172, 488, 3703]. **Decomposition** [1909, 592, 3711, 2022, 978, 2751]. **decreasing** [1130, 3606]. **DECsystem** [912]. **DECsystem-10** [912]. **defects** [816, 680, 3110]. **defined** [1412, 3049]. **Definite** [2452, 1210, 99]. **Definition** [532, 533, 387, 569, 1050]. **Definitions**

[1610]. **deformed** [2556]. **Degree**
[3011, 3441, 3231, 2920, 763, 2854, 3218, 3455]. **Degrees**
[1731, 1847, 1795, 349]. **Del** [4192]. **Delay** [993]. **Delayed** [832, 3873].
delays [1992]. **Delegation** [3967]. **delta** [1412]. **demands** [773]. **Demons**
[3657]. **Demonstrating** [1422]. **Demonstration** [3611, 3612].
Demonstrations [163]. **Deng** [2868]. **denoising** [4045]. **dénombrable**
[804]. **dénombrables** [3]. **dense** [1896]. **d'ensembles** [2890]. **denses** [178].
Densities [1107, 2349, 687, 2570, 2256, 3098]. **Density** [2288, 452, 717, 3811,
1498, 2680, 1338, 3410, 1108, 3098, 2720, 1246, 255, 1130, 424, 2018].
denumerable [804]. **Department** [4106]. **Dependence** [557, 1361, 867].
Dependency [2331, 1646, 2404, 1596]. **Dependent**
[3525, 1494, 3179, 298, 1079, 537, 942, 1594, 752, 1689, 1950, 962, 1447, 3586,
2380, 3754, 1194, 2313, 3373, 3890, 2017]. **deployed** [3469]. **deposition**
[2339]. **Depth** [2573, 3137]. **Derandomization** [2443, 2323, 3671].
Derflinger [3004]. **Derivation** [3397, 3165]. **Derivative**
[2252, 1962, 3683, 3748]. **Derived** [3695, 1705, 4037, 2476]. **Describe** [1496].
Description [129, 665, 803, 158, 160]. **Design**
[2322, 3512, 3275, 3391, 2912, 3148, 466, 2428, 1919, 2685, 3173, 4027, 1159,
2775, 3549, 4079, 3658, 304, 2859, 644, 3024, 3569, 3203, 2948, 2371, 518, 4056,
3442, 3876, 521, 3231, 2637, 4015, 3466, 4076, 3703, 3264, 3502, 1203, 3504,
3385, 3545, 3519, 3536, 2526, 833, 3235, 3489, 1588, 1099, 1595, 4171, 4094].
Designed [863, 869, 872, 885, 886, 887, 3369]. **Designing**
[3960, 3405, 1350, 3448, 2389, 3215, 2009]. **Designs** [4259, 3221]. **desired**
[666]. **Desktop** [1030]. **detecting** [584]. **Detection**
[3182, 3553, 3663, 3341, 3917, 3572]. **Detector** [3815, 3869, 3552, 3598].
Detector-Based [3869]. **Detectors** [3484]. **Determinants** [2441].
Determination [198, 244, 832, 1403, 1154, 550, 16, 17]. **Determinazione**
[17, 16]. **Determine** [2769, 866]. **Determining** [19, 1755]. **determinism**
[1789]. **Deterministic** [3991, 2998, 4066, 4031, 274, 300, 3418, 3821, 3675,
3691, 2892, 2475, 3849, 3074, 3634, 3532, 3415, 2509, 2701, 626, 2827, 3259, 62].
dev [2762, 2915, 3724, 2820]. **developer** [3041]. **Developing** [4081].
Development [272, 4170, 2796, 4039, 1582, 1613, 1578, 1877].
Developments [899, 3901, 4078, 870, 2094, 4107, 1856, 987]. **deviate**
[1037, 363]. **Deviates**
[1022, 435, 330, 2525, 828, 647, 1847, 187, 204, 148, 392, 2647, 1051, 3767,
1794, 349, 182, 141, 770, 480, 158, 160, 1572, 3056, 191, 70, 168]. **Deviation**
[2072, 381, 3700]. **Deviations** [3400, 1, 1575, 247, 2203, 35]. **Device**
[1074, 3920, 3952, 3704, 3542, 3494]. **Devices**
[3774, 3663, 4014, 3876, 3879, 3167, 3726, 3595, 2820]. **Devroye** [1311].
diameter [1951]. **diaphony** [2360, 2076, 3439]. **Dice**
[3229, 3784, 2524, 3706, 167]. **DiceHash** [3170]. **Dickson** [2994, 3017]. **did**
[3935]. **Diego** [4249, 4137, 4183, 4268]. **DIEHARD** [2201, 2079]. **Dieharder**
[3534, 3776, 4044]. **dielectric** [3586]. **Dieter** [896]. **Difference**
[2252, 197, 1821, 276, 20]. **Differences** [1514]. **Different**

[2704, 3047, 2217, 157, 2458, 2793]. **differentiable** [3570]. **Differential** [3860, 2924, 2255, 2862, 3200, 2734, 3752, 1356, 3201, 138]. **Differentials** [3861]. **Difficult** [2724]. **Difficult-to-Pass** [2724]. **Diffie** [2746]. **diffusion** [3101]. **digamma** [1713]. **Digit** [266, 431, 1603, 3281, 273, 2074, 3684]. **Digital** [4085, 3160, 4025, 549, 3006, 4270, 3548, 1924, 2775, 272, 2691, 3010, 638, 3662, 354, 145, 414, 245, 3431, 2370, 2627, 603, 654, 3446, 1301, 204, 528, 880, 2309, 2400, 4247, 3358, 3615, 429, 540, 1489, 2021, 4087, 2329, 234, 403, 552, 1714, 1715, 1110, 4286, 218, 2688, 1066, 3422, 3569, 2190, 203, 1849, 833, 147, 1389, 1761, 2813, 4092, 3483, 2910, 4046, 894, 4096]. **Digitalized** [3407]. **Digitalrechnern** [894]. **Digitization** [2387]. **Digits** [103, 108, 109, 110, 111, 123, 124, 125, 126, 237, 63, 144, 3027, 1010, 523, 285, 259, 1016, 148, 392, 2647, 628, 168, 2985, 71, 89, 635, 81, 91, 92, 83, 93, 94, 2942, 76, 1536, 602, 561, 695, 696, 1081, 87, 130, 162, 2645, 529, 1047, 79, 372, 2668, 671, 177, 100]. **digraph** [3274]. **Dimension** [3367, 3368, 1032]. **Dimensional** [270, 196, 201, 3193, 919, 3196, 1850, 1552, 205, 54, 2008, 3625, 717, 1800, 1803, 1338, 2685, 2770, 3416, 221, 222, 2199, 738, 2392, 3049, 188, 3058, 2310, 3063, 3806, 2566, 2133, 2321, 807, 3372]. **Dimensionality** [3007]. **dimensionally** [2385]. **dimensions** [2236, 692, 730]. **Diode** [3744]. **Dipole** [647]. **Dirac** [11]. **Direct** [1154, 760, 2257, 76, 3759, 576]. **directed** [1899, 1951, 2311, 2006]. **Directions** [4106]. **Dirichlet** [3639, 3778, 2416]. **Disappearance** [2404]. **discarding** [2493]. **Disclosure** [3984]. **DISCO** [4171]. **discontinuous** [2244, 1166, 190]. **Discrépance** [1032, 541]. **Discrepancies** [1882, 2284, 2318, 2412]. **Discrepancy** [2139, 3006, 1808, 2043, 2259, 1724, 2694, 2602, 1938, 1939, 2062, 3026, 614, 2211, 2390, 2217, 3125, 3247, 3357, 2004, 1313, 1586, 1786, 1322, 1403, 1497, 905, 1694, 1901, 1800, 4270, 1621, 1622, 1720, 1722, 1810, 1814, 1925, 1928, 2044, 2340, 2341, 1515, 173, 301, 302, 408, 3022, 2178, 731, 1180, 2454, 1457, 2533, 2076, 2795, 2955, 2875, 2803, 453, 454, 616, 1250, 1303, 1385, 1564, 1760, 1761, 2306, 3697, 3126, 3246, 3606, 34, 2118, 398, 541, 2133, 1032, 741]. **Discrete** [4176, 2019, 1100, 2141, 2578, 2914, 3392, 2252, 1216, 1614, 1159, 3181, 3009, 638, 858, 1116, 2511, 2933, 3939, 3822, 1363, 1077, 868, 2879, 3113, 2302, 2737, 2394, 1086, 840, 1577, 1096, 1198, 2978, 3985, 2983, 850, 3376, 811, 2319, 3925, 3960, 3152, 950, 1005, 1947, 2180, 1955, 4054, 922, 2625, 311, 1857, 617, 4110, 1089, 1872, 712, 1584, 1588, 714, 2757, 1599, 2940]. **Discrete-Event** [1100, 2141, 2578, 2914, 3392, 1159]. **Discrete-Time** [2252, 3152]. **discreteRV** [3822]. **discrets** [1588]. **Discriminating** [2858]. **discriminatory** [3373]. **discs** [939]. **disjoint** [1908]. **disjunctions** [1905]. **Disk** [1917, 2975]. **Diskrepanz** [741]. **Diskret** [3057]. **Disney** [4181]. **Disorder** [54, 3053]. **Dispersion** [1105, 1385, 2313]. **dissipative** [3711, 3521, 3595]. **Dissociated** [2432]. **dissociation** [3053]. **Distance** [3643, 2696, 3740, 1553, 3344, 741, 3850]. **Distance-Bounding** [3643]. **distances** [3521, 1707, 1708]. **Distanz** [741]. **Distinct** [1514, 958]. **Distinguishers** [3484, 2786]. **Distinguishing** [2605, 2619]. **DistMe** [3238, 3698]. **distribute** [4077]. **Distributed**

[399, 2237, 4268, 543, 3400, 1700, 2028, 196, 636, 2348, 323, 2274, 1935, 201, 3667, 2864, 3791, 1737, 1740, 606, 562, 2307, 3694, 1192, 368, 1141, 2570, 3767, 633, 316, 3927, 1491, 3145, 178, 3075, 318, 214, 3293, 1507, 43, 1508, 2437, 1350, 2782, 686, 1233, 1357, 478, 306, 3429, 331, 1292, 3432, 1008, 1460, 2797, 2960, 1749, 226, 3878, 2633, 1992, 806, 1200, 1884, 713, 1483]. **Distributing** [3879]. **Distribution** [431, 348, 818, 467, 3529, 719, 1104, 2847, 169, 2251, 951, 2506, 857, 551, 637, 2262, 2264, 3008, 3179, 3009, 1112, 1113, 1114, 1116, 2696, 2352, 863, 323, 826, 4051, 304, 769, 2274, 2447, 2940, 2355, 1071, 2941, 3734, 866, 328, 1366, 1445, 3669, 3670, 2185, 3867, 869, 647, 560, 648, 3029, 923, 3796, 2796, 1128, 694, 872, 970, 2799, 86, 4001, 4075, 1043, 562, 40, 3231, 615, 2469, 2736, 2966, 1767, 2304, 699, 59, 3693, 2741, 259, 3238, 667, 975, 2819, 1575, 2744, 530, 668, 369, 883, 981, 885, 886, 207, 3061]. **Distribution** [845, 2746, 3605, 887, 888, 462, 395, 535, 890, 122, 2008, 3267, 2572, 632, 1404, 3854, 902, 1898, 3639, 853, 950, 1210, 240, 678, 3817, 2849, 1803, 405, 3292, 856, 1501, 952, 1711, 3779, 635, 4030, 553, 1160, 2047, 764, 765, 2053, 1229, 1067, 199, 2514, 246, 3099, 84, 39, 17, 85, 922, 2071, 693, 3028, 3102, 2072, 3034, 3437, 3210, 733, 734, 3912, 1247, 1974, 2888, 2810, 659, 660, 698, 742, 800, 2547, 2548, 2638, 2639, 2967, 927, 928, 617, 2096, 565, 121, 664, 666, 702, 704, 2648, 2743, 2969, 3698, 974, 3353, 1018]. **distribution** [624, 190, 370, 1255, 1256, 460, 3604, 34, 35, 423, 1879, 2479, 1259, 164, 988, 1021, 374, 1674, 13, 5, 14, 2908, 56, 3624, 577, 3862, 3375]. **Distribution-Free** [719, 467, 1229, 164]. **Distributione** [17]. **Distributions** [578, 673, 1022, 2019, 1796, 2248, 1279, 2036, 1216, 2850, 2926, 506, 1524, 3568, 2067, 2452, 1455, 1544, 1847, 3211, 2379, 656, 3799, 1569, 527, 1016, 4017, 2558, 69, 3985, 2011, 850, 266, 3412, 945, 990, 1324, 896, 718, 1270, 151, 2582, 3080, 1336, 1424, 1713, 1807, 3297, 1157, 64, 2171, 3904, 593, 594, 554, 2510, 1166, 958, 1005, 2175, 2858, 1947, 2180, 2516, 3666, 2520, 3025, 1733, 3192, 514, 1952, 3101, 1955, 22, 1012, 967, 1845, 2625, 2205, 2888, 740, 2393, 1572, 4103, 1394, 1089, 1872, 1309, 711, 1140, 1874, 1021, 3255, 1144, 1316, 714, 2127, 751]. **distributions** [2757, 2018, 2321, 3653, 294, 559]. **disturbance** [1152]. **Divergence** [3369]. **Divergent** [3340]. **Diversity** [1997]. **Diversity-Based** [1997]. **Diverted** [338]. **Dividing** [3993]. **Divisible** [3647, 2036, 2817, 3616, 2766, 2393]. **Division** [4096, 1189, 1909, 61, 1784, 2829]. **Divisor** [512, 1294, 1124, 1090]. **divisors** [753]. **Do** [1118, 2605, 2361]. **Document** [3301]. **Documentation** [2876, 4038]. **Does** [2730]. **Doing** [4016, 4019]. **Domain** [1575, 3603, 3711, 1860, 3493]. **Domains** [369, 371, 748, 3113]. **Domenico** [3742]. **Dominated** [3661]. **Donald** [3844]. **Don't** [3892, 2358, 3833]. **Dopant** [3719]. **Dopant-Level** [3719]. **Dorothy** [2149]. **Dose** [338]. **dot** [1751]. **dot-patterns** [1751]. **double** [3283, 3547, 3313, 3573]. **double-scroll** [3283]. **doubly** [461]. **Down** [3769, 505, 1003, 574, 809, 474, 53, 3832, 59, 56]. **Draft** [3881, 2100]. **DRAM** [3920, 3952]. **drastic** [2828]. **Draw** [3985, 2867]. **Drawbacks** [2271]. **Drawing** [4032, 36]. **DRBG** [3924]. **Dress** [3140]. **Drive** [2769, 3168, 2975]. **Driven** [3984]. **Drives** [1917]. **DRM** [2769].

Drones [4067]. **DSS** [2243]. **Dual** [3935, 4056, 4060, 3168]. **dual-drive** [3168]. **Dual-Mode** [4060]. **Dual-ring** [4056]. **Duality** [1224]. **Dudewicz** [1084]. **Due** [3567, 648, 1606, 2889]. **DUHK** [3892]. **d'un** [804]. **d'une** [804, 1588]. **DUPER** [655]. **Durbin** [954, 1113]. **Durbin-Watson** [1113]. **durch** [11]. **Dyadic** [1249]. **Dynamic** [2054, 3428, 1747, 1857, 2384, 3882, 2828, 3992, 3526, 3189, 3675, 2733]. **dynamic-multithreading** [3675]. **Dynamical** [3214, 3707, 3521, 1272, 3785, 3455, 3692]. **Dynamics** [4098, 1617, 3733, 2411, 3711, 1943, 11, 3356, 3595]. **Dyson** [2328].

each [141]. **Early** [1155, 1174]. **Easily** [817, 904, 1130]. **East** [4102]. **Easy** [1518, 3565, 2278, 2359, 2104, 3600, 4042]. **Easy-to-Use** [3565]. **Eat** [3780, 3903]. **Eaton** [1809]. **EC** [3935]. **écarts** [35]. **échantillon** [804]. **échantillonnage** [284]. **Econometric** [2465, 1152, 3339]. **Econometrics** [4263]. **Economical** [1216, 3853, 994]. **Ecrypt** [2911]. **EDF** [1258]. **Edge** [1820, 2307, 4076, 1908]. **edge-disjoint** [1908]. **Edgington** [1004]. **Edition** [1959]. **editor** [2338, 475, 495]. **Editorial** [3769]. **editors** [3057]. **Édouard** [2415]. **Education** [4275]. **Edward** [1084]. **EEG** [3777]. **Effect** [3408, 2162, 377, 2175, 4011, 4055, 1127, 2311]. **Effective** [3007, 1007, 2980, 1608, 3230, 532, 533]. **Effectiveness** [944, 4160, 3361]. **Effects** [3371, 3646, 2988]. **effektiven** [532, 533]. **efficiencies** [164]. **Efficiency** [1228, 1119, 3426, 3732, 2945, 3237, 3142, 2038, 221, 222, 4056, 1679]. **Efficient** [1324, 2325, 3520, 3393, 3721, 3530, 1104, 2585, 3291, 196, 2504, 2927, 3173, 3651, 2255, 3782, 2689, 2172, 2781, 3820, 3094, 3186, 2178, 201, 3667, 3190, 1442, 3326, 1008, 1242, 1376, 3104, 3332, 2956, 1460, 3912, 656, 1187, 1557, 1651, 3592, 2634, 2808, 1562, 2394, 1395, 1663, 3056, 3951, 2651, 1579, 3603, 2312, 1141, 890, 3064, 1669, 1142, 3848, 2489, 2753, 3986, 4022, 1145, 1201, 1675, 850, 1053, 1147, 1262, 3989, 3508, 3412, 3711, 990, 3143, 3810, 2238, 3720, 3929, 2426, 2685, 2770, 1220, 588, 2590, 1626, 3563, 2786, 4057, 3587, 3746, 3747, 2301, 1478, 3481, 2980, 3065, 1200, 3255]. **efficient** [3809, 2991, 3653]. **efficiently** [1909]. **EGD** [2674]. **EICGs** [3409]. **eight** [1230]. **Eighteenth** [4127]. **eighth** [4191, 4266]. **Einflusses** [1755]. **Eins** [5]. **electroconvection** [2699]. **electroencephalogram** [3777]. **Electromagnetic** [3635, 3856]. **Electromagnetism** [4233]. **Electron** [348, 1772]. **Electron-Solid** [1772]. **Electronic** [295, 271, 218, 227]. **electronics** [2827]. **electrons** [11]. **electrophysiology** [2283]. **Elektronen** [11]. **elektronnykh** [351]. **Elementary** [105, 27, 2100, 1984]. **Elements** [206, 260]. **Elias** [3929]. **Eliminating** [1905]. **Elliptic** [3529, 2057, 2941, 2654, 3079, 3093, 4033, 1293, 1632, 2874, 1296, 3123, 4022]. **Elman** [3546]. **Embedded** [4264, 3003, 3087, 3176, 3095, 3024, 2329, 2595, 4224, 3351, 3355]. **embeddings** [2520, 3025]. **Emergence** [524, 507]. **Emission** [3499]. **Emitting** [3744]. **emphasis** [3826]. **empiric** [247]. **Empirica** [17, 16].

Empirical [823, 1522, 200, 2785, 2620, 2718, 3035, 3107, 785, 3212, 793, 664, 1095, 69, 2481, 2128, 678, 2050, 64, 2695, 16, 778, 2183, 2866, 17, 2375, 3106, 2296, 2628, 34, 35, 2129, 3498, 3384]. **empirically** [2823]. **empiriceskoi** [35]. **empirique** [35]. **empirischen** [2695]. **Employing** [4071, 3751]. **emulation** [2504, 3552, 2855]. **emulator** [724]. **enabled** [3462]. **Encoding** [3408]. **Encrypted** [3452]. **encrypting** [2190]. **Encryption** [2761, 433, 434, 3936, 3975, 4058, 796, 4221, 1667, 2482, 2561, 1678, 3507, 3768, 2843, 966, 1179, 1637, 931, 1662, 3601, 3602, 3374, 2131, 3503, 3383, 1035]. **Encyclopedia** [4240, 4269, 4222, 4205, 4281, 4275, 4105, 4118, 4173, 4238, 4282, 4227]. **End** [3857, 2017, 2460]. **End-to-End** [3857, 2017]. **energy** [377, 3843]. **Engine** [3148]. **Engineer** [3868]. **Engineering** [170, 1959, 4118, 4173, 4253]. **Engineers** [645, 277, 1234]. **engines** [2661]. **Enhanced** [3816, 4071, 2105, 3364, 2257, 4041]. **Enhancement** [3301, 3677, 3268, 3407]. **enhancements** [4028]. **Enhancing** [4064, 4052, 1466, 4067]. **ENIAC** [3786, 87]. **Enigma** [2682]. **Enjoy** [3139]. **Enough** [1852]. **ensemble** [2997]. **Enskog** [2352]. **ENT** [4057, 3263]. **entanglement** [3434]. **Enterprise** [2818]. **Enthusiasm** [2769]. **entropies** [1631, 2653, 2976]. **Entropy** [2674, 2148, 3780, 3903, 3863, 998, 2040, 592, 3203, 2291, 3871, 3829, 4074, 3745, 2806, 2887, 3881, 3841, 3927, 3167, 1070, 3785, 4011, 4039, 3885, 3955]. **Entropy-Based** [998, 2040, 2291, 1070]. **Entropy-Uniformity** [2148]. **Enumerating** [2006]. **Enumeration** [3728]. **Environment** [2763, 2023, 2877, 1664]. **Environments** [3409, 3097, 3287]. **EPC** [3478]. **Equal** [667, 217, 1176, 2308]. **Equalization** [3538]. **Equally** [643, 1357]. **Equation** [119]. **Equations** [2255, 2099, 2328, 1356, 161, 132, 133, 138, 3958]. **Equidistributed** [510, 3940, 219, 1175, 2194, 2459, 2714, 2385]. **Equidistribution** [3521, 1812, 2167, 2265, 2344, 2260, 2688, 184, 1068]. **equilibria** [3191]. **Equivalence** [2579, 1908, 1431]. **era** [374]. **Erdos** [2062, 659]. **Ergebnis** [2695]. **Ergodic** [3390, 691, 871, 3000, 3230]. **Erlang** [909]. **ERNIE** [236, 209]. **Erratum** [498, 2995, 433, 1226, 2058, 690, 2182, 600, 2305, 937]. **Error** [648, 1010, 788, 1558, 2, 2906, 2232, 3987, 1804, 3177, 4211, 3437, 3036, 627, 2903]. **error-correcting** [4211]. **Errors** [2112, 2250, 1725, 2071, 2730, 2885, 2889, 2310]. **Erwin** [1959]. **erzeugte** [641, 642]. **erzeugter** [439, 472]. **Erzeugung** [1055, 633, 1233, 1006, 1357, 1508, 331, 1891, 894]. **Erzeugungen** [624]. **Escape** [1703]. **Escrow** [2086]. **Española** [134]. **Especially** [3833]. **Essays** [4099, 3265]. **Esseen** [659]. **estimate** [627]. **Estimates** [506, 1938, 1939, 2062, 1804, 1465, 2207, 1558, 2089, 1879]. **Estimating** [3011, 2796, 1996, 69, 2003, 2854, 616]. **Estimation** [2252, 2696, 1073, 95, 648, 1549, 603, 86, 702, 1993, 2648, 2906, 1592, 540, 1031, 1162, 3320, 1447, 4073, 2888, 34, 3890, 3862]. **Estimations** [2205, 2712, 3121]. **Estimators** [3203, 1962]. **eSTREAM** [2911, 3753, 4259]. **Euclid** [105, 27]. **Euclidean**

[2022, 4006, 759, 2424, 2501, 681, 504, 1568, 3063, 2116, 2410, 2411]. **Eugene** [1004]. **Euro** [2695]. **EUROCRYPT** [4123, 4133]. **Europe** [4284]. **European** [4107]. **Evalua** [3144]. **Evalua-Test** [3144]. **evaluable** [3859]. **Evaluating** [2026, 2799, 1028, 221, 222, 3384]. **Evaluation** [3712, 1497, 3860, 2040, 1033, 771, 772, 509, 245, 865, 1630, 2711, 2612, 332, 3745, 3354, 3847, 2475, 2822, 2232, 2132, 3143, 859, 1071, 2948, 3037, 1974, 1984, 1137, 975, 99, 4061, 423]. **evaluations** [2069]. **even** [3768, 3624]. **even-distribution** [3624]. **Event** [1100, 2141, 2578, 2914, 3392, 2848, 1159, 638, 858, 3530, 554, 1363, 1955]. **Events** [787, 2928, 1220]. **everyone** [3665]. **Evidence** [2872, 3403, 82, 2785, 3053]. **evolution** [3151, 3265]. **Evolutionary** [4241, 2589, 3214, 3697, 4228, 3385, 2606, 2988]. **Evolvable** [2669]. **Evolved** [3031]. **evolving** [3882, 2226]. **Exact** [3647, 551, 1166, 3756, 2319, 1403, 1800, 550, 4030, 1129, 3058, 2476, 51, 2133]. **exact-approximation** [1129]. **Exactly** [3867]. **examination** [4230]. **Example** [582]. **Examples** [1494, 864, 2739, 2983, 2027]. **Exceeding** [3311, 3797]. **Excel** [2464, 2729, 2963, 3224, 2730, 2885, 3225]. **Exceptionally** [1914]. **exchange** [3849]. **Exchangeable** [3553, 1153]. **Excited** [3166, 3551]. **exclusive** [3365]. **Execution** [1492]. **executive** [3053]. **exemplary** [2135]. **Exhaustive** [1115, 1517, 1225, 1226, 1348, 2186, 3573, 3065, 3613, 3614]. **Exist** [3833, 3130]. **Existence** [1823, 875, 2811, 3606, 1266, 1408, 1355]. **expanded** [1768]. **Expanding** [3879]. **Expansion** [687, 411, 442]. **Expansions** [2577, 826, 2962, 2315, 286]. **Expectation** [401, 500, 376, 378, 413, 390, 458, 3757, 421]. **expectations** [3311]. **Expected** [1615, 2474, 3902, 2852, 1933, 1360, 1253]. **expedient** [65]. **experience** [1605, 2244, 952, 2115]. **experiences** [415]. **Experiment** [2845, 3806]. **Experimental** [947, 948, 3281, 3403, 3312, 644, 729, 25, 960, 919, 963, 968, 969, 874, 976, 2825, 3888, 812, 3282, 1940, 1755, 177, 7]. **Experiments** [3637, 152, 863, 353, 777, 869, 1370, 1963, 1181, 872, 885, 886, 887, 138, 429, 90, 137, 3850]. **Explaining** [3007]. **Explicit** [2335, 3858, 3177, 1811, 1926, 2966, 3163, 2045, 2168, 2805, 2223]. **Exploiting** [3711, 2959, 4040]. **Exploration** [3888]. **Exploring** [4285, 2011]. **Exponent** [1731, 1850, 763]. **Exponential** [578, 1922, 3017, 3184, 2355, 3029, 1079, 2630, 309, 790, 2548, 2967, 3233, 4017, 980, 2898, 3260, 1401, 1324, 349, 676, 2774, 2171, 2438, 1628, 2858, 3666, 3102, 334, 1246, 253, 802, 2549, 2648, 2743, 2969, 3056, 263, 461, 2313, 988, 3255, 2233]. **Exponentially** [214, 3568, 3250, 316, 3297, 226, 3878]. **Exponentiation** [2779, 2190, 1662]. **exponentiations** [1595]. **exponents** [2872]. **Expressing** [252]. **expression** [2069]. **Extendable** [3837]. **Extendable-Output** [3837]. **Extended** [2428, 1167, 1524, 2613, 3827, 1561, 1201, 498, 1269, 4161, 1444, 1837, 3575, 482, 3443, 1248, 2487, 2490]. **Extending** [3528, 4008, 1191]. **Extends** [1836]. **Extensible** [2515, 2811]. **Extension** [3677, 2307, 3603, 3249, 676]. **Extensions** [632, 924, 2303, 2183]. **extensively** [1910, 2365]. **extracted** [3913]. **Extracting** [2996, 2213, 1770]. **Extraction** [3418, 3745, 3696].

Extractor [3704, 3986]. **Extractors** [3858, 2519, 3871, 2665, 2653, 2976, 2490, 3509]. **Extrapolation** [1374]. **Extraterrestrial** [2103]. **Extreme** [1724, 8]. **Extremely** [481, 3747, 743, 600, 601, 3624]. **extremely-high-throughput** [3624].

fabulous [3318]. **Face** [3368]. **Facilities** [1639, 349]. **Factored** [1327]. **Factorial** [2302]. **Factoring** [1041, 1182, 1296, 1871, 1784, 2829]. **Factorization** [1866, 744, 1368, 701, 1195, 1995, 3699]. **Factorizations** [1062, 1333, 2679]. **fail** [3979]. **failure** [2442]. **Fair** [2769, 2695, 2524, 3101]. **Fairfax** [4141]. **Fairmont** [4149]. **fall** [312, 451]. **Families** [3559, 2856, 2616, 2793, 3980]. **Family** [898, 3156, 1342, 2693, 3876, 709, 1586, 3500, 3519, 3640, 1616, 2257, 1292, 3797, 1021, 3763, 2833]. **Fast** [2672, 1151, 3148, 1056, 3154, 3815, 3001, 1699, 1500, 586, 2768, 3936, 2171, 2694, 1231, 1435, 686, 1437, 508, 3821, 4053, 3187, 3564, 3095, 2281, 2705, 1365, 2523, 1839, 2189, 2530, 2951, 3978, 1744, 3941, 1746, 309, 603, 280, 791, 2879, 2081, 3111, 4058, 1468, 119, 1652, 3690, 3046, 3047, 3048, 743, 3983, 528, 1872, 3242, 1580, 3482, 3807, 3249, 2118, 1786, 3922, 3258, 3370, 713, 2233, 540, 3499, 1268, 950, 774, 1358, 2056, 2789, 2495, 2522, 3100, 1009, 1456, 3327, 3206, 3328, 3579, 334, 1642, 336, 1130, 1976, 1984, 3052, 493, 1668, 2002, 4020, 2230, 714]. **fast** [3375, 2664]. **Fastest** [3229]. **fat** [1599]. **fat-tailed** [1599]. **Fault** [3856, 3532, 3723, 1248]. **Fault-tolerant** [3723, 1248]. **Faulty** [3791]. **Faure** [2752]. **FCRC** [4190]. **FCSR** [2912, 3943, 3365]. **FCSRs** [3638, 3305, 3941]. **FDC** [1962]. **Feather** [4060]. **Features** [3146, 443, 1591]. **February** [4268, 4199, 4232, 4108]. **Feedback** [2585, 1215, 1335, 2768, 1067, 1534, 2531, 518, 651, 3877, 653, 873, 3593, 1574, 3703, 2753, 3988, 3168, 1730, 2072, 967, 3999, 333, 3585, 310, 2078, 2733, 1304, 1388, 3801, 1776, 3957, 3852, 1138]. **Feeding** [3166]. **Feinstein** [319]. **Feistel** [3891]. **Feistel-inspired** [3891]. **Feller** [3397, 1413]. **Fence** [3769]. **Fermat** [3654, 3728]. **fermions** [3723]. **FerroCoin** [4048]. **Ferroelectric** [4048]. **ferromagnetic** [740]. **Festschrift** [4262]. **Few** [2996, 3173, 3137, 3100, 1310]. **few-body** [1310]. **Fibonacci** [3318, 2134, 2237, 3810, 1902, 409, 3559, 1972, 250, 1976, 1977, 2081, 2082, 2083, 2882, 1986, 2470, 1786, 1882, 2567, 231]. **Field** [2240, 4170, 2898, 1604, 1969, 2632, 1252, 930]. **field-programmable** [2632]. **Fields** [4006, 3742, 1243, 1968, 3441, 3589, 1866, 2211, 1793, 317, 3934, 4193, 3731, 959, 1182, 2298, 4172, 1654, 1761, 1865, 2212, 2549]. **Fifteenth** [4116]. **Fifth** [4253, 4176, 4290, 4188]. **Figures** [1489]. **File** [3279]. **Files** [3301]. **filling** [188]. **Filter** [3111, 3816]. **Filtered** [2623, 2912]. **Filtering** [549, 3014, 3702]. **filters** [1714, 1715, 1849]. **Final** [1016, 2462]. **Finalist** [2561]. **Finalists** [2521, 2609, 4259]. **finalizer** [3608]. **Finally** [1354]. **Finance** [3150, 4277, 4269, 3798]. **Financial** [2407]. **Find** [2278, 1392, 2124, 2359, 2104]. **Finding** [512, 2606, 2786, 3995, 3752, 3760, 1013, 1090]. **Finely** [3314]. **Fingerprint** [3321, 3504]. **fini** [2890]. **Finite** [2993, 2025, 1102, 375, 468, 3163, 2252, 1243, 1968, 2298, 3441, 2543, 2544,

4172, 1654, 1865, 1866, 1997, 2983, 317, 2024, 212, 1207, 1800, 3934, 3731, 1528, 1182, 3682, 1757, 1252, 1761, 2549, 2890, 930, 3621, 2133, 577, 4193]. **Finite-Difference** [2252]. **finite-length** [3621]. **FIPS** [1869]. **First** [4068, 1740, 285, 259, 4108, 4143, 4209, 4091, 581, 2681, 1361, 3684, 87]. **First-Order** [1740, 1361]. **Fisher** [947, 948, 960, 963, 968, 969, 976]. **Fishman** [4262]. **fission** [3843]. **Fit** [597, 2961, 19, 840, 69, 88, 102, 3164, 4129, 1166, 1070, 1178, 2537, 98, 626]. **Five** [2924, 1030, 2190]. **Fix** [3868, 2730, 2903]. **Fixed** [1847, 1382, 4062, 1944, 3234]. **fixed-length** [3234]. **fixes** [4026]. **Fixing** [2885]. **FL** [4220]. **Flash** [3982]. **Flaw** [4014, 3725]. **Flaws** [3397]. **flights** [256]. **Flip** [162]. **Flip-flop** [162]. **Flipper** [163]. **flipping** [1875]. **Flips** [1102, 1207]. **float** [3630]. **Floating** [3993, 4032, 3188, 1737, 3084, 3573, 2071, 3880, 668, 2225, 1876, 3255, 713, 3071]. **Floating-Gate** [3188, 3071]. **Floating-Point** [3993, 4032, 2071, 668, 2225, 1876, 3255, 713]. **Flock** [4060]. **flop** [162]. **Florida** [4120, 4198, 4089, 4181, 4110]. **flow** [3101, 1788]. **flow-level** [3101]. **Fly** [3354]. **Fock** [2556]. **folding** [927, 928, 3916, 2988]. **Fonctions** [4, 284]. **Force** [4098]. **forced** [3627]. **forests** [1896]. **Fork** [1410, 1843]. **Fork-Join** [1410, 1843]. **Form** [1830, 2455, 2530, 943, 3101, 2664]. **Formal** [2065]. **formalism** [2666]. **Formalization** [3096]. **Format** [3301]. **Formation** [199, 478]. **forme** [2664]. **Forms** [845, 1210, 1071, 1128, 975]. **formula** [3570, 2795]. **Formulae** [169]. **Formulas** [396]. **Formulation** [2156, 1005, 707]. **Forsythe** [632]. **Fortran** [2690, 724, 2182, 912, 920, 1082, 618, 1773, 1676, 499, 3718, 2245, 477, 2064, 1949, 611, 739, 526, 1137, 936, 940]. **fortune** [1829]. **Forty** [4290]. **Forty-fifth** [4290]. **Forum** [2769]. **forward** [3103, 3066]. **Found** [1798]. **foundation** [570]. **Foundational** [4293]. **Foundations** [4114, 4117, 4120, 4135, 4140, 4146, 4152, 4162, 4185, 4194, 4198, 4219, 4223, 4274, 4289]. **Four** [1475, 2419, 1729, 2293, 2084, 2085, 2462, 2652, 2745, 3372]. **Four-Bit** [1475]. **four-dimensional** [3372]. **Four-Tap** [2419]. **Fourier** [2940, 404, 3939, 3738, 3441]. **Fourth** [4229, 4144, 4159, 4213, 4090]. **FPGA** [3142, 3150, 3282, 4066, 2428, 3542, 2504, 3089, 3783, 3552, 3315, 3324, 3432, 3942, 3442, 3949, 3466, 3475, 3354, 2652, 2745, 3489, 3491, 3763, 3808, 3848, 2832, 3268, 3380, 3626]. **FPGA-Based** [2428, 3354, 3142, 3552, 2832, 3626]. **FPGA-Optimised** [3491]. **FPGAs** [3143, 4049, 2725, 3842, 3883, 3496]. **fractal** [3991]. **fractals** [1571, 4237]. **fraction** [2928, 3999, 286]. **fractional** [3973, 2080, 3052]. **fractions** [1249]. **Framework** [3091, 2491, 3827, 3678, 4061, 3245]. **frameworks** [3925, 3839]. **France** [4123]. **Francisco** [4228, 4232]. **Frank** [3527]. **Free** [719, 3650, 3553, 3378, 1324, 467, 2156, 3178, 1229, 11, 1090, 164, 3620, 3622, 3889]. **FreeBSD** [2735]. **freedom** [349, 1597]. **freie** [11]. **French** [178, 2844, 3, 4, 1900, 762, 322, 1032, 1375, 2196, 284, 697, 736, 343, 2552, 2890, 804, 35, 1588, 2664, 541]. **frequencies** [65, 74]. **Frequency** [3968, 2060, 2177, 3869, 2974, 1050, 628, 4067, 554, 1360, 3338, 2744, 714].

Frequency-Modulated [2974]. **frog** [2347]. **frontiers** [4262, 4237]. **frustration** [3372]. **FTN77** [1936]. **Fukuoka** [4155]. **Full** [3285, 1111, 1034, 3973, 3362, 2830]. **Full-Length** [1111]. **Fully** [3160, 2598, 2910]. **Function** [579, 3897, 3643, 1903, 1217, 1614, 637, 2693, 323, 826, 2448, 3020, 1938, 1939, 2062, 3669, 3670, 2613, 3796, 2796, 653, 86, 2634, 2808, 1867, 2211, 458, 1575, 3603, 2654, 3386, 2572, 816, 498, 3928, 3812, 3640, 1210, 680, 996, 2052, 1073, 306, 1958, 39, 482, 3037, 3109, 1246, 255, 1247, 1974, 2880, 3343, 2212, 3237, 702, 3802, 1310, 1255, 1256, 3257]. **Function-based** [3386]. **functional** [3077, 3284, 1646, 2411]. **Functionalities** [4060]. **Functionality** [2612, 2475]. **Functionals** [1592]. **functioning** [3053]. **Functions** [3713, 348, 2025, 3396, 3813, 3642, 1799, 3858, 3165, 3967, 3181, 2696, 4051, 1167, 1232, 3732, 328, 1641, 485, 3749, 2086, 3685, 3833, 3834, 3837, 2468, 3838, 3695, 2817, 3840, 527, 1665, 3701, 369, 980, 2114, 3369, 1592, 4023, 431, 1325, 3632, 1328, 2913, 3773, 2146, 4, 3816, 3859, 4026, 1338, 1106, 2852, 1031, 1162, 2510, 2446, 3184, 3426, 3566, 1444, 1292, 3739, 3671, 3977, 4095, 2294, 1183, 1297, 1745, 1380, 1130, 3112, 3447, 284, 1860, 2301, 3234, 1984, 2096, 3457, 664, 190, 2564, 670, 1054, 3851, 3809, 2018, 958, 246]. **functions-based** [3566]. **Fundamental** [2577, 3397]. **Fundamentals** [957, 2708, 2814, 3194]. **Funktionen** [246]. **Further** [2424, 2155, 52, 133, 3845, 421, 289, 3923, 3053]. **fused** [2672]. **Fushimi** [2230]. **fusion** [3281]. **Future** [3431]. **Fuzzy** [3601, 3986, 3602].

G [542, 3004, 596, 640, 1964, 1084, 262, 70]. **G5** [380, 391, 435, 677, 598, 480, 647, 362, 363, 364, 620, 462, 630]. **Galois** [2240]. **gambler** [3204]. **Gambling** [2494, 2670, 3768]. **Game** [2892, 3991, 2843, 3191]. **game-playing** [2843]. **gaming** [490]. **Gamma** [673, 4047, 755, 817, 543, 822, 910, 1279, 769, 870, 923, 2381, 2539, 1383, 4017, 2220, 1049, 535, 891, 892, 1020, 715, 808, 3765, 896, 901, 1268, 1058, 856, 377, 2858, 1037, 1237, 331, 965, 3102, 3912, 788, 3444, 831, 1083, 2096, 567, 619, 704, 884, 984, 750, 1021, 3252, 849, 751, 716, 1023, 764, 686, 3747]. **gamma-distributed** [331, 686]. **Gamma-distribution** [764]. **gamma-rays** [1083]. **gammaverteilten** [331]. **gap** [235]. **gas** [816, 680, 2312]. **GASPRNG** [3727]. **Gate** [3188, 2632, 3071]. **Gates** [3137, 3422]. **Gateway** [4225, 4119, 4166]. **Gathering** [2674]. **Gauss** [1860]. **Gaussian** [3141, 2673, 4006, 901, 1024, 1414, 677, 1105, 3290, 2504, 3779, 1617, 3089, 3302, 298, 350, 2855, 3660, 2281, 3788, 2283, 2525, 3432, 2712, 2873, 2953, 3036, 3037, 3211, 3579, 3678, 3588, 3746, 3831, 3875, 654, 1645, 452, 1043, 3799, 879, 365, 3052, 3475, 3476, 3805, 535, 396, 3131, 3254, 3764, 3808, 3848, 1884, 3495, 1592, 893, 2990, 2318, 2412]. **Gaussian-distributed** [3432]. **Gbit** [3611]. **Gbit/s** [3611]. **GCD** [1269, 1835, 1191, 1305, 1999, 2002, 2116, 1887]. **GCDs** [3216]. **GECCO** [4241, 4228]. **GECCO-2001** [4228]. **geeks** [2804]. **gems** [4278, 4288, 4258]. **Gen2** [3286, 3478]. **généateurs** [4082]. **General** [950, 502, 2935, 1938, 1939, 2062, 3870, 3211, 525, 106, 1086, 850, 3267, 2323,

4157, 724, 3827, 385, 972, 1256, 3126, 3606, 3953, 620]. **General-Purpose** [1086]. **Generalised** [2184, 901]. **Generalization** [445, 238]. **generalizations** [3654]. **Generalized** [3929, 1215, 1335, 1709, 2851, 3303, 3029, 1377, 651, 388, 3346, 2752, 1024, 3992, 1902, 3285, 1807, 3779, 1927, 2776, 411, 442, 1358, 3560, 2858, 3788, 1948, 3102, 2072, 3210, 3579, 1858, 1304, 2648, 2743, 2969, 3058, 2749, 1067]. **Generate** [1327, 1027, 1101, 1901, 2605, 1534, 3767, 1894, 2422, 775, 2180, 1235, 3953, 1595, 1888, 1679, 2018]. **Generated** [3275, 3391, 267, 244, 1074, 615, 3840, 373, 3625, 1320, 1794, 583, 758, 1708, 439, 472, 587, 3654, 1427, 1511, 242, 768, 1351, 3092, 641, 1945, 1038, 2287, 2071, 2072, 1180, 3584, 2199, 2380, 698, 800, 1190, 1470, 1565, 2547, 3232, 3692, 930, 839, 1046, 3604, 2907, 233, 2321]. **generates** [2633, 2975]. **générateurs** [1375, 2664, 2552, 2196]. **Generating** [1023, 2135, 2238, 817, 1687, 3894, 2913, 1604, 1796, 903, 949, 3639, 543, 1104, 1903, 2248, 855, 3778, 3409, 3817, 270, 196, 1216, 1217, 1614, 1806, 2507, 997, 1280, 3181, 153, 323, 409, 3556, 3557, 3993, 479, 245, 201, 1946, 3788, 3789, 155, 2525, 1955, 2069, 780, 1736, 1737, 1125, 3029, 1012, 1847, 3579, 309, 2077, 3588, 251, 873, 253, 254, 280, 281, 311, 335, 791, 970, 1131, 2381, 2539, 1650, 2086, 794, 1383, 3686, 834, 3592, 1300, 1384, 204, 205, 525, 2810, 1569, 1572, 3461, 2471, 1988, 2103, 528, 621, 705, 3353, 2219, 1254, 2220]. **Generating** [1096, 461, 2227, 1141, 628, 2313, 2562, 2488, 1317, 850, 2127, 1146, 716, 2986, 3069, 1401, 1055, 2575, 3812, 678, 1909, 1106, 1108, 770, 1934, 1233, 3661, 94, 1529, 1834, 3666, 1541, 965, 1842, 922, 3102, 1457, 2626, 3678, 788, 334, 226, 255, 283, 336, 831, 1129, 2382, 2540, 3878, 489, 2388, 3751, 924, 3044, 2393, 567, 619, 665, 344, 1872, 704, 623, 2398, 568, 3843, 1094, 884, 984, 2823, 1584, 4043, 750, 848, 193, 167, 1674, 4084, 714, 1483, 4045, 2569, 3710, 1891]. **Generation** [3511, 3959, 1022, 1406, 2420, 3925, 1267, 2839, 3770, 852, 542, 755, 756, 897, 898, 899, 900, 3520, 2327, 2915, 2998, 1329, 2243, 1495, 2332, 2500, 2334, 2153, 3535, 854, 760, 2583, 822, 1105, 1276, 762, 216, 548, 470, 1337, 2036, 2850, 2926, 1507, 2505, 1107, 1218, 2159, 2771, 3005, 4068, 636, 3301, 1065, 1342, 1222, 2046, 3782, 2434, 1111, 2349, 3010, 91, 92, 2694, 1932, 2352, 596, 2353, 2777, 3310, 640, 445, 2354, 2603, 325, 2281, 1731, 1944, 2863, 3667, 3190, 2608, 598, 1365, 2707, 330, 2709, 2184, 2710, 3430, 1077, 1367, 3669, 3670]. **Generation** [1956, 868, 1634, 4012, 779, 828, 870, 1543, 2288, 1459, 2619, 2871, 3033, 3207, 830, 3794, 1181, 3978, 3336, 249, 3744, 694, 1643, 1749, 3875, 3681, 2200, 1854, 2879, 2082, 2083, 3040, 452, 2204, 2884, 656, 609, 737, 1188, 3114, 131, 187, 1084, 2551, 3691, 3881, 610, 1764, 2094, 2210, 661, 700, 227, 4015, 1086, 666, 3917, 4017, 3983, 260, 1994, 3352, 1395, 1663, 1017, 2974, 3804, 1577, 3123, 2558, 287, 844, 883, 980, 981, 982, 983, 1019, 1097, 1198, 3482, 2000, 1878, 2978, 629, 889, 1257, 1782, 3249, 572, 2315, 3128, 3611, 3920, 3952]. **Generation** [891, 892, 1020, 2662, 136, 165, 1786, 3132, 3254, 1884, 3257, 3258, 2231, 427,

1145, 1201, 538, 539, 1675, 715, 2492, 1598, 3709, 3890, 3627, 3853, 633, 4064, 1265, 432, 2497, 3927, 1491, 1795, 3145, 3276, 3854, 1898, 1328, 2997, 3521, 3522, 3716, 3717, 3718, 3772, 1268, 1899, 2142, 3074, 3634, 349, 3151, 991, 2916, 3720, 853, 3964, 2150, 3157, 820, 1060, 1900, 182, 1498, 1418, 950, 909, 1700, 402, 1801, 3899, 403, 2426, 2336, 3080, 2033, 2338, 469, 1336, 1338, 994, 1613, 1711, 2851, 3410, 995, 996, 1029, 1109, 1219, 1712, 1713, 1807, 2256, 3297, 3779].
generation
[999, 1158, 1425, 218, 2048, 2169, 322, 2853, 1429, 2437, 767, 554, 1069, 1287, 1432, 1520, 3013, 556, 185, 1289, 1357, 642, 2857, 3730, 3973, 3424, 3865, 3820, 3022, 2064, 1073, 1831, 2517, 2705, 2789, 1441, 3189, 1037, 202, 1444, 1733, 1531, 1532, 827, 1075, 3997, 118, 1177, 1238, 3199, 1008, 4013, 1452, 782, 1454, 4054, 1011, 1039, 3908, 1965, 2373, 2376, 2870, 3674, 3910, 1845, 129, 3675, 4073, 3743, 1460, 4036, 3828, 3874, 1244, 158, 1462, 3831, 2536, 792, 1080, 3747, 1856, 1977, 2461, 2541, 2542, 1857, 160, 130, 1132, 3688, 3880, 563, 564, 1655].
generation [1762, 1763, 1982, 2093, 2095, 617, 3347, 879, 3756, 419, 3916, 491, 3839, 1085, 1045, 3595, 3918, 3052, 3467, 3053, 1091, 1047, 3056, 3121, 935, 977, 4061, 1196, 882, 2557, 979, 3059, 3805, 2312, 1199, 987, 149, 2118, 3612, 2230, 2565, 1480, 3067, 3133, 3764, 1588, 2566, 1315, 3955, 1144, 1316, 849, 3706, 575, 631, 671, 713, 3377, 3138, 2568, 3623, 3708, 2416, 1597, 1260, 2418, 2671, 2757, 3862, 1590, 3375, 1900, 322, 1588, 1508, 1006, 624, 894, 762, 1525, 1539, 1540, 1311, 3004, 3082]. **Generations** [3533, 3577, 3287, 2405].
Generator [3628, 1151, 3512, 1206, 1897, 3515, 3275, 3391, 2240, 3149, 2140, 295, 3524, 3635, 757, 3815, 3529, 1208, 3642, 1331, 906, 502, 1419, 821, 1500, 3538, 3405, 4048, 2028, 3166, 3286, 3407, 4025, 4066, 3648, 2032, 2428, 1156, 1609, 2337, 3290, 1913, 2925, 3968, 1615, 2772, 271, 2161, 3085, 3086, 3087, 3176, 3548, 2687, 2433, 2775, 3551, 4031, 1161, 3182, 2172, 2596, 3554, 1519, 3419, 824, 2511, 2697, 2933, 1353, 1434, 1522, 2443, 2599, 2935, 3420, 200, 243, 686, 1437, 3183, 3422, 3423, 3314, 508, 3019, 1290, 2448, 3316, 2860, 3662, 354, 4053, 1362, 3565, 1122, 3567, 3664]. **Generator** [3188, 3024, 1832, 4070, 2790, 1630, 3824, 2450, 3324, 1836, 3196, 1538, 1633, 3200, 3791, 2946, 2947, 3574, 1010, 332, 481, 1295, 3672, 4014, 3673, 3031, 649, 1743, 1744, 3214, 3872, 2958, 3442, 1552, 520, 521, 654, 2538, 1082, 2081, 2202, 1466, 1187, 2387, 2206, 1859, 3687, 3593, 4038, 3341, 1869, 3451, 3452, 2964, 3231, 3453, 3914, 4059, 929, 2394, 3119, 3120, 743, 1990, 3696, 841, 933, 1048, 229, 1576, 4018, 3476, 3242, 3701, 3354, 1197, 530, 531, 747, 936, 1580, 1581, 2402, 1582, 2114, 2655, 3062, 986, 2480, 3358, 3483, 890, 3064, 2119, 2900, 3611, 3129, 3250, 3251].
Generator [3363, 1479, 3253, 3364, 3848, 3256, 3493, 3367, 3368, 1589, 3369, 3371, 2124, 1676, 3376, 3378, 3622, 428, 1053, 1147, 1319, 1791, 3499, 3268, 3380, 3381, 3502, 3271, 3382, 3273, 3504, 3385, 1262, 3386, 3412, 2760, 3387, 2571, 1407, 815, 3389, 1601, 3960, 3274, 3141, 1683, 3144, 816, 3513, 3514, 2021, 2022, 2324, 2912, 1490, 3991, 2241, 3771, 4065, 3992, 1056, 3395, 1493, 466, 3526, 2917, 3721, 1691, 3153, 2918, 3814, 3280, 3399, 3157, 3158, 3281, 3282, 3531, 3532, 1417, 677, 1103, 3079, 634, 3283, 3816, 3284, 1608, 1906, 3404, 1420, 546, 3285, 3539, 1275, 320, 3168, 679, 680]. **generator**

[1704, 2849, 3170, 2035, 3542, 1421, 2504, 3543, 1805, 3411, 994, 2685, 3723, 471, 3546, 4027, 4028, 552, 3300, 1110, 4050, 3415, 3178, 3089, 912, 1510, 1625, 1721, 1223, 1283, 1347, 763, 3550, 2932, 3783, 475, 724, 3552, 1516, 2595, 3784, 1286, 2855, 1350, 2350, 3727, 2598, 3905, 2699, 2446, 1168, 379, 412, 3421, 1526, 774, 776, 3312, 3313, 1358, 2056, 2176, 3093, 3660, 4033, 3315, 2058, 2059, 3906, 3562, 3319, 3566, 1940, 2362, 1943, 2944, 1947, 2516, 3099, 3189, 3323, 3736, 1236, 1629, 224, 382, 2283, 1237, 2449, 154, 2363, 1949, 2182, 2495, 2522].
generator [3572, 2791, 1293, 1123, 3432, 3325, 1448, 2187, 2188, 2287, 3197, 3198, 3326, 3201, 2526, 3976, 1009, 1453, 1636, 2948, 600, 601, 248, 784, 1126, 1373, 3434, 2293, 3327, 3435, 1013, 3206, 3328, 3329, 785, 2073, 2873, 2874, 2953, 3036, 3037, 2534, 1550, 484, 2625, 3580, 3581, 2959, 1849, 2875, 3440, 3583, 3586, 3873, 2197, 2721, 1969, 602, 1642, 652, 3587, 3746, 3337, 1554, 1555, 2299, 2723, 3445, 2880, 3590, 1976, 3798, 2385, 4075, 3591, 795, 455, 833, 2733, 796, 1083, 3448, 925, 835, 3449, 836, 3342, 3450, 1015, 1252, 3454, 662, 3235, 3755, 3117, 2215, 3349, 1471, 162, 492, 526]. **generator**
[3463, 972, 1660, 3236, 3949, 2396, 2553, 2102, 1307, 803, 620, 2554, 1991, 3466, 622, 367, 3598, 1662, 3055, 2896, 2897, 3057, 1664, 3700, 706, 3846, 3885, 3058, 710, 1777, 2401, 3478, 493, 3601, 3602, 1668, 2113, 2224, 2225, 2653, 2976, 4041, 1876, 3480, 846, 1877, 289, 2977, 2478, 2656, 2825, 2563, 208, 2827, 3127, 2979, 4003, 3610, 2748, 1784, 2749, 2750, 2751, 2829, 2980, 2981, 3362, 3487, 3488, 3252, 3489, 3490, 1200, 2408, 3366, 1787, 4021, 2489, 3134, 3370, 3494, 3705, 3261, 3262, 3497, 3617, 3618, 1593, 3068, 3264, 3379, 3266, 1792, 3624, 3269, 3503, 3071, 3270, 3958]. **generator**
[2758, 2910, 3626, 3506, 2990, 4046, 3766, 1263, 1600, 2321, 2991, 1892, 3545, 3653, 4072, 2012, 1221, 460, 462, 3259, 3374]. **Generatoren** [1055, 1057].
Generators [1402, 2573, 2322, 2837, 293, 4047, 2134, 2237, 2994, 3390, 1487, 3713, 3893, 3277, 3148, 2675, 2326, 3150, 2763, 2998, 580, 2144, 3394, 4082, 3523, 1606, 2245, 3638, 2148, 904, 3930, 4007, 1416, 3401, 3775, 2846, 3001, 3159, 2152, 907, 908, 3160, 1212, 2427, 910, 3408, 2429, 1215, 1277, 1335, 3169, 2923, 404, 2588, 1706, 3294, 1504, 1918, 1340, 1709, 1919, 2254, 3173, 3175, 3651, 3652, 3936, 4008, 4078, 2686, 723, 3655, 1343, 2041, 2163, 2164, 4069, 1426, 1344, 1620, 3179, 2051, 3549, 4009, 2692, 3012, 3658, 766, 823, 1000, 1033, 1115, 1517, 3819, 1228, 725, 1118, 1820]. **Generators**
[1521, 3016, 304, 771, 772, 1823, 2779, 2780, 2936, 3659, 3729, 4052, 1359, 3732, 2057, 2060, 2177, 3094, 3186, 3940, 3095, 2278, 2607, 2066, 2941, 865, 3428, 4035, 279, 327, 3995, 3996, 2711, 2366, 2189, 3740, 2612, 560, 2613, 1546, 1242, 1377, 1378, 1741, 2195, 2295, 2371, 2377, 2455, 2456, 2457, 2529, 2530, 2531, 2620, 2717, 2718, 3035, 3105, 3107, 3330, 3578, 3795, 3998, 4083, 3869, 1740, 3334, 3212, 2719, 2956, 2957, 3215, 3679, 3441, 2378, 4074, 1641, 2466, 3745, 358, 3876, 3877, 1184, 1186, 1853, 1855, 2800, 2727, 3223, 1648, 2731, 4058, 3749, 1469, 1557, 1559, 1756]. **Generators**
[1299, 2208, 2634, 2808, 1862, 2641, 2739, 3691, 739, 874, 612, 657, 797, 798, 3690, 1867, 3838, 3460, 1392, 3119, 1986, 1087, 1774, 3842, 3883, 420, 1475, 2819, 3470, 3471, 3472, 3473, 2109, 3239, 805, 2649, 3474, 3241, 1665, 3475, 2110, 3355,

4076, 1095, 2475, 2651, 2822, 3060, 2226, 571, 2483, 2485, 536, 2659, 2660, 2406, 2902, 1400, 1585, 1785, 2010, 1142, 3491, 574, 2832, 3135, 1672, 1673, 2232, 1885, 2835, 3888, 808, 1318, 2128, 2494, 2670, 428, 1677, 429, 495, 3765, 851, 1681, 2419, 1055, 1149, 1204, 1320, 1322, 1485, 3711, 2672, 1893, 2496, 3142, 3143]. **generators** [3891, 1266, 1408, 1326, 3810, 499, 3712, 2137, 3632, 2139, 1686, 3145, 1688, 2325, 3519, 3715, 3855, 2328, 3633, 3718, 1057, 3074, 3634, 3773, 3393, 3278, 2580, 2024, 3856, 3152, 1692, 1152, 1058, 1414, 2919, 3931, 1059, 2920, 1209, 2026, 1696, 2678, 2766, 3002, 3078, 2425, 909, 1499, 1699, 2921, 1211, 721, 3164, 3777, 1910, 3167, 3966, 3722, 3541, 1911, 2157, 2249, 547, 2250, 1915, 2034, 2158, 2251, 1028, 1916, 3293, 2339, 1339, 1505, 1506, 3295, 1423, 1502, 1503, 3544, 1612, 1710, 2770, 2927, 3174, 3296, 3901, 1341, 1424, 635, 2928, 3724, 3298, 3299, 1616, 407, 1425, 2773]. **generators** [2257, 2258, 2508, 1509, 3302, 1427, 1428, 1512, 1718, 1346, 2930, 1930, 1931, 2050, 2170, 2267, 2346, 2347, 2436, 2589, 2590, 1725, 1163, 1818, 859, 955, 956, 1225, 1226, 1348, 1819, 2053, 3904, 440, 1035, 275, 2351, 862, 1002, 2934, 3092, 3905, 1355, 3785, 2937, 3558, 2781, 1729, 1824, 773, 477, 1233, 1289, 1357, 2601, 2701, 2783, 2784, 3184, 3731, 3425, 1527, 3426, 1438, 1826, 1827, 1936, 688, 4034, 3563, 3564, 1937, 2063, 2279, 2280, 2359, 2606, 3907, 1439, 2282, 3735, 778, 4010, 867, 3427, 3322, 1440, 1948, 3569, 1175, 3738, 1732]. **generators** [2519, 2520, 3025, 1533, 356, 383, 2183, 2945, 1838, 2186, 2285, 2286, 2364, 2365, 3573, 1007, 3199, 1450, 2866, 920, 1734, 3205, 2453, 3575, 1738, 2949, 3030, 3103, 829, 1375, 1376, 1458, 1640, 1846, 2191, 2193, 2194, 2196, 2291, 2292, 2372, 2374, 2375, 2458, 2459, 2616, 2618, 2714, 2793, 2868, 2951, 3104, 3106, 3438, 1547, 3909, 1127, 2950, 3209, 3332, 2296, 1742, 3210, 1183, 1297, 3335, 871, 2628, 3942, 3439, 3109, 4000, 3218, 1245, 2199, 2721, 1972, 2078, 3680, 3338, 3682, 448, 449, 486, 522, 1644, 1750, 1973, 1975, 2801, 2725, 3220, 3981, 2383, 2632, 2881, 2882, 3683]. **generators** [3748, 1752, 1979, 2384, 2386, 2803, 3041, 3110, 1753, 1858, 793, 3225, 3112, 3447, 2806, 2887, 1755, 1651, 456, 3945, 3751, 3340, 2089, 3836, 1758, 611, 3116, 3344, 2209, 658, 1133, 1304, 1566, 2549, 2637, 2738, 1567, 1765, 1766, 3234, 2889, 3455, 3456, 618, 2552, 2891, 2968, 3050, 3459, 1659, 1135, 1306, 1393, 1472, 1768, 1769, 2101, 1394, 2104, 3464, 3051, 1137, 2107, 842, 2397, 3950, 1092, 1573, 881, 1093, 3884, 3847, 2309, 2112, 1579, 1875, 1398, 1478, 1779, 2899, 3760, 2652, 2745, 1780, 2477, 3481, 4062, 3919, 263, 2227, 2001, 1781, 3607, 2826]. **generators** [2486, 3807, 4020, 4042, 1312, 3609, 2657, 2658, 2487, 3360, 2901, 2316, 2663, 2830, 2982, 3065, 3066, 3130, 3486, 3613, 3614, 1669, 1883, 2009, 3131, 3255, 3763, 3808, 3492, 2984, 2664, 2490, 2665, 1671, 989, 2833, 4022, 2754, 2834, 3496, 1098, 2123, 1099, 3923, 4004, 2233, 1886, 3619, 1790, 2669, 2129, 2235, 2015, 463, 3498, 2320, 3070, 3501, 3889, 2759, 3383, 3384, 3851, 3508, 3509, 2333, 3208, 3333, 400, 515, 483]. **generators-part** [2657]. **Generazione** [991, 491]. **Genetic** [2580, 2607, 2702, 2703, 646, 690, 3031, 2798, 4228, 2902, 2987, 2150, 2922, 2725, 3689, 4241]. **Gentle** [3059, 2500, 2884]. **Genuine** [3701, 2907]. **Geographic** [2333]. **Geometric** [3633, 769, 1954, 2208, 2833, 2795, 1758, 2666]. **Geometrical** [3372, 2076].

Geometrically [2864, 2782, 2797]. **Geometry** [2390, 2391, 1064, 3298, 3970, 1958]. **geophysics** [1591]. **George** [4262, 262]. **Georgia** [4209, 4196, 4124]. **Germain** [2881]. **German** [1055, 633, 2992, 1057, 439, 472, 1508, 2695, 1035, 2442, 1233, 1357, 641, 642, 221, 246, 278, 1006, 331, 11, 33, 1755, 741, 668, 624, 532, 533, 570, 5, 1891, 894, 176]. **Germany** [4272]. **Getting** [3371, 2493]. **GFSR** [2058, 1407, 1431, 2059, 1752, 1979, 2389, 1313, 1314, 1400, 1882, 2008]. **GI** [1964]. **GI/G/1** [1964]. **Gibbs** [1802, 2038, 2055, 740]. **gigahertz** [1490]. **Gill** [507]. **Giovanni** [3742]. **Gitterstruktur** [1055]. **Given** [1105, 1217, 1614, 1534, 1, 3812, 151, 996, 260, 2313, 1674]. **giving** [141]. **Glasgow** [4193]. **gleichverteilte** [1057]. **gleichverteilten** [633]. **gleichverteilter** [1233, 1357]. **Gleichverteilung** [5, 246]. **Gleitkommadarstellung** [668]. **glimpse** [781]. **Global** [3140, 735, 2211, 1364, 2212]. **GLP** [2689]. **Gmunden** [4171]. **GMW** [1139]. **GNU** [3306]. **Gnumeric** [2885]. **goddess** [2537]. **goddess-of-fit** [2537]. **goes** [3117, 3469]. **Goldreich** [4050]. **Good** [2322, 1724, 508, 1828, 2278, 2359, 2607, 3026, 3430, 2713, 2372, 2456, 2619, 2811, 1392, 743, 933, 1048, 3125, 3126, 3247, 2902, 1790, 398, 464, 1906, 2932, 1725, 1824, 3023, 1629, 2285, 692, 730, 2949, 1375, 1846, 2458, 1013, 2872, 609, 875, 2643, 2104, 3469, 1875, 4042, 3613, 3614, 2986, 3069]. **Goodness** [4129, 597, 2961, 840, 69, 88, 102, 3164, 1166, 1070, 1178, 98, 626, 19]. **Goodness-of-Fit** [2961, 840, 4129, 3164, 1166, 1070, 1178, 626]. **Gossip** [3821]. **Gowers** [3582]. **Gozd** [4195]. **GP** [4228, 3694]. **GP-2001** [4228]. **GP-GPU** [3694]. **GPGPU** [3700]. **GPU** [3810, 3520, 3717, 3772, 3727, 3420, 3820, 4278, 4288, 3976, 3680, 4258, 3462, 3694, 3595, 3507]. **GPU-based** [3976]. **GPU-enabled** [3462]. **GPUs** [3772, 3538, 3826, 3950]. **Gradient** [3320, 1549]. **Graduate** [4214]. **Grain** [3097]. **Grand** [4206]. **Grande** [2429]. **Granular** [3984]. **Graph** [3011, 518, 1908, 2930, 2052, 2854, 1951, 2006]. **Graphic** [3477, 3758, 3395]. **Graphical** [1477, 1667, 1783]. **Graphics** [3544, 3462, 3393, 3720, 3206, 3688, 1473, 1661, 3508, 3627]. **Graphs** [4009, 1896, 2179]. **gray** [1715]. **gray-scale** [1715]. **Greater** [900, 2220, 470]. **Greatest** [512, 1294, 1124, 1090, 753]. **Greece** [4253]. **Greedy** [3484]. **Green** [1310]. **grenades** [2367]. **Grenoble** [4107]. **gretl** [3709]. **Grid** [1218, 2877, 3272]. **GRNG** [3848]. **Group** [1988, 781, 3575, 3123]. **Group-Valued** [1988]. **Grouped** [840, 42]. **grouping** [50]. **Groups** [1912, 2697, 2621, 2024, 1528, 3682]. **growth** [3455]. **Guangdong** [4279]. **guarantee** [1285]. **guaranteed** [3808]. **Guarantees** [1728, 2017]. **Guest** [2338, 3136]. **Guide** [3631, 1061, 1271, 2620, 2718, 2636, 1020, 2193, 3107, 2635]. **Guideline** [4012]. **Guidelines** [1728, 1578]. **Guitar** [2769].

H [294, 896, 170, 3560, 559, 249, 3217, 1878]. **H2PEC** [1366]. **Haar** [1939, 2062]. **Håstad** [3954]. **Hadamard** [3764, 3848]. **Halcomb** [170]. **Halftoning** [3548]. **halls** [3051]. **Halton** [3303, 3346, 3243]. **Hamburg**

[4096]. **Hamiltonian** [3000]. **Hammersley** [911]. **Hamming** [1603, 2228]. **hand** [2367]. **Handbook**
[4201, 3897, 4263, 4235, 4287, 2726, 2300, 1084, 292, 999]. **Handel** [2725]. **Handel-C** [2725]. **Hard**
[2573, 3892, 639, 1392, 4044, 1325, 1409, 1766, 3351, 3372]. **Hard-coded**
[3892]. **hard/soft** [3351]. **hardcore** [3773]. **Hardness** [4029, 2812, 3987]. **hardnesses** [2754, 2834]. **Hardware** [1407, 3719, 3814, 3815, 2332, 3774, 3282, 3933, 3080, 4264, 2772, 3087, 3302, 3304, 3660, 4053, 2613, 3208, 3875, 4002, 1656, 2215, 3476, 3364, 3254, 4084, 3989, 3412, 2571, 1056, 2595, 3312, 3183, 3326, 4224, 2948, 2873, 2953, 3036, 3037, 3678, 3743, 2959, 3941, 3587, 3588, 2725, 455, 1570, 3805, 2990, 3653, 3333]. **Hardware-based**
[3364, 2873]. **Hardware-optimized** [3302]. **Harmonic** [847]. **Harvard**
[4085, 4104]. **harvesting** [3929]. **hasard** [697, 736]. **Hash**
[3642, 3645, 3566, 2387, 3837, 3838, 1665, 3603, 3457, 3237, 3802]. **Hash3**
[3608]. **Hashing** [2160, 3722, 2087, 3922]. **HASPRNG** [3333]. **Hastings**
[2788]. **HAVEGE** [2823]. **Having** [1847, 452, 958, 255]. **Hawaii** [4211]. **HC**
[2909]. **HC-256** [2909]. **Heads** [2841]. **heap** [1907]. **heap-ordered** [1907]. **heat** [2867]. **Heavy** [3373, 3530]. **heavy-tailed** [3530]. **Heavy-traffic** [3373]. **Hecke** [742]. **hedging** [3469]. **Heikes** [921]. **Held** [4086, 4087, 4093, 4088, 4139, 4231, 4161, 4212, 4095, 4089, 4214, 4236, 4103, 4163, 4174, 4106, 4108]. **Helios** [3857]. **Hellman** [2746]. **Helmholtz** [3553]. **help** [2398]. **HEMT**
[1490]. **Hermite** [3089, 1172]. **Herstellung** [176]. **Heston** [3748]. **Heterogeneous** [3409, 4031, 2864, 3287, 3351]. **Heuristic**
[72, 2098, 3103, 2823, 3486]. **Heuristic-Based** [2098]. **heuristics** [3066]. **HI**
[4273]. **Hidden** [1725, 3958]. **hiding** [3425]. **hierarchical** [3192, 3037]. **Hierarchy** [2200, 3493, 3000, 1611]. **High**
[2420, 3512, 2147, 3814, 2765, 2680, 3167, 4069, 4079, 3315, 3316, 3996, 3324, 3196, 3869, 4280, 2534, 3677, 4056, 654, 2081, 3798, 3688, 3450, 3460, 1196, 3132, 3134, 101, 3622, 1062, 1333, 2679, 2767, 2685, 2770, 3084, 3178, 3302, 2590, 2855, 3423, 3093, 1733, 1949, 2182, 118, 3206, 3328, 129, 3581, 1969, 3587, 3588, 1976, 795, 2392, 227, 3053, 2975, 3063, 1199, 3806, 3612, 122, 2488, 2566, 3624, 2991]. **High-density** [2680]. **high-dimensional** [2685, 2770, 2392, 3063, 3806]. **High-efficiency** [4056]. **High-entropy** [3167]. **high-functioning** [3053]. **high-order** [3093]. **High-Performance** [2765, 3196, 3324, 3688, 3581]. **high-period** [3084]. **High-Quality**
[2147, 3996, 2590, 1949, 2182, 1969, 2488, 2566]. **High-Speed**
[2420, 3316, 3869, 3460, 3814, 2534, 1196, 2767, 3302, 1733, 118, 129, 795, 227]. **High-Throughput** [4079, 3677]. **Higher**
[2029, 3288, 1706, 2447, 3284, 3570, 1253, 2984]. **Higher-Order** [1706]. **Highly** [1626, 3049]. **highly-uniform** [3049]. **Hilbert** [3046]. **Hill**
[170, 4232, 895, 1805, 3225]. **Hilton** [4153, 4147]. **Hirschberg** [1894]. **Histogram** [3538, 1627]. **Histograms** [3757, 1315]. **Historical** [2755]. **History** [71, 89, 723, 2788, 3908, 3910, 2807, 68, 1390, 374, 3265]. **Hit**
[1796, 2037, 4068, 1802]. **Hit-and-Run** [1796, 1802]. **Hitachi** [2132].

Hitting [2443]. **HK97** [3627]. **Hlawka** [875, 464]. **HMAC** [3924]. **HMAC-DRBG** [3924]. **Hoare** [4217]. **Hoeffding** [2307]. **Home** [2518]. **homogeneous** [12, 1628]. **Homomorphism** [518, 2426]. **homomorphisms** [3274]. **Hong** [4231]. **Honolulu** [4211, 4273]. **honor** [4262, 4291]. **honour** [4217]. **Hopfield** [3492]. **Hopping** [4067]. **Hörmann** [3004]. **Horner** [2569, 242]. **Horseshoes** [2367]. **Horton** [1920]. **Hot** [4204]. **HotBits** [2907]. **Hotel** [4149, 4093, 4192, 4147, 4119, 4102, 4121, 4166, 4181, 4232, 4131, 4206]. **Houston** [4116]. **Huge** [3111]. **hundred** [1230]. **Hurst** [2351]. **HW** [3215]. **Hyatt** [4210, 4289, 4206]. **Hybrid** [3860, 3299, 4052, 354, 2565, 3364, 3142, 3284, 558]. **hyperbolas** [2130, 2413]. **Hyperbolic** [2817, 901, 1024, 1807, 1958, 1993]. **Hypercube** [4130, 937, 938, 1364]. **Hypercubes** [4144]. **Hypergeometric** [1366, 1177]. **hyperplane** [2257]. **Hyperplanes** [2259]. **Hyperrectangles** [1806]. **hyperspheres** [3388, 3063]. **Hypotheses** [175]. **Hypothesis** [443].

I. [895]. **IBM** [4091, 724, 816, 680, 1434, 1522, 479, 2608, 155, 1552, 493, 463, 4072]. **IBM-Compatible** [1522, 1552]. **ibre** [1055]. **IC** [2767, 3549, 3422, 3423, 2396, 2553, 3490]. **ICCMSE** [4253]. **ICCS** [4295]. **ICGA** [4228]. **ICGA-2001** [4228]. **ICICTA** [4279]. **icosahedral** [167]. **ideal** [816, 680]. **identical** [958]. **Identically** [2570, 3429]. **Identification** [1463]. **Identifying** [3321]. **identities** [1397]. **identity** [2581, 1958]. **IEEE** [4223, 4273, 4274, 4289]. **IETF** [3948]. **If** [1496]. **IFIP** [4272]. **II** [4213, 1265, 3399, 1715, 1810, 2268, 1827, 1939, 1237, 4295, 254, 1979, 2085, 2463, 656, 1652, 698, 1476, 533, 2658, 892, 2232, 1594, 2133]. **II.5** [766]. **IIASA** [4163]. **iid** [3292]. **III** [4202, 2269, 2062, 2462, 800]. **Illiac** [153]. **Illinois** [4138, 4234, 4114]. **Illumination** [2099]. **illusion** [3018]. **Illustrated** [25]. **illustrations** [7]. **Illustrative** [2983]. **IMA** [4212, 4244]. **IMACS** [4199]. **Image** [3548, 3601, 3602, 3374, 3383, 3906, 3566, 3580, 1467, 3503]. **image-cryptographic** [3906]. **Images** [1793, 2329, 1526]. **immediate** [2065]. **Immune** [2677]. **Immunity** [3512, 3811, 4050]. **immunity-resiliency** [4050]. **Impact** [3278, 3395, 1135, 2987]. **Impagliazzo** [4070]. **Imperfections** [648]. **implement** [74]. **Implementation** [1897, 4006, 3894, 3150, 1411, 1694, 1212, 2028, 2585, 3169, 1919, 3173, 2775, 3304, 1228, 1521, 1362, 2954, 3744, 1970, 3876, 4171, 2735, 611, 739, 3460, 1471, 2742, 1990, 1991, 3703, 1885, 3273, 1407, 2238, 3720, 3721, 3282, 2426, 3291, 2504, 2685, 4027, 475, 2855, 2783, 3312, 3183, 1949, 2182, 3432, 3326, 2292, 3587, 2725, 3947, 2215, 1664, 1779, 2652, 2745, 3485]. **Implementations** [1500, 2429, 2456, 3877, 3900, 2372, 2632]. **implemented** [1275, 4049, 3542, 1729, 1123, 3743, 1130, 3120]. **Implementing** [1331, 821, 3940, 1639, 1855, 1082, 933, 1048, 2791]. **implicated** [3725]. **implications** [4050, 3305, 556]. **implicitly** [1412]. **imply** [3308]. **Importance** [3088, 1353, 3576]. **important** [469]. **Impossibility** [3040, 1649]. **Impossible** [2734, 2124]. **Improper** [644, 1224]. **Improve**

[3212, 2554]. **Improved** [1690, 3861, 1809, 1928, 2340, 1164, 2511, 2933, 2443, 3871, 2378, 2886, 3343, 2210, 3050, 3761, 4064, 905, 4030, 2044, 3851]. **Improvement** [3449, 1984, 1193, 2137, 2721, 3478]. **Improvements** [3732, 791, 3964, 3426, 2225]. **improves** [3891]. **Improving** [757, 3294, 1504, 3175, 3425, 281, 3118, 839, 3608, 3505, 3730, 1493]. **incident** [3935]. **included** [2940, 3693]. **including** [1164, 2079, 1261]. **Incomplete** [2677, 2549, 2737, 1247]. **incomputability** [3629, 3403]. **Incorporating** [4052]. **Increase** [3452]. **Increasing** [1068]. **Indefiniteness** [3161, 3387, 4021]. **indentation** [3627]. **Independence** [175, 4024, 3521, 2581, 1816, 1929, 2345, 2688, 2053, 1227, 2624, 801, 1387, 1566, 746]. **independences** [2084, 2085, 2462]. **Independent** [2996, 1413, 1102, 1207, 2154, 3649, 2160, 3011, 864, 3787, 2179, 1455, 1544, 1010, 523, 417, 971, 1192, 2216, 527, 1575, 395, 315, 942, 2570, 3959, 2572, 1486, 902, 2422, 3899, 2854, 48, 774, 1438, 381, 689, 3429, 84, 1957, 920, 1462, 416, 561, 695, 696, 1081, 2080, 1014, 3754, 34, 2747, 1594, 577]. **Indexing** [1837]. **Indifference** [2092, 3689]. **Indifference-Zone** [2092, 3689]. **Indistinguishability** [2728, 1523]. **Individuals** [8]. **induced** [3356]. **Induction** [3166, 1578]. **industry** [4108]. **inequalities** [1064, 1109, 305, 3570, 1961, 738, 740]. **Inequality** [413, 2062]. **inexpensive** [2571]. **Inference** [2036, 555, 1165, 1727, 2778, 3555, 1997, 4113, 2969]. **Inferences** [3637, 2743]. **Inferring** [1416, 1417, 3093, 1046, 1087, 1088]. **Infinite** [3049, 3367, 3368, 3855, 471, 3735, 1241, 1263]. **Infinite-dimensional** [3049]. **Infinitely** [3647, 2036, 2817, 3616, 2393]. **Influence** [3607, 1885, 4065, 2930, 1755, 3882]. **Information** [4210, 2333, 319, 3298, 691, 4247, 394, 4108, 811, 4095, 2973, 4164, 3265, 4108]. **Ingmar** [3318]. **Initial** [3567]. **Initialization** [2140, 2583, 1449, 3462, 3110]. **Initializing** [896, 1215, 1335]. **injection** [3338]. **inner** [2833]. **input** [3724, 2517]. **inputs** [2453]. **insertion** [1253]. **Inspired** [4052, 3891]. **Instance** [911]. **Institute** [4109, 4104, 4103, 4163]. **Integer** [1206, 2507, 2160, 3733, 1537, 3978, 3231, 3983, 2219, 1095, 1887, 1689, 3771, 1349, 3866, 784, 1126, 2960, 2080, 567, 619, 1599]. **integer-valued** [1689, 3771, 3866]. **Integers** [3008, 3993, 1294, 1411, 2253, 635, 113, 774, 1124, 1296, 3797, 1871, 1090]. **Integral** [1895, 822, 1010, 1397, 715, 349, 132, 3602, 716, 3601]. **Integrale** [278]. **Integrals** [152, 1932, 509, 330, 2003, 2509, 221, 222, 278, 99, 423, 573]. **integrands** [2244, 3022]. **integrated** [2598]. **Integration** [3003, 2266, 1001, 2794, 2090, 2217, 2115, 1605, 2244, 905, 4270, 1356, 2939, 1828, 3022, 1071, 2284, 1535, 2869, 3437, 1251, 2890, 975, 3246, 627, 2564, 2747, 2828, 670, 398, 464, 541, 807, 2890, 541]. **integrations** [1085]. **integrators** [2289]. **integrity** [4164]. **Integro** [3400]. **Integro-Local** [3400]. **Intel** [2056, 3662, 3431, 2450]. **Intelligent** [4279, 3545]. **Intensive** [2950, 4163, 4142]. **Inter** [3493]. **Inter-domain** [3493]. **Interactions** [1772]. **interactive** [1801]. **interchanges** [1736]. **interdependence** [587]. **Interface** [4124, 4111, 4116, 4104, 4141, 4142, 2064, 3335, 4039]. **Interfaces** [2429].

Interim [1797]. **Interleaver** [3703]. **interleaving** [3927]. **intermediate** [3125]. **intermediate-rank** [3125]. **Internal** [1907, 918, 2722]. **International** [4190, 4267, 4276, 4283, 4155, 4169, 4264, 4272, 4256, 4224, 4295, 4280, 4186, 4281, 4252, 4171, 4275, 4163, 4226, 4253, 4227, 4180, 4228, 4195, 4200, 4250, 4128, 4202, 4193, 4184, 4109, 4178, 4211, 4255, 4242, 4218, 4213, 4244, 4279, 4248]. **Internet** [3231, 2682, 2804, 3984, 3493]. **Internet-like** [3493]. **Interpolation** [2737, 3089, 1726, 776, 3835, 846]. **Interpretation** [6, 728, 384, 3406, 2076, 626]. **interruptions** [1025]. **Interval** [2423, 719, 957, 4032, 3978, 3983, 61, 3347, 2017]. **Intervals** [2331, 1806, 957, 1735, 44, 973, 150]. **intrainverted** [1730]. **Intrinsic** [2245, 1522, 1299, 1769]. **Intrinsically** [3681, 3920, 3952]. **Introduction** [3926, 2848, 2029, 3288, 2683, 3083, 3202, 1848, 2297, 3213, 1243, 1968, 262, 1330, 1693, 2247, 2676, 3398, 2921, 2338, 1734, 2720]. **invalidates** [3464]. **Invariance** [581]. **Invariant** [1904, 3046]. **Invariants** [3220]. **Inventor** [3527]. **Inverse** [1105, 4051, 3021, 3098, 3211, 187, 4233, 2559, 890, 893, 901, 1024, 3779, 1435, 324, 1073, 3788, 2068, 3579, 3980, 1974, 2886, 879, 1993, 1255, 1256]. **Inversen** [1035]. **inverses** [3216]. **Inversion** [3289, 3037, 3412, 3928, 3080, 3410, 3089, 3660, 2180, 2789, 3579, 3759, 1884, 3958]. **Inversion-based** [3037]. **inversions** [1511, 1470, 46]. **Inversive** [2030, 1618, 1620, 1623, 1624, 1719, 1813, 2262, 2344, 2050, 2051, 2348, 2063, 2296, 2640, 2736, 3262, 3163, 2031, 1621, 1625, 1717, 1718, 1720, 1721, 1810, 1811, 1814, 1816, 1924, 1926, 1927, 1928, 2045, 2166, 2167, 2168, 2340, 2341, 2342, 2169, 2345, 2688, 1819, 2514, 1948, 2287, 2955, 2632, 4001, 1564, 1982, 2547, 2548, 2549, 2638, 2639, 2967, 3232, 2309, 2223, 2979, 3260, 3261, 3497, 2130, 2413, 3958]. **inverted** [2096]. **invertible** [3623, 3708]. **Inverting** [323, 3034]. **investigating** [415]. **investigation** [2695, 4055]. **Investigations** [1673, 1678, 2155, 1755]. **investing** [3832]. **invitation** [4098]. **Invited** [2513, 1641]. **Involving** [197, 341, 342]. **ion** [4080]. **IoT** [4035, 4012, 4014, 4016, 4081]. **iris** [3766]. **Irrational** [2502, 458, 2119, 1536]. **ISAAC** [2495]. **ISBN** [3742, 3707]. **Ising** [2328, 2157, 1531, 1630, 2310, 2486]. **Island** [4122, 4120, 4266]. **isotrope** [541]. **Isotropic** [541]. **ISSAC** [4186]. **ISSAC'93** [4169]. **Issue** [3734, 2338]. **Issues** [2838, 3174, 3854, 2038]. **István** [1756, 1862]. **Italian** [991, 470, 16, 17, 491]. **Italy** [4184]. **Item** [272, 264]. **items** [1476, 70]. **Iterate** [3561]. **Iterated** [2898, 2234, 247, 2880]. **Iterating** [1770]. **iteration** [112]. **Iterations** [2602, 3376, 3783, 3425, 1958, 3457]. **Iterative** [1988, 1682, 1726]. **IV** [3091, 3830, 940]. **Ivy** [3662]. **IX** [4189, 170].

J [896, 1273, 3004, 1071, 1540, 1039, 1084, 937]. **J.** [170]. **J3Gen** [3750]. **jaguar** [4197]. **James** [2500, 2884, 3059]. **Jansson** [515, 400, 483]. **January** [4126, 4208, 2678]. **Japan** [4155]. **Japanese** [167, 1984]. **Java** [2842, 2429, 3665, 2876, 3839, 3120]. **Java-implemented** [3120]. **JavaTalk** [2367]. **Jersey** [4289]. **Jitter** [3513, 3514]. **JMASM** [2926, 3029]. **JMASM1** [2690]. **jobs** [1843]. **jobstreams** [985]. **Johan** [3954]. **John**

[1525, 1539, 1820, 2970, 4094]. **Join** [1410, 1843]. **Joint** [328, 4228]. **Jonathan** [4291]. **Jordan** [741]. **Jordanscher** [741]. **Jose** [4276]. **Joseph** [262]. **Joy** [3139]. **Jr** [170]. **Julius** [2682]. **July** [4169, 4193, 4109, 4086, 4256, 4186, 4207, 4266, 4103, 4228, 4175]. **Jump** [3094, 3186, 3187]. **jumps** [3973]. **Junction** [4048]. **Junction-Based** [4048]. **June** [4182, 4234, 4249, 4267, 4276, 4290, 4098, 4241, 4202, 4284, 4157, 4113, 4086, 4273, 4095, 4295, 4187, 4214, 4266, 4226, 4175, 4188, 4215]. **Jungles** [2395]. **Juniper** [3935]. **Justification** [2254, 1015].

Kakutani [3346]. **kappa** [3767]. **KASUMI** [2611]. **Keccak** [3640]. **KENO** [2106]. **KENO-Va** [2106]. **kernel** [3046]. **Kernels** [3047, 2006]. **Key** [3512, 3396, 2332, 3165, 3967, 3415, 916, 2518, 2946, 3977, 3038, 1649, 2086, 1559, 2555, 1994, 880, 3761, 1677, 3992, 3157, 3532, 2453, 3448, 1983, 3236, 4061, 4077]. **key-scheduling** [4061]. **Key-Stream** [3512]. **keyed** [433, 434]. **Keys** [3892, 3663, 1649, 3879, 2108, 2126, 3935, 2471, 4077, 2979]. **Keystream** [2596, 2935, 2964, 3312, 3602]. **keystreams** [1817]. **Khintchine** [2710]. **Kiev** [4128, 4169]. **Kinderman** [2903]. **kinetic** [3827]. **kinetics** [4065]. **Kingston** [4218]. **KISS** [3445, 3599]. **Klimov** [2918]. **Kloosterman** [1814]. **Kloosterman-type** [1814]. **KMCLib** [3827]. **Known** [1859, 3410, 2346, 804]. **Knoxville** [4130]. **Knuth** [3954, 1747, 697, 736, 3844]. **Kochen** [3629]. **Koen** [3081]. **Koksma** [2062]. **Kolmogorov** [64, 405, 72, 1166, 1848, 2297, 3213, 790, 2799, 98, 840, 190, 3605]. **Kong** [4231]. **Kongruenz** [1055]. **Kongruenz-Generatoren** [1055]. **konvexe** [33]. **konvexer** [741]. **Korea** [4242]. **Körper** [33]. **Kreyszig** [1959]. **kriging** [3646]. **krivoi** [35]. **Kronecker** [3644]. **KY** [4255].

L [542, 596, 640]. **Laboratory** [4085, 4087]. **Lag** [612]. **Lagged** [2134, 2237, 1972, 2081, 2082, 2083, 1986, 3810, 2264, 1163, 1977, 2882, 1976]. **Lagged-Fibonacci** [1972, 2081, 2082, 2083, 3810, 1977, 2882, 1976]. **Lagrange** [1712]. **Lai** [3443]. **Lake** [4181, 4188]. **Lamar** [3031]. **lamp** [2804]. **Landau** [2582, 3938, 711, 1140]. **Language** [992, 3909, 4003, 3762]. **language-based** [4003]. **languages** [3889]. **Laning** [170]. **Lansing** [4102]. **Laplace** [2594, 687, 3115, 3353]. **laptops** [2333]. **Large** [4085, 3400, 3651, 3652, 864, 687, 27, 2956, 3797, 3980, 2207, 187, 3350, 1575, 3075, 2927, 3174, 3296, 2856, 1358, 65, 74, 247, 96, 3942, 1085, 623, 232]. **Large-Order** [3651, 3652]. **Large-Scale** [4085, 187, 2207, 3075, 96, 3942]. **large-size** [74]. **largely** [990]. **Laser** [3352, 3424, 4013, 3440, 3612, 3379]. **Lasers** [3229, 3258, 3370]. **Last** [2229]. **Latches** [4040]. **Latin** [2392, 3146, 3970, 3571]. **LatMRG** [2193]. **Lattice** [544, 583, 2030, 3003, 2503, 722, 2689, 2931, 2361, 3026, 2713, 3795, 3870, 2794, 606, 2469, 2811, 3061, 3125, 3247, 3357, 1585, 2755, 1055, 1148, 1204, 1320, 2149, 1915, 2852, 1510, 1815, 1345, 1346, 1164, 2600, 4033, 3563, 3564, 3023, 1171, 1172, 2515, 3322, 1535, 2287, 692, 730, 2290, 2292, 2458, 2532, 2615, 3437, 2533, 2622, 3943, 1969, 875, 3046, 3048, 1092, 3126, 3246, 3606,

2312, 1883, 3957, 398, 464, 3870]. **lattice-based** [3957]. **lattice-bases** [1171]. **lattice-sublattice** [3322]. **lattices** [2158, 2869, 3980, 2897]. **Lausanne** [4264]. **lava** [2804]. **LavaRnd** [2643]. **Law** [3540, 3350, 1575, 2234, 3177, 2774, 3308, 16, 199, 2175, 247, 17, 4000, 3226, 804, 2399, 3525, 3397, 3192, 3043, 2898, 911]. **Laws** [864, 1544, 2817, 577]. **Laxenburg** [4163]. **Layer** [3825]. **Layers** [3219]. **LC** [2974]. **LCG** [2689]. **LCGs** [2269, 2590, 2293]. **Leading** [3027, 635, 1068]. **leads** [1905]. **leads-to** [1905]. **Leakage** [2492]. **Leap** [3995, 3381, 2347]. **leap-frog** [2347]. **learnability** [2236]. **Learning** [3248, 2001]. **Least** [756, 545, 105, 1447]. **Least-Remainder** [105]. **leave** [3935]. **Lecons** [4]. **Lecture** [3742]. **Lectures** [265, 4]. **L'Ecuyer** [1479]. **Lee** [498]. **Left** [3597, 1999, 469]. **Left-Shift** [1999]. **legacy** [3900]. **Legal** [2769]. **Legge** [17]. **leggi** [16]. **Lehmann** [3318]. **Lehmer** [1709, 2257, 2258, 768, 3560, 3740, 920, 249, 3217, 2215, 492, 2116, 233]. **Lemma** [2659, 2487]. **Lemmas** [2597]. **Length** [3893, 183, 375, 468, 1274, 241, 1620, 1111, 1034, 832, 1859, 929, 1907, 1278, 217, 471, 1427, 1511, 1718, 1164, 867, 1948, 2519, 1453, 600, 601, 1748, 3234, 662, 2007, 3365, 3621, 3138, 3809]. **lengths** [2913, 2031]. **Less** [756, 900, 1058, 3039]. **Lesson** [1771]. **lessons** [3935]. **Letter** [475, 1236, 1852, 3057, 495]. **letters** [2970]. **leurs** [3]. **Leuven** [4256]. **Level** [3719, 2546, 1157, 3101, 1838, 3118, 2823]. **Lévy** [4073]. **Lewis** [763]. **Lexical** [2512]. **Lexington** [4255]. **Leydold** [3004]. **LFIB4** [4003]. **LFSR** [2335, 3934, 3291, 2459, 3448, 3917, 4076, 3381]. **LFSR-Based** [3917, 4076]. **LFSRs** [3960, 3965]. **Libgcrypt** [3863]. **Liblice** [4095]. **libraries** [2181]. **Library** [3524, 3897, 1065, 1342, 1231, 2620, 2718, 3035, 3107, 2719, 3336, 2202, 1560, 1861, 4019, 1481, 1602, 1684, 3522, 3717, 3718, 3772, 2916, 3966, 3413, 3306, 3727, 3865, 2939, 3106, 2541, 2542]. **Lie** [1988]. **Life** [2421, 3698]. **light** [3612]. **Lightweight** [3876, 3501]. **Like** [2769, 2935, 2964, 2989, 478, 2086, 3802, 3493]. **Likelihood** [2350, 1031, 1162]. **Limit** [718, 1272, 2506, 1513, 2594, 3742, 3589, 3043, 2216, 2898, 2404, 3620, 577, 64, 3092, 3429, 1748, 3588, 3831, 416, 2807, 1194, 190, 2154]. **Limitations** [4070]. **limiting** [1755]. **Limits** [635, 86, 39, 2318, 2412]. **Lin** [2868]. **Lindberg** [1413]. **Line** [2159, 2764, 448, 449, 3355]. **linéaire** [1375]. **linéaires** [2552, 2890]. **Linear** [399, 2994, 3930, 4007, 1415, 2585, 2923, 2768, 2034, 951, 3654, 2347, 2348, 1112, 1113, 1114, 3554, 1118, 861, 3014, 2860, 2057, 3094, 3186, 3187, 3940, 2281, 2607, 2941, 3664, 2523, 3669, 3670, 516, 783, 1377, 1378, 2455, 2531, 3105, 3330, 2627, 2957, 1850, 873, 485, 605, 1978, 832, 3593, 3115, 615, 877, 1866, 1088, 368, 2654, 3703, 2406, 373, 2753, 3708, 211, 1204, 1403, 3891, 3773, 583, 1497, 1060, 1417, 2425, 1699, 3168, 1915, 2158, 112, 3171, 1506, 1341, 587, 3864, 1809, 1425, 1512, 1223, 1283, 1346, 2267, 2346, 2435, 2436, 955]. **linear** [1349, 1287, 1351, 3307, 2934, 3092, 1730, 2701, 2784, 3093, 3731, 4033, 1121, 3563, 3564, 2606, 1006, 3199, 966, 1179, 3030, 1375, 2193, 2290, 2292, 2458, 2714, 2951, 1180, 2296, 871, 3585, 2721, 255, 2383, 2881, 2805, 3112, 2733,

1757, 3116, 698, 799, 800, 801, 878, 1190, 1563, 2889, 2552, 2890, 2891, 3049, 3050, 930, 1393, 1768, 1769, 972, 1046, 3801, 2896, 2897, 3057, 1776, 1256, 987, 1312, 2981, 3130, 3362, 3487, 3613, 3067, 3133, 2984, 1671, 1674, 13, 2908, 3503, 1890, 2321, 1055, 3976]. **Linear-Algebra** [1866]. **linear-complexity** [1563]. **linear-size** [3773]. **Lineare** [1055]. **linearer** [1006]. **linearity** [3979]. **linearization** [3852]. **Linearly** [3275, 3391, 3251, 1170, 2007]. **Link** [3341]. **linkage** [4108]. **links** [2063]. **Linux** [4028, 3019, 3672, 4038, 3244]. **Lipschitz** [3739]. **LISA** [4189]. **List** [672, 1985, 1775]. **list-update** [1985]. **Lists** [949, 903]. **Littlewood** [1961]. **LLL** [3023]. **LLL-spectral** [3023]. **LLRANDOM** [649]. **Lmcgrid** [3272]. **Load** [2268]. **loaded** [2524]. **Loads** [3166]. **Local** [3713, 3400, 735, 606, 1382, 1556, 1647, 1867, 3632, 1364, 3109, 1194]. **Locality** [3713, 3632]. **localization** [1695, 3411]. **location** [2648]. **Log** [760, 2511, 2394, 1108, 1947, 2516]. **log-concave** [1108, 1947, 2516]. **Log-Normal** [760]. **Logarithm** [2933, 2737, 2234, 3521, 247, 4054, 2898]. **Logarithmic** [893, 3765, 1018]. **logarithmically** [1008]. **logarithms** [1405, 1293]. **logic** [1905, 3422]. **logiciel** [1375]. **Logistic** [3407, 3115, 2102, 4064, 3284, 1704]. **logit** [1704]. **logspace** [1409, 1688]. **logspace-hard** [1409]. **lois** [804]. **London** [3742]. **Long** [3713, 906, 4025, 1914, 1506, 1805, 2434, 3316, 447, 2538, 1859, 1393, 2010, 1319, 3632, 3002, 3078, 1339, 2685, 2770, 1428, 1516, 774, 2364, 2715, 1975, 2088, 3050, 706, 2758]. **long-cycle** [2685, 2770]. **Long-Period** [906, 3316, 2010, 3002, 3078, 1516, 774, 3050, 706, 2758]. **Long-Range** [2434, 1506, 1805, 1339, 1428]. **Longest** [2538]. **Longest-period** [2538]. **Look** [3290, 3658, 795, 846]. **Look-Up** [3290, 795, 846]. **Lookup** [834]. **Loop** [861]. **loops** [3245]. **Lorentzian** [684]. **Loss** [3863]. **lot** [3388]. **Loteria** [134]. **Lottery** [2100, 134]. **Louis** [4152]. **Louisiana** [4149]. **Lovasz** [2052]. **Low** [3713, 1901, 4025, 1918, 3007, 2694, 3441, 1250, 1385, 1761, 2211, 2390, 2217, 1586, 1786, 1882, 3272, 4063, 3632, 2920, 1417, 905, 1694, 1800, 3293, 3022, 3189, 4011, 3435, 1013, 1457, 2533, 2795, 2875, 3218, 3750, 3591, 1760, 2306, 3697, 2118, 2133]. **low-cost** [3750, 3591]. **Low-Degree** [3441]. **low-dimensional** [1800, 2133]. **Low-Dimensionality** [3007]. **Low-Discrepancy** [2694, 2211, 2390, 1586, 1901, 1250, 1385, 1761, 905, 1694, 3022, 2533, 2795, 1760, 3697, 2118]. **low-dispersion** [1385]. **Low-Order** [1918, 1417]. **Low-overhead** [4063]. **low-power** [3293]. **Lower** [1720, 2341, 1450, 1564, 2750, 1928, 3122]. **Lowness** [3866]. **LP** [2422, 2000]. **LPRng** [2545, 2105]. **LR** [1549]. **LSI** [1161]. **LSTMs** [3997]. **LT** [3408]. **Luby** [2136, 1858, 3231]. **Luc** [1311]. **Lucas** [3728, 3559, 2415]. **luck** [3909]. **luminescent** [3744]. **Lüscher** [2182, 1949]. **LUT** [3132, 3763]. **LUT-SR** [3763]. **LUTs** [3491]. **LWR** [4059]. **LWR-based** [4059]. **LXM** [4020]. **Lyapunov** [2872, 1850]. **lying** [1321]. **LZSS** [3404].

M [1025, 1963, 70, 3223, 1025, 1963, 3373]. **M.** [319, 394]. **M/M/1** [1963]. **M/M/m** [1025]. **M/PH/1** [3373]. **MA** [4267, 4224]. **Mach** [3168].

Machine [151, 2769, 142, 920, 3868, 838, 166, 3896, 774, 479, 2207, 3469, 192]. **Machine-independent** [920, 774]. **Machinery** [4085]. **Machines** [293, 1799, 3967, 327, 119, 3249, 118, 129]. **MacMillan** [507]. **MACs** [2025]. **MaD0** [3872]. **Made** [1518, 1841]. **Madland** [3843]. **Magma** [3536]. **Mahalanobis** [135]. **Main** [3479]. **Maine** [4160]. **mainly** [312, 451]. **maintenance** [3453]. **Majorana** [3723]. **Majority** [3987]. **Majorizing** [980]. **Make** [2769]. **Makes** [3431]. **makespan** [1788]. **Making** [3898, 2560, 2932, 3494]. **Man** [128]. **Management** [2427, 4222, 4180, 3272]. **Managing** [3841]. **Manhattan** [3740]. **MANIAC** [1205]. **Manipulating** [552]. **Manipulation** [3822]. **mantissa** [668, 1018]. **Mantisse** [668]. **Manual** [1279, 1959, 195, 3306]. **Many** [2211, 4010, 2715, 1196, 670]. **Map** [3407, 3625, 4064, 3960, 3992, 3873, 2102, 3359]. **Maple** [1959]. **Mapping** [3475, 1430, 1035, 3570]. **Mappings** [3271, 2786]. **Maps** [2627, 3389, 2997, 3284, 871, 3454, 4041, 4046]. **March** [4087, 4144, 4268, 4124, 4116, 4279, 4089, 4174, 4248]. **Margin** [3219]. **Marginal** [2248, 1847]. **Marginals** [2583]. **margins** [2313]. **Marinucci** [3742]. **Mario** [3874]. **Mark** [4131]. **Markov** [2580, 212, 1102, 1207, 2252, 3416, 959, 513, 663, 712, 2011, 1793]. **marks** [2329]. **Marotto** [3562]. **Marriott** [4137, 4110, 4225, 4119, 4166]. **MARS** [2521]. **Marsa** [4003]. **Marsa-LFIB4** [4003]. **Marsaglia** [3388, 2325, 2846, 1345, 1346, 1362, 2079, 2101, 1089, 3888, 3923]. **Marshall** [2938]. **Martuljek** [4195]. **Maryland** [4148, 4239]. **mashinakh** [351]. **masked** [3731]. **Masking** [3986]. **mass** [741, 1597]. **Massachusetts** [4104]. **Massen** [741]. **Massey** [2999, 3443, 3921]. **Massively** [4013, 1943, 3680]. **Mat** [3057]. **Materials** [3301]. **Math** [2149, 221, 695, 696, 2804]. **MathCW** [3897]. **Mathematica** [3686, 3751, 2111]. **Mathematical** [3897, 4093, 4160, 4088, 4109, 4113, 1237, 1238, 96, 3742, 4090, 250, 1083, 3838, 2395, 4092, 55, 57, 4100, 4199, 3707, 942, 465, 496, 236, 720, 1224, 2470, 209]. **Mathematical-Function** [3897]. **Mathematicians** [2645]. **Mathematics** [2421, 4093, 2845, 4088, 4109, 916, 4292, 1959, 1560, 1861, 4260, 4261, 4101, 139, 4291, 1750, 4108]. **mathématiques** [4090]. **MathLink** [2147]. **MATLAB** [3194, 2726, 3227, 2908]. **Matrices** [2335, 1185, 3132, 1267, 1631, 1131]. **Matrix** [1601, 2248, 592, 1289, 1357, 2210, 1320, 1154, 1427, 3319, 3666, 53, 4075, 1566, 2093, 2095, 3623, 3708, 1233]. **Matrixgeneratoren** [1233, 1357]. **matter** [4026]. **max** [1465]. **Maximal** [183, 1620, 1453, 832, 929, 2753, 1718, 2781, 3692, 3365]. **Maximal-Length** [929, 1453]. **Maximally** [3940, 2194, 2459]. **Maximum** [1278, 1031, 1162, 2274, 2864, 1767, 1908, 3100, 84, 2007, 3138]. **Maximum-length** [1278, 2007]. **Maxwell** [3592, 3799, 3124]. **May** [4122, 4127, 4132, 4138, 4143, 4148, 4159, 4168, 4177, 4182, 4190, 4191, 4209, 4216, 4229, 4239, 4254, 4283, 4091, 4180, 3754]. **mbedTLS** [3924]. **MC** [2289]. **McEliece** [3836]. **McGill** [655, 1193]. **McGraw** [170]. **McGraw-Hill** [170]. **MCNP** [1281, 3420]. **MCS** [4226]. **McShane** [507]. **MCV** [743, 803]. **Mean**

[579, 1105, 769, 2864, 603, 2, 540, 1714, 1715, 2776, 1987]. **mean-square** [1714, 1715]. **meaning** [441]. **Means** [3649, 3031, 3128, 2119, 2606, 3449]. **Measure** [2239, 2361, 2576, 2937, 2950, 2107, 2663]. **measurement** [3293, 3424]. **measurements** [558, 3618]. **Measures** [2993, 3582, 2741, 635, 1817, 2284]. **measuring** [3480]. **Mechanical** [531]. **mechanics** [2921]. **Mechanism** [3989]. **medians** [438]. **Medical** [24, 299, 47, 73, 114, 115, 171, 172, 3583]. **Meeting** [4107, 4102, 4098, 4228]. **Meetings** [1155, 1174]. **Mehrfach** [641, 642]. **mehrfacher** [278]. **Mellin** [537]. **Mellon** [4106]. **Memorial** [4204]. **Memory** [2420, 2237, 3810, 2943, 3975, 3800, 3982, 3479, 3927, 1749, 1754]. **memoryless** [1302]. **Memristor** [3648]. **Mengen** [741]. **Merge** [595]. **merit** [1489]. **Merlin** [3122]. **Mersenne** [2766, 3285, 2769, 2851, 763, 3940, 1731, 917, 2876, 2385, 3041, 2550, 3462, 3242, 3477, 3758, 1784, 2829]. **Mersenne-Exponent** [1731]. **Mervin** [270]. **mesh** [3521]. **Message** [2025, 993]. **Messerschmitt** [1699]. **Metaheuristic** [4052, 4055]. **Metamodels** [1735, 3646]. **Metastability** [4040, 3256, 2959]. **Metastability-Based** [3256]. **Method** [2019, 267, 179, 761, 270, 196, 1216, 1217, 2507, 636, 1281, 2432, 1821, 220, 352, 644, 511, 25, 201, 1832, 1946, 648, 1010, 1125, 2954, 249, 2379, 2077, 603, 281, 335, 337, 359, 2381, 2539, 1978, 146, 2387, 2086, 187, 205, 615, 2210, 2214, 661, 19, 744, 528, 621, 705, 974, 880, 4294, 2220, 1667, 2978, 2900, 3986, 3494, 1675, 850, 540, 1401, 3767, 632, 945, 1404, 2323, 1268, 1412, 234, 1060, 1800, 195, 1211, 1273, 3080, 320, 994, 952, 1712, 3547, 587, 1220, 2169, 2170, 593, 594, 273, 768, 770, 351, 1005, 1358, 3660, 94]. **method** [3563, 1529, 1834, 1945, 67, 76, 4086, 1733, 1075, 2190, 922, 1011, 1039, 1180, 2953, 3036, 2535, 3678, 3587, 385, 831, 1129, 1130, 2382, 2540, 78, 1558, 924, 3044, 2888, 1015, 3947, 698, 800, 1190, 1982, 2093, 2095, 2305, 839, 665, 1089, 99, 189, 568, 881, 4112, 1094, 3759, 1398, 2899, 393, 712, 750, 2751, 2009, 193, 2903, 1884, 1316, 3849, 714, 177, 2235, 1483, 1888, 4045, 2569, 233, 7, 4046, 3852, 2133, 178]. **Méthode** [178]. **Methoden** [633, 1755]. **Methodology** [3549, 728, 2612, 2475, 4201]. **Methods** [578, 673, 4098, 2138, 3150, 2025, 3289, 548, 682, 2255, 1106, 1218, 2046, 2594, 638, 2353, 2777, 4287, 4277, 645, 513, 2184, 1446, 1449, 4265, 830, 791, 1650, 4089, 489, 834, 204, 616, 876, 1764, 2640, 2305, 1086, 4163, 703, 2217, 1873, 844, 4253, 1583, 2003, 2407, 2906, 4142, 465, 496, 633, 990, 1324, 896, 3812, 2580, 1493, 212, 2246, 3163, 112, 4230, 4285, 2048, 3416, 2509, 4231, 1164, 4235, 198, 223, 326, 914, 277, 1234, 3666, 4213, 1239, 3195, 4257, 965, 2716, 2868, 3826, 3208, 96, 788, 1128, 2461, 1762, 1763, 1981, 4187]. **methods** [4207, 4214, 2547, 4236, 4246, 3232, 491, 1045, 4092, 261, 1195, 1995, 3699, 2472, 884, 979, 984, 987, 290, 164, 4043, 2230, 848, 138, 1596, 1679, 1755, 2500, 2884, 1878, 3059]. **Metodi** [991, 491]. **Metric** [660, 2741, 3152]. **Metropolis** [1205, 2498, 2499, 2921, 1802, 1281, 2055, 2273, 2938, 2788]. **MHz** [2910]. **Miami** [4198]. **Michael** [2136]. **Michigan** [4102, 265]. **Mickey** [3147]. **Micro** [1504, 1142]. **Micro-Computers** [1504, 1142]. **Microanalysis** [257].

microcomputer [1168]. **Microcomputers** [1609, 1231, 1522, 1538, 1633, 1552, 1581, 1149, 1499, 1906, 1275, 1158, 1629, 1075, 1448, 1132, 1093, 2224]. **Microcontroller** [3982]. **microprocessors** [835]. **Microscopy** [1772]. **Microsoft** [4217, 2464, 2729, 2730, 2963, 3224, 3225, 1676]. **mid** [94]. **mid-square** [94]. **middle** [161]. **Milder** [3659]. **Millennial** [4217]. **Miller** [3527, 3728]. **Million** [63, 148, 392, 2647, 168, 1230]. **Milwaukee** [4185]. **MIMD** [1472]. **MIMO** [3617]. **min** [1465, 2653, 2976]. **min-entropies** [2653, 2976]. **min-max** [1465]. **mincing** [529]. **Miniature** [3815]. **Minicomputer** [821, 1143]. **minicomputer-based** [1143]. **Minimal** [2993, 1500, 1426, 2613, 1603, 1705, 3307, 3999, 3621]. **minimization** [3351, 1788]. **Minimum** [1903, 2696]. **Mining** [3663]. **Minkowski** [1148, 1171, 1172]. **Minkowski-reduced** [1148, 1171]. **Minneapolis** [4180]. **Minnesota** [4180, 4212]. **Miscellanea** [721, 822, 657, 716]. **Miscellaneous** [4084]. **Mises** [1501, 384]. **mismatches** [1839]. **Missing** [2769, 1417, 3093, 2286]. **Mission** [2124]. **Misson** [4268]. **Missouri** [4152]. **MISTY** [2706, 2611]. **MISTY-Type** [2611]. **misunderstandings** [1287]. **Mitchell** [1677]. **mitigations** [4011]. **mittels** [1006, 1891]. **Mixed** [293, 327, 839, 972]. **Mixing** [3677, 1298, 566, 1726, 1235, 3608]. **MIXMAX** [3998, 3981, 3846, 3885]. **Mixture** [1494, 1125, 2135, 1045, 3248]. **mixture-of-subsets** [3248]. **Mixture-plus-Acceptance-Rejection** [1125]. **Mixtures** [1544]. **ML** [1705]. **ML-sequences** [1705]. **MMIX** [3844]. **Mobile** [3804, 498, 482, 3610]. **Möbius** [443]. **mod** [173, 397]. **Mode** [3200, 2645, 4060, 3201]. **Model** [2915, 3860, 3790, 186, 54, 3062, 1482, 3272, 813, 2328, 4065, 3856, 3526, 1152, 2680, 3816, 2156, 2157, 1531, 3101, 1747, 3748, 3453, 1993, 2310, 2311, 3248, 2486, 1597, 3270, 1599]. **Model-Based** [3790]. **Modeling** [4251, 1606, 3962, 2248, 4230, 3869, 3119, 1772, 3768, 1040, 1638, 2528, 3032, 228, 1588]. **Modelirovanie** [351]. **modélisation** [1588]. **modelled** [3157]. **Modelling** [2824, 4199, 1160, 1220]. **Models** [543, 506, 1740, 1863, 2135, 3730, 959, 3192, 1837, 2795, 4110, 985, 2313, 2125, 3890, 2017]. **Modern** [3512, 4098, 3894, 1159, 2444, 4253, 3772, 4035, 4103]. **modification** [2022, 1608]. **Modified** [1022, 3407, 2168, 420, 2751, 3956, 1023, 320, 2287, 3878, 193]. **Modified-Logistic** [3407]. **Modular** [2779, 3021, 1189, 2559, 1435, 2190, 3216, 2886, 3958]. **Modulated** [2974]. **modulator** [3168]. **Module** [3024, 4081, 3281]. **Modules** [2642, 4084]. **moduli** [2425, 2158, 1708, 1341, 1358, 2383, 2881, 3344]. **Modulo** [3008, 250, 369, 373, 231, 2137, 955, 1287, 1351, 306, 731, 2714, 2951, 3980, 4001, 4075, 2552, 3050, 1769, 1480, 5, 3043]. **Modulus** [3652, 823, 1000, 1033, 1115, 1517, 2110, 571, 2981, 2672, 1510, 1621, 1625, 1720, 1721, 1810, 1925, 1926, 2167, 2168, 2340, 2341, 1347, 859, 956, 1225, 1226, 1348, 2186, 2287, 785, 3439, 2548, 2967, 1784, 2829, 3487, 3488, 3261, 3262, 3497, 2320]. **Molecular** [2574, 3905, 1943]. **molecular-dynamics** [1943]. **Moment** [1903, 1064, 1614, 2302, 740]. **Moment-Generating** [1903]. **Moments** [775, 3559, 3570, 2185, 1253]. **Monaco** [4226]. **Monica** [4088]. **monitoring**

[3355]. **Monkey** [1853, 2101]. **Monkeying** [2961]. **Monographs** [3707]. **Monotone** [1107, 333, 2960, 2180, 3098, 3671]. **Monotonicity** [1116]. **Monster** [2538]. **Monte**
[4098, 178, 2500, 112, 4270, 4231, 1630, 4257, 4265, 2884, 4187, 4207, 4214, 4236, 4246, 2305, 2106, 99, 189, 3059, 4226, 1878, 1789, 1205, 432, 2138, 3150, 348, 2144, 178, 2580, 179, 3075, 212, 3637, 1605, 2244, 1606, 1330, 1693, 2246, 2247, 2676, 3398, 234, 1415, 905, 2152, 1155, 90, 195, 503, 3541, 1911, 152, 2039, 3544, 3175, 1281, 4285, 1220, 3656, 197, 3416, 2266, 2347, 2436, 2509, 591, 4231, 1285, 3417, 1725, 2173, 2270, 1117, 727, 2353, 2777, 3905, 1231, 198, 351, 220, 1825, 3786, 511, 128, 223, 326, 914, 1828, 513, 2358, 2515]. **Monte**
[3567, 3427, 4086, 1174, 1531, 961, 2709, 156, 157, 1239, 3195, 2185, 4257, 1454, 1372, 648, 1010, 2716, 2871, 3207, 4265, 3436, 3208, 1181, 3827, 2533, 2622, 3108, 3942, 1970, 2877, 159, 3683, 146, 656, 78, 4089, 3799, 2089, 2090, 3947, 876, 1764, 4187, 4207, 4214, 4236, 4246, 132, 2890, 491, 1135, 663, 1771, 1988, 1307, 744, 703, 2217, 2397, 261, 2472, 133, 4112, 4294, 1577, 1666, 2112, 1310, 4226, 1875, 3702, 2310, 393, 1141, 712, 1583, 3806, 290, 2828, 2900, 2407, 138, 2904, 1589, 1787, 2489, 2906, 1591, 265, 464, 465, 496, 2018].
Monte-Carlo [178, 1606, 234, 1220, 648, 3827]. **Monterey**
[4144, 4189, 4215, 4108]. **Montgomery** [2068, 2190, 2886, 2559]. **monthly** [3453]. **Montreal** [4177, 4101, 4229, 4186]. **Monty** [3678, 2381, 2382]. **Mordell** [4022]. **morphological** [1714, 1715]. **MOSFET** [3223]. **most** [431, 3772, 2190]. **mostly** [2764, 1933]. **mother** [1973]. **Motion** [3553]. **mots** [762]. **mouse** [3323]. **movement** [3323]. **moyennes** [284]. **MP** [1394]. **MPI** [3794]. **MPPC** [3815]. **MR** [2149, 1273, 1071, 1039, 937, 896]. **MR1414863** [2305]. **MR2084569** [3057]. **MT19937** [2948]. **Mulders** [3563]. **Muller** [270, 721, 770, 3036, 3587, 3746, 657]. **Multi** [3861, 4056, 927, 928, 3416, 1358, 221, 222, 967, 3873, 3943, 159, 1987, 2759, 3626, 2991]. **multi-access** [2759]. **Multi-Bit** [3861, 4056, 3626]. **multi-class** [967, 1987]. **multi-delayed** [3873]. **multi-dimensional** [3416, 221, 222]. **Multi-folding** [927, 928]. **multi-moduli** [1358]. **multi-programmed** [2991]. **multi-sequences** [3943]. **multi-stage** [159]. **multicomputer** [1843]. **Multicore** [3819]. **multicyclic** [665]. **Multidimensional**
[2941, 2284, 3796, 1251, 1592, 495, 905, 2849, 2514, 2939].
multidimensionally [1175]. **Multigroup** [290]. **Multiloop** [1914]. **Multimedia** [3249]. **Multinomial** [1104]. **Multiparty** [1409, 1688, 2925]. **multiphase** [4063]. **Multiple** [2427, 241, 152, 3173, 3651, 3652, 2434, 1001, 2936, 641, 1290, 509, 1438, 3787, 2456, 2530, 3795, 2956, 794, 2206, 1863, 2092, 2210, 934, 3475, 2902, 1484, 1680, 3274, 3633, 3164, 3285, 2927, 3174, 3296, 1283, 278, 1535, 2285, 2286, 2365, 3573, 2949, 3103, 1846, 2191, 2193, 2292, 2372, 1462, 1759, 1864, 2093, 2095, 3915, 1776, 3246, 573, 1784, 2663, 2750, 2751, 2829, 2830, 2980, 2982, 3065, 3066, 3362, 3486, 3488, 3614, 2664, 3266].
Multiple-Comparison [1680]. **Multiple-Recursive** [2210, 2093, 2095]. **Multiple-Valued** [241]. **multiples** [2664]. **Multiplexed** [2700]. **Multiplication** [2190, 1189, 1598]. **Multiplications** [3021]. **Multiplicative**

[267, 544, 407, 823, 1000, 1033, 1115, 1348, 1517, 3322, 2189, 1740, 657, 2110, 571, 536, 2320, 2149, 909, 1608, 721, 320, 1707, 439, 1428, 859, 956, 1225, 1226, 556, 1435, 2186, 3980, 2199, 2882, 1015, 3344, 931, 3070]. **multiplicatively** [472]. **multiplicatively-generated** [472]. **Multiplicators** [497]. **Multiplier** [4076, 1784, 2829, 3130, 3613, 2320]. **Multipliers** [2455, 2530, 1060, 2425, 1906, 1341, 2258, 2508, 688, 3573, 3030, 785, 2899, 4042, 2750, 2980, 3065]. **multiplikativ** [439, 472]. **Multiply** [745, 2672, 2251, 2781, 642]. **multiply-with-carry** [2251, 2781]. **Multiprocessor** [1492, 1919, 1682]. **multiprocessors** [4130, 1749]. **multiprogrammed** [985]. **multiprogramming** [1157]. **multisequences** [3957]. **multispin** [1307]. **Multistep** [1301, 1489]. **multithreading** [3675]. **multivariable** [223]. **Multivariate** [2836, 580, 1796, 3003, 2850, 1344, 2602, 1942, 1291, 2288, 2794, 3456, 3348, 3475, 3476, 3254, 432, 2916, 3077, 2256, 1182, 2629, 793, 2888, 3457, 3458, 1572, 985, 3953]. **Murmur** [3608]. **musical** [3768]. **mutual** [927, 928]. **Mutually** [864]. **MUX** [4063]. **mV** [3411]. **My** [2126, 3935].

N.A.T.O [4096]. **nach** [11]. **Nacional** [134]. **Name** [3574, 804]. **Nanotubes** [3914]. **Naor** [3796, 2654]. **Nash** [3191]. **National** [4087, 4210, 4236, 134, 4098, 91]. **NATO** [4103]. **Natural** [2161, 1352, 3685, 3834, 525, 2231, 2107]. **Nature** [4052, 789]. **Nature-Inspired** [4052]. **Naval** [4108, 649]. **NBA** [2100]. **NC** [2588]. **NDSS** [4268]. **NDSTRNG** [4066]. **near** [2606, 4095]. **nearby** [2196]. **nearest** [1364]. **Nearly** [4029, 1507, 255]. **NEC** [1986]. **Need** [723]. **Needs** [729]. **Negative** [2274, 845, 349, 1244]. **nei** [991]. **neighbor** [1364]. **neighborhood** [2652, 2745]. **neighborhood-of-four** [2652, 2745]. **Nested** [1001, 2489]. **net** [2091, 4058, 2245]. **Netherlands** [4133, 4295]. **Nets** [3006, 2391, 2965, 2097, 2400, 4270, 2813, 2476, 627]. **Netscape** [2174]. **Network** [4268, 2032, 3314, 3663, 2711, 4058, 3452, 3371, 2122, 2242, 3546]. **networked** [3309]. **Networking** [4280]. **Networks** [1410, 3933, 3012, 3314, 3685, 3834, 3191, 3828, 3882, 1992, 3492]. **neuen** [11]. **Neuere** [633]. **Neumann** [3346, 3510, 3628, 1026, 3902, 553, 593, 594, 1820, 1436, 924, 1770, 2970, 4094]. **Neural** [3933, 2711, 3546, 3730, 3492]. **Neuroscience** [1381]. **neutron** [1220, 3552]. **Nevada** [4182, 4223, 4274, 4187]. **Newer** [633]. **Newman** [596, 640, 542]. **News** [2333, 3913]. **Newton** [3992, 3077]. **Newton-based** [3077]. **Nicholas** [2498]. **nicht** [633]. **nicht-gleichverteilten** [633]. **Niederreiter** [1878, 1901, 2742, 2476]. **Nillsen** [3707]. **nineteenth** [4132]. **Ninth** [4104, 4189]. **Nisan** [4070, 3543]. **NIST** [3079, 2946, 2865, 3118, 3693, 3485, 3921]. **NIST-Recommended** [2946]. **Nix** [3843]. **NJ** [2136]. **nm** [3411, 3743]. **NMA** [4213]. **No** [196, 3868, 896, 1273, 1071, 1039, 2305, 3057, 937, 2006, 70]. **node** [2436, 1828]. **nodes** [3191]. **Noise** [180, 819, 2255, 30, 353, 354, 1850, 452, 3341, 55, 57, 2974, 628, 429, 2673, 2504, 2855, 478, 3423, 3424, 3660, 2283, 3198, 2873, 2953, 3036, 2959, 3440, 251, 2396, 2553, 3052, 3702, 3480, 2827].

noise-based [2396, 2553]. **noise-like** [478]. **Noises** [3382]. **Noisy** [1793]. **nom** [804]. **Nombres** [343, 4082, 2844, 762, 322, 697, 736, 2552, 4101]. **Nomograms** [1279]. **Non** [1406, 3390, 3893, 3813, 1801, 4066, 822, 1219, 2771, 350, 3022, 25, 1833, 516, 3577, 787, 2719, 3336, 520, 521, 1382, 3950, 845, 2827, 2406, 3067, 3133, 2408, 715, 3412, 12, 3292, 1710, 1223, 1283, 1346, 3904, 767, 1955, 2614, 2290, 2626, 871, 2205, 40, 3048, 3916, 567, 619, 1993, 189, 3845, 3759, 1784, 2829, 3259, 51, 716, 3503, 1311]. **Non-adaptive** [3813]. **Non-Archimedean** [3390]. **Non-biased** [2408]. **Non-Boolean** [3893]. **Non-Deterministic** [4066, 2827, 3259]. **non-homogeneous** [12]. **non-iid** [3292]. **non-integer** [567, 619]. **Non-Integral** [822, 715, 716]. **Non-interactive** [1801]. **non-linear** [1223, 1283, 1346, 871, 3503]. **non-Mersenne** [1784, 2829]. **Non-Negative** [845]. **Non-Normal** [25, 516, 40, 1993]. **non-parametric** [51]. **Non-Poisson** [520, 521]. **non-prime** [3048]. **non-random** [189]. **Non-Randomness** [1382, 3845]. **non-recursive** [3916]. **Non-standard** [3950, 1955]. **Non-Stationary** [350, 787, 2614]. **non-successive** [2290]. **Non-Uniform** [1406, 2771, 2719, 3336, 1219, 3022, 1833, 3577, 3067, 3133, 3412, 1710, 3904, 767, 2626, 3759, 1311]. **non-uniformity** [2205]. **nonalgebraic** [2758]. **nonanalytic** [1292]. **Nonce** [3528]. **Noncentral** [826]. **nondeterministic** [2065]. **Nonempirical** [2727]. **Nonidentically** [3400, 606, 1192]. **nonintegral** [855]. **Noninverse** [1578]. **Noninvertible** [1298]. **Nonlinear** [2994, 3928, 2046, 2165, 2263, 3008, 3179, 1034, 824, 3014, 2447, 3872, 1298, 1559, 1859, 3690, 1763, 2469, 2966, 2015, 1677, 2919, 3284, 1506, 1510, 1812, 1815, 1923, 1929, 2260, 1347, 2784, 3184, 2187, 2188, 3197, 3205, 3439, 310, 2805, 3112, 1386, 1387, 2637, 2738, 3233, 3455, 3456, 881, 3604, 2984, 1597, 3852]. **Nonnegative** [3647, 3350, 978, 3616]. **Nonnormal** [1344, 2888]. **Nonnormality** [399, 1121, 368]. **Nonoverlapping** [2043, 2045, 1814, 2223]. **Nonparametric** [674, 555, 1165, 1727, 2778, 3555, 3669, 3670, 292]. **nonprobabilistic** [1631]. **nonrandom** [627]. **Nonrandomness** [3484, 1368]. **Nonrecursive** [549, 3271, 2758]. **Nonsingular** [3988]. **nonskewed** [1256]. **nonsuccessive** [2750]. **Nonuniform** [993, 3082, 3005, 1221, 2863, 2916, 2917, 3004, 2853, 782, 1874, 3653]. **nonuniformly** [633]. **NOR** [3982]. **Norfolk** [4174]. **Nörlund** [60]. **Norm** [3582]. **Normal** [1321, 578, 1022, 579, 755, 2675, 3715, 580, 818, 3636, 582, 904, 3400, 1903, 760, 1279, 438, 857, 323, 643, 2704, 25, 598, 1365, 330, 516, 3867, 779, 1543, 1455, 1544, 332, 3029, 1743, 1744, 254, 280, 281, 335, 359, 450, 791, 1645, 2633, 187, 204, 3946, 418, 699, 700, 838, 3840, 148, 392, 2647, 1575, 4018, 287, 845, 890, 749, 2314, 8, 168, 1051, 2906, 808, 3267, 2570, 632, 1324, 1404, 991, 3076, 3721, 182, 2678, 1210, 240, 15, 546, 58, 1336, 994, 4030, 553, 1160, 2171, 2439, 2440, 2593, 141, 593, 594, 770, 1121, 1071]. **normal** [1529, 1238, 1128, 158, 18, 416, 283, 336, 339, 1974, 1014, 160, 489, 795, 40, 927, 928, 1394, 363, 2646, 1993, 975, 3056, 882, 230, 135, 191, 846, 289, 164, 4043, 2233, 70, 3710, 3862, 2992, 435, 303, 480, 364]. **Normale** [2992]. **Normali** [991]. **Normalisation** [3510, 3628]. **Normality** [516, 749].

Normalizing [893]. **Normally** [399, 636, 323, 368, 43, 1508, 3878, 2633]. **normally-distributed** [1508]. **normalverteilter** [1508]. **NORTA** [2583]. **North** [4146, 4167]. **Norway** [4248]. **Note**
[127, 2846, 270, 58, 589, 590, 378, 725, 1286, 224, 1174, 921, 446, 2958, 1186, 86, 417, 205, 390, 458, 422, 3371, 2756, 1679, 406, 896, 2241, 3771, 1058, 236, 182, 1029, 1920, 1523, 2279, 2280, 1945, 3109, 1253, 2416]. **Notebook** [2147]. **Notes** [399, 582, 239, 298, 955, 323, 409, 243, 516, 2526, 3742, 250, 388, 365, 368, 942, 406, 150]. **notion** [1241, 650, 1050]. **Novel** [3512, 2507, 4052, 3376, 3526, 3157, 3282, 4027, 3312, 3313, 3906, 2944, 3583, 3448, 3506, 3766]. **Novelty** [4079]. **November**
[4155, 4231, 4211, 4114, 4117, 4146, 4153, 4179, 4219, 4280, 4243, 4236, 4121]. **ns** [3371]. **ns-2** [3371]. **NSWC** [1560, 1861, 1481]. **NTL** [4019]. **Nuclear** [3786, 3552, 1591, 4093]. **Num** [221]. **Number**
[3628, 1402, 1406, 2322, 2420, 293, 4047, 2134, 2237, 2994, 1487, 1206, 1897, 3770, 852, 3277, 400, 3148, 3149, 2140, 2326, 2327, 3150, 2763, 2998, 2144, 3394, 3395, 4082, 3523, 3524, 3635, 757, 2243, 2245, 2148, 1495, 1413, 3815, 2332, 3529, 3930, 4007, 1208, 2500, 1416, 3533, 2333, 2334, 2846, 3001, 3159, 906, 2152, 907, 908, 3534, 2153, 502, 1904, 821, 1500, 3538, 3405, 4048, 2028, 2427, 3286, 3407, 4025, 4066, 3648, 2428, 1276, 1156, 1609, 2337, 2429, 3290, 1215, 1277, 1335, 3169, 404, 548, 2769, 1504, 1918, 2850, 2926, 1709, 1919, 2505, 3175, 3651, 3936, 4008, 4078, 2686]. **Number**
[2772, 2161, 3085, 3086, 3087, 3176, 3301, 3548, 1065, 1342, 2040, 2687, 3655, 1343, 2041, 2163, 2164, 4069, 1426, 1344, 1618, 1620, 2046, 3179, 3782, 2051, 2433, 2434, 2775, 3549, 3551, 4031, 1161, 3182, 2692, 3012, 3658, 766, 1033, 1115, 1517, 3819, 1519, 824, 1820, 863, 1521, 2353, 2777, 3016, 1353, 1434, 1522, 3420, 2780, 200, 243, 1437, 3183, 3422, 3423, 4052, 508, 2603, 3019, 1290, 3316, 3662, 4053, 3094, 3186, 1362, 3095, 2278, 2281, 1731, 2066, 245, 1122, 3567, 3664, 3188, 3024, 1832, 3428, 3190, 2608, 4035, 279, 327, 3995, 2790, 1630, 3996, 3430]. **Number** [2450, 3324, 515, 3196, 1538, 1633, 1956, 3200, 3791, 2946, 2366, 2189, 2947, 869, 4012, 2612, 1455, 2288, 332, 481, 2713, 1295, 1639, 1741, 2195, 2295, 2371, 2377, 2456, 2457, 2529, 2619, 2620, 2717, 2718, 2871, 3033, 3035, 3105, 3107, 3207, 3330, 3578, 3795, 3998, 4083, 3672, 4014, 3673, 3031, 830, 3869, 1740, 649, 3208, 3333, 3334, 4170, 3742, 3212, 1743, 1744, 651, 2719, 3214, 3215, 3679, 3872, 2958, 3744, 1850, 4074, 2466, 3745, 358, 1552, 3875, 872, 3876, 3877, 44, 2200, 1184, 1186, 1853, 1854, 1855, 2079, 2538, 2800, 2081, 2082, 2083, 2202, 2727, 3040, 3223, 2204]. **Number**
[2731, 2884, 4058, 656, 1466, 1187, 2387, 1469, 1557, 2206, 1859, 1756, 1299, 3799, 1188, 3114, 1084, 4038, 1862, 2551, 2641, 2739, 3691, 610, 739, 874, 2301, 3452, 657, 797, 798, 3690, 1764, 1867, 2094, 2210, 3914, 1767, 68, 1390, 661, 4059, 929, 3460, 1392, 4015, 1986, 1660, 1193, 1087, 743, 4154, 1774, 1990, 3696, 3842, 3883, 1994, 420, 1475, 841, 3352, 1395, 2819, 933, 1048, 3470, 3471, 3472, 3473, 2109, 229, 3239, 934, 1017, 805, 2649, 3474, 3475, 3476, 3242, 3701, 2974, 2110, 3804, 3354, 3355, 1197, 2475, 2651, 2822, 531, 3244, 936, 4247, 3060, 885]. **Number** [886, 1580, 1581, 1582, 2114, 4019, 3062, 986, 887, 3247, 2226, 1878,

571, 2480, 2483, 2485, 629, 889, 1257, 3358, 3483, 890, 536, 3249, 2119, 3611, 3129, 3920, 3952, 2660, 2662, 2902, 3363, 1400, 1479, 2010, 3253, 3364, 1142, 3132, 3254, 3491, 3848, 3256, 3367, 3368, 574, 2832, 1672, 3369, 3259, 1673, 2232, 3371, 1052, 427, 1885, 2124, 2835, 1145, 1201, 3263, 1676, 3707, 3376, 1318, 2492, 2128, 2494, 2670, 3378, 3622, 428, 1053, 1147, 1319, 2987, 1791, 88, 3499, 3268, 3380, 1598, 3765, 3381, 3502, 3271, 3709, 3382, 3273, 3504, 851, 3385, 4101, 1262, 3386, 2419, 3412, 2760]. **number**
[3387, 2571, 1149, 1204, 1322, 1485, 3711, 2672, 1407, 815, 3389, 4064, 1265, 3142, 1326, 1683, 816, 3513, 3514, 3810, 2021, 1896, 499, 2497, 3712, 2137, 2324, 3927, 1686, 1490, 3276, 3991, 2325, 3519, 2241, 3855, 2328, 4065, 3992, 2997, 3521, 3522, 3633, 3717, 3718, 3772, 1056, 1057, 3074, 3634, 349, 3393, 3856, 1493, 466, 675, 3526, 3152, 3720, 3721, 1691, 3153, 1692, 3814, 1497, 3279, 3280, 3399, 1414, 2919, 3964, 2150, 3157, 3281, 1059, 3531, 820, 1060, 1900, 1209, 2026, 677, 1696, 2678, 2766, 3002, 3078, 1103, 1418, 3079, 3776, 2425, 2767, 4202, 634, 909, 1499, 1699]. **number**
[4160, 1700, 2921, 1701, 1702, 3283, 3284, 1211, 3899, 403, 1608, 1906, 3404, 1420, 721, 546, 3164, 3285, 3539, 3777, 1908, 3080, 3287, 1910, 3167, 1275, 320, 3966, 3722, 3541, 1911, 2157, 2249, 680, 1704, 2033, 2250, 3170, 2034, 2158, 2251, 2338, 469, 1028, 1916, 2035, 3293, 2339, 1339, 1505, 1506, 1707, 1805, 3295, 3411, 994, 1423, 1502, 1503, 3544, 1612, 1613, 1711, 2770, 2851, 3723, 3901, 1341, 471, 3546, 1920, 4027, 635, 504, 2928, 3724, 3298, 3299, 1616, 4028, 3300, 407, 1110, 3725, 999, 1158, 1425, 2773, 2257, 2258, 2508, 3178, 3089, 1509, 912, 3302, 1428, 1511]. **number**
[1625, 1717, 1718, 1721, 2048, 1223, 1283, 1346, 1347, 2930, 1931, 2050, 2170, 2267, 2346, 2589, 2590, 3550, 1429, 2932, 3783, 724, 2593, 1725, 1163, 1516, 2595, 1818, 1225, 1226, 1348, 2053, 3904, 440, 273, 1229, 727, 3784, 1286, 1069, 1287, 1350, 1432, 1520, 275, 3013, 2351, 3727, 862, 1002, 3905, 2699, 3785, 2446, 556, 1168, 379, 412, 2781, 1729, 1824, 773, 477, 2857, 776, 3730, 3973, 2601, 2783, 3424, 3865, 2056, 2176, 2784, 3184, 3731, 3425, 3315, 1826, 1827, 1936, 2058, 2059, 3562, 688, 4034, 3563, 3564, 1937, 3566, 2063, 2279]. **number** [2280, 2359, 1940, 2064, 2606, 3907, 1439, 2282, 3735, 778, 4010, 2362, 1943, 867, 3427, 2944, 1440, 1441, 76, 3323, 1948, 1236, 1629, 224, 382, 202, 1175, 3738, 1237, 2449, 154, 1531, 1532, 1533, 1949, 2182, 356, 383, 2495, 1075, 2522, 3997, 3572, 2183, 118, 1123, 1178, 2945, 3432, 1838, 1448, 2186, 2285, 2286, 2364, 2365, 3573, 1007, 2187, 2188, 3197, 3198, 3201, 2526, 1450, 2866, 3976, 920, 1009, 1240, 1452, 1734, 782, 3205, 1453, 1636, 1454, 2948, 2453, 4054, 600, 601, 248, 2949, 3030, 3103, 829, 1373, 3434, 1376, 1640, 1846, 1965, 2191, 2196, 2291, 2292, 2293, 2372, 2373]. **number**
[2374, 2375, 2376, 2616, 2618, 2715, 2868, 2870, 2951, 3106, 3438, 3674, 3910, 3327, 1547, 1180, 3435, 1127, 3206, 3328, 2950, 785, 2872, 2874, 3037, 3209, 2296, 3827, 129, 483, 1742, 3675, 3210, 1550, 484, 871, 3580, 3581, 4073, 2628, 3743, 2959, 4036, 1849, 3942, 3109, 3440, 3583, 3586, 3828, 3874, 1969, 1642, 1851, 1972, 652, 3746, 3831, 3680, 3337, 3338, 3682, 448, 449, 486, 522, 655, 792, 1080, 1185, 1554, 1555, 1644, 1750, 1975, 2299, 2723, 2801, 3445, 2725,

2880, 3220, 3981, 3590, 1856, 1976, 1977, 2461, 2541, 2542, 3683, 3748, 3798, 3684, 2384, 2385, 2803, 3041]. **number**
[3110, 3225, 3112, 4075, 3591, 2806, 2887, 1755, 1651, 795, 455, 456, 833, 3751, 796, 3340, 1083, 1132, 3448, 925, 835, 3342, 611, 3688, 3450, 3045, 613, 1015, 658, 1133, 1304, 1655, 1762, 1763, 2093, 2549, 2637, 2738, 3234, 3048, 3347, 3454, 2889, 3455, 3456, 618, 662, 3235, 879, 3756, 3117, 2552, 2891, 2968, 3459, 2215, 3349, 3839, 1471, 1135, 492, 526, 1085, 1306, 1472, 1768, 2101, 972, 1394, 3236, 3949, 2553, 2102, 566, 3595, 2104, 1307, 3464, 803, 3051, 3918, 1136, 620, 2554, 1991, 3467, 260, 1137, 622, 367, 842, 3598, 2397, 1662]. **number**
[3950, 3053, 1092, 1573, 3055, 1093, 2744, 3121, 1664, 935, 977, 4061, 1196, 3700, 706, 2557, 3846, 3884, 3885, 3058, 710, 624, 2112, 3059, 2401, 1579, 3478, 1875, 493, 3601, 1398, 1478, 1668, 1779, 2113, 2224, 2225, 2899, 3760, 2652, 2745, 1780, 1876, 2311, 2477, 3480, 846, 1877, 4062, 3919, 3805, 3606, 2227, 2478, 1199, 2656, 2825, 3607, 987, 2826, 2486, 3807, 4020, 4042, 2563, 208, 3127, 3609, 2657, 2658, 4003, 3610, 3360, 3612, 2901, 2316, 2405, 2565, 2748, 2663, 2749, 2751, 2830, 2980, 2981, 2982, 3065, 3066, 3130, 3486, 3487, 3488, 3613, 3614, 3252, 3489, 3490, 1480]. **number**
[1669, 1883, 2009, 3067, 3131, 3133, 3763, 3808, 2408, 3492, 3366, 167, 2984, 4021, 2489, 1671, 1315, 989, 3134, 2833, 4022, 3494, 3496, 1098, 2123, 1099, 3706, 4004, 2567, 3618, 232, 1595, 1886, 3068, 3619, 1790, 2669, 3377, 2129, 2235, 3379, 2015, 463, 2988, 3138, 2568, 3266, 3498, 3623, 3708, 1792, 2418, 2320, 2671, 2757, 3070, 3501, 3269, 4045, 3503, 3071, 3270, 3958, 2758, 2910, 2759, 3383, 3384, 3506, 2990, 4046, 3508, 3766, 1263, 1600, 577, 2991, 3862, 3545, 3653, 4072].
Number-theoretic [2301]. **Numbers** [3511, 497, 814, 2992, 2836, 2574, 1685, 2839, 2138, 3714, 2240, 946, 1327, 3520, 2675, 295, 1329, 3636, 949, 2147, 3774, 2677, 239, 183, 760, 2502, 2030, 1214, 216, 2587, 3818, 551, 636, 271, 723, 1617, 2431, 1222, 1619, 1623, 1719, 1922, 2043, 2049, 2165, 2259, 2261, 2263, 3008, 2343, 2266, 2348, 2692, 860, 1067, 3419, 49, 323, 409, 864, 3310, 1352, 3556, 3557, 3972, 3993, 4032, 244, 2447, 2602, 2354, 510, 325, 380, 2605, 2704, 3823, 3321, 1833, 1074, 355, 2707, 329, 2709, 155, 1537, 4071, 1840, 3740, 1735].
Numbers [225, 1737, 1545, 560, 648, 1548, 2617, 1739, 27, 249, 694, 1971, 1381, 654, 450, 834, 131, 1301, 457, 615, 876, 877, 2469, 2640, 2736, 2966, 1656, 3461, 838, 1660, 3350, 2815, 2816, 361, 391, 1989, 3840, 1474, 3597, 528, 3241, 1873, 530, 462, 346, 3128, 630, 136, 373, 1313, 2231, 539, 1146, 1483, 2417, 911, 1055, 1321, 1403, 1601, 3768, 1489, 2022, 1491, 3715, 1328, 3716, 3718, 3896, 178, 3278, 991, 2580, 3075, 1604, 1690, 3076, 2764, 318, 3721, 1605, 2244, 1607, 2844, 758, 1498, 104, 402, 503, 2582, 3778, 1909, 2681, 214].
numbers [215, 762, 3291, 1278, 2849, 58, 2503, 470, 1501, 1422, 297, 439, 472, 550, 587, 683, 43, 473, 3084, 1508, 113, 218, 1621, 1622, 1624, 1720, 1722, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1923, 1924, 1925, 1926, 1927, 1928, 1929, 2044, 2045, 2047, 2166, 2167, 2168, 2260, 2262, 2264, 2340, 2341, 2342, 1345, 2265, 2688, 2435, 3937, 322, 153, 2052, 2171, 2438, 2439, 2440, 242, 1819, 184, 767, 768, 1230, 1351, 2442, 2598, 142, 199, 219]. **numbers**
[117, 476, 3018, 1005, 185, 641, 642, 478, 1120, 2514, 3820, 66, 75, 2061, 2277,

2357, 479, 2787, 67, 1235, 3789, 4011, 4035, 1006, 1733, 415, 2284, 331, 1536, 21, 1368, 1369, 1038, 2287, 26, 31, 32, 22, 2867, 2367, 307, 2369, 3792, 2071, 4055, 2294, 2952, 3826, 1844, 1012, 1013, 2454, 1966, 2075, 2624, 2955, 3678, 519, 2199, 1462, 1643, 1749, 2078, 3588, 312, 451, 2460, 77, 3878, 2805, 697, 736, 4001, 489, 2207, 2388, 609, 737, 2633, 3044, 836, 28, 3689, 1759, 1864, 2810, 698, 800, 801, 802, 837, 878, 1044, 1190, 1251]. **numbers** [1386, 1387, 1389, 1470, 1564, 1565, 1865, 1868, 1981, 2547, 2548, 2638, 2639, 2967, 3232, 343, 3457, 3458, 1570, 419, 2306, 491, 930, 258, 45, 121, 839, 2471, 362, 665, 459, 344, 2646, 260, 3698, 2398, 974, 99, 286, 3353, 1195, 1995, 3699, 568, 134, 2894, 882, 1094, 3600, 230, 711, 1140, 2975, 2223, 2823, 460, 3604, 461, 534, 192, 626, 712, 2313, 149, 749, 2314, 572, 4043, 1783, 2229, 165, 1314, 2121, 3764, 193, 9, 107, 210, 2488, 2566, 1884, 3257, 940, 3849, 3260, 3261, 3497, 2013, 2014, 2491, 494, 575]. **numbers** [1674, 713, 714, 2907, 2130, 2413, 2493, 5, 2986, 3069, 1888, 70, 2569, 233, 3890, 29, 3507, 3627, 894, 2018, 1892, 1590, 176, 3375, 3646, 2584, 2252, 1119, 1728, 915, 777, 732, 921, 1370, 2451, 1863, 2092, 538, 944, 1484, 1680, 631, 3318]. **Numer** [937]. **numeration** [1032, 1032]. **Numeri** [991, 470, 491]. **Numerical** [717, 2838, 1213, 4088, 682, 350, 1001, 1821, 1627, 4277, 1356, 509, 277, 645, 1234, 1446, 1963, 2465, 3227, 1773, 2217, 493, 1782, 4094, 291, 670, 265, 1596, 4101, 1607, 3410, 3864, 1626, 2939, 2061, 1071, 2789, 2181, 4213, 1535, 23, 1379, 3439, 1128, 1251, 2306, 975, 1879, 2115, 2564, 2747, 1587, 1884, 398, 541, 807, 2324, 2241]. **Numerics** [4184, 4195, 4200]. **numérique** [541, 4101]. **numeros** [134]. **nVidia** [3328]. **NY** [4283, 4221].

O [1071]. **Ob** [35]. **obeying** [2018]. **Obfuscation** [3277]. **Obituary** [2498]. **Object** [1818, 2715, 3581]. **object-oriented** [2715, 3581]. **Objectives** [2594]. **Oblivious** [3994]. **observation** [1602, 1684, 1714, 1715]. **Observations** [874, 1096, 349, 23]. **Obtain** [3317, 2607]. **Obtained** [3774, 549, 1761, 134, 1021]. **Obtaining** [703, 880, 67, 974, 1398, 177]. **obtenida** [134]. **OCCAM** [1471]. **Occupancy** [2692]. **October** [4210, 4130, 4242, 4120, 4135, 4140, 4146, 4152, 4162, 4185, 4194, 4198, 4223, 4274, 4289, 4102]. **octrees** [1930]. **odd** [2006]. **Odell** [542, 596, 640]. **Odyssey** [4225]. **off** [4050, 2776]. **Offer** [2610]. **Office** [4098]. **Offord** [1961]. **offs** [1688]. **Offset** [3188]. **Olds** [4102]. **OMAC** [3343]. **On-line** [3355]. **On-the-Fly** [3354]. **on/off** [2776]. **One** [2019, 3713, 756, 3527, 2159, 2271, 2448, 3732, 2702, 1632, 1183, 1297, 1641, 448, 449, 485, 2538, 739, 2098, 2218, 1665, 3366, 3625, 1599, 3632, 900, 3426, 1444, 3191, 1447, 188, 2663, 1200, 5, 3384, 3851]. **One-chip** [3366]. **one-class** [3384]. **one-dependent** [1447]. **One-Dimensional** [3625, 188]. **One-line** [448, 449]. **one-shot** [3191]. **One-Sided** [485]. **One-Table** [2019]. **One-Time** [3527, 2271, 2218]. **One-Way** [3713, 3732, 1641, 2448, 1632, 1183, 1297, 3632, 3426, 1444, 3851]. **Ones** [1392, 2104]. **Online** [3951, 2651, 3751, 3117]. **Only** [2769, 3410, 3422, 3666, 2521]. **Ontario** [4218, 4175]. **OpenACC** [4003].

OpenBSD [2430]. **OpenCL** [3966]. **OpenMP** [4003]. **OpenSSL** [3850, 3153]. **Operating** [3085, 3086, 3300, 3101, 1255]. **operation** [3145, 4041]. **Operational** [2033, 4096]. **Operations** [2331, 4222, 4161, 1737, 1627, 2874, 1143, 4161]. **operator** [2022]. **operators** [112, 2411]. **opinion** [2801]. **Optical** [3168, 2687, 3681, 2563, 3622, 3325, 2557]. **Optimal** [3893, 1060, 2153, 2425, 1341, 3780, 3903, 4029, 1714, 1715, 595, 688, 646, 690, 732, 3752, 1301, 3231, 1476, 1400, 1420, 2350, 2606, 2519, 3433, 2069, 3221, 3116, 837, 2899, 1714, 1715]. **Optimality** [595, 1119, 1089]. **optimisation** [3689]. **Optimised** [2406, 3132, 3491]. **Optimization** [3548, 2590, 4277, 4052, 4071, 2451, 1963, 1964, 4233, 2117, 1484, 4128, 3278, 3395, 3077, 2589, 2787, 4163, 3697, 4003]. **Optimized** [3347, 3476, 3302, 3949]. **Optimizing** [3921, 3380]. **Optimum** [663, 628]. **Oracle** [3895]. **orbit** [3973]. **Orbits** [2158, 2997]. **Order** [2421, 1706, 1918, 3651, 3652, 3009, 643, 1378, 1740, 2956, 3226, 54, 703, 2667, 1270, 1417, 3932, 2927, 3174, 3296, 1066, 3093, 1361, 2705, 2648, 46, 3362, 3488, 3614]. **Order-Disorder** [54]. **Ordered** [2696, 1795, 150, 1907, 1031, 3180, 1162, 41]. **ordering** [2614]. **Orders** [2447, 1068, 2663, 2984]. **ordinal** [438]. **ordinateur** [762]. **Oregon** [4216, 4202]. **organic** [3541]. **Oriented** [3154, 2686, 3451, 3452, 3242, 1818, 2715, 3581]. **Origin** [1820]. **origins** [4286]. **Orlando** [4220, 4110]. **Orleans** [4149]. **Orono** [4160]. **ors** [3365]. **orthogonal** [1267]. **Oscillation** [2974]. **Oscillator** [3523, 3635, 3551, 4056, 3829, 4074, 3268, 3505, 3513, 3514, 3856, 2767, 3550, 3313, 3338, 3342, 3496]. **Oscillator-Based** [3523, 4074, 3513, 3514, 3856, 2767, 3496]. **Oscillators** [3681, 4015, 3423, 208]. **Other** [1487, 2962, 175, 593, 594, 117, 1536, 2533, 2622, 263, 987, 750, 4084, 3384]. **Otherwise** [2245]. **Ottawa** [4250]. **outage** [3453]. **Output** [3895, 2772, 3863, 3837, 4018, 3756, 3618, 3809]. **overhead** [4063]. **overlap** [4004]. **Overview** [3753, 2755, 2430, 2951]. **Oxford** [4217, 4109].

P [596, 640, 262, 170, 2987, 2988]. **P-RnaPredict** [2987, 2988]. **P.** [895, 542, 135]. **P1363** [2518]. **PA** [4111]. **PaCAL** [3793]. **Package** [3793, 1639, 649, 3211, 3139, 499, 3536, 3778, 1940, 2715, 3581, 655, 613, 618, 1193]. **Packing** [3063, 3388, 717, 501, 1176, 1476, 424, 939]. **packings** [430]. **Pad** [3527, 2271, 2218]. **Padé** [1958]. **Page** [2911, 2518]. **Pages** [3742, 2136]. **Pair** [281, 349]. **pair-wise** [349]. **Pairs** [551, 2043, 3740, 1079, 2746, 752, 1814, 2045, 2264, 2340, 141, 2223]. **Pairwise** [971, 746, 2747]. **Palace** [4220]. **Palásti** [717, 501]. **Palo** [4290, 4204]. **Pan** [954, 1113]. **Pannonian** [4113]. **Paper** [196, 236, 31, 3596]. **Papers** [3734, 2527, 4248, 4098, 4162, 1261, 2016, 239, 323, 409, 406, 4250, 4242]. **Papoulis** [389]. **paradigm** [4054]. **Paragon** [2056]. **Parallel** [2571, 672, 2134, 2237, 1897, 1492, 2333, 2334, 2152, 2153, 2425, 3287, 3409, 2337, 1343, 2263, 2051, 2266, 2348, 2434, 2435, 4031, 1429, 3823, 1441, 1294, 1454, 3794, 3208, 3333, 1977, 2081, 2082, 2083, 2383, 2632, 2881, 3683, 3748,

2202, 2468, 3462, 3694, 1772, 1990, 1395, 3698, 3600, 2219, 3951, 4174, 2226, 3485, 2662, 3764, 4195, 2987, 3070, 1683, 3716, 3717, 3718, 3772, 3720, 2422, 1209, 1418, 2156, 3966, 2249, 1916, 1505, 2039, 1423, 1503, 3296, 1425, 1509, 2170, 2347, 1285, 1432, 3727, 3092, 1822, 1438, 4212, 3023, 1363, 2358, 1943, 1124, 4013, 3826, 3675, 3678]. **parallel**
[2628, 3942, 2875, 3583, 1746, 2197, 1970, 1972, 3680, 3590, 1856, 1976, 2461, 2882, 3448, 3839, 1472, 1991, 1664, 2000, 2227, 2312, 2826, 2748, 1588, 2488, 2491, 2235, 2988, 2568, 1792, 2757, 1590, 4184, 4200, 1789]. **parallèle** [1588]. **parallelism** [3772]. **Parallelization** [3533, 1339, 2289, 2877, 2106, 3711]. **Parallelized** [2078, 2640, 1851]. **Parameter**
[756, 900, 822, 2689, 3553, 4073, 2220, 1058, 2712, 3912, 3444, 567, 619, 2476]. **Parameterized** [4069, 1860]. **Parameterizing** [3409, 2882]. **Parameters**
[2153, 2456, 3341, 715, 855, 2054, 1828, 2606, 829, 2372, 2089, 2091, 972, 2648, 843, 3702, 3252, 716, 3851]. **Parametric** [3681, 51]. **Parametrical** [3548]. **Paraperm** [3794]. **Paris** [4123]. **Park** [4146]. **parking** [3388]. **parsing**
[2156]. **Part**
[2164, 4295, 2624, 2657, 2268, 2269, 2463, 3470, 3471, 3472, 3473, 532, 533, 2658]. **Partial** [1517, 3985, 1348, 84, 1249, 3614]. **Partially** [2379].
Partially-Specified [2379]. **Particle**
[4071, 3214, 2214, 3595, 3767, 3711, 3278, 3395, 95, 2305]. **particle-in-cell**
[3767]. **particular** [2918]. **Partition** [239, 1652]. **Partitioning**
[852, 1001, 2930]. **Partitions** [2219]. **parts**
[1325, 2345, 2688, 2514, 2454, 2080, 2639]. **PASCAL**
[1391, 1328, 1616, 1122, 1319]. **Pass** [2724]. **passage** [581]. **Passau** [4272]. **Passive** [3149, 3964, 3750]. **Password** [1869, 1461]. **past** [3436]. **Patchwork**
[1542, 1891, 1891]. **Patchwork-Verwerfung** [1891]. **path**
[1907, 3421, 3434, 3340]. **paths** [1908]. **Patience** [2769]. **Pattern**
[2037, 4031, 747, 3384, 3189, 3624]. **Pattern-Based** [4031]. **patterned**
[3985]. **Patterns** [1514, 552, 4034, 3741, 1751, 932]. **Paved** [3757]. **Payne**
[763]. **PC** [1508, 1434, 1554]. **PCB** [3282]. **PCIe** [3737]. **PCKS** [2327]. **PCs**
[2276]. **PDEs** [1821]. **PDF** [3289, 3020]. **Pdfs** [3616]. **Peaks** [797]. **Pearson**
[296, 2888, 1572]. **Peccati** [3742]. **Peculiarities** [2630, 2321]. **pedagogical**
[1790]. **peer** [3276]. **peer-to-peer** [3276]. **Pennsylvania** [4190, 4191, 4162].
pentanomials [2120, 2671]. **Pentium** [3249]. **Percentage** [818, 699, 902].
percolation [3209]. **Peres** [4036, 3756]. **Perfect**
[2506, 1556, 1557, 1757, 3280, 3399, 1651, 2087, 836, 1579, 1890]. **perfectly**
[1136]. **Performance** [1682, 2765, 1802, 3408, 595, 1628, 1630, 3196, 1843, 2192, 4280, 1469, 574, 3143, 2242, 3278, 3152, 547, 3315, 3562, 3324, 4055, 2616, 3581, 3798, 3688, 1133, 1992, 1199, 3134, 2017]. **perilous** [3356].
Period [852, 906, 4025, 1620, 3316, 3940, 3677, 2538, 2010, 2753, 2766, 3002, 3078, 3285, 2031, 470, 3084, 1427, 1511, 1718, 2345, 2688, 1516, 768, 2781, 774, 2701, 1358, 2514, 1948, 2364, 2454, 2624, 1975, 2639, 3692, 3050, 706, 2830, 3362, 2758, 233, 1263]. **Periodic** [2997, 181, 749]. **periodo** [470]. **Periods**
[345, 3365, 1902, 2176, 708, 1705]. **Permutation**

[1151, 4025, 1912, 2605, 4070, 3685, 3834, 3837, 3138, 3162, 2684, 997, 321, 2073, 1245, 1858, 3456, 1659]. **Permutation-Based** [3837]. **Permutations** [3894, 3396, 1724, 3794, 1569, 406, 433, 434, 2142, 3898, 1515, 1526, 444, 1632, 1736, 1380, 313, 260, 1775, 706, 3604, 166, 177]. **Permuted** [2097]. **Personal** [2958, 2480, 1690, 1826, 1827, 2058, 2059, 1550]. **Perspective** [2587, 3748, 3798]. **perspectives** [4217]. **PERT** [926]. **Perturbed** [3982]. **Perturbing** [3267]. **PETASYS** [1686]. **Petrov** [2154]. **PGA** [3291]. **PH** [3373, 3667]. **PH-Distributed** [3667]. **Phase** [3681, 873, 161, 3479, 3423, 3424, 3440, 3337, 3373]. **phase-dependent** [3373]. **Phase-Shift** [873]. **Phenomena** [3027]. **phenomenon** [3684]. **Philadelphia** [4190, 4191]. **Philip** [507]. **Philosophy** [4102]. **Phoenix** [4158]. **Phone** [3804]. **Photo** [3815]. **Photodiode** [3363]. **Photon** [2687, 3128, 3363, 3377, 3572, 3434, 3598, 3618, 3379]. **photon-number** [3434]. **photon-number-resolving** [3572, 3598]. **Photonic** [3253]. **Photonic-based** [3253]. **PHP** [3850]. **Phys** [2058, 2182]. **Physical** [4087, 1606, 3962, 3815, 1074, 2612, 3203, 560, 4074, 3223, 2974, 2822, 3128, 3258, 2014, 2125, 3499, 2257, 1723, 2351, 2363, 737, 2810, 1666, 3134, 3370, 2013]. **Physically** [1593, 3898]. **Physics** [2839, 1771, 4247, 1330, 1693, 2246, 2247, 2676, 3398, 2921, 3467, 2666]. **Pi** [2962, 3039, 2645]. **Picturebook** [2268, 2269]. **Picturing** [1473, 1661]. **piecemeal** [624]. **Piecewise** [3669, 3670, 2627, 3067, 3133]. **Piecewise-Linear** [3669, 3670]. **Pillai** [446]. **Pinsker** [319, 394]. **pipelining** [1699]. **Pitfalls** [2441]. **Pittsburgh** [4111, 4162]. **Pivot** [2600]. **PKI** [3140]. **pLab** [2268, 2269, 1966]. **Place** [2710, 1775]. **placement** [2680]. **Places** [2211, 81]. **Plains** [4140]. **Planar** [1652]. **plane** [501]. **planes** [1624, 312, 451]. **Plans** [272]. **Plasma** [348]. **Platform** [4081]. **platforms** [3675]. **Plausible** [2845]. **playing** [2843]. **Plaza** [4102, 4131]. **PLC** [3617]. **PLFG** [2748]. **plots** [2130, 2413]. **PLP** [3245]. **plus** [1125]. **pocket** [1098]. **PODS** [4168]. **PODS'09** [4266]. **Point** [2694, 3993, 1078, 1737, 2529, 3207, 2370, 1382, 1303, 1586, 2755, 1800, 3084, 4032, 324, 2356, 4203, 3573, 2071, 2615, 3741, 2533, 2622, 2875, 604, 1014, 3880, 1250, 1760, 1761, 2890, 3049, 932, 668, 3759, 2225, 1876, 985, 3255, 713]. **Points** [818, 270, 196, 2931, 201, 2713, 205, 699, 3061, 3247, 1141, 1786, 902, 221, 222, 3023, 1941, 692, 730, 1635, 2196, 1553, 875, 1865, 1868, 2212, 3048, 2890, 4062, 3606, 423, 2562, 848, 1587, 398, 464, 2133]. **Poisson** [896, 673, 945, 1022, 897, 899, 3854, 1421, 3968, 995, 1424, 1615, 2432, 765, 1834, 1541, 1634, 1545, 1460, 2197, 520, 521, 1247, 1394, 2556, 530, 1019, 3482, 460, 888, 462]. **Poisson-Truncated** [1545]. **poker** [415]. **Poland** [4200]. **Polar** [1898, 281]. **policies** [2586]. **policy** [3101]. **Poly** [3893]. **Poly-Size** [3893]. **Poly1305** [3825, 3948]. **Polya** [1106]. **polyalphabetic** [796]. **polygonaler** [624]. **Polygons** [857]. **Polylogarithmic** [3871]. **polynomes** [1047]. **Polynomial** [4025, 3187, 1368, 2712, 2869, 1374, 2794, 3337, 3749, 1867, 2737, 2811, 3934, 3307, 1458, 3109, 3447, 1651, 3455, 3456, 3458, 3692, 624, 1480, 3958]. **polynomial-time** [1458]. **polynomially** [3297]. **Polynomials**

[2994, 2602, 2523, 3441, 1301, 1866, 1786, 1882, 3988, 1689, 2920, 3162, 3965, 1705, 3017, 1447, 3739, 1041, 1182, 3218, 3457, 1196, 1886, 3621, 397]. **polyominoes** [2142]. **Poor** [757, 128, 3913]. **popular** [2190, 658]. **Population** [1996, 8, 18, 135]. **Populations** [25, 12, 40]. **Portability** [1002]. **Portable** [1897, 3897, 2333, 3173, 3301, 2041, 2773, 4031, 1832, 2189, 481, 1242, 1295, 2956, 1082, 1187, 1774, 1990, 936, 1580, 1053, 1147, 1262, 1590, 1421, 2685, 2770, 2927, 1005, 1358, 2787, 1376, 3104, 1969, 1975, 1991, 1398, 1478, 1668, 3760, 1780, 1876, 1669, 1792]. **Portfolio** [2911]. **Portland** [4216, 4202]. **Posamentier** [3318]. **Positive** [1689, 1112, 2452, 421, 888, 902, 1210, 2872, 1465]. **Possible** [2232, 2102]. **possibly** [2308]. **post** [3234]. **post-processing** [3234]. **Posterior** [3757, 2011]. **Postgraduate** [649, 4108]. **Postprocessing** [3549, 3745, 3178]. **pour** [322, 1375, 2196, 2890, 1588]. **Power** [3561, 3321, 418, 3349, 2905, 1401, 758, 2333, 3283, 3284, 585, 3293, 3415, 1621, 1625, 1720, 1721, 1810, 1925, 1926, 2167, 2168, 2340, 2341, 1347, 1166, 3189, 3435, 3439, 416, 2880, 2548, 2967, 988, 3261, 3262, 3497, 3862]. **power-normal** [3862]. **Power-Up** [3321]. **POWER7** [3743]. **powerful** [3922]. **Powers** [748, 1062, 1333, 2679, 4075]. **pp** [3707]. **Practical** [1893, 2322, 3900, 2604, 3185, 2631, 3480, 1900, 195, 2363, 1734, 2658]. **Practically** [3413, 2354]. **Practice** [2579, 2686, 3430, 4201, 2061, 961, 1240, 2121]. **Practice-Oriented** [2686]. **practitioners** [3734]. **PractRand** [3781]. **Prague** [4095]. **PRAM** [2156]. **PRAND** [3717, 3772]. **pratiques** [1900]. **PRBS** [558]. **Precautions** [575, 631]. **precision** [3573, 1014, 2225, 1876, 3653]. **Predefined** [2023]. **Predict** [2772, 1546, 1738]. **Predictability** [3863]. **predictable** [3153]. **Predicting** [2919, 3731]. **Prediction** [2037, 2987, 2325, 264]. **Preferential** [4009]. **preferred** [554]. **prefix** [2197]. **Preliminary** [2326, 763, 104]. **Prescribed** [2847, 1795, 2437, 2810, 2744]. **Presentations** [394]. **presented** [4098]. **Preserving** [1116, 4077]. **Press** [2136, 3742]. **pretty** [2104]. **Previously** [2538]. **PRG** [3739]. **Price** [170, 3742]. **pricing** [3683, 3748]. **Primality** [3728, 701, 2415]. **Prime** [1329, 2587, 3006, 1290, 3940, 1195, 1995, 3699, 2110, 571, 2417, 2766, 2425, 2155, 3285, 1804, 2851, 1341, 1621, 1810, 917, 2186, 1451, 785, 2383, 4075, 2548, 3048, 1784, 2829, 3487, 3261, 3262, 3497]. **prime-modulus** [785]. **prime-power** [2548]. **Primes** [2160, 943]. **Primitive** [1731, 397, 1047, 1196, 2007, 2671]. **Primitives** [2604, 3185]. **Princeton** [2136, 4292]. **Principle** [3815, 3553]. **Principles** [4168, 180, 819, 1337, 2683, 3083, 858, 2371, 4266, 4201, 2644, 1525, 1539, 1540]. **Printer** [2105]. **prior** [374]. **Priori** [244]. **priority** [695, 696]. **privacy** [4077]. **privacy-preserving** [4077]. **Private** [1649, 2145]. **Prize** [2867, 3954]. **PRNG** [4012, 3931, 3863, 2861, 3677, 3750, 2735, 3956]. **PRNGlib** [2202]. **Proactive** [2032]. **Probabilistic** [1821, 3728, 926, 3361, 1596, 1908, 1334, 2444, 1732, 1747, 2797, 2960, 455, 1563, 627, 576]. **probabilità** [16]. **probabilités** [3]. **Probabilities** [954, 1113, 1575, 3896, 3, 3100, 140].

Probability [3926, 1895, 294, 4098, 3895, 2154, 169, 2037, 3181, 82, 305, 559, 1246, 656, 562, 2636, 360, 1134, 1657, 2740, 2644, 2100, 1192, 2216, 527, 262, 207, 4165, 911, 4099, 151, 1338, 1109, 4271, 16, 2175, 381, 1451, 256, 1562, 666, 570, 2666, 4004, 4113, 389, 2635]. **Probable** [1, 973, 2, 2155, 1804, 1451]. **probablistic** [566]. **Probably** [1329]. **Problem** [2151, 3402, 52, 2933, 304, 1463, 388, 3838, 1782, 1607, 2844, 952, 3560, 3320, 962, 3217, 3943, 188, 3958]. **problème** [2844]. **Problems**
[197, 592, 105, 1123, 27, 790, 341, 342, 1866, 1658, 4233, 1677, 2921, 195, 1908, 1213, 1224, 773, 223, 203, 1766, 3755, 189, 2895, 707, 425, 166, 1591].
procédé [322]. **Procedure** [1104, 1214, 954, 1113, 1001, 3972, 445, 309, 280, 1770, 1602, 1684, 322, 776, 334, 283, 336, 3689]. **Procedures** [2584, 3787, 254, 567, 619, 2650, 1141, 1680, 1692, 584, 320, 2464, 2729, 2963, 3224, 344, 849].
Proceedings [4122, 4143, 4168, 4191, 4283, 4290, 4087, 4144, 4125, 4133, 4088, 4157, 4111, 4116, 4130, 4212, 4086, 4152, 4153, 4295, 4280, 4186, 4110, 4225, 4226, 4253, 4175, 4106, 4188, 4189, 4232, 4108, 4141, 4101, 4190, 4239, 4249, 4254, 4137, 4183, 4128, 4149, 4107, 4123, 4124, 4093, 4169, 4192, 4115, 4193, 4217, 4184, 4109, 4139, 4231, 4151, 4113, 4218, 4162, 4219, 4223, 4213, 4220, 4147, 4243, 4206, 4158, 4187, 4207, 4214, 4236, 4103, 4163, 4119, 4102, 4121, 4228, 4181, 4208, 4131, 4200, 4176, 4127, 4132, 4138, 4148, 4159, 4177, 4182, 4209, 4216, 4229, 4234, 4267, 4276, 4196, 4085, 4091, 4155, 4264].
Proceedings
[4284, 4156, 4104, 4179, 4274, 4289, 4224, 4090, 4171, 4266, 4174, 4244, 4180, 4166, 4195, 4199, 4167, 4202, 4178, 4211, 4272, 4255, 4279, 4252, 4136].
Process [4068, 2077, 3358, 1712, 529, 985, 3374, 1599].
Process-Voltage-Temperature [3358]. **Processes**
[170, 300, 350, 1830, 2708, 691, 2452, 97, 102, 1066, 4271, 274, 198, 1528, 3666, 4095, 2614, 4073, 3945, 360, 1134, 1657, 2740, 228, 62, 1789, 319, 389, 394].
Processing [672, 3544, 4174, 4091, 3720, 1209, 4212, 1363, 2283, 1454, 3206, 3688, 3234, 1992, 1664, 2568]. **processor** [3395, 1531, 1532, 3743, 4080, 3373].
Processors [2434, 3819, 4256, 3431, 3462, 3477, 3758, 3393, 3932, 1418, 1509, 1432, 1628, 1643, 1472, 3508, 3627]. **Produce** [1118, 4051, 4010]. **Produced** [1416, 3824, 560, 1087, 1088, 1417, 3093, 2290, 1566, 2750]. **Producing** [337, 359, 75, 76, 385, 2980]. **Product**
[2610, 3101, 207, 3124, 3247, 902, 1163, 1944, 1246]. **Production**
[169, 331, 176]. **Products** [3043, 395, 535, 2052, 3575, 2833]. **Professor** [4217]. **Profile** [2994, 2852, 2784, 2805, 3112, 1757, 1563, 2984, 1890].
Program
[3522, 3718, 2147, 1221, 3865, 225, 3263, 1028, 2388, 617, 1391, 1137, 940].
Programmable [2283, 1836, 2632]. **Programmed** [817, 904, 1698, 2991].
Programmierung [894]. **Programming** [3897, 4031, 3031, 2098, 1658, 3844, 4228, 894, 4109, 1224, 2181, 2725, 614, 2227, 3762]. **Programs** [1492, 3401, 3775, 3402, 375, 468, 1030, 3994, 4070, 711, 1140, 1481, 3735, 925, 1992, 1901].
progressive [3956]. **project** [2601, 2911]. **Projections** [3193]. **proliferating** [4035]. **Proof** [2020, 2837, 2496, 720, 405]. **Proofs**

[1964, 3685, 3834, 3987, 2843, 2444, 2107]. **Proper** [2140, 1353, 2241]. **Properties** [582, 854, 2035, 549, 2344, 2349, 2932, 861, 508, 186, 2627, 447, 418, 743, 1885, 2912, 3633, 2425, 1905, 2251, 297, 1812, 2167, 2260, 2265, 2345, 2688, 2170, 726, 2350, 143, 2783, 1363, 917, 778, 2364, 1038, 3205, 1640, 3439, 1745, 1754, 1566, 99, 804, 2896, 3057, 3123, 2830, 1788, 2235]. **Property** [181, 3267, 3521, 1153, 3299, 3909, 1302, 806]. **property-based** [3909]. **proportional** [3101]. **Proposal** [497, 1110, 3219, 1637, 1984]. **Proposals** [1656, 1570]. **Proposed** [1186]. **Propositional** [2837, 2496]. **Propriétés** [804]. **Prospective** [511]. **Protect** [639]. **protection** [2329, 4063]. **Protocol** [2032, 3367, 3368, 3197, 4077, 1099]. **Protocols** [3643, 3879, 3948, 2222, 1409, 1688, 3332]. **Proton** [348]. **Proton-Electron** [348]. **Provable** [3064, 1893]. **Provably** [2322, 3396, 2172, 3129, 1442, 3618]. **Proved** [3774]. **Providence** [4122, 4266]. **Providing** [2017]. **Proving** [2701]. **Ps** [3663]. **PSA** [4102]. **'pseudo** [2591, 1055, 2573, 497, 3389, 1151, 4047, 754, 946, 2327, 3150, 2915, 3992, 267, 2144, 991, 2841, 2764, 2243, 1606, 3638, 904, 1496, 544, 1027, 1101, 1208, 181, 1416, 1695, 2153, 239, 503, 183, 760, 2582, 586, 3407, 2032, 3290, 216, 1706, 217, 3544, 2850, 2926, 3651, 3546, 551, 2261, 4031, 1514, 2172, 3819, 3904, 1117, 1519, 1035, 1820, 409, 2511, 2933, 3016, 771, 772, 3420, 243, 1527, 2604, 3185, 3316, 1438, 353, 354, 380, 3567, 865, 2608, 1444, 1732, 355, 2707, 329, 3997, 155, 3430, 2525, 2947, 2792, 3209, 2627, 2958, 447, 3796, 249, 3584, 1245, 1641]. **Pseudo** [1381, 450, 77, 1556, 4058, 1187, 2387, 2086, 131, 3341, 2634, 2808, 1561, 2468, 657, 615, 837, 876, 877, 1656, 206, 4059, 929, 3694, 2394, 3595, 361, 391, 1087, 743, 3053, 933, 1048, 2109, 229, 1576, 3241, 3121, 4018, 1777, 1582, 2654, 2655, 571, 192, 2480, 346, 536, 2119, 2900, 2662, 136, 3367, 3368, 574, 1589, 2832, 1673, 2231, 2232, 2754, 2834, 1052, 427, 1145, 1201, 808, 3376, 429, 1053, 1147, 2568, 810, 3625, 1262, 941, 1149, 1320, 1322, 1407, 3142, 1794, 2135, 2022, 1686, 3277, 3991, 3148, 3519, 4065, 3393, 3151, 2580, 3526, 3721, 2918]. **pseudo** [1152, 2149, 1497, 3281, 1900, 2026, 677, 2425, 909, 104, 3816, 3404, 721, 3777, 3168, 762, 3291, 1028, 3542, 1422, 3294, 3543, 297, 3295, 3901, 1341, 439, 550, 587, 3724, 3299, 407, 113, 218, 1428, 1223, 1283, 1346, 322, 2932, 3970, 153, 1285, 242, 2053, 184, 768, 770, 1168, 1729, 1289, 1357, 478, 3313, 3906, 3562, 917, 2787, 1944, 1235, 3789, 3189, 224, 2519, 3324, 3432, 2287, 3199, 3326, 1008, 1636, 2948, 248, 1012, 1180, 3206, 3328, 2454, 2955, 2628, 1849, 3439, 3442, 1642, 3337, 3220, 3748, 3798, 2385, 284, 3591, 2806, 2887, 456, 796, 3836, 3044]. **pseudo** [1758, 3449, 2301, 698, 800, 801, 802, 1190, 3454, 1570, 419, 2306, 492, 258, 1085, 3463, 3236, 3237, 665, 803, 666, 3918, 3466, 3698, 974, 3950, 568, 3055, 882, 3847, 710, 624, 3601, 3602, 2653, 4041, 2311, 1199, 345, 572, 4043, 3359, 2229, 2405, 2565, 2748, 165, 2408, 193, 1588, 3492, 3257, 2490, 3849, 3494, 1099, 3264, 3850, 2986, 3069, 1483, 3623, 3708, 3269, 3503, 2910, 3626, 3383, 3890, 3508, 3509, 439, 472, 642, 362, 630]. **pseudo-aléatoire** [1900, 322]. **pseudo-aléatoires** [762, 284, 1588]. **Pseudo-Casuali** [991].

pseudo-disturbance [1152]. **Pseudo-Inversen** [1035]. **Pseudo-Random** [497, 946, 2327, 2915, 267, 2144, 2243, 1606, 904, 544, 1027, 1101, 1208, 181, 1416, 239, 183, 760, 586, 2032, 3290, 216, 2850, 2926, 3651, 551, 4031, 1514, 3819, 1519, 1820, 409, 2933, 3016, 771, 772, 3420, 243, 3316, 353, 380, 3567, 865, 355, 329, 2525, 2947, 2627, 2958, 3796, 1381, 4058, 1187, 2086, 131, 2808, 2468, 657, 615, 876, 206, 4059, 929, 3694, 361, 391, 1087, 743, 1048, 2109, 229, 4018, 1582, 571, 2480, 346, 536, 2662, 136, 574, 1589, 1673, 2231, 2232, 427, 1145, 1201, 808, 3376, 429, 1053, 1147, 3625, 1262, 941, 2573, 754, 2764].
Pseudo-random
[3638, 1496, 503, 217, 3544, 2261, 2172, 1117, 2511, 1527, 1438, 2608, 1444, 1732, 3997, 1245, 1641, 77, 1556, 2387, 2634, 837, 877, 3595, 3053, 933, 3121, 1777, 2654, 2655, 192, 2119, 2900, 2754, 2834, 2568, 810, 1149, 1320, 1322, 1407, 3142, 1794, 2135, 2022, 1686, 3277, 3991, 3148, 3519, 4065, 3393, 2580, 3721, 2918, 2149, 1497, 2026, 677, 909, 104, 3816, 3404, 721, 3777, 3168, 3542, 1422, 3294, 3543, 297, 3295, 3901, 1341, 439, 550, 587, 3724, 3299, 407, 113, 218, 1346, 3970, 153, 1285, 242, 184, 768, 770, 1168, 1289, 1357, 478, 3562].
pseudo-random
[917, 2787, 1944, 1235, 3789, 224, 2519, 3324, 3432, 2287, 3199, 3326, 1008, 1636, 2948, 248, 1012, 1180, 2454, 2955, 2628, 1849, 3439, 3442, 3337, 3220, 3748, 3798, 2385, 284, 456, 796, 3836, 3044, 1758, 3449, 2301, 698, 800, 801, 802, 1190, 419, 2306, 492, 258, 3463, 665, 803, 666, 3918, 3698, 3055, 882, 3847, 3601, 3602, 2653, 4041, 1199, 345, 572, 4043, 3359, 2229, 2405, 2565, 2748, 165, 193, 3257, 2490, 1099, 3264, 2986, 3069, 1483, 3623, 3708, 3269, 3503, 3626, 3508, 3509, 630, 362].
Pseudo-random-number [3209, 2887, 2311]. **Pseudo-Randomness** [2604, 3185, 2792, 447, 1695, 3584, 1561, 3237]. **pseudo-uniform** [1028]. **Pseudo-Zufallszafflen** [1055]. **Pseudo-Zufallszahlen** [439, 472, 642]. **pseudoentropy** [3705]. **pseudoinverses** [1035]. **pseudonoise** [2944]. **Pseudoprime** [3728]. **Pseudorandom**
[2420, 2836, 2496, 2837, 2994, 3390, 1897, 3632, 3713, 3893, 852, 2240, 3520, 2326, 3394, 2025, 2146, 3396, 3813, 3529, 3930, 4007, 2920, 3642, 3643, 3401, 3775, 907, 908, 821, 2028, 3165, 1274, 2030, 1156, 1215, 1335, 2588, 2925, 3967, 549, 2684, 2686, 2507, 2162, 3655, 4069, 1716, 1222, 1618, 1619, 1620, 1623, 1719, 1922, 2043, 2046, 2049, 2165, 2259, 2263, 3008, 3179, 2169, 2344, 2051, 2266, 2348, 3012, 766, 2693, 1067, 824, 2441, 863, 2697, 1353, 1434, 1522, 3557, 1524, 1823, 2779, 443, 3558, 3659, 3729, 2447]. **Pseudorandom**
[2857, 4052, 3560, 3994, 2602, 2448, 3732, 1826, 1827, 1936, 2355, 2060, 2177, 4053, 3095, 1122, 3664, 1943, 4070, 3736, 1175, 3196, 1840, 2711, 2366, 869, 4012, 1452, 1734, 3575, 2613, 332, 3438, 4083, 3672, 1547, 1739, 1844, 3031, 1742, 3334, 651, 3872, 3582, 3441, 2378, 1551, 1971, 872, 3876, 3877, 520, 521, 653, 654, 873, 3682, 2081, 2082, 2083, 2727, 3040, 452, 2543, 2544, 2883, 1647, 3447, 3749, 4037, 607, 1298, 3685, 3833, 3834, 2733, 3687, 1301, 2208, 797, 798, 3690, 1565, 1868, 1982, 2094, 2095, 2210, 2469, 2640, 2736, 2966, 1567, 1765, 3838, 3457].
Pseudorandom
[3692, 930, 3119, 2741, 3695, 1136, 1990, 420, 1475, 2107, 1395, 2649, 3474, 1665,

3242, 885, 886, 1097, 887, 2001, 2478, 712, 3064, 2487, 2659, 2406, 1313, 1400, 1585, 1671, 1885, 2124, 3137, 3263, 2128, 2494, 2670, 1146, 495, 2987, 1889, 3271, 3889, 3851, 1681, 911, 2760, 1055, 1403, 2672, 1893, 1601, 3960, 1266, 1408, 1489, 2021, 499, 2324, 2139, 2912, 1490, 1409, 1688, 3715, 3855, 2997, 3521, 3633, 3716, 3773, 991, 2024, 1607, 2919, 3964, 1059, 1060, 1699, 3536, 402, 1801, 3859, 4026, 2681, 3722, 762, 2849, 1916, 470, 2035, 2339, 1707, 1708, 471, 4027, 472]. **pseudorandom** [3298, 473, 1110, 3654, 4050, 2258, 2508, 912, 1427, 1511, 1621, 1622, 1624, 1625, 1717, 1718, 1720, 1721, 1722, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1923, 1924, 1925, 1926, 1927, 1928, 1929, 2044, 2045, 2047, 2048, 2166, 2167, 2168, 2260, 2262, 2264, 2340, 2341, 2342, 1345, 1347, 2265, 2345, 2688, 1931, 2050, 2170, 2267, 2346, 589, 590, 322, 3783, 1819, 2510, 1286, 1230, 1287, 1351, 2350, 2351, 862, 3905, 1355, 3785, 2937]. **pseudorandom** [556, 379, 2856, 774, 185, 642, 3973, 2783, 2514, 2784, 3184, 3731, 3820, 3426, 4034, 3563, 3564, 2061, 2063, 2277, 2279, 2280, 2357, 479, 2606, 2282, 867, 1440, 1948, 382, 2520, 3025, 415, 827, 1533, 1949, 2182, 356, 2183, 1293, 2945, 1838, 1369, 2187, 2188, 2526, 1450, 3977, 1241, 3205, 1453, 2453, 4054, 600, 601, 1373, 2950, 2073, 3332, 2296, 1183, 1297, 2624, 1550, 484, 871, 3581, 3217, 3797, 3873, 3980, 4000, 3218, 1380, 1462, 1748, 2078, 1856, 1976, 1977, 2461, 2541, 2542, 2384, 2386, 2803, 3041, 3110, 1858, 3878, 2805, 3112, 4001, 4075, 1558, 3688, 3343]. **pseudorandom** [1015, 3880, 2209, 658, 878, 1044, 1133, 1251, 1252, 1304, 1386, 1387, 1389, 1470, 1564, 1566, 1762, 1763, 1865, 1981, 2093, 2547, 2548, 2549, 2637, 2638, 2639, 2738, 2967, 3232, 1766, 3455, 3456, 3458, 618, 3755, 3916, 3839, 1659, 526, 2101, 839, 972, 459, 1991, 1137, 1662, 1477, 1092, 1573, 1047, 881, 4061, 3700, 2557, 3123, 708, 2401, 3478, 2223, 2976, 1399, 3481, 3604, 4062, 2977, 626, 987, 3807, 4020, 4042, 4003, 1783, 1314, 2009, 2984, 1787, 2665, 940, 3705, 3260, 3261, 3497, 2123, 494, 4004, 713, 2233]. **pseudorandom** [1595, 2129, 2130, 2235, 2413, 2493, 2015, 2988, 3138, 2758, 233, 812, 4046, 1600, 2018, 3545, 3375]. **pseudorandom-number** [2672]. **Pseudorandomness** [2993, 2239, 3402, 3644, 4029, 726, 2698, 2445, 2513, 3939, 3668, 3974, 2521, 2609, 2706, 2611, 2621, 2198, 3443, 2546, 1653, 2667, 3987, 2576, 2145, 2444, 3944, 3136, 2756, 2136]. **pseudozufallsvektoren** [1357]. **Pseudozufallszahlenfolgen** [624]. **psevdosluchainykh** [351]. **PSI** [1433]. **PSO** [4071]. **PSW** [3728]. **PUB** [1869]. **Public** [2332, 916, 2518, 1983, 2555, 880, 3320, 2453, 3911]. **Public-Key** [916, 2518, 2555]. **Publications** [262, 394]. **Publicly** [3859, 3170]. **Published** [3742]. **PUF** [4049, 4060, 4040, 3920, 3952]. **PUF-TRNG** [4060]. **PUFs** [3986]. **Pulse** [3551, 1836, 679, 3552]. **Pulse-Excited** [3551]. **Pulse/Data** [1836]. **Pulses** [520, 521, 3379]. **punched** [36]. **punctured** [3836]. **Pure** [3913]. **Purpose** [1086]. **Purposes** [4005, 2957]. **PVT** [3483]. **PVT-variation** [3483]. **pW** [3411]. **pyramids** [1467]. **Python** [3793, 3678, 2381, 2382, 4293].

Q.R.N.G. [3516]. **QRNG** [4077, 4067]. **Qs** [3663]. **QTPM** [4081].

Quadratic [2043, 2047, 2264, 661, 2098, 1658, 845, 1210, 1622, 1722, 1925, 2044, 2342, 1284, 2265, 1071, 1128, 975]. **Quadrature** [919, 789, 735, 1043, 396, 2515]. **Quality** [2147, 3541, 4069, 1833, 3996, 2707, 3824, 2081, 1095, 3132, 3256, 2987, 3891, 3278, 3395, 1916, 2590, 1945, 1949, 2182, 3206, 3328, 1969, 3587, 1976, 609, 2476, 2477, 2488, 2566, 2988, 2991]. **quanta** [1220]. **Quantendynamik** [11]. **Quantifiers** [3295]. **Quantis** [3704]. **Quantitative** [3150, 742, 4269, 3798]. **quantity** [227]. **Quantum** [3510, 3511, 3628, 2839, 3515, 3535, 3161, 3782, 3419, 3907, 3995, 1631, 3198, 3434, 3673, 3745, 3681, 3879, 4059, 1994, 3598, 3804, 531, 2656, 3127, 3609, 3135, 3379, 4081, 4023, 4072, 3387, 3629, 3403, 3723, 377, 3178, 3726, 3905, 3427, 3429, 2522, 3572, 3197, 11, 4080, 3686, 3751, 3450, 3467, 4061, 3480, 2825, 2563, 3360, 3612, 3366, 4021, 3370, 3706, 3618, 3068, 3377]. **Quantum-Mechanical** [531]. **Quantum-Safe** [4059]. **Quantumlike** [707]. **quark** [4197]. **'quasi** [2591, 906, 585, 3416, 2436, 116, 4071, 4257, 4265, 2798, 2090, 876, 1764, 4207, 4246, 1474, 2217, 1254, 1580, 1878, 1583, 3806, 2003, 2407, 315, 2906, 1317, 465, 1605, 2244, 905, 4270, 3937, 4231, 1358, 221, 222, 324, 1828, 2356, 4203, 2515, 2283, 2284, 2615, 2716, 3436, 2622, 1558, 3947, 4187, 4214, 4236, 2890, 3759, 1668, 2000, 1679, 496, 1263, 2871, 3207, 99]. **Quasi-** [1474]. **Quasi-Convergent** [315]. **Quasi-Monte** [4257, 4265, 4207, 4246, 1878, 3416, 2436, 2090, 876, 1764, 2217, 1583, 3806, 2407, 2906, 465, 4270, 4231, 4187, 4214, 4236, 905, 1828, 2515, 2716, 3436, 2622, 3947, 2890, 496, 2871, 3207]. **Quasi-Monte-Carlo** [99]. **Quasi-Random** [906, 4071, 1254, 2003, 1317, 585, 116, 1580, 1605, 2244, 3937, 1358, 221, 222, 324, 2356, 4203, 2284, 2615, 1558, 3759, 1668, 2000, 1679, 1263]. **quasi-white** [2283]. **quasicrystals** [2701]. **Quasigroup** [3111]. **Quasigroups** [3557]. **Quasirandom** [2574, 1331, 2152, 3537, 1228, 2212, 2893, 1781, 3287, 2791, 1379, 1865, 1868, 1879, 2115, 576]. **Quaternion** [3495]. **quatrième** [4090]. **Quebec** [4177, 4229]. **Query** [450]. **Quest** [1354, 3517]. **questions** [85]. **Queue** [993, 1963, 1964, 1025, 2776, 967, 3373]. **Queueing** [1410, 1248]. **Queuing** [1492, 622, 805]. **Quick** [2041]. **QuickCheck** [3945]. **Quickly** [1934]. **Quicksort** [2506]. **Quinary** [929]. **Quincunx** [3465]. **Quintessential** [3465]. **quintic** [3089]. **quotient** [1246]. **quotients** [3654, 1249]. **QX** [4072].

R [2149, 4006, 3778, 2850, 2926, 3211, 3335]. **R16** [809]. **R18** [772]. **R24** [865]. **R52** [1113]. **R53** [1114]. **R57** [1173]. **R58** [1187]. **Rabbit** [3073, 2765]. **Rabin** [1325, 3728]. **Racah** [425]. **Rackoff** [1858]. **Radial** [348]. **Radiation** [338, 11]. **Radical** [324]. **Radical-inverse** [324]. **radio** [498, 482]. **radioactive** [2907]. **Radisson** [4131]. **Radix** [2183]. **Radix-** [2183]. **RAGE** [3120]. **RAGuard** [3989]. **rake** [3319]. **Raleigh** [4167]. **Ralley** [1084]. **Ramage** [2903]. **Raman** [3535, 3782]. **RAMs** [3315]. **Ramsey** [2409]. **RAN1** [2241, 2324]. **Rand** [1306, 71, 89, 3265, 1372]. **RandNLA** [3864]. **Random** [3510, 3511, 3628, 1402, 3388, 1264, 1323, 497, 814, 1150, 1406, 2322, 1151, 3512, 579, 399, 293, 4047, 2134, 2237, 3768, 1487, 1685, 1206, 103,

108, 109, 110, 111, 123, 124, 125, 126, 895, 2497, 2839, 3515, 3769, 3770, 3713, 3961, 4006, 542, 755, 756, 817, 897, 898, 899, 900, 946, 3145, 3854, 1327, 3894, 2577, 2675, 12, 3149, 2140, 2327, 3150, 2763, 2915, 2579, 2998, 3895, 3896, 295, 267, 349, 2144, 3394, 3395, 4082, 3523, 2841, 3075, 3524, 3635, 757, 1329, 3525, 401, 500, 582, 1494, 435, 2243, 2421, 180, 819, 949, 1606, 1692]. **Random** [2147, 2245, 2331, 2423, 2148, 1495, 1152, 904, 1413, 544, 3815, 2332, 3774, 1027, 1101, 1208, 3531, 181, 237, 3400, 1416, 3533, 2333, 2677, 2334, 2766, 2846, 3001, 3159, 906, 319, 1418, 1104, 2847, 3534, 2153, 2154, 1799, 3160, 1499, 3535, 239, 240, 502, 1419, 1903, 2921, 1701, 1702, 2248, 1500, 854, 183, 3644, 760, 403, 761, 3538, 1212, 586, 3405, 4048, 2427, 2583, 3166, 3286, 3407, 3646, 4025, 4066, 2336, 3408, 3540, 3409, 3647, 376, 2584, 3648, 320, 2032, 2428, 1276, 1214, 1609, 2249, 2337, 2429, 3649, 3290, 1277, 3169, 1912, 241, 216, 404, 469, 3082, 548, 2769]. **Random** [1279, 1337, 2252, 2253, 1706, 2036, 951, 1504, 1918, 1216, 1502, 2038, 2850, 2926, 1340, 1709, 1919, 2505, 3175, 3651, 3818, 3936, 4008, 4078, 3410, 1107, 1217, 1218, 1424, 1614, 1615, 1713, 1806, 2159, 2256, 2771, 3005, 3297, 3779, 4068, 1280, 2772, 551, 636, 30, 2160, 271, 2161, 2928, 4028, 3085, 3086, 3087, 3176, 3301, 3548, 723, 1065, 1158, 1342, 2040, 2687, 1617, 2431, 1343, 2041, 2163, 2164, 1509, 1221, 1426, 1344, 1716, 2432, 2343, 3782, 2433, 2434, 2775, 3549, 3551, 4031, 3181, 1514, 2349, 3009, 4009, 1161, 1112, 1113, 1114, 2691, 3010, 3182, 3011, 2692]. **Random** [298, 3658, 1033, 1115, 1517, 1430, 378, 3553, 3819, 2597, 440, 3971, 300, 350, 725, 554, 1118, 860, 1519, 506, 1432, 1520, 3418, 3419, 49, 1932, 1119, 275, 1820, 2696, 596, 323, 409, 864, 2933, 1521, 2353, 2777, 3310, 303, 826, 1352, 3016, 4051, 3556, 769, 1728, 771, 772, 1167, 1232, 1525, 3420, 2780, 640, 685, 3972, 3993, 4032, 2274, 200, 243, 244, 144, 686, 445, 3559, 3730, 1120, 1437, 3183, 3422, 3423, 3314, 643, 413, 508, 2354, 2603, 3019, 1290, 3316, 65, 66, 74, 3662, 325, 353, 354, 3733, 557, 687, 3020, 380, 3094, 3186, 3822]. **Random** [1362, 3565, 597, 915, 777, 2278, 4203, 2281, 1731, 2605, 1439, 2066, 245, 1830, 1941, 1942, 3567, 3823, 3735, 865, 4010, 2362, 3321, 3188, 3024, 3427, 1832, 1833, 1946, 2863, 3667, 3428, 3190, 3790, 4035, 279, 327, 3995, 598, 202, 1074, 2790, 154, 1532, 1630, 1365, 355, 3996, 2707, 329, 330, 383, 2708, 2709, 2864, 3824, 155, 2184, 2710, 3430, 2450, 118, 2525, 1077, 1367, 3669, 3670, 516, 4071, 1538, 1633, 2364, 1956, 3200, 3791, 1078, 2946, 1449, 1539, 868, 1540, 1634, 2189, 2947, 1841, 3740, 3202, 2612, 779, 828, 870, 1543, 732, 921, 1370, 1735, 3574, 2451]. **Random** [225, 517, 647, 1737, 1455, 1544, 3793, 2288, 1545, 560, 648, 1010, 1125, 481, 3029, 1242, 1295, 1548, 1639, 1741, 2195, 2295, 2371, 2373, 2374, 2375, 2377, 2456, 2457, 2529, 2617, 2618, 2619, 2620, 2717, 2718, 2870, 2871, 3033, 3035, 3105, 3107, 3207, 3330, 3577, 3578, 3674, 3795, 3826, 3998, 4014, 3673, 830, 1013, 3794, 3869, 3329, 1845, 1079, 1740, 649, 923, 1847, 3208, 3333, 2075, 1181, 3210, 3978, 3212, 1743, 1744, 2719, 3336, 2627, 3214, 3215, 3679, 2958, 3942, 3796, 249, 2630, 3744, 2796, 384, 4074, 694, 2379, 2466, 3745, 2798, 309, 358, 1552, 1381, 2077, 3875, 2380, 3680]. **Random** [3681, 2200, 3589, 97, 254, 280, 281, 282, 312, 337, 340, 450, 451, 523, 561, 695, 696, 791, 792, 970, 1080, 1081, 1184, 1186, 1464, 1645, 1852, 1853, 1854, 1855,

2079, 2080, 2460, 2538, 2800, 2879, 386, 606, 3684, 2202, 3223, 2204, 1648, 2728, 2731, 4058, 1649, 1466, 1187, 1469, 1043, 1557, 2086, 794, 2206, 389, 2087, 2732, 834, 1859, 562, 1132, 1299, 3592, 3799, 2088, 1188, 1300, 1384, 3114, 2389, 131, 417, 187, 457, 1084, 4038, 3228, 525, 390, 3341, 2808, 2551, 2641, 2739, 3691, 3881, 3115, 610, 739, 874, 2468, 418, 2302]. **Random** [3451, 3452, 657, 2635, 2636, 1863, 2092, 3231, 615, 876, 1764, 1867, 3914, 1767, 2304, 971, 2214, 3346, 343, 1569, 661, 1656, 3235, 206, 700, 4059, 929, 2552, 2891, 3460, 1392, 3461, 3694, 2394, 2099, 838, 1, 4015, 1192, 1472, 1770, 3120, 1986, 1086, 1660, 2470, 973, 2216, 3350, 2816, 1988, 2104, 1193, 361, 391, 458, 1989, 1087, 743, 365, 527, 1474, 1774, 4017, 3983, 3467, 3597, 3696, 148, 392, 2647, 703, 528, 3842, 3883, 621, 705, 1994, 2893, 529, 841, 3352, 1775, 55, 57, 2819, 262, 1996, 1048, 3470, 3471, 3472, 3473, 1093, 368, 2109, 229]. **Random** [3239, 1575, 934, 1017, 805, 1576, 2649, 3474, 3241, 4018, 1873, 2474, 3757, 3475, 3476, 3701, 2974, 2110, 3951, 3804, 1254, 3354, 3355, 1577, 709, 1095, 1197, 530, 369, 287, 2475, 2651, 2822, 982, 983, 1019, 1049, 1096, 531, 2898, 3244, 747, 625, 936, 3060, 207, 421, 422, 1581, 3124, 1198, 371, 748, 2402, 1582, 2114, 3482, 3062, 986, 2226, 534, 571, 2978, 462, 1879, 2480, 628, 424, 2483, 2485, 629, 889, 1257, 2003, 149, 394, 395, 535, 3358, 3483, 890, 1311, 208, 346, 536, 3249, 426, 2315, 537, 3128, 2564, 3611, 630, 3129]. **Random** [3920, 3952, 2660, 847, 891, 892, 988, 2316, 2317, 2405, 2662, 3250, 3251, 2902, 136, 373, 3363, 2983, 1479, 1480, 2010, 3253, 3364, 1142, 3132, 3254, 3491, 3848, 1587, 9, 107, 210, 3256, 3493, 168, 3367, 3368, 2904, 574, 669, 1051, 1589, 2409, 2832, 315, 3135, 1672, 3369, 3258, 3259, 1673, 2231, 2232, 3371, 1052, 3495, 1098, 427, 2124, 2835, 1145, 1201, 1317, 3616, 538, 539, 1592, 2567, 1202, 3374, 1675, 850, 715, 808, 1676, 942, 2234, 3376, 1318, 2492, 3378, 3622, 428, 429, 893, 1053, 1147, 1319, 1791, 3499, 3267, 752, 811, 70, 3268, 3380]. **Random**
[2417, 1260, 1793, 1598, 2319, 266, 944, 2671, 430, 3765, 3381, 3502, 3625, 3709, 3382, 1484, 1680, 3273, 3504, 851, 3385, 1262, 4023, 3386, 2570, 2419, 3862, 406, 3412, 941, 3387, 3767, 3959, 2571, 431, 1149, 1204, 1320, 1321, 1322, 1485, 3711, 2572, 2573, 3853, 632, 633, 1405, 316, 1407, 815, 717, 3389, 4064, 1265, 3925, 3142, 3143, 1894, 1486, 1326, 1683, 3144, 816, 3513, 3514, 1602, 1684, 3810, 754, 1267, 1794, 2135, 498, 3712, 2022, 2137, 3927, 3632, 1686, 1491, 901, 1024, 1687, 3276, 3277, 433, 434, 3991, 2325, 902, 3148, 3519, 1898, 1689, 2241, 1328]. **random**
[2913, 2328, 3771, 3812, 4065, 3992, 3522, 3717, 3718, 3772, 1268, 1899, 2142, 1056, 1057, 3074, 3634, 3393, 150, 3278, 581, 3151, 2580, 2581, 3856, 1493, 1604, 1690, 466, 675, 2764, 3526, 3152, 318, 2916, 2917, 3720, 3721, 1691, 3153, 1412, 2918, 1605, 2244, 2422, 3638, 3639, 3898, 3929, 853, 1496, 718, 583, 2149, 3814, 1497, 2844, 3279, 3280, 3399, 1414, 501, 2150, 3157, 3158, 3281, 3282, 1153, 758, 235, 3532, 820, 194, 1900, 1209, 2026, 182, 1498, 238, 677, 1696, 2678, 3002, 3078, 1698, 1103, 584, 71, 89, 950, 1210, 3079, 3776, 2425, 2767, 634, 909, 1700]. **random**
[104, 3283, 3816, 195, 1211, 503, 585, 3899, 2582, 1273, 1608, 1906, 3404, 1420,

721, 546, 678, 1063, 3164, 3285, 3539, 3777, 3778, 3080, 1909, 1910, 3167, 1275, 3168, 37, 3966, 3817, 214, 215, 3541, 1911, 2157, 547, 679, 3291, 680, 1704, 1278, 1611, 2033, 2250, 3170, 2034, 2158, 2251, 2338, 2503, 3004, 1028, 405, 3292, 3293, 3542, 1336, 1421, 1501, 1422, 3294, 3543, 1338, 217, 297, 1339, 1505, 1506, 1805, 3295, 3411, 994, 1423, 1503, 3544, 1612, 1613, 1710, 1711, 2685, 2770, 2851, 3723, 3901, 1341, 3546, 995, 996, 1029, 1064, 1106, 1108, 1109, 1219, 1712, 1807]. **random** [1920, 635, 997, 439, 550, 587, 683, 43, 3724, 3299, 1616, 3084, 1508, 3300, 3413, 407, 3725, 999, 1809, 113, 3415, 3088, 1425, 2773, 377, 2257, 1031, 3178, 3089, 218, 3302, 684, 1428, 2261, 1223, 1283, 1346, 588, 2930, 2774, 2435, 2589, 2590, 1066, 3550, 3937, 3180, 2853, 1429, 2932, 3970, 2437, 153, 1285, 2854, 724, 1162, 2171, 2438, 2439, 2440, 2593, 1725, 3552, 141, 1163, 1516, 2172, 2595, 1818, 1225, 1226, 1348, 242, 2053, 1227, 3904, 48, 60, 91, 92, 593, 594, 273, 184, 274, 1117, 767, 1229, 727, 3784, 768, 1069, 1350]. **random** [1035, 3013, 3727, 825, 2442, 2511, 1002, 2598, 3905, 116, 142, 2699, 770, 199, 219, 2446, 174, 476, 913, 958, 3018, 1168, 412, 2781, 3421, 2782, 1729, 1526, 1824, 444, 1288, 773, 775, 1005, 477, 1233, 1289, 1357, 83, 93, 478, 776, 2601, 3312, 3313, 1358, 3424, 3865, 2056, 2176, 3425, 3315, 1527, 3661, 221, 222, 324, 1438, 75, 1121, 2058, 2059, 3906, 3562, 688, 1937, 3096, 3319, 959, 3566, 2356, 2359, 1071, 1940, 2064, 3907, 381, 1528, 917, 2787, 2942, 3734, 778, 305, 689, 1944, 1073, 2944, 1529, 1831, 1834, 1945, 2517, 2789, 3788, 1441]. **random** [67, 76, 3666, 1235, 3789, 3189, 2608, 3323, 4011, 1236, 1629, 3569, 224, 3570, 1006, 3738, 1443, 1444, 1732, 2519, 3191, 1237, 2449, 1733, 1531, 2363, 3429, 2284, 2495, 1075, 2522, 3997, 3572, 1950, 1176, 331, 962, 3194, 3324, 3100, 1292, 84, 1177, 21, 1238, 95, 1123, 2185, 1447, 2945, 3432, 3325, 1448, 2186, 2285, 2286, 2365, 3573, 1007, 1955, 1957, 1038, 2287, 3197, 3198, 3199, 3326, 3201, 1008, 731, 26, 31, 32, 1451, 2866, 3976, 4013, 780, 920, 1009, 1240, 2867, 480, 2367, 357, 782, 1635, 307, 2369, 1636, 1454, 2948, 3792, 2453, 4095, 922, 1011, 1039, 248]. **random** [3908, 2712, 3102, 2949, 3030, 3103, 784, 1126, 829, 4055, 3434, 1376, 1640, 1846, 1965, 2191, 2196, 2291, 2292, 2293, 2294, 2372, 2376, 2615, 2616, 2715, 2868, 2951, 2952, 3104, 3106, 3910, 3327, 1012, 1180, 3435, 1127, 3206, 3328, 2454, 1960, 1961, 785, 482, 2872, 2874, 3037, 3209, 1966, 3827, 3675, 2623, 2534, 650, 2626, 3335, 3579, 2955, 3580, 3678, 4073, 2628, 3743, 1460, 2959, 4036, 1849, 519, 3439, 3109, 3440, 3583, 3586, 1746, 3828, 3874, 2797, 2960, 1244, 3442, 1245, 1641, 2199, 1969, 158, 3444, 334, 602, 18, 2722, 1642, 1643, 1749, 1851, 1972, 652, 1246, 3588, 3746, 3831, 3832, 251]. **random** [2536, 3337, 3338, 416, 3682, 226, 252, 253, 255, 283, 311, 336, 385, 448, 449, 486, 522, 655, 1129, 1185, 1553, 1554, 1555, 1644, 1750, 1973, 1975, 2299, 2382, 2540, 2723, 2801, 3039, 3445, 387, 1465, 2725, 3220, 3747, 3981, 3590, 3221, 3683, 3748, 3798, 1857, 2385, 2084, 2085, 2462, 77, 1556, 1753, 3225, 2387, 284, 697, 736, 1014, 3591, 2806, 2887, 1755, 160, 130, 489, 1651, 2205, 795, 455, 456, 833, 2388, 3113, 3686, 3751, 796, 1558, 3340, 609, 737, 1083, 3448, 2633, 924, 2089, 925, 61, 313, 3836, 835, 3044]. **random** [3754, 2467, 1758, 3449, 836, 2634, 28, 3342, 611, 3450, 2301, 3045, 3689, 613, 1302, 1759, 1864, 2209, 2810, 563, 564, 698, 800, 801, 802, 837, 877, 1190,

1563, 1655, 927, 928, 3453, 3234, 617, 2305, 3347, 3454, 2889, 662, 1570, 879, 3756, 419, 2306, 227, 3117, 2968, 3459, 1391, 2215, 360, 1134, 1657, 2740, 3349, 2393, 1572, 491, 1471, 1135, 162, 492, 258, 1085, 45, 2644, 1768, 3463, 1394, 1045, 3236, 3949, 2396, 2553, 2471, 2102, 566, 3595, 1307, 362, 364, 2308, 3464, 665, 803, 3051, 666, 702, 344, 3918, 1136, 228, 2646, 620, 2554]. **random** [3466, 1872, 1992, 1993, 260, 622, 367, 1194, 842, 623, 3598, 188, 2397, 3698, 2398, 1476, 974, 975, 189, 3353, 3950, 3053, 1091, 568, 933, 1397, 843, 3843, 46, 3055, 804, 2473, 134, 3121, 2894, 1664, 935, 977, 1196, 2556, 882, 1094, 706, 3600, 1309, 978, 3846, 3884, 3885, 3847, 3058, 668, 1018, 746, 710, 624, 2112, 1777, 532, 533, 569, 1579, 711, 1140, 2975, 3759, 135, 1875, 3702, 191, 493, 370, 3601, 3602, 1398, 1478, 1580, 1668, 1779, 2113, 2224, 2225, 2899, 3760, 2823, 2652, 2745, 2653, 4041, 1780, 1876, 2311, 2477, 1050, 3480, 846, 1877]. **random** [1255, 1256, 460, 2654, 2655, 2000, 3919, 263, 289, 461, 3805, 2227, 2312, 1199, 192, 345, 2479, 2824, 2313, 2656, 2825, 3607, 2826, 1584, 2486, 2562, 2563, 79, 2827, 3127, 3609, 2657, 2658, 572, 3610, 2119, 2747, 2828, 2900, 4043, 3359, 3360, 3612, 2901, 3953, 2229, 2565, 2748, 939, 2663, 2749, 2751, 2830, 2980, 2981, 2982, 3065, 3066, 3130, 3486, 3487, 3488, 3613, 3614, 3252, 3489, 848, 165, 3490, 1669, 1883, 2121, 1200, 3067, 3131, 3133, 3763, 3764, 3808, 2408, 193, 1588, 3492, 3366, 2488, 2566, 167, 1884, 3257, 4021, 2489, 2490, 1315, 989, 3134, 2833, 3955, 3370, 4022]. **random** [2754, 2834, 3849, 3494, 849, 3496, 2668, 2013, 2014, 2491, 1099, 3706, 3617, 36, 4004, 3956, 575, 631, 671, 1674, 3618, 714, 2127, 2907, 232, 1593, 177, 1594, 1886, 3068, 3264, 3619, 3850, 1790, 2669, 3377, 3379, 716, 463, 2986, 3069, 1483, 2568, 3266, 3498, 3623, 3708, 1888, 810, 2416, 2908, 1792, 2418, 20, 2320, 2757, 3070, 3501, 3624, 3269, 4045, 3503, 3071, 3270, 2569, 1679, 2910, 2759, 1599, 3626, 3383, 3384, 3506, 3890, 29, 3507, 2990, 3508, 3627, 3766, 3809, 894, 1263, 3509, 577, 2991, 1892, 3653, 4072, 1590, 176, 100, 268, 1028, 2842, 269, 170, 321]. **Random** [308, 129, 3742, 656, 363, 314, 3059, 2012, 2762, 3724, 2820, 2915, 294, 400, 2500, 515, 559, 483, 2884, 1756, 1862, 1878]. **random-access** [3191]. **Random-Bit** [1419, 547]. **random-difference** [20]. **Random-Number** [3648, 1609, 1342, 2687, 1731, 1538, 1633, 3745, 3223, 2206, 3914, 1994, 2110, 531, 1581, 1318, 3378, 1319, 2419, 1692, 1418, 403, 2552, 1900, 1103, 1608, 2033, 3723, 778, 2196, 2291, 2715, 3675, 655, 2723, 3445, 2889, 1660, 2102, 1307, 3598, 3360, 2320]. **random-pulse** [679]. **Random-Start** [3346]. **Random-Variate** [2978]. **random-walk** [2311]. **randomised** [1896]. **Randomization** [947, 948, 2032, 953, 1282, 2042, 3090, 1935, 644, 729, 960, 1535, 963, 968, 969, 976, 2752, 2906, 3532, 2027, 3415, 3937, 80, 1004]. **randomize** [2668]. **Randomized** [2052, 2694, 3561, 1369, 1840, 2794, 1758, 2208, 2307, 3864, 2716, 3436, 702]. **randomizer** [1513]. **Randomly** [866, 2097, 667, 2219, 1482, 22, 1842, 3437]. **randomly-shifted** [3437]. **Randomness** [3510, 674, 4005, 3768, 2996, 1026, 127, 3636, 2330, 63, 1904, 3161, 720, 2502, 3407, 1917, 1918, 3414, 1921, 2929, 3015, 1433, 1354, 2174, 685, 2604, 3185, 3317, 2861, 2610, 26, 38, 3740, 2865, 2792, 1371, 3677, 447, 3745, 2079, 2201,

2724, 2962, 3446, 1382, 1556, 1647, 524, 3879, 120, 1867, 3345, 2213, 2812, 3348, 3118, 3693, 1870, 285, 2892, 2395, 3468, 3597, 3696, 2971, 2650, 3701, 175, 2482, 2561, 1880, 3704, 2985, 2569, 3629, 3959, 4024, 2840, 3517, 3811, 467, 3000, 437, 1695, 213, 3403, 104, 3081, 1334, 3650, 1610, 3295, 42, 3969, 81, 1723, 3726, 441]. **randomness** [143, 117, 352, 1361, 3866, 1076, 1953, 23, 3204, 599, 3741, 3911, 786, 3109, 3584, 4080, 487, 2203, 3913, 1561, 3915, 839, 2645, 3237, 1473, 1661, 932, 3469, 2744, 3240, 2895, 2973, 3845, 164, 2828, 50, 3615, 940, 989, 3496, 3886, 2125, 4084, 51, 41, 2272, 507, 570, 3707]. **randoms** [903]. **'RANDU'** [724]. **RANEXP** [1940]. **RANF** [1123]. **Range** [2434, 8, 405, 1339, 1506, 1805, 1428, 2351, 1393]. **RANGEN** [2690]. **ranges** [2479]. **Rank** [1026, 1361, 3026, 3870, 3046, 3048, 3125]. **rank-** [3046, 3048]. **Rank-1** [3026, 3870]. **Rank-based** [1361]. **Ranking** [2148, 3972, 2175, 3689]. **ranks** [2380]. **ranlip** [2916]. **RANLUX** [2275, 2276, 1949, 2182, 2402]. **ranshi** [2176]. **RANTEST** [940]. **ranut** [2678]. **Rapid** [1974]. **rapides** [2664]. **rapidly** [74]. **rapprochés** [2196]. **Rare** [2848, 3530, 2928]. **raspredelenija** [35]. **Rate** [2252, 3829, 628, 3450, 3756]. **Rates** [1528, 1962, 290, 381]. **Ratio** [1026, 769, 1946, 2184, 828, 923, 417, 2304, 1675, 1401, 1945, 780, 2535, 1128, 1584]. **Ratio-of-Uniforms** [1946, 2184, 1675, 1401, 2535]. **Rational** [169, 3114, 2211, 2815, 3666, 1041, 3999]. **Ratios** [339, 3754, 1512]. **RAW** [3842, 3883]. **ray** [1930]. **ray-generators** [1930]. **rays** [1237, 1083]. **rBeta2009** [3778]. **RC4** [3151, 4008, 2596, 2935, 3219, 2631, 2732, 2964, 3594, 3802, 2108, 3845, 3887, 2126, 3500, 2989]. **RC4-Like** [2935, 2964, 2989, 3802]. **RC4A** [3845]. **RC6** [2521, 2609]. **RCR** [3983]. **RDRAND** [3963]. **Re** [2723, 3464]. **Re-seeding** [3464]. **reactor** [4093, 3552]. **read** [4049]. **read-write** [4049]. **Reading** [10]. **Real** [3714, 2162, 3181, 3428, 4035, 3612, 731, 2207, 2975]. **Real-Time** [3428]. **Real-Valued** [3181]. **realistic** [3726]. **realization** [3522, 3865, 3466, 2825, 2658]. **Really** [639]. **Reasonably** [1]. **Reasoning** [2845, 3245]. **receiver** [3319]. **Rechenautomaten** [176]. **recherche** [1375]. **Recipes** [1773, 2324, 2241]. **Reciprocal** [376, 378, 413, 390, 421, 422, 1373, 2317]. **Reciprocals** [748, 370]. **Reciprocation** [709]. **reciprocity** [1069]. **Recognition** [3368, 3384, 2156]. **Recommendable** [2457]. **Recommendation** [2998, 3074, 3634, 3165, 3691, 3881, 3955]. **Recommendations** [4005, 2144, 1921, 2929]. **Recommended** [2946]. **Reconfigurable** [3087, 3183, 3920, 3952, 3254, 2595, 2959, 3545]. **Reconfiguration** [3428]. **Reconstructing** [1349]. **Reconstruction** [2523, 3877]. **Record** [316, 1934, 4204, 2743]. **Recovery** [3780, 3903, 3761, 3900, 3236]. **recrystallization** [4065]. **rectangle** [1403]. **Rectangles** [2378, 3710, 2139, 1553]. **Recurrence** [373, 3707, 955, 1287, 1351, 930]. **Recurrences** [3187, 1374, 583, 1902, 2034, 2290, 2714, 2951, 2552, 2890, 2891, 3049, 3050, 1399, 2552, 2890]. **Recurring** [2070, 211, 3307, 799, 3233, 749, 2007]. **Recurring-with-carry** [2070].

récursifs [2664]. **recursion** [1520, 1006, 13]. **Recursions** [3095, 2082, 2083, 2031, 1977]. **Recursive** [2677, 2427, 3173, 3651, 3652, 1615, 2936, 2447, 3565, 2456, 2530, 3795, 2956, 603, 2210, 2902, 540, 3633, 3164, 3285, 2927, 3174, 3296, 1283, 642, 2285, 2286, 2365, 3573, 2949, 3103, 1846, 2191, 2193, 2292, 2372, 2722, 4075, 2093, 2095, 3916, 3245, 1784, 2663, 2750, 2751, 2829, 2830, 2980, 2982, 3065, 3066, 3362, 3486, 3488, 3614, 2664, 3266]. **recursively** [641]. **recycle** [1443]. **Redefining** [3597]. **Rédei** [3184, 3112]. **Redondo** [4219]. **reduce** [1515]. **Reduced** [3861, 113, 2605, 3830, 2734, 3761, 1148, 583, 2922, 1171, 1172]. **Reduced-Round** [3761, 2922]. **reducible** [1886]. **Reducing** [2502, 2185]. **reduction** [3563, 3564, 3433, 2532, 3943, 2828]. **Redux** [2769]. **Reexamined** [1436]. **Reference** [2143, 3306]. **Refutation** [3039]. **Regarding** [2983, 1265]. **Regency** [4210, 4289]. **Regenerative** [2027, 915, 918]. **REG≫** [4082]. **region** [1456]. **Regional** [4156, 3550, 4167]. **Regions** [1141]. **Register** [1215, 1335, 1111, 1034, 3014, 410, 1534, 2531, 651, 653, 873, 488, 3593, 3703, 1585, 2419, 2422, 1275, 3168, 1516, 726, 1036, 2282, 1009, 3585, 1643, 1749, 2078, 1304, 1388, 1565, 3801, 1776, 2112, 1067]. **Registers** [2585, 518, 1574, 3249, 3491, 2753, 3988, 1730, 2072, 3999, 333, 310, 3957, 3852, 1138]. **Regression** [1735, 3171, 3977, 746]. **Regular** [3401, 3775, 3851]. **Regularities** [486, 522]. **Regularity** [2942, 3308]. **Regularly** [3757, 3088]. **Rehearsal** [3140]. **Reinfall** [2442]. **reinforce** [4046]. **Reingold** [3796, 2654]. **Rejection** [1518, 445, 1436, 1832, 1946, 2067, 2180, 1125, 2077, 844, 808, 1891, 3853, 1023, 2917, 3902, 2055, 2273, 775, 3661, 1834, 3098, 3666, 1542, 1011, 1039, 2720, 1094, 979, 849]. **Rejection-inversion** [2180]. **Rejoinder** [948, 886]. **Rekursion** [1006]. **rekursiv** [641, 642]. **rekursiv-erzeugte** [642]. **Related** [1895, 3396, 330, 790, 901, 1915, 1424, 1170, 2868, 935, 977]. **Related-Key** [3396]. **Relating** [1730]. **relation** [1431, 3322, 13, 3958]. **relational** [2054]. **Relations** [1537, 494, 930, 1769]. **relationship** [1950, 1951]. **Relationships** [847, 556]. **Relative** [1228, 1018]. **Relatively** [2003]. **relativistic** [11]. **relativistischen** [11]. **relevance** [2170, 374, 2235]. **Reliability** [1419, 2463, 2465, 3118, 3576]. **Reliable** [3072, 3001, 3462, 3772]. **Remainder** [545, 105, 106, 1305, 2749]. **Remark** [269, 1113, 1114, 380, 1173, 865, 2791, 480, 308, 255, 1187, 700, 391, 620, 625, 1051, 809, 1262, 1428, 1722, 1113, 1114, 772, 1173, 865, 1187, 809]. **Remarks** [318, 906, 196, 3937, 250, 1855, 1386, 421, 1889, 3305, 2113]. **removal** [2282]. **Renaissance** [4196]. **rendering** [3702]. **rendus** [4090]. **renormalization** [781]. **Rényi** [405]. **Repeatable** [520, 521]. **Repeating** [2780, 224]. **Repetition** [3016, 2936, 2206]. **Repetitions** [1996]. **Replacement** [2077]. **replica** [3849]. **replica-exchange** [3849]. **Replicated** [3983]. **replication** [1025]. **Reply** [2593, 1538, 671]. **Report** [1797, 3645, 3983, 3468, 104]. **Representation** [2288, 3742, 3589, 973, 1907, 684, 273, 3999, 1477, 668, 1783, 713]. **Representations** [1904, 1603]. **Reprise** [3047]. **reproducibility** [1285]. **Reproducible** [1897, 3932, 854, 3823, 2081, 1990, 2560, 1976, 1991].

reproducing [3046]. **Reproduction** [991]. **Republic** [4236]. **request** [2840]. **requests** [1987]. **Require** [3987]. **Requirement** [2769]. **Requirements** [2642, 2971, 3826]. **Requires** [3664]. **requiring** [2787]. **rescaled** [2351]. **Research** [4098, 24, 299, 4222, 3823, 4146, 4101, 47, 73, 114, 115, 171, 172, 4272, 4161, 4096]. **Reseeding** [3677]. **reservation** [2586]. **Reservoir** [1967, 1202]. **reset** [3469]. **Residue** [4025, 3179, 758]. **residues** [585, 917, 13]. **resiliency** [4050]. **Resilient** [3858]. **Resistant** [3642, 3405, 3532, 3415]. **Resolution** [3459, 867]. **Resolution-stationary** [3459]. **resolving** [3572, 3598]. **Resonances** [2402]. **Resort** [4220]. **Resource** [2239, 3255, 2576, 2586]. **Resource-Bounded** [2239, 2576]. **respect** [741, 2404]. **Response** [1633, 967, 1870, 985, 2776, 702]. **Response-time** [985]. **restricted** [3573, 3613]. **restriction** [2980]. **Restrictions** [3659, 3130]. **result** [377, 742]. **Resulting** [30]. **Results** [1895, 2331, 1332, 104, 2269, 766, 2698, 3571, 3983, 1873, 2904, 4106, 427, 1697, 2922, 3541, 405, 2050, 2063, 381, 1563, 2306, 1659, 133, 3498, 2318, 2695]. **retrieval** [273]. **Retrospective** [511]. **return** [2681]. **Rev** [3474]. **Reverse** [2982]. **Review** [294, 2136, 400, 2500, 1797, 2154, 3004, 596, 1525, 507, 640, 1004, 3318, 3996, 515, 1539, 1540, 559, 2295, 483, 3742, 2884, 3042, 389, 1756, 1084, 1862, 2635, 3059, 135, 1878, 1311, 167, 168, 3707, 3082, 2048, 1533, 3202, 3798, 1780, 3619]. **Reviews** [895, 542, 2333, 319]. **Revised** [4242, 1173, 1072, 4248, 4250, 3074, 3103]. **revision** [3919]. **Revisited** [2999, 3967, 3571, 3672, 2559, 2146, 4057, 3950]. **Revisiting** [2324, 3831]. **RFC** [1921, 2929]. **RFID** [3149, 3964, 3286, 3304, 3332, 3750, 3591, 3463, 3367, 3368]. **Rhode** [4122, 4266]. **Rice** [1071, 3124]. **Richard** [170]. **rid** [2493]. **Riemann** [443]. **Right** [3371, 3676]. **Rigorous** [3238, 3698]. **Ring** [3635, 3593, 3342, 4015, 3505, 3856, 3423, 3941, 4056, 3338, 3496]. **ring-oscillator-based** [3338]. **Rings** [3179, 3268, 1705]. **Ripley** [1635, 3741]. **Riproduzione** [991]. **RISC** [4039]. **RISC-V** [4039]. **Risk** [3148, 2144, 3453]. **risk-based** [3453]. **RNA** [2987, 2988]. **RnaPredict** [2987, 2988]. **RNG** [1692, 3900, 1161, 3203, 2878, 4016]. **RNGAVXLIB** [3865]. **RNG≫** [4082]. **RNGs** [2422, 3780, 3903, 3413, 3971, 2802, 2403, 2481, 2484]. **RNGSSELIB** [3522, 3718]. **road** [1723]. **robots** [2661]. **Robust** [3276, 548, 3087, 3200, 3203, 3879, 1864, 2747, 3724, 3201, 1465, 2564]. **Robustness** [1340, 1710, 3221, 2214, 3505, 2305]. **Rockefeller** [4153]. **rocket** [256]. **Rodney** [3707]. **Roles** [2627]. **Ron** [3676]. **Roof** [2149]. **Root** [390]. **rooted** [1795]. **Roots** [794]. **ROP** [3989]. **Rosenbluth** [2938]. **Rotation** [1850, 2119]. **Round** [3645, 3861, 2925, 2605, 2702, 2706, 3830, 2734, 3761, 2922]. **Rounding** [2250, 4002, 3932, 2071]. **Rounds** [2924, 2703]. **Route** [3782]. **Routine** [1319]. **Routines** [789]. **RSA** [1325, 3064, 3269]. **RSA-Based** [3064]. **RSAEuro** [2143]. **rstream** [2952]. **Rudin** [3946]. **ruin** [962, 3204]. **rule** [242, 2569]. **Rules** [3003, 2361, 3026, 2713, 3870, 2794, 1043, 2811, 3125, 3247,

3357, 1535, 2532, 3437, 2533, 2622, 3046, 3048, 3126, 3246, 3606]. **Rumba** [3146]. **Rumor** [3821]. **Run** [1796, 1802, 1931, 2782]. **running** [3395]. **Runs** [237, 437, 505, 3180, 1003, 3348, 574, 809, 2913, 474, 1953, 53, 2797, 2960, 59, 56]. **Runs-Down** [1003]. **Runs-Up** [1003]. **Runuran** [3335]. **Russian** [3057, 351, 35]. **Russians** [3868]. **RV** [1238]. **RVGEN** [2536].

S [3159, 319, 1004, 1071, 446, 394, 870, 3744, 992, 2132, 3611]. **S-3800** [2132]. **Saarbrücken** [4126]. **SAC** [4250, 2605, 2861]. **SAC'99** [4218]. **Safari** [2395]. **SAFE** [3936, 4059, 2110, 4058]. **SAFE-NET** [4058]. **Salford** [1936]. **Salsa** [3146, 3860, 3861, 3830]. **Salsa20** [3155, 3156, 3528, 2924, 3571, 3752, 3761]. **Salt** [4188]. **Salzburg** [4207]. **Same** [4060, 370]. **Sample** [719, 1105, 3649, 637, 769, 3013, 59, 804, 36]. **Sampler** [591, 2038]. **samplers** [1802]. **Samples** [1216, 1996, 2003, 8, 432, 853, 65, 74, 18, 40, 135, 34, 232]. **Sampling** [578, 673, 945, 1150, 2019, 3961, 4066, 3647, 856, 1279, 1501, 2162, 272, 764, 765, 1116, 1518, 725, 49, 863, 1231, 513, 3787, 25, 3568, 2067, 1366, 1445, 3867, 869, 1967, 2379, 872, 3799, 1, 4015, 663, 3951, 885, 886, 887, 628, 163, 1202, 101, 632, 990, 1324, 1404, 3768, 2135, 896, 12, 1607, 240, 151, 43, 4030, 3088, 3938, 593, 594, 2055, 2273, 117, 66, 74, 75, 2284, 95, 157, 3433, 26, 31, 32, 1372, 3576, 2535, 1746, 1130, 159, 284, 3835, 28, 2809, 2392, 565, 260, 189, 1309, 2564, 2828, 988, 122, 374, 9, 107, 210]. **sampling** [137, 2127, 3138, 70, 4063, 29]. **Sampling-Based** [4066]. **Sampling-Vectorized** [3951]. **Samuel** [4262]. **San** [4249, 4276, 4137, 4183, 4268, 4228, 4208, 4232]. **Santa** [4088, 4178, 4252]. **SAR** [4231]. **Satisfied** [413, 556]. **Satisfying** [530, 462, 1349, 3351, 460, 13]. **Saturday** [4241]. **Saturday-Wednesday** [4241]. **Saunders** [3210, 2819]. **Savage** [2537]. **Saving** [3938]. **SC'11** [4280]. **Scalable** [3296, 3333, 3925, 3784, 3727, 2875, 2541, 2542, 2333, 3208]. **Scale** [2236, 4085, 790, 187, 10, 3075, 15, 1715, 4013, 96, 3942, 1465, 2207, 1085, 2648]. **Scale-sensitive** [2236]. **Scaling** [2310, 3369]. **Scan** [3585]. **Scan-based** [3585]. **Scatter** [3308, 2130, 2413]. **scattered** [377]. **Scattering** [3535, 11]. **Schedules** [672]. **scheduling** [1843, 3453, 4061]. **schemata** [2669]. **schemata-based** [2669]. **Scheme** [3400, 1988, 3068, 3443, 796, 1659, 3602]. **Schemes** [1821, 2546, 745, 1203, 3929, 1442, 2380, 159]. **Schneier** [3244]. **Schnorr** [1576]. **School** [2847, 4108, 649]. **School-Based** [2847]. **Schwinger** [2328]. **Sci** [1071]. **Science** [4111, 4222, 4116, 4104, 4114, 4117, 4120, 4135, 4140, 4146, 4152, 4162, 4185, 4194, 4198, 4219, 4223, 4274, 4289, 4295, 4281, 4126, 4118, 4173, 4102, 4247, 4253, 4238, 4106, 4141, 4142, 4124, 4217, 4205, 4237, 4105, 3698, 4164]. **sciences** [4227]. **Scientific** [4098, 3001, 1155, 4096, 1174, 1773, 2560, 4174, 3306, 2801, 4187, 4103]. **Scientist** [2838]. **Scientists** [645, 277, 1234]. **Scope** [2512]. **scores** [438]. **Scrambled** [3930, 4007, 3346, 3888, 3243]. **Scrambling** [2691, 3891]. **scramblings** [2813, 3923]. **screening** [3361, 2663]. **scroll** [3283, 3313]. **SEAC** [90]. **SEAL** [2693]. **Search** [3651, 1000, 1433, 3790, 836, 937, 938,

2685, 3174, 2590, 956, 3023, 730, 1375, 1846, 1558, 2899, 2661, 3613, 3614]. **Searches** [2689, 2285, 1456]. **Searching** [3995, 2949, 2902]. **Seattle** [4143, 4280]. **secant** [1807]. **Second** [4085, 4130, 31, 4224, 3118, 889, 4199, 4148, 4216, 3362]. **Second-level** [3118]. **second-order** [3362]. **Secondary** [2987]. **Secret** [2923, 1312, 2492]. **Secure** [3520, 2763, 3396, 1495, 3643, 4008, 4078, 2172, 2608, 2711, 3199, 3828, 3223, 4058, 2818, 3479, 3129, 1145, 1201, 3809, 2760, 4027, 3820, 3569, 1442, 2363, 4054, 1373, 3215, 3463, 3236, 3055, 2401, 1312, 4022, 3706, 2759, 3936, 1900]. **Securely** [3879]. **sécuritaire** [1900]. **Security** [4210, 3523, 3857, 3724, 2431, 1921, 2929, 3304, 3658, 2779, 2859, 2706, 3825, 3219, 4243, 2634, 2808, 2642, 3452, 3838, 3755, 2971, 1576, 3244, 3064, 2900, 4188, 4208, 4081, 3924, 4067, 4282, 4064, 2146, 2843, 3079, 4150, 1170, 3583, 1461, 796, 3343, 3349, 3355, 2977]. **Seed** [3893, 2427, 3567, 3371, 1154, 2519, 1776, 3494, 3565]. **Seeding** [1353, 2387, 3711, 1007, 3464]. **Seeds** [2801, 3917, 1240, 3356]. **seeming** [2645]. **Segmentation** [1793, 3037]. **Select** [2584]. **Selected** [4052, 4218, 2527, 656, 4248, 4250, 2267, 4242, 2970, 1261, 4250]. **Selecting** [1240]. **Selection** [1214, 3169, 272, 3010, 3972, 3787, 3567, 1469, 2092, 3171, 2374, 2622, 3689, 1015, 2473]. **Selective** [45]. **Self** [3166, 3733, 3701, 4247, 3384, 3899, 2600, 1825, 1440, 1530, 2386, 3601, 2009]. **self-adaptive** [3601]. **self-assembly** [3899]. **Self-Avoiding** [3733, 2600, 1825]. **Self-Excited** [3166]. **Self-Similarity** [4247]. **self-test** [1440, 1530, 2386, 2009]. **Self-testing** [3701]. **selfish** [3191]. **Selfridge** [3728]. **Semi** [1254, 1317, 471]. **semi-infinite** [471]. **Semi-Random** [1254, 1317]. **Semiconductor** [3352, 3258, 3370]. **seminar** [4091]. **Seminumerical** [2368]. **Semiparametric** [1482]. **sense** [875, 464]. **sensitive** [2236]. **Sensitivity** [2339]. **Sensor** [3012, 3452, 3828]. **sensors** [3610]. **Seoul** [4242]. **September** [4085, 4107, 4264, 4184, 4255, 4161, 4130, 4212, 4096, 4171, 4253, 4195, 4189, 4200, 4101]. **Sequence** [1496, 1331, 3644, 4025, 1614, 1716, 1228, 409, 443, 1534, 2711, 384, 386, 3946, 3119, 1088, 4018, 4076, 669, 3263, 2419, 911, 1056, 3158, 905, 584, 1701, 1702, 1275, 3168, 37, 471, 552, 588, 3180, 1068, 1230, 2350, 3307, 3312, 3313, 324, 1438, 3906, 3022, 867, 3736, 3569, 306, 2791, 1038, 3199, 3326, 1009, 357, 1373, 3332, 2534, 650, 733, 734, 2199, 1748, 1382, 2386, 453, 454, 1014, 2091, 3755, 3916, 1046, 3466, 1196, 3123, 1777, 1050, 1781, 3359, 50, 2489, 3621, 13, 1260, 3383, 2321]. **Sequences** [3510, 2993, 2138, 3275, 3391, 852, 267, 1496, 1027, 1101, 181, 237, 1416, 1901, 906, 2154, 183, 375, 468, 586, 3409, 549, 2507, 1618, 1111, 2592, 3010, 1118, 861, 3014, 2700, 143, 410, 1359, 510, 245, 328, 3824, 3193, 225, 3207, 447, 3582, 2798, 3877, 520, 521, 873, 605, 2543, 2544, 2883, 1556, 1647, 1298, 832, 2389, 3946, 2211, 2390, 2391, 2965, 3346, 2097, 2306, 929, 2216, 2741, 2742, 3695, 1087, 2217, 2893, 1663, 1254, 1097, 1585, 1882, 2008, 2752, 2409, 1317, 2234, 1319, 1889, 752, 3625, 211, 1794, 2238, 1409, 2913, 178, 2422, 1497, 235]. **sequences** [1417, 1694, 3536, 585, 1801, 2426, 3965, 3163, 1278, 1611, 1803, 1915, 1705,

217, 1707, 1708, 4270, 3654, 113, 1427, 1511, 1717, 1284, 589, 590, 3970, 1032, 2691, 3303, 726, 1069, 1431, 173, 301, 302, 408, 3092, 116, 1036, 174, 556, 2856, 641, 3973, 2601, 3560, 3093, 221, 222, 2515, 917, 2944, 827, 1241, 2070, 693, 3028, 2072, 1180, 1960, 1457, 2872, 1379, 2795, 3217, 3584, 3943, 2797, 1462, 1185, 387, 3684, 2203, 3944, 4037, 1558, 1757, 660, 799, 1303, 1385, 1388, 1563, 1565, 1760, 3233, 3692, 566, 2308, 1136, 3801, 3697, 1477, 568, 843]. **sequences** [881, 2821, 708, 624, 3243, 2476, 569, 1139, 3759, 345, 806, 1879, 2115, 2118, 2007, 2120, 2228, 2230, 2317, 3365, 1588, 3260, 494, 2567, 576, 1595, 3850, 1483, 810, 1679, 1890, 3626, 41, 812, 4150, 4255, 4242, 697, 736]. **Sequential** [1150, 272, 3972, 1935, 560, 784, 1126, 120, 501, 1213]. **Serial** [216, 52, 244, 2717, 877, 550, 1822, 117, 174, 411, 442, 1361, 2188, 1190, 1389, 1470, 51]. **Series** [1914, 170, 1740, 3742, 787, 250, 1986, 315, 231, 23, 1135, 20, 1599]. **Serpent** [2521, 2609]. **server** [2680, 2776, 1987]. **Service** [3515, 3516, 2769, 1025, 3450, 45]. **Services** [3241, 3320]. **ses** [1900]. **Session** [265]. **Set** [2677, 957, 2443, 2209, 2904, 1490, 727, 22, 3797, 158, 160, 1768, 666, 36]. **SETA** [4255, 4242]. **Sets** [2573, 2694, 3202, 3207, 2370, 365, 1586, 2755, 2139, 349, 1800, 42, 2436, 141, 276, 1828, 2356, 4203, 2179, 2615, 2533, 2622, 741, 1250, 1303, 1760, 1761, 2890, 3049, 567, 619, 974, 2133, 3202]. **Setting** [3371, 3576]. **seventeenth** [4122]. **Seventh** [1959, 4208, 4182]. **Several** [1910, 1835, 2365, 3679, 1507, 658, 1018]. **SFQ** [3382]. **SHA** [3645, 3837]. **SHA-3** [3645, 3837]. **Shadowing** [1726]. **Shamir** [2918]. **Shape** [822, 2220, 715, 1058, 855, 3912, 3444, 3252, 716]. **Shapes** [3729, 2892, 3558]. **Shapiro** [3946]. **Shared** [2492, 1801]. **Sharing** [2086, 1994, 3101, 3373]. **Shell** [2818]. **Shenzhen** [4279]. **Sheraton** [4121]. **Sherif** [2114]. **Sherman** [127]. **Shewhart** [1203]. **Shift** [2585, 1215, 1335, 1111, 1034, 1067, 3014, 410, 1036, 1534, 2531, 518, 651, 653, 873, 488, 3593, 1574, 2400, 1999, 3703, 1585, 3491, 2753, 3988, 2419, 2422, 1275, 3168, 1516, 726, 1730, 2282, 1009, 4054, 2072, 3999, 333, 3585, 310, 1643, 1749, 2078, 1304, 1388, 1565, 1305, 3046, 3801, 1138, 1776, 2112, 3497, 3957, 4046, 3852]. **shift-invariant** [3046]. **Shift-Nets** [2400]. **Shift-Register** [1111, 3014, 653, 488, 1585, 1275, 1516, 2282, 1009]. **Shift-Register-Sequence** [2419]. **shift-remainder** [1305]. **Shifted** [3357, 3437, 3606]. **Shifts** [2821, 3002, 3078, 161]. **shooting** [1698]. **shootout** [3931]. **Short** [239, 323, 409, 406, 4160, 1164, 600, 601, 4001]. **Shortest** [722, 1534, 2897]. **Shot** [2974, 3191, 3480]. **Should** [1197]. **Show** [2841, 1798]. **shown** [3768]. **Shrinkage** [3668, 3974]. **Shrinking** [1913, 2599]. **Shub** [2977]. **shuffled** [2489]. **Shuffles** [2732]. **Shuffling** [409, 745, 1493]. **Shunt** [338]. **SIAM** [4176, 4098, 1071, 4174, 937]. **sic** [2668]. **Side** [3857, 3405, 3236]. **side-channel** [3236]. **Sided** [485, 3605]. **Sieve** [4170]. **SIGACT** [4168, 4266]. **SIGACT-SIGMOD-SIGART** [4168]. **SIGART** [4168, 4266]. **Sigla** [957]. **SIGMOD** [4168, 4266, 4180]. **SIGMOD-SIGACT-SIGART** [4266]. **sign** [1958]. **Signal** [1365, 1980, 2644]. **signals** [754, 3777, 478].

signature [1860]. **Signatures** [880]. **Signed** [1603]. **significance** [1168]. **Significant** [259, 431, 2942]. **Significantly** [3861, 3541]. **signing** [2190]. **silico** [3627]. **SIMD** [3242]. **SIMD-Oriented** [3242]. **Similar** [3946]. **Similarity** [2335, 4247]. **SIMPL** [766]. **SIMPL/1** [766]. **Simple** [1486, 582, 1691, 1208, 1608, 910, 1615, 3821, 1079, 2539, 2386, 2086, 832, 3599, 2653, 2976, 1256, 3509, 2575, 853, 1153, 1803, 1108, 2437, 4197, 1288, 75, 3099, 2193, 2625, 3216, 623, 2486, 3252]. **simplest** [2073]. **simplexes** [3853]. **Simplicial** [3886]. **Simplicity** [2060, 2177]. **simplified** [3215, 1858]. **simplifying** [3705]. **Simply** [2704, 1841]. **Simscript** [766]. **simulate** [1526]. **Simulated** [2584, 1784, 2829, 1909, 1229, 3058]. **Simulating** [2836, 4006, 1419, 761, 1221, 1273, 553, 2888, 1391, 1089]. **Simulation** [4137, 4183, 4251, 4196, 4149, 1100, 2141, 2578, 2914, 3392, 1606, 543, 1061, 1271, 2334, 2848, 3537, 4192, 1218, 2506, 377, 1619, 2051, 2348, 3417, 638, 858, 300, 350, 863, 1231, 915, 777, 4245, 3823, 918, 1630, 2708, 2709, 4220, 1449, 869, 732, 921, 1370, 1735, 2451, 1548, 1963, 1964, 2192, 1040, 1638, 2528, 3032, 2794, 1971, 4147, 2077, 872, 656, 4206, 4097, 490, 4158, 2092, 3690, 2640, 4110, 4293, 2814, 4225, 4163, 1772, 1308, 3054, 4119, 4112, 4294, 885, 886, 4226, 2311, 4121, 887, 4166, 4181, 347, 3371, 2122, 4131, 4262, 432, 901, 1024, 4201]. **simulation** [1152, 3077, 1330, 1693, 2247, 2676, 3398, 3530, 213, 1911, 1502, 473, 1066, 274, 1288, 1120, 3734, 4096, 2517, 1531, 2284, 1176, 1291, 3100, 1955, 1454, 2952, 2075, 3581, 3912, 3689, 1759, 1981, 257, 2890, 1135, 622, 1396, 2111, 1666, 985, 374, 1591, 576, 751, 3624, 3270, 4110, 4163, 1756, 1862]. **Simulation-Based** [2451]. **Simulations** [3637, 1159, 1617, 3786, 3787, 3567, 1381, 2877, 1469, 3462, 3694, 3238, 1577, 2904, 429, 3767, 3142, 3768, 3393, 3075, 3541, 2157, 3544, 3175, 1725, 2351, 3905, 1168, 1825, 3730, 1363, 1943, 3427, 2185, 1372, 3327, 2873, 3827, 3942, 1969, 3680, 2392, 3595, 2397, 3698, 2112, 2312, 2489, 3849, 2013, 2014, 3508, 2018]. **simulative** [1755]. **simultaneously** [1794]. **SiN** [3223]. **Sinai** [2997]. **sine** [1993]. **Singapore** [4236]. **Singer** [4120]. **Single** [2687, 3799, 3363, 2586, 2776, 3309, 1309, 2225, 1876]. **Single-Photon** [2687, 3363]. **single-precision** [2225, 1876]. **single-resource** [2586]. **single-variate** [1309]. **singular** [3022]. **Sir** [4217]. **site** [3209]. **Six** [2132]. **Sixteenth** [4124]. **Sixth** [4174, 4228, 4177, 4088]. **Size** [3893, 719, 2162, 3521, 3773, 65, 74, 1951]. **sizes** [2458, 1476]. **sketch** [3121]. **sketch-based** [3121]. **SKIPJACK** [1797]. **Slice** [2809]. **Slot** [3868]. **sloth** [3911]. **Slovenia** [4195]. **Small** [2420, 3013, 3314, 3095, 1562, 3690, 2003, 3959, 42, 1360, 381, 3912, 283, 1249, 1303, 662, 974]. **Small-bias** [1562]. **small-deviation** [381]. **Small-World** [3314]. **smaller** [2186]. **Smart** [3876, 3223, 2767, 4272]. **Smart-Card** [3223]. **Smirnov** [405, 72, 64, 790, 98, 840, 190, 3605]. **Smith** [70]. **Smooth** [3406, 3625]. **smoothed** [3077]. **SNARKs** [4077]. **Snippet** [3301, 3709]. **Sobol'** [3193, 2476, 1331, 2791]. **SoC** [4066]. **Social** [2838, 3314, 2801, 4227]. **Society** [4093, 4160, 4088, 3742]. **socioeconomic** [257]. **Sofia** [4213]. **Soft** [3176, 3351]. **Soft-Core** [3176]. **Software** [3897, 3154, 2585, 2354, 827, 1446,

2619, 2620, 2718, 3035, 3107, 3870, 3678, 2632, 3111, 2204, 2463, 2465, 1656, 2742, 4100, 3273, 1626, 2787, 1238, 1375, 2885, 3339, 1570, 2823]. **Software-Oriented** [3154]. **Software/hardware** [3678]. **SOI** [3743]. **Sojourn** [2007, 2120, 2230, 2228]. **Solid** [517, 1772, 625]. **Solution** [2844, 2255, 132, 138]. **Solutions** [1415, 197, 105, 27, 1213]. **Solving** [1488, 3943, 934, 3958, 223, 1591]. **Some** [674, 1266, 1408, 150, 582, 904, 2678, 3002, 3078, 3159, 63, 1906, 910, 152, 297, 2926, 1340, 1711, 473, 3305, 766, 242, 864, 826, 2698, 1728, 556, 276, 2861, 381, 3570, 415, 355, 22, 2457, 2630, 256, 341, 342, 1975, 2724, 2461, 874, 418, 802, 1388, 1866, 2966, 1394, 3840, 1779, 2113, 2225, 537, 2983, 1142, 427, 943, 1889, 1605, 3963, 104, 405, 1710, 441, 2054, 198, 1528, 2183, 1838, 1368, 1038, 85, 2290, 3444, 3230, 3455, 132, 2895, 2750, 2123, 812]. **Sophie** [2881]. **Sophie-Germain** [2881]. **Sorrento** [4184]. **sort** [1253]. **Sorted** [949, 903]. **Sosemanuk** [3154]. **sound** [2364, 3839]. **Source** [1102, 3858, 3321, 3871, 653, 2222, 4084, 1207, 2767, 219, 3566, 3735, 4039, 2979]. **Sources** [1264, 1323, 2996, 30, 3418, 3881, 1254, 1317, 1334, 1551, 1851, 3913, 2810, 2314, 3955, 3496]. **sous** [804]. **Southeast** [4156, 4167]. **Sowey** [935, 977]. **SP** [3079, 3881, 3474]. **SP800** [2940, 3693]. **SP800-22** [2940, 3693]. **Spa** [4220, 2065]. **Space** [3187, 3111, 1688, 3416, 825, 689, 1567, 1765, 188, 2556]. **space-bounded** [1567, 1765]. **Spaces** [4006, 3973, 1562, 3046, 3063]. **Spacings** [366, 1953, 2294, 2616]. **Spanish** [134]. **sparing** [1143]. **Sparre** [238]. **Sparse** [1524, 2717]. **sparsest** [3739]. **sparsity** [3785]. **Spatial** [2529, 3081, 3741, 932, 3359]. **Special** [3018, 3734, 3795, 2338, 2896, 3057, 3266]. **Species** [186]. **Specific** [3781, 4256, 1012, 2018]. **Specification** [3975]. **Specifications** [2518]. **Specified** [2583, 1847, 2379, 3353]. **Specker** [3629]. **Spectral** [4006, 1706, 771, 772, 1173, 865, 1072, 3998, 3981, 452, 3344, 2896, 3057, 3380, 2435, 688, 3023, 2360, 2286, 2292, 2750, 2830, 3362, 1314]. **spectrally** [4042]. **Spectrum** [2940, 3441, 3885, 4067, 3843]. **Speed** [2420, 3316, 3869, 654, 3460, 3352, 101, 3622, 3380, 3814, 2767, 3178, 3302, 2855, 3423, 1733, 118, 2190, 129, 2534, 795, 227, 565, 1196, 2975, 122]. **Speedy** [1670]. **Sphere** [196, 201, 3742, 3589, 604, 848, 1587, 1144, 430]. **Spheres** [205, 1176, 3372, 270]. **Spherical** [341, 342]. **Spherically** [169]. **Spin** [3784, 3198, 738]. **spintronics** [3784]. **spirals** [1321]. **Splittable** [3722, 3847, 3807, 4020]. **Splitter** [2687]. **splitters** [3360]. **Splitting** [1639, 2170, 2235, 2568]. **sponge** [3640]. **spongy** [3802]. **sponsored** [4098, 4109]. **Spontaneous** [3499]. **Spooler** [2105]. **Spread** [4067]. **Spreading** [3821, 3319]. **spreadsheet** [2885]. **Spritz** [3802]. **SPRNG** [2333, 2541, 2542]. **sprout** [3356]. **Square** [826, 44, 390, 3451, 1714, 1715, 2600, 94, 1635, 3209, 88, 14]. **squared** [1360, 1178]. **Squarefree** [3008]. **Squares** [3946, 3970, 1447, 161]. **squaring** [1315]. **Squeeze** [884, 984, 831, 1094]. **SR** [3763]. **SRAM** [4049, 3321]. **SRS** [1953]. **SRU** [611]. **SSE2** [3522]. **St** [4152]. **Stability**

[319, 1821, 691, 394, 2242, 2614]. **Stable**
[761, 4068, 3568, 2520, 3025, 2452, 4017, 1273, 3297, 1391]. **Stack** [2894].
STACS [4126]. **Stage** [1104, 3549, 159]. **staircase** [1757, 1890]. **Standard**
[1500, 3649, 1426, 2518, 1869, 3837, 3700, 816, 680, 4030, 1955, 1637, 1662,
3950, 3096, 4221, 2482, 2561]. **Standards** [91, 2555, 167]. **Stanford** [4204].
Star [3006, 3026, 3125, 3247, 3357, 3126, 3606]. **Start** [586, 3346]. **Start-Up**
[586]. **STATCOM** [3166]. **State**
[1102, 3321, 3111, 119, 3132, 1207, 3900, 3416, 1963, 1964, 4110, 133, 3626].
state-of-the-art [4110]. **State-transition** [3132]. **States**
[3419, 2206, 3982, 3686, 3751, 3480]. **stationarity** [820]. **Stationary**
[350, 691, 787, 3101, 2614, 3234, 3459]. **Statist** [1273, 1071, 1039, 695, 696].
Statistic [127, 954, 1113, 840, 1270, 1229, 1635, 3741, 1042]. **Statistical**
[4005, 2838, 900, 3072, 2579, 3394, 818, 719, 854, 1706, 951, 2254, 1030, 587,
505, 1816, 2345, 3091, 954, 1112, 1113, 1114, 24, 47, 73, 114, 115, 171, 172,
299, 1033, 2596, 1230, 1351, 862, 2512, 555, 1165, 1727, 2778, 3555, 1434, 771,
772, 2700, 2937, 1168, 1003, 2783, 508, 3317, 777, 414, 245, 1173, 865, 1072,
1236, 1954, 964, 2865, 648, 2371, 3869, 787, 2627, 4281, 1648, 2463, 1187, 87,
2641, 801, 878, 1044, 1387, 1566, 3693, 285, 743, 2649, 2650, 3474, 2558, 845,
888, 2403, 2481, 2483, 2484, 2485, 3485, 3921, 1481, 2232]. **Statistical**
[809, 1053, 1147, 1262, 990, 4024, 4091, 3521, 3633, 1330, 1693, 2246, 2247, 2676,
3398, 236, 3413, 1809, 912, 1929, 2688, 859, 2351, 351, 4113, 1363, 3735, 1291,
2364, 4095, 2950, 3979, 2624, 4000, 1753, 2464, 2729, 2885, 2963, 3224, 1304,
3915, 4103, 1137, 1396, 2472, 2894, 393, 2663, 3808, 209, 989, 3850, 2017, 468].
Statistically [863, 869, 872, 885, 886, 887, 3839]. **statisticheskii** [351].
Statisticians [4107]. **Statistics**
[2020, 4091, 820, 3301, 2687, 4111, 3009, 1820, 4116, 4287, 507, 2274, 4113,
643, 4104, 2726, 524, 54, 703, 537, 292, 4141, 4142, 4107, 4124, 4099, 215,
4139, 1430, 4235, 2782, 1169, 1360, 2705, 3226, 2648, 2743, 1258, 2404].
STATLIB [1481]. **Steady** [1963, 1964]. **Steady-state** [1963, 1964].
Stealthy [3719]. **Stein** [2432]. **Step** [1359, 3119, 1133, 1389]. **steps** [504].
Stern [2923]. **Still** [359, 4035]. **Stimulated** [3535]. **STOC**
[4239, 4249, 4254, 4290]. **STOC'12** [4283]. **Stochastic**
[4128, 3962, 4109, 2255, 2051, 2594, 1932, 304, 915, 3790, 2451, 1963, 1964,
186, 1850, 97, 1467, 608, 4002, 389, 3462, 3694, 3238, 1308, 3054, 4076, 3356,
1673, 3270, 102, 1152, 3932, 3646, 4230, 4271, 198, 1356, 3730, 1120, 1843,
2952, 3327, 1960, 3748, 833, 360, 1134, 1657, 2740, 3698, 707, 62, 2017].
Stochastically [2696, 1031, 1162]. **Storage** [4280, 273]. **Storjohann** [3563].
STR [4079]. **Strahler** [1920]. **Strahlung** [11]. **straight** [1253]. **Strange**
[1703]. **strata** [3433]. **Strategies** [3780, 3903, 735, 3361]. **Strategy**
[595, 3832, 1985]. **Stratified** [1094, 3433]. **Stream**
[3512, 1488, 2911, 3147, 3154, 3156, 2765, 3641, 2427, 2768, 3091, 3097, 3111,
3222, 3594, 4259, 2108, 2557, 2655, 3500, 2909, 2989, 1681, 3274, 3157, 3305,
1229, 2520, 3025, 3197, 3941, 3585, 1468, 1754, 3448, 3802, 2979, 3264].
Stream-Cipher [2655, 1681, 3264]. **Streams**

[2263, 2266, 2952, 3694, 934, 3716, 3718, 2435, 3734, 2715]. **Street** [3832]. **Strela** [192]. **strength** [3801, 4061]. **strength-** [3801]. **Strengthen** [3687]. **Stretch** [3713, 3632]. **Streuung** [11]. **Stringency** [2831]. **Stringent** [989, 4057]. **Strings** [2507, 1894]. **Strong** [3629, 3275, 3391, 1027, 1101, 864, 2354, 2711, 2203, 3350, 4060, 1097, 1317, 2155, 1804, 3543, 2823]. **strongly** [1194]. **Structural** [1640, 2721]. **Structure** [544, 1618, 2706, 3795, 605, 798, 2469, 1585, 2987, 1055, 1204, 1320, 583, 2149, 3162, 3934, 1915, 1510, 1717, 1815, 1284, 2267, 3322, 2287, 1456, 2458, 2615, 2199, 2722, 1851, 1185, 658, 799, 1769, 1092, 1883]. **Structures** [3565, 873, 2290, 1646]. **stückweise** [624]. **student** [4073, 853, 870, 965, 40, 2908]. **Studies** [1209, 1042, 264, 356]. **Study** [1340, 3993, 520, 285, 4103, 1399, 3250, 3251, 3489, 2985, 2258, 2508, 3303, 767, 1536, 3037, 1461, 257, 372, 2123, 3384, 3372]. **Studying** [3591]. **Sub** [1474, 1204]. **Sub-** [1474]. **sub-lattice** [1204]. **subdivisions** [1930]. **Subgroup** [1280]. **subharmonic** [208]. **sublattice** [3322]. **Sublinear** [4009, 1124, 1294]. **Submission** [2877]. **Subroutines** [1560, 1861, 1481]. **Subsequences** [2268, 2269, 447, 2346, 1350, 1175, 4001, 4004]. **Subset** [3529, 3375, 2849, 3171, 1442, 4062]. **Subsets** [942, 3797, 3248, 1594]. **Subspaces** [2452]. **substitute** [3839]. **Substitution** [3685, 3834, 796, 4022, 2127]. **Substitution-Permutation** [3685, 3834]. **substreams** [2715]. **substructure** [3448]. **Subtle** [1798]. **Subtract** [1785, 3919, 1883]. **Subtract-with-Borrow** [1785, 3919, 1883]. **subtractions** [2071]. **subtractive** [753]. **Successful** [1354, 3832]. **successive** [2290, 2454]. **Such** [1, 479, 3039]. **Suggestions** [2204]. **Suitable** [1552, 3477, 3758, 3816, 1338, 1085]. **Suite** [3394, 3534, 2649, 2650, 3474, 3776, 4057, 3693, 2865, 3485, 3921]. **Suited** [1832]. **Suites** [3825, 697, 736, 178, 1032, 1588]. **Sulla** [16, 17]. **Sum** [3529, 3540, 1292, 2803, 562, 1192, 2572, 2137, 1063, 2849, 1944, 1442, 2185, 2294, 4062, 3375]. **Sum-discrepancy** [2803]. **sum-functions** [2294]. **summability** [48, 60]. **summands** [4043]. **summary** [71, 89]. **Summer** [265]. **Sums** [1413, 3400, 1922, 3011, 825, 3559, 687, 689, 1455, 1544, 418, 2737, 2304, 1575, 3985, 2983, 2570, 718, 3530, 238, 3088, 1814, 2854, 1227, 3017, 3184, 381, 305, 3429, 962, 3100, 84, 416, 339, 2205, 802, 2548, 2549, 2967, 3233, 3260, 577]. **Super** [2706, 3744, 2073, 655, 3445, 3874]. **SUPER-DUPER** [655]. **Super-luminescent** [3744]. **Super-Pseudorandomness** [2706]. **Supercomputer** [1678, 2132, 1686, 2056, 1473, 1661]. **Supercomputers** [1487, 1464, 1645, 1696, 1626, 1452, 1734]. **Supercomputing** [4190, 4155, 4153, 4179, 1570, 1656, 3810]. **Superconductive** [3611, 3382]. **supercube** [2392]. **superior** [1660]. **superiore** [470]. **supplement** [3844, 935, 977]. **supplies** [1660]. **Support** [2983, 2257, 3827, 1860]. **supported** [1941]. **Supposed** [1]. **suppression** [2257]. **Surface** [196, 241, 201, 2795, 604, 848]. **Survey** [1406, 3641, 1332, 1034, 511, 3875, 3446, 2213, 982, 983, 291, 2906, 1697, 2342].

survival [1031, 1162]. **SWAC** [92]. **Swan** [4181]. **Swarm** [4071, 3278, 3395]. **SWB** [1915]. **Swendsen** [2889]. **Switched** [3087, 3466]. **Switched-Capacitor** [3087]. **Switching** [756, 898]. **Switzerland** [4264]. **SX** [1986]. **SX-3** [1986]. **Symbolic** [4169, 1821, 4186, 4171]. **Symbolic-Numerical** [1821]. **Symmetric** [2332, 169, 4068, 3304, 597, 621, 3137, 853, 1063, 1130, 2404]. **symmetrical** [3034]. **symmetrized** [1751]. **Symmetry** [2830]. **Symposia** [4098]. **Symposium** [4176, 4122, 4127, 4132, 4138, 4143, 4148, 4159, 4168, 4177, 4182, 4191, 4209, 4216, 4229, 4234, 4239, 4249, 4254, 4267, 4276, 4283, 4290, 4085, 4155, 4268, 4124, 4093, 4169, 4088, 4217, 4111, 4116, 4161, 4113, 4104, 4086, 4114, 4117, 4120, 4135, 4140, 4146, 4152, 4162, 4185, 4194, 4198, 4219, 4223, 4273, 4274, 4289, 4186, 4126, 4089, 4171, 4175, 4106, 4199, 4188, 4208, 4141, 4142, 4087, 4202, 4139, 4211, 4266, 4101]. **Symptoms** [3510]. **synchronization** [3299, 3356]. **synchronized** [1682, 3389, 1992]. **Syndrome** [2172]. **Synthesis** [488, 3943, 310, 3957]. **Synthesizers** [2468]. **synthetic** [1934]. **System** [4268, 2240, 1100, 2141, 2578, 2914, 3392, 992, 1419, 4025, 2584, 3085, 3086, 3176, 2433, 957, 1938, 1939, 2062, 787, 2956, 2387, 3044, 2814, 1, 2105, 1475, 1143, 3368, 3167, 3293, 3411, 2770, 3300, 2932, 1032, 3552, 2598, 3730, 76, 3736, 2283, 1843, 1966, 3584, 1970, 1860, 2888, 3755, 3259, 80, 484, 466, 675]. **SYSTEM/360** [484]. **Systematic** [2285, 3231, 2889, 937, 938, 2899, 2310]. **système** [1032]. **systèmes** [343, 1588]. **Systems** [4168, 672, 1264, 1323, 4210, 1492, 2333, 586, 4066, 4264, 2769, 170, 1919, 2431, 4031, 3733, 915, 4256, 1850, 2728, 2086, 4171, 3460, 4163, 2655, 3250, 3251, 4189, 2835, 1682, 3276, 3521, 1272, 3541, 2586, 1723, 3785, 3320, 1441, 3789, 4035, 1955, 4224, 738, 1248, 343, 257, 3455, 3456, 3458, 3692, 4266, 1987, 3351, 1666, 3884, 3885, 1310, 749, 1588, 1143, 1671, 3849, 2013, 576, 2991, 3545, 3707]. **Systolic** [2150, 1269].

T [596, 640, 2067]. **T-Concave** [2067]. **T.** [542]. **Tabla** [134]. **Table** [2019, 3290, 834, 846, 79, 3848, 1324, 692, 519, 795, 45, 3764]. **table-free** [1324]. **Table-Hadamard** [3848, 3764]. **Table-Lookup** [834]. **Tables** [317, 6, 24, 299, 444, 21, 32, 2458, 2459, 18, 313, 2091, 2550, 135, 191, 69, 50, 70, 47, 73, 114, 115, 171, 172, 1360, 307, 2369, 7, 895, 134]. **Tabular** [3289]. **tabulated** [2018]. **tabulation** [3922]. **tackled** [2645]. **Tackling** [3986]. **Täfelungen** [1035]. **Tag** [3452, 3286, 3591]. **Tags** [3149, 3964, 3463, 3478]. **Tail** [954, 1113, 687, 1336, 3100, 3588]. **tailed** [3530, 1599]. **Tails** [2841, 883, 981, 3088]. **Taken** [8]. **Talk** [2513]. **tandem** [3282]. **tangent** [1958]. **Tap** [2419]. **taps** [2477]. **Target** [1698]. **Targeting** [3254, 3856]. **Targets** [341, 342]. **task** [1628]. **TaskLocalRandom** [3839]. **tasks** [3839]. **Tatzmannsdorf** [4113]. **Tausworthe** [1056, 1803, 1709, 763, 1513, 475, 1068, 1431, 2194, 798, 1044, 526, 1664, 1669, 574, 669]. **Tb** [3744]. **TDC** [4079]. **TDIST** [2908]. **TEA** [2922, 2605, 2702, 2703, 2786, 2862, 2734, 2303, 2131]. **Teach** [2769]. **Teaching** [3301, 3194]. **Technical**

[2143, 2066, 1855, 2801, 2109, 4199, 4215, 3827, 239, 323, 409, 406]. **Technique** [1436, 2067, 832, 3616, 1023, 75, 2787, 3916]. **Techniques** [4123, 3641, 3533, 3538, 4133, 2428, 1916, 272, 2711, 1549, 2801, 656, 4097, 3145, 4129, 473, 4033, 558, 157, 1591, 3624, 100]. **Technologies** [3975]. **Technology** [2333, 3968, 4104, 4279, 4260, 4261, 4205]. **Teil** [532, 533]. **Telegraphic** [1850]. **Temperature** [3358, 3607]. **tempering** [2493]. **temporal** [1905]. **ten** [15]. **Tennessee** [4130]. **Tenth** [4228]. **term** [3573, 2949, 3103, 3065, 3486, 3614]. **terms** [2286, 252, 1196]. **termwise** [3365]. **TERO** [3962]. **TERO-Based** [3962]. **Terrain** [2103]. **TES** [1650]. **Test** [4005, 2328, 2579, 1026, 127, 3394, 947, 948, 237, 3534, 239, 1274, 2030, 2162, 505, 766, 3016, 771, 772, 2780, 2936, 144, 597, 2861, 1173, 960, 865, 1072, 963, 3740, 2865, 968, 969, 3038, 44, 1186, 2961, 2727, 1648, 120, 877, 1658, 3118, 1870, 3917, 3468, 976, 2649, 3474, 1873, 1095, 747, 2402, 2114, 3485, 1880, 3921, 2831, 2905, 3259, 3263, 809, 88, 894, 3388, 717, 3144, 754, 235, 3776, 2155, 2681, 320, 1804, 474, 1345, 1346, 1931, 2435, 1163, 117, 174, 411, 442, 3421, 93, 688, 2360, 1440, 1530, 3189, 224, 415, 2945, 2286, 2188, 2074]. **test** [2628, 4057, 2537, 3981, 3683, 98, 2386, 2803, 1753, 3344, 1133, 1190, 1389, 1470, 3693, 2101, 46, 2894, 2895, 626, 2486, 2007, 2120, 2228, 2230, 2830, 3362, 1314, 2009, 51, 232, 29, 3144, 2940, 1630, 3976]. **Test-Pattern** [747]. **tested** [1910, 3427, 2365, 3832]. **Testing** [2579, 2144, 2581, 1274, 3169, 1065, 1342, 1343, 2163, 2164, 2692, 823, 412, 3565, 866, 3428, 155, 1956, 225, 1741, 2620, 2718, 3035, 3107, 3741, 3212, 3679, 2629, 519, 1299, 1084, 2551, 3460, 933, 1048, 2650, 3240, 2403, 2481, 2482, 2483, 2484, 2485, 2561, 629, 889, 1257, 2826, 136, 1672, 2128, 1146, 851, 499, 2497, 466, 1692, 3081, 1916, 3298, 999, 763, 1817, 91, 92, 351, 3421, 202, 3976, 2193, 2374, 3106, 1966, 4000, 158, 160, 130, 3915, 618, 701, 344, 2973, 3701, 1877, 572, 50, 165, 940, 2491, 4084, 3850, 2129, 2415, 1057]. **TESTRAND** [1084, 999, 1065, 1342]. **Tests** [674, 946, 63, 2157, 1706, 998, 637, 2268, 3728, 1434, 1522, 1003, 200, 83, 3317, 23, 3204, 1735, 648, 2196, 2294, 2371, 2529, 2717, 3212, 790, 1853, 2201, 2724, 2641, 3348, 3118, 3693, 932, 175, 2651, 1258, 1259, 2494, 2670, 4024, 467, 437, 1694, 104, 3164, 42, 3413, 3781, 953, 1282, 2042, 3090, 242, 2053, 1230, 1351, 862, 1166, 1070, 117, 1168, 1361, 3023, 3735, 1236, 2183, 1953, 1178, 2866, 2291, 2292, 2375, 2616, 785, 2296, 3979, 786, 4000, 793, 2209, 878, 1044, 2306, 1768, 972, 3464, 2744, 532, 533, 1874, 626, 164, 2229]. **tests** [2316, 2317, 2405, 2750, 989, 2833, 3886, 2013, 2014, 2125, 2196, 2079, 1004]. **TESTU01** [3042, 2620, 2718, 3106, 3331, 3035, 3107]. **Texas** [4116, 4208, 4121]. **Texture** [813, 959]. **Textured** [1793]. **theatres** [1255]. **thefts** [3725]. **Their** [513, 2711, 2529, 2627, 1243, 1968, 2468, 1055, 3, 3859, 3654, 1922, 1627, 3905, 4255, 4242, 2282, 3322, 448, 449, 1654, 2549, 3123, 370, 149, 3609, 2759]. **Theme** [4142]. **Theorem** [1413, 2710, 106, 3629, 238, 1069, 3562, 3429, 33, 3588, 3831, 416, 2807, 3230, 659, 1194, 2404, 2749, 1272, 2594, 3043, 2898]. **theorem-based** [3562]. **Theorems** [2020, 3400, 2154, 72, 355, 3742, 3589,

606, 2216, 2741, 701, 581, 1513, 64, 660, 190, 3620]. **theoretic** [2301]. **Theoretical** [778, 4126, 972, 3066, 1791, 3498, 2193, 2306, 665]. **Theorie** [246, 4, 4101]. **Theory** [4122, 4127, 4132, 4138, 4143, 4148, 4159, 4177, 4182, 4191, 4209, 4216, 4229, 4234, 4239, 4249, 4254, 4267, 4276, 4283, 4290, 3390, 1492, 180, 819, 2148, 4123, 2154, 4133, 637, 38, 3202, 833, 2100, 2101, 2216, 4154, 4247, 4019, 4094, 2904, 2409, 1261, 1054, 4101, 911, 102, 436, 4093, 4, 4202, 4160, 2027, 4230, 2061, 246, 961, 4095, 1547, 1969, 256, 4172, 742, 2738, 68, 1390, 1660, 566, 2107, 2973, 570, 2121, 3136]. **there** [2130, 2413]. **thereof** [3494]. **Thermal** [3382, 2959]. **thermostat** [3356]. **Things** [3984]. **Thinking** [2769]. **Third** [3645, 4221, 1257, 4202, 4193, 4242, 4095, 3614]. **third-order** [3614]. **Third-Round** [3645]. **thirty** [4209, 4216]. **thirty-first** [4209]. **Thiry** [4229]. **Thiry-Fourth** [4229]. **Thomas** [1084]. **Thomson** [236]. **thought** [3039]. **Thoughts** [685, 1573, 2088]. **Three** [1078, 1086, 3360, 1908, 692]. **Three-Point** [1078]. **Threshold** [2586, 3749, 3209, 3447]. **Throughput** [4069, 4079, 3677, 3283, 3624]. **Tied** [2769]. **Tight** [1933]. **tile** [3899, 2701]. **tilings** [1035]. **Tillich** [3237]. **Tilted** [3568, 4017, 3297]. **Time** [3527, 681, 2252, 1615, 2271, 2780, 2943, 3428, 732, 1740, 1967, 2218, 1688, 1689, 581, 2764, 3152, 2681, 3938, 2776, 1933, 775, 1458, 967, 3586, 3832, 1014, 2088, 3342, 3235, 1135, 985, 3612, 2007, 2120, 2228, 2229, 2230, 1788, 3618, 3377, 20, 1599, 3506, 3890, 1628]. **time-dependent** [3586, 3890]. **time-space** [1688]. **time-tested** [3832]. **Times** [2538, 945, 1628, 1992, 895]. **Timestamp** [2492]. **timing** [3351]. **Tina** [3524]. **tiny** [2131, 2761, 3507]. **Tippett** [43, 49, 28, 29]. **TKIP** [3887]. **TLP** [906, 1038]. **TLS** [4011, 4035, 3825, 3887]. **TODAES** [3596]. **today** [4134]. **Together** [4060]. **Token** [3791]. **Tolerance** [719, 3129]. **Tolerant** [3358, 3723, 1248, 3483]. **tomorrow** [4134]. **Too** [3780, 3903, 3599, 469]. **Tool** [3870, 2536]. **Toolbox** [3537]. **Toolkit** [3631, 2193, 3238]. **Tools** [3072]. **Top** [2546]. **Top-Level** [2546]. **topics** [935, 977]. **Topologies** [3493]. **topology** [2733]. **Tosser** [3431]. **Tossing** [3894, 1798]. **Touted** [2538]. **tracing** [1930]. **Tract** [70]. **trade** [1688, 4050]. **trade-off** [4050]. **trade-offs** [1688]. **tradeoff** [4054]. **Tradeoffs** [2943]. **Traffic** [506, 2776, 147, 3373]. **Training** [586]. **trajectory** [3356]. **Transactions** [4095]. **transcendental** [1368, 372]. **Transfer** [592, 33]. **Transfer-Matrix** [592]. **Transform** [1895, 2335, 3939, 2940, 3231, 851, 1704, 3738, 3353, 3764]. **Transformation** [657, 3346, 893, 3765, 1699, 721, 43, 927, 928, 1993, 2557, 2404, 1021]. **Transformation-Based** [3765]. **Transformations** [296, 2281, 2184, 2611, 794, 3633, 1268, 194, 2038, 1726, 3322, 1256]. **Transformed** [2349, 1946, 808, 1834, 3098, 2720]. **Transforming** [2847]. **Transforms** [537]. **Transition** [54, 3132]. **transmission** [95, 482, 1992, 4077, 498, 4150]. **Transparent** [3989]. **Transport** [3825, 1220, 1285]. **transportation** [3320]. **transpositions** [997]. **Trapdoor** [1099, 1054]. **trapezoidal** [3570]. **trapped** [4080]. **trapped-ion** [4080]. **Treatment** [2686, 1858, 87]. **tree** [1285, 1315]. **Trees** [1782, 1687, 1795, 1907, 1920, 1117, 1438, 1842]. **Trends** [3140, 1655]. **Trial**

[1189]. **Trials** [646, 690, 147, 393]. **Triangle** [4146]. **triangles** [2179]. **Triangular** [1413, 3400, 3692]. **Trident** [3454]. **Trier** [4161]. **trigamma** [1713]. **Trinomials** [1731, 2203, 2007]. **triple** [2843, 2946]. **triples** [2047, 2262, 2341]. **trivariate** [4043]. **trivial** [773]. **Trivium** [3172]. **TRNG** [3962, 4079, 4056, 3829, 4060, 4063]. **TRNGs** [3982, 3505]. **Trojans** [3719]. **True** [2840, 3149, 2763, 3635, 3538, 4048, 4066, 3648, 3087, 3176, 2775, 3182, 2595, 3726, 1354, 3321, 3188, 3428, 2612, 3869, 3743, 3440, 3914, 3117, 3460, 4015, 3696, 3354, 2651, 2822, 3062, 3358, 3483, 3611, 3129, 3256, 2832, 3378, 3380, 3143, 3513, 3514, 3856, 3157, 3158, 3281, 3282, 3283, 3312, 3313, 3315, 3323, 2534, 3580, 3586, 3338, 3607, 3489, 3496, 3706, 3501, 3071, 3259, 3374]. **Truly** [3286, 3551, 860, 2699, 3424, 3744, 1989, 538, 539, 3152, 3929, 2767, 3784, 2598, 602, 3686, 3751, 575, 631, 671]. **Truncated** [2923, 2924, 1545, 418, 1482, 856, 1349, 1170]. **trust** [2358]. **Trusted** [4081]. **trustless** [3918]. **Trustworthy** [3911]. **trx** [3911]. **Tsallis** [3058]. **Tucson** [4117]. **Tunable** [3314, 2864]. **Tuning** [2831, 2905]. **Tunnel** [4048]. **tuples** [2454]. **Turán** [2062, 659]. **Turbo** [3703, 1616, 1372]. **TURBO_RAND** [1231]. **Turbulence** [1917, 1454]. **turbulent** [2699]. **Turing** [4284, 3076, 3636, 3967, 4286]. **turn** [2524]. **Tutorial** [1406, 1159, 1623, 1719, 1459, 1091]. **Tweedie** [3854]. **Twelfth** [4168]. **twentieth** [4138]. **Twenty** [2501, 4143, 4148, 4159, 4177, 4182, 4191, 4266]. **twenty-eighth** [4191, 4266]. **twenty-first** [4143]. **twenty-fourth** [4159]. **twenty-second** [4148]. **twenty-seventh** [4182]. **twenty-sixth** [4177]. **Twin** [3630]. **Twin-float** [3630]. **Twist** [2660]. **Twisted** [1752, 1979]. **Twister** [3968, 2385, 2769, 2876, 3041, 3462, 3242, 3477, 3758]. **twisters** [2550]. **twisting** [3175]. **Two** [3140, 2020, 1104, 993, 1500, 3858, 548, 2053, 2703, 3572, 3193, 3196, 1294, 1545, 3871, 1850, 653, 417, 54, 2819, 3605, 2002, 4043, 373, 1317, 428, 811, 717, 498, 1493, 1059, 402, 1625, 1720, 1721, 1925, 1926, 2167, 2340, 2341, 1347, 1287, 1351, 2701, 479, 3789, 1124, 3573, 780, 2949, 3103, 1640, 482, 186, 2076, 3439, 2199, 1246, 2804, 738, 3913, 2967, 1090, 2310, 34, 2663, 3065, 3486, 3614, 1480, 2566, 2756, 2321]. **Two-bit** [3572]. **Two-Dimensional** [3193, 3196, 1850, 54, 717, 2199, 738, 2310, 2566, 2321]. **Two-Queue** [993]. **Two-Sided** [3605]. **Two-Source** [3858, 3871]. **Two-Stage** [1104]. **two-term** [3573, 2949, 3103, 3065, 3486, 3614]. **Twofish** [2521]. **Type** [2706, 155, 2611, 790, 2972, 890, 2232, 3273, 4065, 405, 1814, 1166, 1526, 356, 702, 3257, 3623, 3708]. **Types** [3679, 577].

Übertragungsprinzip [33]. **UHF** [3964]. **UHF-RFID** [3964]. **UK** [4284, 4244]. **uklonenijah** [35]. **Ukraine** [4169]. **Ulam** [3657]. **Ulrich** [896]. **Ultimate** [2268, 3593]. **Ultra** [3501]. **Ultra-lightweight** [3501]. **ultracomputers** [1306]. **Ultrafast** [3782, 3872, 3325, 4013, 3618]. **Ultrahigh** [3352]. **Ultrahigh-Speed** [3352]. **Unavoidable** [1066]. **Unbiased** [1102, 1334, 1207, 588]. **Unbounded** [3011, 2854, 3098]. **uncertain** [3311]. **uncertainty** [4230, 1224, 3342]. **unclonable** [3898]. **Unconditional** [3218]. **Unconstrained** [2098]. **Uncorrelated** [1494, 298]. **Uncovering** [2470].

Underlying [866]. **Understanding** [3027, 3841]. **unequal** [140]. **unicorn** [3911]. **Unified** [2020, 2049, 1549, 4040, 290, 2010, 569, 3136]. **Uniform** [814, 1406, 1795, 1696, 404, 1423, 1503, 3818, 2771, 1280, 683, 1437, 828, 517, 693, 3028, 1459, 1965, 2295, 2376, 2377, 2457, 2619, 3578, 1079, 786, 2719, 3336, 358, 1552, 1082, 1650, 3114, 2094, 1580, 2121, 3132, 3491, 428, 3381, 3386, 3853, 1405, 2236, 1794, 1268, 1057, 2678, 909, 402, 3080, 3817, 2338, 1028, 1507, 1710, 1711, 2685, 2770, 1219, 1930, 2053, 3904, 767, 1350, 3421, 1358, 1527, 688, 3022, 246, 1833, 382, 2283, 1238, 780, 85, 2294, 3577, 733, 734, 2626, 252, 2385, 609, 659, 742, 927, 928, 3049, 121, 1394, 664, 367, 974, 625, 3759]. **uniform** [1668, 806, 2562, 1259, 848, 3067, 3133, 3255, 3763, 940, 5, 1888, 2757, 3412, 3096, 3033, 426, 1311]. **uniform-Gaussian** [2283]. **uniformément** [178]. **Uniformity** [2148, 998, 867, 2717, 3582, 495, 3013, 2629, 2205, 1133, 1879]. **Uniformization** [1198]. **Uniformly** [270, 196, 201, 1737, 1740, 562, 205, 1141, 806, 178, 1507, 2437, 1233, 478, 306, 1292, 2960, 1200, 713, 1483]. **uniformly-distributed** [178]. **Uniforms** [1946, 2184, 1675, 1401, 1945, 2185, 2535, 1584]. **Unifying** [3746]. **Unimodal** [1107, 2256, 1130]. **Unique** [3419, 1374, 3267]. **unit** [430]. **units** [3395, 3720, 3206, 96, 3688, 3544]. **unity** [1058]. **Univariate** [2926, 1077, 514, 1952, 2625]. **Universal** [3812, 2917, 2160, 1362, 2626, 2719, 3336, 1648, 1874, 3771, 2058, 2059, 1947, 2625, 652, 1555, 2878, 1753]. **universe** [4286]. **University** [4085, 2136, 4231, 4161, 4212, 4104, 4204, 3742, 4187, 4207, 4214, 4236, 4103, 1193, 4106, 4199, 265, 4101, 4089]. **UNIX** [4188]. **Unknown** [2331, 1214, 790, 39, 1014]. **unleash** [2804]. **unperceivable** [2329]. **Unpredictability** [2453]. **Unpredictable** [1208, 3610, 2446, 1458, 3590]. **unpublished** [3076]. **unreasonable** [4160]. **unrestricted** [1784, 2829]. **unsigned** [1411]. **Unsupervised** [1793]. **Untersuchung** [2695]. **Untersuchungen** [1057, 1755]. **Untrusted** [3879]. **UNU.RAN** [3335, 3336]. **UNURAN** [2719]. **Unveiling** [4034]. **Up-and-Down** [574]. **update** [1985]. **updates** [3827]. **Upper** [1512, 2286, 2044, 2340]. **URAND** [652]. **urandom** [2820]. **URNG** [2787]. **USA** [4234, 4239, 4249, 4202, 4178, 4211, 4255, 4220, 4224, 4252, 4187, 4214, 4176, 4190, 4267, 4276, 4283, 4290, 4144, 4241, 4111, 4223, 4274, 4289, 4243, 4221, 4225, 4174, 4188, 4189, 4215]. **usable** [3532, 1748]. **Usage** [3841, 1991]. **Use** [3892, 2579, 2144, 127, 3972, 3565, 3194, 157, 1298, 2904, 2018, 2241, 1419, 1109, 3905, 1360, 959, 1235, 448, 449, 655, 159, 455, 1993, 46, 3609, 576, 1886, 20, 3070, 3545]. **Used** [2144, 2850, 2607, 3881, 2822, 2351, 3955, 3494, 100]. **useful** [4084]. **Usenix** [4215]. **User** [2620, 2718, 3107, 3989, 2193, 2471, 2823]. **user-based** [2471]. **user-level** [2823]. **User-Transparent** [3989]. **users** [3041]. **Uses** [2769, 1396, 2867]. **Using** [2574, 1894, 3961, 3277, 2996, 3772, 2998, 3897, 1494, 2025, 1495, 3815, 3535, 3538, 586, 3165, 2584, 1214, 2925, 1425, 2349, 272, 1515, 3553, 3557, 2443, 353, 513, 915, 777, 2281, 866, 3190, 1630, 3669, 3670, 3196, 2711, 2946, 828, 2451, 1010, 3029, 3212, 2795, 2957, 3677, 2798,

2082, 2083, 2883, 4058, 794, 3879, 3799, 3691, 1561, 1653, 3452, 3689, 657, 2092, 1766, 4293, 3462, 838, 663, 3982, 2397, 3238, 2973, 2974, 2111, 1198, 2114, 2003, 3985, 3249, 2315, 2406, 3132, 3491, 3499, 1793, 2132, 3381, 3382, 1484, 1680, 4067, 1322, 2672, 2839, 2137, 3928, 1025, 3074, 3634]. **using** [2331, 3002, 3078, 1699, 721, 3167, 3168, 3722, 1911, 2157, 3546, 473, 1157, 3415, 1285, 1229, 2601, 2701, 3563, 3023, 1441, 1006, 1237, 3997, 2945, 3199, 3102, 2949, 3434, 2953, 3036, 3580, 3586, 3980, 4080, 2197, 3587, 3588, 2725, 1977, 795, 3686, 1083, 147, 2810, 1251, 3235, 3916, 2552, 3119, 3467, 260, 622, 2112, 3805, 4077, 3248, 208, 4003, 3764, 3922, 1884, 2489, 2490, 4063, 3383]. **Utah** [4188]. **utilisant** [2552]. **utility** [215]. **utilizing** [3342]. **UWB** [3411].

V [2154, 499, 2543, 618, 4039, 4094]. **v.** [242]. **VA** [4176, 4174, 4225, 2106]. **Vacuum** [3419, 3480]. **Valentin** [2154]. **valeurs** [2196]. **Validating** [2796]. **Validation** [1735, 3281, 3282, 3312, 3259]. **Valuable** [2610, 3768]. **Value** [579, 401, 3161, 197, 3387, 4057, 2087, 1987, 4021, 3494]. **Valued** [241, 3181, 1988, 1689, 3771, 825, 3866, 689]. **Values** [2993, 728, 3228, 2474, 2221, 371, 811, 316, 3081, 2852, 2290, 87, 2205, 2750]. **VANETs** [3687]. **Variable** [579, 500, 2847, 376, 30, 2349, 378, 826, 3559, 413, 3020, 1043, 390, 3451, 458, 421, 422, 3267, 1704, 3096, 731, 252, 255, 702, 804, 668, 2399, 1256, 263, 289, 3497, 3809]. **variable-length** [3809]. **Variables** [399, 294, 755, 756, 817, 897, 898, 899, 900, 2579, 3525, 582, 1494, 2331, 2423, 1413, 3400, 319, 1903, 761, 822, 3540, 3647, 3649, 241, 951, 1614, 1280, 2160, 2432, 3181, 3009, 1112, 1113, 1114, 3011, 298, 3553, 2597, 506, 2696, 864, 4051, 2274, 686, 445, 643, 557, 687, 3822, 597, 1942, 1946, 598, 2708, 2864, 516, 1078, 868, 559, 1841, 779, 828, 870, 1543, 1455, 1544, 3793, 1545, 1125, 3029, 1079, 923, 2630, 2796, 2379, 309, 97, 254, 280, 281, 282, 335, 337, 359, 523, 791, 970, 1464, 1645, 2381, 2539, 2879]. **Variables** [606, 389, 562, 3592, 1300, 1384, 417, 3228, 525, 3115, 418, 2302, 2635, 2636, 1767, 2304, 971, 700, 1, 1192, 1086, 973, 2216, 3350, 1988, 365, 527, 621, 705, 368, 1575, 2474, 1577, 709, 369, 1096, 207, 3124, 371, 748, 845, 394, 395, 535, 537, 847, 891, 892, 2983, 2409, 315, 3495, 3616, 1592, 850, 808, 942, 893, 752, 811, 2319, 266, 2570, 3959, 431, 2572, 633, 1405, 316, 3925, 1486, 2135, 498, 901, 1024, 902, 1689, 3771, 3812, 1268, 581, 2581, 1412, 718, 1153, 194, 238, 1698, 584, 950, 1210, 1273, 1063, 405, 3292]. **variables** [1507, 995, 996, 1064, 1809, 3088, 1031, 684, 2774, 3180, 2437, 2854, 1162, 1227, 48, 60, 1349, 825, 913, 958, 2782, 1288, 775, 776, 1170, 1121, 1071, 381, 2942, 305, 689, 1529, 1834, 3570, 3429, 1950, 962, 3194, 3100, 1292, 84, 1238, 2185, 1447, 1957, 1008, 247, 780, 965, 922, 1011, 1039, 2712, 3102, 1960, 1961, 482, 2623, 1460, 2797, 2960, 1244, 1128, 334, 1246, 2380, 416, 226, 252, 253, 283, 311, 336, 339, 340, 385, 561, 695, 696, 1081, 1129, 2080, 2382, 2540, 1465, 3747, 3221, 2084, 2085, 2462, 1014, 3113, 924, 3754]. **variables** [2467, 1302, 927, 928, 617, 360, 1134, 1657, 2740, 2393, 2644, 1045, 566, 1993, 1194, 623, 975, 1091, 1397, 2556, 978, 1018, 746, 370, 1255, 2824, 2747, 166, 670, 849, 1594, 716, 2908, 1599, 577, 2154, 262]. **Variance** [1415, 3011, 2864, 2532, 2813, 2854, 3433, 3576]. **Variances** [1214]. **Variant**

[3155, 3477, 1011, 1039, 3237]. **Variants** [2720, 3594, 3758]. **Variate** [1212, 910, 3082, 1337, 1706, 2036, 1340, 1107, 1218, 1615, 2159, 2771, 3005, 4068, 725, 1525, 2863, 2184, 2710, 1077, 1367, 3669, 3670, 1539, 1540, 1634, 1242, 1459, 3577, 1181, 3336, 608, 4017, 844, 980, 982, 983, 1019, 1198, 2978, 1311, 1020, 3853, 3141, 3854, 3771, 2916, 1058, 2336, 3004, 1421, 2038, 1710, 2685, 3410, 1029, 1109, 1219, 1424, 1712, 1713, 1807, 2256, 3297, 3779, 2853, 1073, 2517, 2789, 3908, 3104, 3329, 1845, 3335, 3444, 1863, 1309, 979, 1256]. **Variates** [543, 1104, 1105, 1279, 1217, 1221, 3667, 732, 2077, 1650, 794, 1383, 2220, 883, 981, 2315, 1675, 715, 1484, 1680, 1401, 1891, 1023, 2575, 1898, 3639, 909, 678, 855, 856, 1336, 1507, 1106, 1108, 3661, 1944, 1831, 1945, 2180, 3788, 3666, 1177, 1541, 780, 2626, 3579, 788, 2536, 831, 1857, 563, 564, 1391, 567, 619, 1872, 704, 3843, 884, 984, 1584, 750, 3953, 1200, 1316, 2127, 2233, 2416, 3710, 542, 596, 640]. **Variation** [246, 3358, 3292, 3483]. **Variational** [1310]. **Variations** [2592]. **Various** [703, 2921, 788, 100]. **Varying** [1574, 3088]. **Vavilov** [2582, 711, 1140]. **VAX** [1342]. **VAX-11** [1342]. **Vector** [1487, 3961, 4006, 401, 2334, 3819, 2094, 2210, 1577, 3928, 2917, 1427, 2169, 1531, 1532, 247, 1457, 1643, 738, 3800, 3835, 1252, 1655, 1762, 1763, 1982, 2095, 3692, 665]. **Vectorial** [3638]. **Vectorized** [3951, 1211, 1516, 1394]. **Vectors** [544, 2248, 2583, 722, 2344, 517, 287, 1049, 3482, 1320, 2422, 583, 2149, 3778, 1803, 2345, 1164, 1233, 1289, 1357, 2290, 1566, 2547, 2897, 625, 2000, 2750]. **Vegas** [4182, 4223, 4274, 4187]. **Verifiability** [3967]. **Verifiable** [3857, 3170]. **Verification** [2859]. **Verified** [2423, 3924]. **Vermont** [4194]. **Versatile** [520]. **Verschlüsselungsabbildungen** [1035]. **Version** [3712, 1026, 1122, 3335, 3336, 2678, 3776, 3107, 3331, 3803]. **Versions** [2605, 933, 1048, 2922, 2076, 742]. **Versus** [735, 2493]. **verteilten** [1891]. **Verteilung** [668, 624]. **Vertical** [2288]. **Verwerfung** [1891]. **Very** [1199, 1319, 1358, 1009, 1975, 2088, 2392, 670]. **Very-Long-Cycle** [1319]. **very-long-period** [1975]. **VI** [2544]. **Via** [1980, 1891, 2148, 2502, 3080, 3409, 1501, 2252, 3175, 2160, 3301, 2432, 2509, 3939, 3559, 3973, 4033, 3738, 2532, 3037, 4000, 3337, 1043, 2307, 3049, 3240, 980, 2749, 2902, 1675, 2127, 3507, 3509]. **VIBNN** [3933]. **Victoria** [4159, 4254]. **Vienna** [4157, 4199]. **View** [1549, 1184, 2010, 778, 4110]. **Vigenère** [1914]. **vignettes** [3265]. **Virginia** [4210, 4243, 4166, 4141, 4119]. **Virtual** [3469]. **visit** [2229]. **Vista** [4181]. **Visual** [3120]. **VLSI** [4273, 1441, 3831, 1664, 2009, 1671, 1595]. **VMPC** [3845]. **Vol.** [656]. **volatility** [3748]. **Voltage** [3358]. **Volume** [4094]. **volumes** [3844]. **Voting** [3857]. **vs** [909, 2812, 164]. **vulnerabilities** [3469]. **vychislitelnykh** [351].

W [2149, 3188, 3286]. **W.** [498, 236, 3004]. **WA** [4280, 1549, 1962]. **Wadsworth** [262]. **Wahrscheinlichkeit** [570]. **Wahrscheinlichkeitstheorie** [570]. **wake** [3342]. **wake-up** [3342]. **Walk** [2402, 2417, 195, 3832, 2209, 2311, 2316, 2317, 2405, 3956]. **Walking** [3714]. **Walks** [1276, 2099, 2893, 2253, 2600, 1825, 1941, 2945]. **Wall** [3832]. **Wallace** [3159, 2953]. **Walsh** [1938, 2114, 1314, 851]. **Walsh-spectral**

[1314]. **Walt** [4181]. **Wang** [3938, 2889]. **Warbler** [3876]. **warning** [1360, 2889]. **Warp** [1628]. **was** [3676]. **Washing** [2769]. **Washington** [4143, 4168, 4098, 4241, 4179, 4147, 4206, 3707, 4131]. **Watson** [954, 1113]. **wave** [161]. **Waveforms** [549]. **Waveguide** [3782]. **wavelet** [4045]. **Waverly** [4196]. **Way** [3713, 2769, 3732, 3029, 1641, 1665, 3632, 2422, 2448, 3426, 1444, 1632, 3102, 1183, 1297, 3851]. **ways** [441]. **WCC** [4248]. **WCDMA** [3319]. **Weak** [3418, 864, 3663, 3038, 2634, 2808, 2108, 2126, 4026, 1334, 3379]. **Weakly** [1649, 1892]. **Weakness** [2700]. **Web** [2769, 3241, 2661]. **webcam** [2804]. **Wednesday** [4241]. **Weibull** [2089, 704]. **Weierstrass** [3386]. **weighing** [82]. **Weight** [304, 2727, 1603, 2072, 2228]. **Weighted** [3006, 3026, 747, 3125, 3247, 3357, 718, 2360, 3570, 2185, 3126, 3246, 3606]. **weights** [3606, 3373]. **Well** [2361, 1832, 2346]. **well-known** [2346]. **Weyl** [1607, 4069, 2404, 2564, 2828, 2489]. **WG** [4272]. **WGNG** [2855]. **wheel** [1829]. **Where** [3935]. **Which** [2579, 1197, 219, 370]. **while** [1116, 3351]. **Whit** [3676]. **White** [4140, 1365, 628, 2673, 2855, 2283]. **whitens** [3291]. **Who** [729]. **whole** [1325]. **Whose** [4018, 431, 1350, 1175, 166]. **Wichmann** [3225, 1805]. **wide** [2242]. **wide-area** [2242]. **Widespread** [3663]. **Width** [88]. **Wigderson** [4070]. **Williamson** [2149]. **Window** [612]. **Windows** [3085, 3086, 3300]. **Windsor** [4175]. **Winter** [4137, 4183, 4196, 4149, 4192, 4220, 4147, 4206, 4158, 4110, 4225, 4119, 4121, 4166, 4181, 4131]. **Wireless** [3012, 3452, 3231, 3191, 3583, 3828]. **Wisconsin** [4185]. **Wisdom** [2769]. **wise** [3959, 1486, 1326, 349, 2160, 1957]. **within** [2243, 1707, 2055, 494]. **Without** [3021, 1189, 1598, 2160, 1617, 1737, 2487, 2659, 3849]. **WMC** [1491]. **WMC-distributed** [1491]. **Worcester** [4224]. **word** [546, 600, 601, 662]. **word-length** [600, 601, 662]. **words** [3855, 3735, 2744, 3240]. **Work** [1281, 4103]. **Works** [4094]. **Workshop** [4123, 4133, 4264, 4212, 4224, 4163, 4195, 4108, 4200, 4248, 4250, 4184, 4218]. **workstation** [1690]. **World** [4284, 3314, 4035, 3229, 4181, 3874]. **WPA** [3887]. **WPA-TKIP** [3887]. **write** [4049]. **Writings** [4084]. **wrong** [3676]. **WSC'01** [4225]. **Wyndham** [4220].

X [1394]. **X-MP** [1394]. **X9.31** [2946]. **Xilinx** [4049]. **Xing** [2742]. **XOR** [2025, 4041, 2487, 2659]. **xorgens** [2678]. **xoroshiro** [3931]. **xoroshiro128** [4053, 3979]. **xors** [3002, 3078]. **Xorshift** [3990, 2846, 2802, 2968, 3888, 3923]. **xorshift1024** [3979]. **Xorshift1024*** [3979]. **xorshift128** [4034, 3979]. **xoshiro** [3931]. **XP** [2729]. **XSadd** [3803]. **XTEA** [2922, 2862, 2734, 2414]. **xviii** [3707]. **XXIV** [70].

Yarrow [2401, 2526, 2735]. **Yarrow-160** [2526]. **year** [2501]. **Years** [3140, 2088]. **yesterday** [4134]. **York** [4132, 4283, 170, 4140, 4153, 4221]. **Yorker** [4093]. **You're** [4016]. **Yuen** [3197].

Zahienfolgen [641]. **Zahlen** [5, 2992]. **Zakopane** [4200]. **Zaman** [2325]. **Zehnder** [3168]. **Zémor** [3237]. **Zero** [1415, 3173, 2098, 60, 3576, 2750, 1200].

Zero-One [2098]. **Zero-Variance** [1415, 3576]. **Ziggurat** [2954, 2990, 2540, 3878, 3947, 3302, 2633, 3805]. **Ziggurat-based** [2990]. **Zipf** [2175, 804, 1599]. **zk** [4077]. **zk-SNARKs** [4077]. **Zone** [2092, 3689]. **Zufälligkeit** [570]. **Zufallsgeneratoren** [1035]. **Zufallsgröße** [668]. **Zufallsszahlen** [1508]. **Zufallstests** [532, 533]. **Zufallsvariablen** [633]. **Zufallsvektoren** [1233]. **Zufallszafflen** [1055]. **Zufallszahlen** [1006, 1891, 894, 176, 1057, 439, 472, 2442, 642, 331]. **Zufallszahlengeneratoren** [1755]. **zur** [1055, 633, 1233, 1357, 1755, 278, 1006, 668].

References

Pearson:1900:CGS

[1] Karl Pearson. On a criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen in random sampling. *Philosophical Magazine*, 50(302):157–175, July/December 1900. CODEN PHMAA4. ISSN 0031-8086. URL `http://www.tandfonline.com/doi/pdf/10.1080/14786440009463897`.

Student:1908:PEM

[2] Student. The probable error of a mean. *Biometrika*, 6(1):1–25, March 1908. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2331554`.

Borel:1909:PDL

[3] Émile Borel. Les probabilités dénombrables et leurs applications arithmétiques. (French) [Countable probabilities and their arithmetic applications]. *Rendiconti del Circolo matematico di Palermo*, 27(??):247–271, ???? 1909. CODEN RCMMAR. ISSN 0009-725X (print), 1973-4409 (electronic). URL `http://springerlink.com/content/121284`.

Borel:1914:LTF

[4] Émile Borel. *Leçons sur la Théorie des Fonctions. (French) [Lectures on the theory of functions]*. Gauthier-Villars, Paris, France, second edition, 1914. x + 259 pp. LCCN ????

Weyl:1916:GZM

[5] H. Weyl. Über die Gleichverteilung Zahlen modulo Eins. (German) [On the uniform distribution of numbers modulo one]. *Mathematische Annalen*, 77(3):313–352, September 1916. CODEN MAANA3. ISSN 0025-5831 (print), 1432-1807 (electronic). URL `http://resolver.sub.uni-goettingen.de/purl?GDZPPN002266423`.

Fisher:1922:ICT

[6] R. A. Fisher. On the interpretation of χ^2 from contingency tables, and the calculation of P. *Journal of the Royal Statistical Society*, 85(1):87–94, January 1922. CODEN ???? ISSN 0952-8385. URL `http://www.jstor.org/stable/2340521`.

Yule:1922:AMA

[7] G. Udny Yule. On the application of the χ^2 method to association and contingency tables, with experimental illustrations. *Journal of the Royal Statistical Society*, 85(1):95–104, January 1922. CODEN ???? ISSN 0952-8385. URL `http://www.jstor.org/stable/2340522`.

Tippett:1925:EIR

[8] L. H. C. Tippett. On the extreme individuals and the range of samples taken from a normal population. *Biometrika*, 17(3/4):364–387, December 1925. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2332087`.

Tippett:1927:RSN

[9] Leonard Henry Caleb Tippett. *Random sampling numbers*, volume 15 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1927. viii + 26 pp. LCCN QA47 .T7 no. 15. With a foreword by editor Karl Pearson.

Yule:1927:RS

[10] G. Udny Yule. On reading a scale. *Journal of the Royal Statistical Society*, 90(3):570–587, ???? 1927. CODEN ???? ISSN 0952-8385. URL `http://www.jstor.org/stable/2341205`. See related later work [1016].

Klein:1929:SSD

[11] O. Klein and T. Nishina. Über die Streuung von Strahlung durch freie Elektronen nach der neuen relativistischen Quantendynamik von Dirac. (German) [On the scattering of radiation by free electrons according to the new relativistic quantum dynamics of Dirac]. *Zeitschrift für Physik*, 52(11–12):853–868, November 1929. CODEN ZEPYAA. ISSN 0044-3328. URL `http://www.springerlink.com/content/p6606272608242k2/`. This paper introduces the Klein–Nishina distribution of random numbes.

Baker:1930:RSN

[12] G. A. Baker. Random sampling from non-homogeneous populations. *Metron*, 8(??):67–88, ???? 1930. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Ward:1931:DRS

[13] Morgan Ward. The distribution of residues in a sequence satisfying a linear recursion relation. *Transactions of the American Mathematical Society*, 33(1):166–190, ???? 1931. CODEN TAMTAM. ISSN 0002-9947 (print), 1088-6850 (electronic).

Wilson:1931:DCS

[14] Edwin B. Wilson and Margaret M. Hilferty. The distribution of chi-square. *Proceedings of the National Academy of Sciences of the United States of America*, 17(12):684–688, December 1, 1931. CODEN PNASA6. ISSN 0027-8424 (print), 1091-6490 (electronic). URL `https://www.pnas.org/doi/abs/10.1073/pnas.17.12.684`.

Champernowne:1933:CDN

[15] D. G. Champernowne. The construction of decimals normal in the scale of ten. *Journal of the London Mathematical Society*, 8(4):254–260, ???? 1933. CODEN JLMSAK. ISSN 0024-6107 (print), 1469-7750 (electronic).

Glivenko:1933:SDE

[16] V. I. Glivenko. Sulla determinazione empirica delle leggi di probabilità. (Italian) [On the empirical determination of a probability law]. *Giornale dell'Istituto Italiano degli Attuari*, 4(??):92–99, ???? 1933. CODEN ???? ISSN 0390-5780.

Kolmogorov:1933:SDE

[17] Andrei Nikolaevich Kolmogorov. Sulla determinazione empirica di una legge di distributione. (Italian) [On the empirical determination of a distribution law]. *Giornale dell'Istituto Italiano degli Attuari*, 4(??):83–91, ???? 1933. CODEN ???? ISSN 0390-5780.

Mahalanobis:1934:TRS

[18] P. C. Mahalanobis. Tables of random samples from a normal population. *Sankhyā (Indian Journal of Statistics)*, 1(2–3):289–328, May 1934. CODEN SNKYA5. ISSN 0036-4452. URL `http://www.jstor.org/stable/40383681`. With the cooperation of Subhendu Sekhar Bose, Prabhat Ranjan Ray, and Sudhir Kumar Banerji.

Pearson:1934:NMD

[19] Karl Pearson. On a new method of determining "Goodness of fit". *Biometrika*, 26(4):425–442, December 1934. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2331988`. According to [374, page 36], this paper introduced the

$P_n(\lambda)$ test for "determining whether a sample of size n, supposed to have been drawn at random from a parent population having a known probability integral has probably been drawn at random." See [28] for its first use on random numbers from a uniform distribution.

Working:1934:RDS

[20] Holbrook Working. A random-difference series for use in the analysis of time series. *Journal of the American Statistical Association*, 29(185):11–24, March 1934. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2278456`.

Kadyrov:1936:TRN

[21] M. Kadyrov. *Tables of random numbers*. Izdat. Sredne-Aziatkogo Gos. Univ., Taškent, USSR, 1936. ???? pp. LCCN ????

Kermack:1937:SDA

[22] W. O. Kermack and A. G. McKendrick. Some distributions associated with a randomly arranged set of numbers. *Proceedings of the Royal Society of Edinburgh*, 57(??):332–376, 1937. CODEN PRSEAE. ISSN 0080-4541 (print), 2053-5902 (electronic).

Kermack:1937:TRS

[23] W. O. Kermack and A. G. McKendrick. Tests for randomness in a series of numerical observations. *Proceedings of the Royal Society of Edinburgh*, 57(??):228–240, 1937. CODEN PRSEAE. ISSN 0080-4541 (print), 2053-5902 (electronic).

Fisher:1938:STB

[24] Ronald Aylmer Fisher and Frank Yates. *Statistical Tables for Biological, Agricultural and Medical Research*. Oliver and Boyd, Edinburgh, UK; London, UK, 1938. viii + 90 + 1 pp. LCCN HA33 .F53.

Hey:1938:NME

[25] G. B. Hey. A new method of experimental sampling illustrated on certain non-normal populations. *Biometrika*, 30(1/2):68–80, June 1938. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2332225`.

Kendall:1938:RRS

[26] M. G. Kendall and B. Babington-Smith. Randomness and random sampling numbers. *Journal of the Royal Statistical Society*, 101(??):147–166, 1938. CODEN ???? ISSN 0952-8385.

Lehmer:1938:PSE

[27] D. H. Lehmer. Problems and solutions: Elementary problems: Solutions: Euclid's algorithm for large numbers. *American Mathematical Monthly*, 45(4):227–233, April 1938. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Nair:1938:TRS

[28] K. N. Nair. On Tippett's random sampling numbers. *Sankhyā (Indian Journal of Statistics)*, 4(1):65–72, 1938. CODEN SNKYA5. ISSN 0036-4452. URL `http://www.jstor.org/stable/40383888`.

Yule:1938:TTR

[29] G. Udny Yule. A test of Tippett's random sampling numbers. *Journal of the Royal Statistical Society*, 101(1):167–172, 1938. CODEN ???? ISSN 0952-8385. URL `http://www.jstor.org/stable/2980656`.

Dietze:1939:CCN

[30] E. Dietze and W. D. Goodale, Jr. The computation of the composite noise resulting from random variable sources. *The Bell System Technical Journal*, 18(4):605–623, October 1939. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol18/bstj18-4-605.pdf`; `http://www.alcatel-lucent.com/bstj/vol18-1939/articles/bstj18-4-605.pdf`.

Kendall:1939:SPR

[31] M. G. Kendall and B. Babington-Smith. Second paper on random sampling numbers. *J. Roy. Stat. Soc., Supplement*, 6(1):51–61, ???? 1939. CODEN ???? ISSN 1466-6162. URL `http://www.jstor.org/stable/2983623`.

Kendall:1939:TRS

[32] Maurice G. (Maurice George) Kendall and Bernard Babington-Smith. *Tables of random sampling numbers*, volume 24 of *Tracts for Computers*. Cambridge University Press, Cambridge, UK, 1939. x + 60 pp. LCCN QA47 .T7 no.24.

Mahler:1939:UKK

[33] Kurt Mahler. Ein Übertragungsprinzip für konvexe Körper. (German) [A theorem on transfer for convex bodies]. *Časopis pro pěstování matematiky a fysiky*, 68(3–4):93–102, ???? 1939. CODEN ???? ISSN 0528-2195. URL `http://dml.cz/dmlcz/109441`.

Smirnov:1939:EDB

[34] N. Smirnov. On the estimation of the discrepancy between empirical curves of distribution for two independent samples. *Bulletin Mathématique de l'Université de Moscou, Série internationale 2*, 2(2): 1–16, ???? 1939. CODEN ???? ISSN ????

Smirnov:1939:OUE

[35] N. V. Smirnov. Ob uklonenijah empiričeskoi krivoi raspredelenija. (Russian). [sur les écarts de la courbe de distribution empirique. (French)] [On deviations from the empirical distribution curve]. *Recueil Mathématique (Matematičeskiĭ Sbornik), N.S.*, 6(48):3–26, ???? 1939. CODEN MATSAB. ISSN 0368-8666.

Vickery:1939:DRS

[36] C. W. Vickery. On drawing a random sample from a set of punched cards. *J. Roy. Stat. Soc., Supplement*, 6(1):62–66, 1939. CODEN ???? ISSN 1466-6162. URL `http://www.jstor.org/stable/2983624`.

Church:1940:CRS

[37] A. Church. On the concept of a random sequence. *Bulletin of the American Mathematical Society*, 46(??):130–135, ???? 1940. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic).

Kendall:1941:TR

[38] M. G. Kendall. A theory of randomness. *Biometrika*, 32(1):1–15, January 1941. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2332245`.

Kolmogoroff:1941:CLU

[39] A. Kolmogoroff. Confidence limits for an unknown distribution function. *Annals of Mathematical Statistics*, 12(4):461–463, December 1941. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2235958`.

Nair:1941:DSC

[40] A. N. K. Nair. Distribution of Student's 't' and the correlation coefficient in samples from non-normal populations. *Sankhyā (Indian Journal of Statistics)*, 5(??):383–400, ???? 1941. CODEN SNKYA5. ISSN 0036-4452.

Young:1941:ROS

[41] L. C. Young. On randomness in ordered sequences. *Annals of Mathematical Statistics*, 12(3):293–300, September 1941. CODEN AASTAD. ISSN

0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2235858`.

Dodd:1942:CTR

[42] Edward L. Dodd. Certain tests for randomness applied to data grouped into small sets. *Econometrica*, 10(??):249–257, ???? 1942. CODEN ECMTA7. ISSN 0012-9682.

Dodd:1942:TTR

[43] Edward L. Dodd. A transformation of Tippett random sampling numbers into numbers normally distributed. *Boletín de Matemáticas*, 15(??):73–77, ???? 1942. CODEN BOMAD4. ISSN 0120-0380.

Mann:1942:CNC

[44] H. B. Mann and A. Wald. On the choice of the number of class intervals in the application of the chi square test. *Annals of Mathematical Statistics*, 13(3):306–317, September 1942. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177731569`; `http://www.jstor.org/stable/2235942`.

Peatman:1942:TRN

[45] J. G. Peatman and R. Shafer. A table of random numbers from Selective Service numbers. *Journal of Psychology*, 14(??):295–305, ???? 1942. CODEN JOPSAM. ISSN 0022-3980 (print), 1940-1019 (electronic).

Rosander:1942:UIT

[46] A. C. Rosander. The use of inversions as a test of random order. *Journal of the American Statistical Association*, 37(219):352–358, September 1942. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2279003`.

Fisher:1943:STB

[47] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural, and medical research*. Oliver and Boyd, Edinburgh, UK; London, UK, second edition, 1943. 98 pp. LCCN HA33 .F53 1943.

Forsythe:1943:CSI

[48] G. E. Forsythe. Cesàro summability of independent random variables. *Duke Mathematical Journal*, 10(??):397–428, 1943. CODEN DUMJAO. ISSN 0012-7094 (print), 1547-7398 (electronic). URL `http://projecteuclid.org/euclid.dmj/1077471948`.

Gage:1943:CTR

[49] Robert Gage. Contents of Tippett's "Random Sampling Numbers". *Journal of the American Statistical Association*, 38(222):223–227, June 1943. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2279542`.

Swed:1943:TTR

[50] Frieda S. Swed and C. Eisenhart. Tables for testing randomness of grouping in a sequence of alternatives. *Annals of Mathematical Statistics*, 14 (1):66–87, March 1943. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177731494`; `http://www.jstor.org/stable/2236004`.

Wald:1943:ETR

[51] A. Wald and J. Wolfowitz. An exact test for randomness in the nonparametric case, based on serial correlation. *Annals of Mathematical Statistics*, 14(4):378–388, December 1943. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2235925`.

Dixon:1944:FCP

[52] W. J. Dixon. Further contributions to the problem of serial correlation. *Annals of Mathematical Statistics*, 15(2):119–144, June 1944. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236194`.

Levene:1944:CMR

[53] H. Levene and J. Wolfowitz. The covariance matrix of runs up and down. *Annals of Mathematical Statistics*, 15(1):58–69, March 1944. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177731314`; `http://www.jstor.org/stable/2236211`.

Onsager:1944:CST

[54] Lars Onsager. Crystal statistics. I. A two-dimensional model with an order-disorder transition. *Physical Review*, 65(3–4):117–149, February 1944. CODEN PHRVAO. ISSN 0031-899X (print), 1536-6065 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRev.65.117`.

Rice:1944:MAR

[55] S. O. Rice. Mathematical analysis of random noise. *The Bell System Technical Journal*, 23(3):282–332, July 1944. CODEN BST-

JAN. ISSN 0005-8580. URL http://bstj.bell-labs.com/BSTJ/images/Vol23/bstj23-3-282.pdf; http://www.alcatel-lucent.com/bstj/vol23-1944/articles/bstj23-3-282.pdf.

Wolfowitz:1944:ADR

[56] J. Wolfowitz. Asymptotic distribution of runs up and down. *Annals of Mathematical Statistics*, 15(2):163–172, June 1944. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://www.jstor.org/stable/2236196.

Rice:1945:MAR

[57] S. O. Rice. Mathematical analysis of random noise. *The Bell System Technical Journal*, 24(1):46–156, January 1945. CODEN BSTJAN. ISSN 0005-8580. URL http://bstj.bell-labs.com/BSTJ/images/Vol24/bstj24-1-46.pdf; http://www.alcatel-lucent.com/bstj/vol24-1945/articles/bstj24-1-46.pdf.

Copeland:1946:NNN

[58] A. H. Copeland and P. Erdős. Note on normal numbers. *Bulletin of the American Mathematical Society*, 52(??):857–860, ???? 1946. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic).

Olmstead:1946:DSA

[59] P. S. Olmstead. Distribution of sample arrangements for runs up and down. *Annals of Mathematical Statistics*, 17(1):24–33, March 1946. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://www.jstor.org/stable/2235901.

Forsythe:1947:NSR

[60] George E. Forsythe. On Nörlund summability of random variables to zero. *Bulletin of the American Mathematical Society*, 53(??):302–313, 1947. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic). URL http://projecteuclid.org/euclid.bams/1183510599.

Moran:1947:RDI

[61] P. A. P. Moran. The random division of an interval. *J. Roy. Stat. Soc., Supplement*, 9(??):92–98, ???? 1947. ISSN 1466-6162.

Ulam:1947:CSD

[62] S. M. Ulam and John von Neumann. On combinations of stochastic and deterministic processes. *Bulletin of the American Mathematical Society*, 53(11):1120, November 1947. CODEN BAMOAD. ISSN

0002-9904 (print), 1936-881X (electronic). URL `http://www.ams.org/journals/bull/1947-53-11/S0002-9904-1947-08918-7/S0002-9904-1947-08918-7.pdf`. The abstract notes "... starting with almost every x_1 (in the sense of Lebesgue measure) and *iterating* the function $f(x) = 4 \cdot (1-x)$ one obtains a sequence of numbers on $(0, 1)$ with a computable algebraic distribution. By playing suitable games with numbers 'drawn' in this fashion, one can obtain various other distributions, either given explicitly or satisfying given differential or integral equations.".

Brown:1948:STR

[63] Bernice Brown. Some tests of the randomness of a million digits. Report RAND RAOP-44, RAND Corporation, Santa Monica, CA, USA, 1948. ???? pp.

Feller:1948:KSL

[64] W. Feller. On the Kolmogorov–Smirnov limit theorems for empirical distributions. *Annals of Mathematical Statistics*, 19(2):177–189, June 1948. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236265`.

Hamaker:1948:RFE

[65] H. C. Hamaker. Random frequencies, expedient for the construction of artificial samples of large size. *Statistica Rijswijk*, 2(??):129–137, ???? 1948. CODEN ???? ISSN ????

Hamaker:1948:RSN

[66] H. C. Hamaker. Random sampling numbers. *Statistica Rijswijk*, 2(??): 97–106, ???? 1948. CODEN ???? ISSN ????

Horton:1948:MOR

[67] H. Burke Horton. A method for obtaining random numbers. *Annals of Mathematical Statistics*, 19(1):81–85, March 1948. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236060`.

Ore:1948:NTH

[68] Øystein Øre. *Number theory and its history*. McGraw-Hill, New York, NY, USA, 1948. x + 370 pp. LCCN QA241 .O7.

Smirnov:1948:TEG

[69] N. Smirnov. Tables for estimating the goodness of fit of empirical distributions. *Annals of Mathematical Statistics*, 19(2):279–281, June 1948.

CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236278`.

Wold:1948:RND

[70] Herman O. A. Wold and Maurice G. (Maurice George) Kendall. *Random normal deviates: 25,000 items compiled from Tract no. XXIV (M. G. Kendall and B. Babington-Smith's Tables of random sampling numbers)*. Cambridge University Press, Cambridge, UK, 1948. xiii + 51 pp. LCCN QA47 .T7 no.25. See [32].

Brown:1949:HRR

[71] George W. Brown. History of RAND's random digits—summary. Report P-113, RAND Corporation, Santa Monica, CA, USA, June 1949. 6 pp. URL `http://www.rand.org/pubs/papers/2008/P113.pdf`.

Doob:1949:HAK

[72] J. L. Doob. Heuristic approach to the Kolmogorov–Smirnov theorems. *Annals of Mathematical Statistics*, 20(3):393–403, September 1949. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236535`.

Fisher:1949:STB

[73] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural, and medical research*. Hafner Pub. Co., New York, third edition, 1949. viii + 112 pp. LCCN HA33 .F53 1949.

Hamaker:1949:RSF

[74] H. C. Hamaker. Random sampling frequencies: an implement for rapidly constructing large-size artificial samples. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen*, 52(??):432–439, ???? 1949. CODEN PKNAAU. ISSN 0370-0348.

Hamaker:1949:STP

[75] H. C. Hamaker. A simple technique for producing random sampling numbers. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen*, 52(??):145–150, 1949. CODEN PKNAAU. ISSN 0370-0348.

Horton:1949:DMP

[76] H. Burke Horton and R. Tynes Smith III. A direct method for producing random digits in any number system. *Annals of Mathematical Statistics*, 20(1):82–90, March 1949. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236805`.

Mauchly:1949:PRN

[77] J. W. Mauchly. Pseudo-random numbers. Report ??, Eckert-Mauchly Computer Corporation, ????, 1949.

Metropolis:1949:MCM

[78] Nicholas Metropolis and S. Ulam. The Monte Carlo method. *Journal of the American Statistical Association*, 44(247):335–341, September 1949. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280232`.

Stevens:1949:TRD

[79] W. H. S. Stevens. *Table of 105,000 random decimal digits*, volume 4914. Interstate Commerce Commission, Washington, DC, USA, 1949. LCCN QA276.5 .U5 1949.

Walsh:1949:CCR

[80] John E. Walsh. Concerning compound randomization in the binary system. *Annals of Mathematical Statistics*, 20(4):580–589, December 1949. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177729950`; `http://www.jstor.org/stable/2236313`.

Eisenhart:1950:RDD

[81] C. Eisenhart and L. S. Deming. On the randomness of the digits of π and e to 2000 decimal places. In *National Bureau of Standards Seminar, February 17, Washington, DC*, page ?? ????, ????, 1950.

Good:1950:PWE

[82] Irving John Good. *Probability and the weighing of evidence*. C. Griffin, London, UK, 1950. viii + 119 pp. LCCN QA273 .G65.

Gruenberger:1950:TRD

[83] Fred Gruenberger. Tests of random digits. *Mathematical Tables and Other Aids to Computation*, 4(32):244–245, 1950. CODEN MTTCAS. ISSN 0891-6837.

Kac:1950:DMP

[84] Mark Kac and Harry Pollard. The distribution of the maximum of partial sums of independent random variables. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 2(??):375–384, ???? 1950. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Korobov:1950:SQU

[85] N. M. Korobov. On some questions of uniform distribution. *Izv. Akad. Nauk SSSR*, 14(3):215–238, ???? 1950. CODEN ???? ISSN ????

Massey:1950:NED

[86] Frank J. Massey, Jr. A note on the estimation of a distribution function by confidence limits. *Annals of Mathematical Statistics*, 21(1):116–119, March 1950. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177729891`; `http://www.jstor.org/stable/2236559`.

Metropolis:1950:STV

[87] N. C. Metropolis, G. Reitwiesner, and J. von Neumann. Statistical treatment of values of first 2,000 decimal digits of e and of π calculated on the ENIAC. *Mathematical Tables and Other Aids to Computation*, 4(30): 109–111, 1950. CODEN MTTCAS. ISSN 0891-6837.

Williams:1950:CNW

[88] C. Arthur Williams, Jr. On the choice of the number and width of classes for the chi-square test for goodness of fit. *Journal of the American Statistical Association*, 45(249):77–86, March 1950. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280429`.

Brown:1951:HRR

[89] George W. Brown. History of RAND's random digits—summary. In Householder et al. [4086], pages 31–32.

Cameron:1951:MCE

[90] J. M. Cameron. Monte Carlo experiments on SEAC. Working Paper SEL-52-5, U.S. National Bureau of Standards, Gaithersburg, MD, USA, October 27, 1951. ?? pp.

Forsythe:1951:GTRa

[91] George E. Forsythe. Generation and testing of random digits at the National Bureau of Standards, Los Angeles. *Applied Mathematics Series / National Bureau of Standards*, 12(??):34–35, ???? 1951. CODEN ???? ISSN 1049-4685.

Forsythe:1951:GTRb

[92] George E. Forsythe. Generation and testing of 1,217,370 'random' binary digits on the SWAC. *Bulletin of the American Mathematical Society*, 57

(??):304, ???? 1951. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic). Abstract only.

Gruenberger:1951:TRD

[93] Fred Gruenberger and A. M. Mark. The d^2 test of random digits. *Mathematical Tables and Other Aids to Computation*, 5(??):109–110, 1951. CODEN MTTCAS. ISSN 0891-6837.

Hammer:1951:MSM

[94] Preston C. Hammer. The mid-square method of generating digits. In Householder et al. [4086], page 33.

Kahn:1951:EPT

[95] Herman Kahn and T. E. Harris. 9. estimation of particle transmission by random sampling. *Journal of Research of the National Bureau of Standards. Applied Mathematics Series*, 12(??):27–30, 1951. CODEN ???? ISSN ???? URL `https://dornsifecms.usc.edu/assets/sites/520/docs/kahnharris.pdf`.

Lehmer:1951:MML

[96] D. H. Lehmer. Mathematical methods in large-scale computing units. In Anonymous [4085], pages 141–146. ISSN ???? LCCN QA75 .S9 1949.

Marsaglia:1951:SPC

[97] George Marsaglia. *Stochastic Processes and Classes of Random Variables*. Ph.D. thesis, The Ohio State University, Columbus, OH, USA, 1951. 46 pp. URL `http://ezproxy.lib.utah.edu/docview/302068737?accountid=14677`.

Massey:1951:KST

[98] Frank J. Massey, Jr. The Kolmogorov–Smirnov test for goodness of fit. *Journal of the American Statistical Association*, 46(253):68–78, March 1951. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280095`.

Richtmyer:1951:EDI

[99] R. D. Richtmyer. The evaluation of definite integrals, and a Quasi-Monte-Carlo method based on the properties of algebraic numbers. Report LA-1342, Los Alamos Scientific Laboratory, Los Alamos, NM, USA, 1951.

vonNeumann:1951:VTU

[100] John von Neumann. 13. Various techniques used in connection with random digits. In Householder et al. [4086], pages 36–

38. URL `https://dornsifecms.usc.edu/assets/sites/520/docs/VonNeumann-ams12p36-38.pdf`. Summary written by G. E. Forsythe. Reprinted in [4094, Paper 23, pp. 768–770].

Votaw:1951:HSS

[101] D. F. Votaw, Jr. and J. A. Rafferty. High speed sampling. *Mathematical Tables and Other Aids to Computation*, 5(33):1–8, January 1951. CODEN MTTCAS. ISSN 0891-6837.

Anderson:1952:ATC

[102] T. W. Anderson and D. A. Darling. Asymptotic theory of certain 'goodness of fit' criteria based on stochastic processes. *Annals of Mathematical Statistics*, 23(2):193–212, June 1952. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177729437`; `http://www.jstor.org/stable/2236446`.

Anonymous:1952:RD

[103] Anonymous. Random digits (1–6000). *Journal of the American Statistical Association*, 47(260):710–714, December 1952. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280798`.

Cameron:1952:RST

[104] J. M. Cameron. Results of some tests of randomness on pseudo-random on numbers (preliminary report). *Annals of Mathematical Statistics*, 23(1):138, March 1952. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236409`. Abstract only.

Goodman:1952:EPSa

[105] A. W. Goodman and W. M. Zaring. Elementary problems and solutions: Solutions: Euclid's algorithm and the least-remainder algorithm. *American Mathematical Monthly*, 59(3):156–159, March 1952. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL `http://www.jstor.org/stable/2308186`.

Ore:1952:GCR

[106] Øystein Øre. The general Chinese remainder theorem. *American Mathematical Monthly*, 59(6):365–370, June/July 1952. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Tippett:1952:RSN

[107] Leonard Henry Caleb Tippett. *Random sampling numbers*, volume 15 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1952. viii + 26 pp. LCCN QA47 .T7 no. 15. With a foreword by editor Karl Pearson.

Anonymous:1953:RDa

[108] Anonymous. Random digits (6001–6100). *Journal of the American Statistical Association*, 48(261):167, March 1953. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280898`.

Anonymous:1953:RDb

[109] Anonymous. Random digits (6501–6875). *Journal of the American Statistical Association*, 48(262):383, June 1953. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281306`.

Anonymous:1953:RDc

[110] Anonymous. Random digits (6876–8125). *Journal of the American Statistical Association*, 48(263):672, September 1953. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281029`.

Anonymous:1953:RDd

[111] Anonymous. Random digits (9001–13,750). *Journal of the American Statistical Association*, 48(264):931–934, December 1953. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281094`.

Curtiss:1953:MCM

[112] J. H. Curtiss. "Monte Carlo" methods for the iteration of linear operators. *Journal of Mathematical Physics*, 32(??):209–232, ???? 1953. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Duparc:1953:RSI

[113] H. J. A. Duparc, C. G. Lekkerkerker, and W. Peremans. Reduced sequences of integers and pseudo-random numbers. Report ZW 1953-002, Mathematisch Centrum, Amsterdam, The Netherlands, 1953.

Fisher:1953:STBa

[114] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural and medical research*. Oliver and Boyd, Edinburgh, UK; London, UK, fourth edition, 1953. xi + 126 pp. LCCN QA276 .F498 1953a.

Fisher:1953:STBb

[115] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural, and medical research*. Hafner Pub. Co., New York, NY, USA, fourth edition, 1953. 126 pp. LCCN QA276 .F498 1953.

Gilbert:1953:QRB

[116] E. N. Gilbert. Quasi-random binary sequences. Report MM-53-1400-42, Bell Telephone Laboratories, Murray Hill, NJ, USA, November 27, 1953.

Good:1953:STS

[117] I. J. Good. The serial test for sampling numbers and other tests for randomness. *Proceedings of the Cambridge Philosophical Society. Mathematical and physical sciences*, 49(??):276–284, 1953. CODEN PCPSA4. ISSN 0008-1981.

Juncosa:1953:RNG

[118] M. L. Juncosa. Random number generation on the BRL high-speed computing machines. Report 855, Ballistic Research Laboratories, Aberdeen Proving Ground, MD, USA, 1953.

Metropolis:1953:ESC

[119] Nicholas Metropolis, Arianna W. Rosenbluth, Marshall N. Rosenbluth, Augusta H. Teller, and Edward Teller. Equation of state calculations by fast computing machines. *Journal of Chemical Physics*, 21(6):1087–1092, June 1953. CODEN JCPSA6. ISSN 0021-9606 (print), 1089-7690 (electronic). URL `http://link.aip.org/link/doi/10.1063/1.1699114; http://pubs.acs.org/cgi-bin/chemport/version=1.0&coi=1:CAS:528:DyaG3sXltlKhsw%253D%253D&pissn=0095-2338&pyear=2005&&md5=2eba6ee7d50b361b924c3ff8efeda4b1`. This article introduces the Metropolis algorithm, which the journal *Computing in Science and Engineering* cited in the top 10 algorithms having the "greatest influence on the development and practice of science and engineering in the 20th Century." See [2498, 2499], and the Hasting–Metropolis generalization in [513]. See also [348, 663, 2788].

Moore:1953:STR

[120] P. G. Moore. A sequential test for randomness. *Biometrika*, 40(1/2):111–115, June 1953. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2333102`.

Peck:1953:UDA

[121] L. G. Peck. On uniform distribution of algebraic numbers. *Proceedings of the American Mathematical Society*, 4(??):440–443, 1953. CODEN PAMYAR. ISSN 0002-9939 (print), 1088-6826 (electronic).

Teichroew:1953:DSH

[122] Daniel Teichroew. *Distribution sampling with high speed computers*. Ph.D. dissertation, North Carolina State College, Chapel Hill, NC, USA, 1953. vi + 147 pp. URL `http://search.lib.unc.edu/search?R=UNCb3222025`.

Anonymous:1954:RDa

[123] Anonymous. Random digits (12,876–15,125). *Journal of the American Statistical Association*, 49(265):206–207, March 1954. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281062`.

Anonymous:1954:RDb

[124] Anonymous. Random digits (15,126–17,375). *Journal of the American Statistical Association*, 49(266):410–411, June 1954. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2280958`.

Anonymous:1954:RDc

[125] Anonymous. Random digits (17,376–20,875). *Journal of the American Statistical Association*, 49(267):682–684, September 1954. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281154`.

Anonymous:1954:RDd

[126] Anonymous. Random digits (20,876–21,875). *Journal of the American Statistical Association*, 49(268):928, December 1954. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281560`.

Bartholomew:1954:NUS

[127] D. J. Bartholomew. Note on the use of Sherman's statistic as a test for randomness. *Biometrika*, 41(3/4):556–558, December 1954. CODEN

BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2332738`.

Hammersley:1954:PMM

[128] J. M. Hammersley and K. W. Morton. Poor man's Monte Carlo. *Journal of the Royal Statistical Society. Series B (Methodological)*, 16(??):23–28, ???? 1954. CODEN JSTBAJ. ISSN 0035-9246.

Lehmer:1954:DRN

[129] D. H. Lehmer. Description of "Random number generation on the BRL high-speed computing machines". *Mathematical Reviews*, 15(??):559, ???? 1954. CODEN MAREAR. ISSN 0025-5629.

Meyer:1954:GTR

[130] H. A. Meyer, L. S. Gephart, and N. L. Rasmussen. On the generation and testing of random digits. WADC Technical Report 54–55, Air Res. Dev. Command, Wright-Patterson Air Force Base, OH, USA, 1954.

Moshman:1954:GPR

[131] Jack Moshman. The generation of pseudo-random numbers on a decimal calculator. *Journal of the ACM*, 1(2):88–91, April 1954. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Page:1954:MCS

[132] E. S. Page. The Monte Carlo solution of some integral equations. *Proceedings of the Cambridge Philosophical Society. Mathematical and physical sciences*, 50(??):414–425, 1954. CODEN PCPSA4. ISSN 0008-1981.

Rosenbluth:1954:FRM

[133] Marshall N. Rosenbluth and Arianna W. Rosenbluth. Further results on Monte Carlo equations of state. *Journal of Chemical Physics*, 22 (5):881–884, May 1954. CODEN JCPSA6. ISSN 0021-9606 (print), 1089-7690 (electronic). URL `http://scienze-como.uninsubria.it/bressanini/montecarlo-history/rosenbluth-1954.pdf`.

Royo:1954:TNA

[134] Jose Royo and Sebastian Ferrer. Tabla de numeros aleatorios obtenida de los numeros de la Loteria Nacional Española. (Spanish) [Tables of random numbers obtained from numbers in the Spanish National Lottery]. *Trabajos de Estadística y de Investigación Operativa*, 5(2):247–256, ???? 1954. CODEN ???? ISSN 0213-8190.

Schwartz:1954:RPC

[135] Lorraine Schwartz. Review of P. C. Mahalanobis, *Tables of random samples from a normal population. Mathematical Tables and Other Aids to Computation*, 8(??):228–??, ???? 1954. CODEN MTTCAS. ISSN 0891-6837.

Taussky:1954:GTP

[136] Olga Taussky and John Todd. Generation and testing of pseudo-random numbers. Report 3370, U.S. National Bureau of Standards, Gaithersburg, MD, USA, June 22, 1954. ii + 16 pp. URL `https://nvlpubs.nist.gov/nistpubs/Legacy/RPT/nbsreport3370.pdf`.

Tocher:1954:AAC

[137] K. D. Tocher. The application of automatic computers to sampling experiments. *Journal of the Royal Statistical Society. Series B (Methodological)*, 16(1):39–61, 1954. CODEN JSTBAJ. ISSN 0035-9246. URL `http://www.jstor.org/stable/2984009`. Discussion pp. 61-75.

Todd:1954:ESD

[138] John Todd. Experiments in the solution of differential equations by Monte Carlo methods. *Journal of the Washington Academy of Sciences*, 44(12):377–381, December 1954. CODEN JWASA3. ISSN 0043-0439. URL `http://www.jstor.org/stable/24533326`.

vanWijngaarden:1954:MC

[139] A. van Wijngaarden. Mathematics and computing. In Anonymous [4087], pages 125–129. LCCN QA76 .T4 1953.

vonSchelling:1954:CCU

[140] H. von Schelling. Coupon collecting for unequal probabilities. *American Mathematical Monthly*, 61(??):306–311, ???? 1954. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Fieller:1955:CRN

[141] E. C. Fieller, T. Lewis, and E. S. Pearson. *Correlated random normal deviates; 3,000 sets of deviates, each giving 9 random pairs with correlations* $0.1(0 \times 1)0 \times 9$, volume 26 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1955. 60 pp. LCCN QA47 .T7 no.26. Compiled from Herman Wold's Table of random normal deviates (Tract no. XXV) by E. C. Fieller, T. Lewis, and E. S. Pearson: *Random normal deviates*.

Gilbert:1955:MCR

[142] E. N. Gilbert. Machine computation of random numbers. Report MM-56-114-3, Bell Telephone Laboratories, Murray Hill, NJ, USA, March 12, 1955.

Golomb:1955:SRP

[143] S. W. Golomb. Sequences with randomness properties. Report, Glenn L. Martin Co., Baltimore, MD, USA, 1955. ???? pp.

Greenwood:1955:CCT

[144] Robert E. Greenwood. Coupon collector's test for random digits. *Mathematical Tables and Other Aids to Computation*, 9(49):1–5, January 1955. CODEN MTTCAS. ISSN 0891-6837.

Hastings:1955:ADC

[145] Cecil Hastings, Jr. *Approximations for Digital Computers*. The Rand series. Princeton University Press, Princeton, NJ, USA, 1955. ISBN 0-691-07914-5. viii + 201 pp. LCCN QA76 .H37. Assisted by Jeanne T. Hayward and James P. Wong, Jr.

McCracken:1955:MCM

[146] Daniel D. McCracken. The Monte Carlo method. *Scientific American*, 192(5):90–??, May 1955. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Neovius:1955:ATT

[147] Gösta Neovius. Artificial traffic trials using digital computers. *Ericsson Technics*, 11(??):279–291, 1955. CODEN ???? ISSN 0014-018X.

RAND:1955:MRD

[148] RAND Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Free Press, New York, NY, USA, 1955. ISBN 0-02-925790-5. xxv + 400 + 200 pp. LCCN QA276.5 .R3. URL `http://www.rand.org/pubs/monograph_reports/MR1418.html`. Reprinted in 1966 and 2001 [2647]. See also [9, 71, 89].

Spenser:1955:RNT

[149] Gordon Spenser. Random numbers and their generation. *Computers and Automation*, 4(??):10–11, 23, 1955. CODEN CPAUAJ. ISSN 0010-4795, 0887-4549.

Barton:1956:SNO

[150] D. E. Barton and F. N. David. Some notes on ordered random intervals. *Journal of the Royal Statistical Society. Series B (Methodological)*, 18(1): 79–94, ???? 1956. CODEN JSTBAJ. ISSN 0035-9246. URL `http://www.jstor.org/stable/2983737`.

Butler:1956:MSG

[151] James W. Butler. Machine sampling from given probability distributions. In Meyer [4089], pages 249–264. LCCN QA273 U577.

Davis:1956:SMC

[152] P. Davis and P. Rabinowitz. Some Monte Carlo experiments in computing multiple integrals. *Mathematical Tables and Other Aids to Computation*, 10(53):1–8, January 1956. CODEN MTTCAS. ISSN 0891-6837.

Farrington:1956:GPR

[153] Carl C. Farrington, Jr. Generating pseudo-random numbers in the Illiac. Report 74, Digital Computer Laboratory, University of Illinois, Champaign-Urbana, IL, USA, 1956.

Isida:1956:RNG

[154] Masatugu Isida and Hiroji Ikeda. Random number generator. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 8(??):119–126, 1956. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic).

Johnson:1956:GTP

[155] D. L. Johnson. Generating and testing pseudo random numbers on the IBM Type 701. *Mathematical Tables and Other Aids to Computation*, 10(53):8–13, January 1956. CODEN MTTCAS. ISSN 0891-6837.

Kahn:1956:AMC

[156] Herman Kahn. Applications of Monte Carlo. Research Memorandum RM-1237, RAND Corporation, Santa Monica, CA, USA, 1956. URL `http://www.rand.org/pubs/research_memoranda/RM1237.html`. Also appeared as AECU 3259.

Kahn:1956:UDM

[157] Herman Kahn. Use of different Monte Carlo sampling techniques. In Meyer [4089], pages 146–190. LCCN QA273 U577.

Lytle:1956:DGT

[158] Ernest J. Lytle, Jr. A description of the generation and testing of a set of random normal deviates. In Meyer [4089], pages 234–248. LCCN QA273 U577.

Marshall:1956:UMS

[159] Andrew W. Marshall. The use of multi-stage sampling schemes in Monte Carlo computations. In Meyer [4089], pages 123–140. LCCN QA273 U577.

Metropolis:1956:DGT

[160] N. Metropolis. A description of the generation and testing of a set of random normal deviates. In Meyer [4089], pages 234–248. LCCN QA273 U577.

Metropolis:1956:PSM

[161] N. Metropolis. Phase shifts — middle squares — wave equations. In Meyer [4089], pages 29–36. LCCN QA273 U577.

Pawlak:1956:FFG

[162] Z. Pawlak. Flip-flop as generator of random binary digits. *Mathematical Tables and Other Aids to Computation*, 10(??):28–30, 1956. CODEN MTTCAS. ISSN 0891-6837.

Sprowls:1956:ACF

[163] R. Clay Sprowls. An automatic coin flipper for sampling demonstrations. *The American Statistician*, 10(2):12–13, April 1956. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681598`.

Stuart:1956:ETR

[164] Alan Stuart. The efficiencies of tests of randomness, distribution-free methods vs. normal alternatives. *Journal of the American Statistical Association*, 51(274):285–287, June 1956. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281348`.

Taussky:1956:GTP

[165] Olga Taussky and John Todd. Generation and testing of pseudo-random numbers. In Meyer [4089], pages 15–28. LCCN QA273 U577.

Tompkins:1956:MAP

[166] C. B. Tompkins. Machine attacks on problems whose variables are permutations. In Curtiss [4088], pages 195–212. LCCN ????

Tompkins:1956:RJS

[167] C. B. Tompkins. Review of *Japanese Standards Association, random number generating icosahedral dice. Mathematical Tables and Other Aids to Computation*, 15(73):94–95, January 1956. CODEN MTTCAS. ISSN 0891-6837.

Tompkins:1956:RMR

[168] C. B. Tompkins. Review of *A Million Random Digits With 100,000 Normal Deviates. Mathematical Tables and Other Aids to Computation*, 10(53):39–43, January 1956. CODEN MTTCAS. ISSN 0891-6837.

Cook:1957:RFP

[169] J. M. Cook. Rational formulae for the production of a spherically symmetric probability distribution. *Mathematical Tables and Other Aids to Computation*, 11(58):81–82, April 1957. CODEN MTTCAS. ISSN 0891-6837. URL `http://www.jstor.org/stable/2002156`.

Davis:1957:CJH

[170] Harold Davis. Comment: J. Halcomb Laning, Jr., and Richard H. Battin, *Random Processes in Automatic Control*, McGraw-Hill Series in Control Systems Engineering, McGraw-Hill Book Co., Inc., New York, 1956, ix + 434 p., 23 cm. Price $10.00. *Mathematical Tables and Other Aids to Computation*, 11(58):112, April 1957. CODEN MTTCAS. ISSN 0891-6837. URL `http://www.jstor.org/stable/2002157`.

Fisher:1957:STBa

[171] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural, and medical research*. Oliver and Boyd, Edinburgh, UK; London, UK, fifth edition, 1957. 138 pp. LCCN QA276 .F498 1957a.

Fisher:1957:STBb

[172] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical tables for biological, agricultural, and medical research*. Hafner Pub. Co., New York, NY, USA, fifth edition, 1957. 138 pp. LCCN QA276 .F498 1957.

Gabai:1957:DCS

[173] H. Gabai. On the discrepancy of certain sequences mod 1. *Ill. J. Math.*, 1:1–12, 1957.

Good:1957:STR

[174] I. J. Good. On the serial test for random sequences. *Annals of Mathematical Statistics*, 28(1):262–264, March 1957. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177707053`; `http://www.jstor.org/stable/2237039`.

Savage:1957:ITR

[175] Richard Savage. On the independence of tests of randomness and other hypotheses. *Journal of the American Statistical Association*, 52(277):53–57, March 1957. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281400`.

vonHoerner:1957:HZR

[176] Sebastian von Hoerner. Herstellung von Zufallszahlen auf Rechenautomaten. (German) [Production of random numbers on automatic computers]. *Zeitschrift für Angewandte Mathematik und Physik = Journal of Applied Mathematics and Physics*, 8(??):26–52, 1957. CODEN ZAMPDB. ISSN 0044-2275 (print), 1420-9039 (electronic).

Walsh:1957:EMO

[177] John E. Walsh. An experimental method for obtaining random digits and permutations. *Sankhyā (Indian Journal of Statistics)*, 17(5):355–360, February 1957. CODEN SNKYA5. ISSN 0036-4452. URL `http://www.jstor.org/stable/25048325`.

Bass:1958:MMC

[178] J. Bass and J. Guilloud. Méthode de Monte-Carlo et suites uniformément denses. (French) [The Monte Carlo Method and sequences of uniformly-distributed numbers]. *Chiffres: Revue de l'Association française de Calcul*, 1(??):149–156, ???? 1958. CODEN ???? ISSN 0245-9922.

Bauer:1958:MCM

[179] W. F. Bauer. The Monte Carlo method. *Journal of the Society for Industrial and Applied Mathematics*, 6(4):438–451, December 1958. CODEN JSIMAV. ISSN 0368-4245 (print), 1095-712X (electronic).

Bendat:1958:PAR

[180] Julius S. Bendat. *Principles and Applications of Random Noise Theory*. Wiley, New York, NY, USA, 1958. 431 pp. LCCN TK5101 .B37.

Bofinger:1958:PPP

[181] Eve Bofinger and V. J. Bofinger. On a periodic property of pseudo-random sequences. *Journal of the ACM*, 5(3):261–265, July 1958. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Box:1958:NGR

[182] G. E. P. Box and Mervin E. Muller. A note on the generation of random normal deviates. *Annals of Mathematical Statistics*, 29(2):610–611, June 1958. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177706645; http://www.jstor.org/stable/2237361`.

Certaine:1958:SPR

[183] J. Certaine. On sequences of pseudo-random numbers of maximal length. *Journal of the ACM*, 5(4):353–356, October 1958. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Franklin:1958:EPR

[184] J. N. Franklin. On the equidistribution of pseudo-random numbers. *Quarterly of Applied Mathematics*, 16(??):183–188, ???? 1958. CODEN QAMAAY. ISSN 0033-569x (print), 1552-4485 (electronic).

Gross:1958:AGP

[185] O. Gross and S. M. Johnson. Additive generation of pseudorandom numbers. Research Memorandum RM-2132, RAND Corporation, Santa Monica, CA, USA, 1958. URL `http://www.rand.org/pubs/research_memoranda/RM2132.html`.

Leslie:1958:PSM

[186] P. H. Leslie and J. C. Gower. The properties of a stochastic model for two competing species. *Biometrika*, 45(3/4):316–330, December 1958. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2333181`.

Muller:1958:IMG

[187] Mervin E. Muller. An inverse method for the generation of random normal deviates on large-scale computers. *Mathematical Tables and Other Aids to Computation*, 12(63):167–174, July 1958. CODEN MTTCAS. ISSN 0891-6837.

Renyi:1958:ODP

[188] Alfréd Rényi. On a one-dimensional problem concerning random space filling. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, 3(1–2):109–127, ???? 1958.

Richtmyer:1958:NRS

[189] R. D. Richtmyer. A non-random sampling method, based on congruences, for "Monte Carlo" problems. Report NYO-8674, AEC Computational and Applied Mathematics Center, New York University, New York, NY, USA, 1958.

Schmid:1958:KSL

[190] Paul Schmid. On the Kolmogorov and Smirnov limit theorems for discontinuous distribution functions. *Annals of Mathematical Statistics*, 29(4): 1011–1027, December 1958. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2236943`.

Sengupta:1958:TRN

[191] J. M. Sengupta and Nikhilesh Bhattacharya. Tables of random normal deviates. *Sankhyā (Indian Journal of Statistics)*, 20(3/4):249–286, December 1958. CODEN SNKYA5. ISSN 0036-4452.

Sobol:1958:PRN

[192] I. M. Sobol'. Pseudo-random numbers for the machine "Strela". *Theory of Probability and its Applications*, 3(2):192–197, ???? 1958. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Thomson:1958:MCM

[193] W. E. Thomson. A modified congruence method of generating pseudo-random numbers. *The Computer Journal*, 1(2):83, 86, July 1958. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_01/Issue_02/010083.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_01/Issue_02/tiff/83.tif`.

Bolshev:1959:TRV

[194] L. N. Bol'shev. On transformations of random variables. *Theory of Probability and its Applications*, 4(2):136–149, ???? 1959. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Cashwell:1959:PMM

[195] E. D. Cashwell and C. J. (Cornelius Joseph) Everett. *A practical manual on the Monte Carlo method for random walk problems*, volume 1 of *International tracts in computer science and technology and their application*. Pergamon, New York, NY, USA, 1959. ix + 153 pp. LCCN QC174.5 .C3.

Cook:1959:RRP

[196] J. M. Cook. Remarks on a recent paper: "An Efficient Method for Generating Uniformly Distributed Points on the Surface of an n-Dimensional Sphere" (**2**, No. 4 (1959), 17). *Communications of the ACM*, 2(10):26, October 1959. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [201].

Ehrlich:1959:MCS

[197] Louis W. Ehrlich. Monte Carlo solutions of boundary value problems involving the difference analogue of $\partial^2 u/\partial x^2 + \partial^2 u/\partial y^2 + (K/y)(\partial u/\partial y) = 0$. *Journal of the ACM*, 6(2):204–218, April 1959. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Golenko:1959:DCS

[198] D. I. Golenko. Determination of characteristics of some stochastic processes by Monte Carlo methods. *Computational Mathematics*, ??(5): 93–108, 1959. CODEN ???? ISSN ????

Golenko:1959:FRN

[199] D. I. Golenko. Formation of random numbers with arbitrary law of distribution. *Computational Mathematics*, ??(5):83–92, 1959. CODEN ???? ISSN ????

Green:1959:ETA

[200] Bert F. Green, Jr., J. E. Keith Smith, and Laura Klem. Empirical tests of an additive random number generator. *Journal of the ACM*, 6(4): 527–537, October 1959. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Hicks:1959:EMG

[201] J. S. Hicks and R. F. Wheeling. An efficient method for generating uniformly distributed points on the surface of an n-dimensional sphere. *Communications of the ACM*, 2(4):17–19, April 1959. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remarks [196].

IBM:1959:RNG

[202] IBM. *Random number generation and testing*. International Business Machines Corporation, New York, NY, USA, 1959. vi + 12 + 2 pp. URL `https://ia601901.us.archive.org/2/items/bitsavers_ibmgeneralmberGenerationandTesting1959_839363/C20-8011_Random_Number_Generation_and_Testing_1959.pdf`. Reference manual C20-8011.

Lehmer:1959:CPD

[203] D. H. Lehmer. Combinatorial problems with digital computers. In Macphail [4090], pages 160–173. LCCN QA7 .C37 1957.

Muller:1959:CMG

[204] Mervin E. Muller. A comparison of methods for generating normal deviates on digital computers. *Journal of the ACM*, 6(3):376–383, July 1959. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Muller:1959:NMG

[205] Mervin E. Muller. A note on a method for generating points uniformly on N-dimensional spheres. *Communications of the ACM*, 2(4):19–20, April 1959. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Page:1959:PRE

[206] E. S. Page. Pseudo-random elements for computers. *Applied Statistics*, 8(2):124–131, June 1959. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Schulz-Arenstorff:1959:PDP

[207] Richard Schulz-Arenstorff and James C. Morelock. The probability distribution of the product of n random variables. *American Mathematical Monthly*, 66(2):95–99, February 1959. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Sterzer:1959:RNG

[208] Fred Sterzer. Random number generator using subharmonic oscillators. *Review of Scientific Instruments*, 30(4):241–243, 1959. CODEN RSINAK. ISSN 1089-7623, 0034-6748.

Thomson:1959:EMS

[209] W. E. Thomson. ERNIE — a mathematical and statistical analysis. *Journal of the Royal Statistical Society. Series A (General)*, 122(3):301–

324, 1959. CODEN JSSAEF. ISSN 0035-9238. URL `http://www.jstor.org/stable/2342795`. Discussion pp. 324-333.

Tippett:1959:RSN

[210] Leonard Henry Caleb Tippett. *Random sampling numbers*, volume 15 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1959. viii + 26 pp. LCCN QA47 .T7 no. 15. With a foreword by editor Karl Pearson.

Zierler:1959:LRS

[211] Neal Zierler. Linear recurring sequences. *Journal of the Society for Industrial and Applied Mathematics*, 7(1):31–48, March 1959. CODEN JSIMAV. ISSN 0368-4245 (print), 1095-712X (electronic).

Bazley:1960:AMC

[212] N. W. Bazley and P. J. Davis. Accuracy of Monte Carlo methods in computing finite Markov chains. *Journal of Research of the National Bureau of Standards (1934)*, 64B(??):211–215, ???? 1960. CODEN ???? ISSN 0091-0635.

Butcher:1960:SR

[213] J. C. Butcher. The simulation of randomness. In ????, editor, *Proceedings of the First Australian Computer Conference*, pages 12/1/1–12/1/2. ????, ????, 1960. LCCN ???? URL `????`.

Clark:1960:EDR

[214] Charles E. (Charles Erwin) Clark and Betty Weber Holz. *Exponentially distributed random numbers*. Published for Operations Research Office, Johns Hopkins University by Johns Hopkins Press, Baltimore, MD, USA, 1960. 249 pp. LCCN QA276 .C49.

Clark:1960:USR

[215] Charles E. Clark. The utility of statistics of random numbers. *Operations Research*, 8(2):185–195, March/April 1960. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://www.jstor.org/stable/167201`.

Coveyou:1960:SCG

[216] R. R. Coveyou. Serial correlation in the generation of pseudo-random numbers. *Journal of the ACM*, 7(1):72–74, January 1960. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

DeMatteis:1960:PRS

[217] A. De Matteis and B. Faleschini. Pseudo-random sequences of equal length. Report 88, Comitato AND Nazionale per l'Energia Nucleare, Bologna, Italy, 1960.

Edmonds:1960:GPR

[218] A. R. Edmonds. The generation of pseudo-random numbers on electronic digital computers. *The Computer Journal*, 2(4):181–185, January 1960. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/020181.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/tiff/181.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/tiff/182.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/tiff/183.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/tiff/184.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_02/Issue_04/tiff/185.tif`.

Golenko:1960:SRN

[219] D. I. Golenko and V. P. Smiriagin. A source of random numbers which are equidistributed in $[0, 1]$. *Publications Math. Inst., Hungarian Acad. Sci.*, 5A(3):241–253, 1960. CODEN ???? ISSN ???? English abstract.

Good:1960:MCM

[220] I. J. Good. Monte Carlo method. In *McGraw-Hill Encyclopedia of Science and Technology*, volume 8, pages 586–587. McGraw-Hill, New York, NY, USA, 1960. LCCN ????

Halton:1960:BEC

[221] J. H. Halton. Berichtigung: "On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals" [Num. Math. **2**, 84–90 (1960)]. (German) [Correction]. *Numerische Mathematik*, 2:196, December 1960. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic). See [222].

Halton:1960:ECQ

[222] J. H. Halton. On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals. *Numerische Mathematik*, 2:84–90, December 1960. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic). See correction [221].

Hammersley:1960:MCM

[223] J. M. Hammersley. Monte Carlo methods for solving multivariable problems. *Annals of the New York Academy of Sciences*, 86(??):844–874, 1960. CODEN ANYAA9. ISSN 0077-8923 (print), 1749-6632 (electronic).

Hunter:1960:NTR

[224] D. G. N. Hunter. Note on a test for repeating cycles in a pseudo-random number generator. *The Computer Journal*, 3(1): 9, April 1960. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_01/030009.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_01/tiff/9.tif`.

Kleinrock:1960:PTS

[225] L. Kleinrock. A program for testing sequences of random numbers. Report 51G-0018, MIT Lincoln Laboratory, Cambridge, MA, USA, October 25, 1960.

Marsaglia:1960:GED

[226] George Marsaglia. On generating exponentially distributed random variables. Report ??, Boeing Scientific Research Labs, Seattle, WA, USA, ???? 1960. ?? pp.

Pakov:1960:GRC

[227] G. K. Pakov. Generation of a random correlated quantity on a high-speed electronic computer. *Soviet developments in information processing and machine translation*, ??(??):??, ???? 1960. CODEN ???? ISSN ???? U. S. Joint Publ. Res. Service JPRS: 5784, Nov., 1960.

Postnikov:1960:AMR

[228] A. G. Postnikov. Arithmetic modeling of random processes. *Trudy Matematicheskogo instituta imeni V. A. Steklova = Proceedings of the Steklov Institute of Mathematics*, 57(??):1–84, ???? 1960. CODEN TMISAF. ISSN 0371-9685.

Rotenburg:1960:NPR

[229] A. Rotenburg. A new pseudo-random number generator. *Journal of the ACM*, 7(1):75–77, January 1960. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Schmidt:1960:NN

[230] Wolfgang M. Schmidt. On normal numbers. *Pacific Journal of Mathematics*, 10:661–672, 1960. CODEN PJMAAI. ISSN 0030-8730 (print), 1945-5844 (electronic). URL `http://projecteuclid.org/euclid.pjm/1103038420`.

Wall:1960:FSM

[231] D. D. Wall. Fibonacci series modulo m. *American Mathematical Monthly*, 67(6):525–532, June/July 1960. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Wall:1960:RNT

[232] Donald D. Wall. A random number test for large samples. In Anonymous [4091], pages 7–11. LCCN ????

Yamada:1960:PPN

[233] S. Yamada. On the period of pseudorandom numbers generated by Lehmer's congruential method. *J. Op. Research Soc. Japan*, 3(??):113–123, ???? 1960. CODEN ???? ISSN ????

Biuslenko:1961:MCM

[234] N. P. Biuslenko and Ju. A. Sreider. *The Monte-Carlo method and how it is carried out on digital computers*. Gosudarstv. Izdat. Fiz-Mat. Lit., Moscow, USSR, 1961. CODEN ???? ISSN ???? ???? pp. LCCN ????

Bofinger:1961:GTR

[235] Eve Bofinger and V. J. Bofinger. The gap test for random sequences. *Annals of Mathematical Statistics*, 32(2):524–534, June 1961. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177705058`; `http://www.jstor.org/stable/2237761`.

Bofinger:1961:NPW

[236] Eve Bofinger and V. J. Bofinger. A note on the paper by W. E. Thomson, on *ERNIE — a mathematical and statistical analysis*. *Journal of the Royal Statistical Society*, A124(??):240–243, ???? 1961. CODEN ???? ISSN 0952-8385.

Bofinger:1961:RTS

[237] Eve Bofinger and V. J. Bofinger. A runs test for sequences of random digits. *Australian Journal of Statistics*, 3(2):37–41, August 1961. CODEN AUJSA3. ISSN 0004-9581.

Brandt:1961:GCT

[238] A. Brandt. A generalization of a combinatorial theorem of Sparre Andersen about sums of random variables. *Mathematica Scandinavica*, 9: 325–358, 1961. CODEN MTSCAN. ISSN 0025-5521 (print), 1903-1807 (electronic).

Butcher:1961:PTP

[239] J. C. Butcher. A partition test for pseudo-random numbers (in Technical Notes and Short Papers). *Mathematics of Computation*, 15(74):198–199, April 1961. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Butcher:1961:RSN

[240] J. C. Butcher. Random sampling from the normal distribution. *The Computer Journal*, 3(4):251–253, January 1961. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_04/030251.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_04/tiff/251.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_04/tiff/252.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_03/Issue_04/tiff/253.tif`.

Corrsin:1961:CLS

[241] S. Corrsin and O. M. Phillips. Contour length and surface area of multiple-valued random variables. *Journal of the Society for Industrial and Applied Mathematics*, 9(3):395–404, September 1961. CODEN JSIMAV. ISSN 0368-4245 (print), 1095-712X (electronic).

Fisser:1961:STA

[242] H. Fisser. Some tests applied to pseudo-random numbers generated by v. Hörner's rule. *Numerische Mathematik*, 3:247–249, December 1961. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Greenberger:1961:NNP

[243] Martin Greenberger. Notes on a new pseudo-random number generator. *Journal of the ACM*, 8(2):163–167, April 1961. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Greenberger:1961:PDS

[244] Martin Greenberger. An a priori determination of serial correlation in computer generated random numbers. *Mathematics of Computation*,

15(76):383–389, October 1961. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). See also corrigenda, Math. Comp. **16** (1962), p. 126.

Herrmann:1961:SER

[245] R. G. Herrmann. The statistical evaluation of random number generating sequences for digital computers. Report APEX - 635, General Electric Co., ????, 1961. U.S. Dept. of Commerce, Office of Technical Services.

Hlawka:1961:FBV

[246] Edmund Hlawka. Funktionen von beschränkter Variation in der Theorie der Gleichverteilung. (German) [Functions of bounded variation in the theory of uniform distribution]. *Annali di matematica pura ed applicata. Series 4*, 54(??):325–333, ???? 1961. CODEN ANLMAE. ISSN 0003-4622.

Kiefer:1961:LDE

[247] J. Kiefer. On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm. *Pacific Journal of Mathematics*, 11 (??):649–660, ???? 1961. CODEN PJMAAI. ISSN 0030-8730 (print), 1945-5844 (electronic).

Kuehn:1961:BPR

[248] Heidi G. Kuehn. A 48-bit pseudo-random number generator. *Communications of the ACM*, 4(8):350–352, August 1961. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Liniger:1961:MDH

[249] Werner Liniger. On a method by D. H. Lehmer for the generation of pseudo random numbers. *Numerische Mathematik*, 3:265–270, December 1961. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Mamangakis:1961:MNR

[250] S. E. Mamangakis. Mathematical notes: Remarks on the Fibonacci series modulo m. *American Mathematical Monthly*, 68(7):648–649, August/September 1961. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Manelis:1961:GRN

[251] J. B. Manelis. Generating random noise. *Electronics*, ??(??):66–69, September 8, 1961. ISSN 0883-4989.

Marsaglia:1961:ERV

[252] G. Marsaglia. Expressing a random variable in terms of uniform random variables. *Annals of Mathematical Statistics*, 32(3):894–898, September 1961. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://projecteuclid.org/euclid.aoms/1177704983; http://www.jstor.org/stable/2237849.

Marsaglia:1961:GER

[253] G. Marsaglia. Generating exponential random variables. *Annals of Mathematical Statistics*, 32(3):899–900, September 1961. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://projecteuclid.org/euclid.aoms/1177704984; http://www.jstor.org/stable/2237850.

Marsaglia:1961:PGN

[254] George Marsaglia. Procedures for generating normal random variables, II. Mathematical note 243, Boeing Scientific Research Laboratories, Seattle, WA, USA, October 1961.

Marsaglia:1961:RGR

[255] G. Marsaglia. Remark on generating a random variable having a nearly linear density function. Mathematical Note 242, Boeing Scientific Research Labs, Seattle, WA, USA, 1961.

Marsaglia:1961:SPT

[256] George Marsaglia. Some probability theory associated with clustered-rocket flights. *Planetary and Space Science*, 4(??):194–201, January 1961. CODEN PLSSAE. ISSN 0032-0633 (print), 1873-5088 (electronic). URL http://www.sciencedirect.com/science/article/pii/0032063361901325.

Orcutt:1961:MSS

[257] Guy H. Orcutt, Martin Greenberger, John Korbel, and Alice M. Rivlin. *Microanalysis of socioeconomic systems; a simulation study*. Harper, New York, NY, USA, 1961. xviii + 425 pp. LCCN H61 .O7.

Peach:1961:BPR

[258] Paul Peach. Bias in pseudo-random numbers. *Journal of the American Statistical Association*, 56(295):610–618, September 1961. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL http://www.jstor.org/stable/2282083.

Pinkham:1961:DFS

[259] Roger S. Pinkham. On the distribution of first significant digits. *Annals of Mathematical Statistics*, 32(4):1223–1230, December 1961. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://links.jstor.org/sici?sici=0003-4851%28196112%2932%3A4%3C1223%3AOTDOFS%3E2.0.CO%3B2-T; http://projecteuclid.org/euclid.aoms/1177704862; http://www.jstor.org/stable/2237922.

Rao:1961:GRP

[260] C. Radhakrishna Rao. Generation of random permutations of given number of elements using random sampling numbers. *Sankhyā (Indian Journal of Statistics), Series A. Methods and Techniques*, 23(??):305–307, 1961. CODEN SANABS. ISSN 0036-4452.

Richtmyer:1961:MCM

[261] R. D. Richtmyer. Monte Carlo methods. In Birkhoff and Wigner [4093], pages 190–205. LCCN QC787.N8 S9 1959.

Riffenburgh:1961:RPI

[262] Robert H. Riffenburgh. Recent publications: *Introduction to Probability and Random Variables*, by George P. Wadsworth and Joseph G. Bryan. *American Mathematical Monthly*, 68(5):518, May 1961. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Sibuya:1961:EOR

[263] Masaaki Sibuya. On exponential and other random variable generators. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 13(1):231–237, December 1961. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL http://link.springer.com/article/10.1007/BF02868873.

Solomon:1961:SIA

[264] Herbert Solomon, editor. *Studies in item analysis and prediction*, volume 6 of *Stanford mathematical studies in the social sciences*. Stanford University Press, Stanford, CA, USA, 1961. 310 pp. LCCN BF39 .S64. With contributions by Rosedith Sitgreaves and others.

Wendel:1961:LMC

[265] James G. Wendel. *Lectures on Monte Carlo: University of Michigan Summer Session Courses on Numerical Analysis*. University of Michigan Press, Ann Arbor, MI, USA, 1961. ??–?? pp. LCCN ????

Wouk:1961:DDR

[266] Arthur Wouk. On digit distributions for random variables. *Journal of the Society for Industrial and Applied Mathematics*, 9(4):597–603, December 1961. CODEN JSIMAV. ISSN 0368-4245 (print), 1095-712X (electronic).

Barnett:1962:BPR

[267] V. D. Barnett. The behavior of pseudo-random sequences generated on computers by the multiplicative congruential method. *Mathematics of Computation*, 16(77):63–69, January 1962. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2003811.pdf`.

Behrenz:1962:AR

[268] Peter G. Behrenz. Algorithm 133: RANDOM. *Communications of the ACM*, 5(11):553, November 1962. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Behrenz:1962:RAR

[269] Peter G. Behrenz. Remark on Algorithm 133: Random. *Communications of the ACM*, 5(12):606, December 1962. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Clark:1962:CMM

[270] G. Miller Clark. Corrections to Mervin E. Muller, *A Note on a Method for Generating Points Uniformly on N-Dimensional Spheres*. *Mathematics of Computation*, 16(78):261, 1962. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). See [205].

Dillard:1962:EGR

[271] G. M. Dillard and R. E. Simmons. An electronic generator of random numbers. *IRE Transactions on Electronic Computers*, EC-11(2): 284, April 1962. CODEN IRELAO. ISSN 0367-9950. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5219362`. See comments [295].

Fan:1962:DSP

[272] C. T. Fan, Mervin E. Muller, and Ivan Rezucha. Development of sampling plans by using sequential (item by item) selection techniques and digital computers. *Journal of the American Statistical Association*, 57 (298):387–402, June 1962. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2281647`.

Foster:1962:MRS

[273] Malcolm B. Foster. A method of representation, storage and retrieval of 13 random codes in a 4-digit number or 16 random codes in a 5-digit number. *Communications of the ACM*, 5(3):165, March 1962. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Franklin:1962:DSR

[274] Joel N. Franklin. Deterministic simulation of random processes. Technical Report 118, Computing Center, California Institute of Technology, Pasadena, CA, USA, 1962.

Galler:1962:RNG

[275] Bernard A. Galler. *Random number generators*, pages 56–59. McGraw-Hill, New York, NY, USA, 1962. LCCN QA76.5 .G3.

Gordon:1962:SND

[276] Basil Gordon, W. H. Mills, and L. R. Welch. Some new difference sets. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 14(??):614–625, ???? 1962. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Hamming:1962:NMS

[277] R. W. (Richard Wesley) Hamming. *Numerical methods for scientists and engineers*. International Series in Pure and Applied Mathematics. McGraw-Hill, New York, NY, USA, 1962. xvii + 411 pp. LCCN QA297 .H28.

Hlawka:1962:ABM

[278] Edmund Hlawka. Zur angenäherten Berechnung mehrfacher Integrale. (German) [Toward approximate calculation of multiple integrals]. *Monatshefte für Mathematik*, 66(2):140–151, April 1962. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/g5m4457x5525866p/`.

Hull:1962:RNG

[279] T. E. Hull and A. R. Dobell. Random number generators. *SIAM Review*, 4(3):230–254, July 1962. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://link.aip.org/link/?SIR/4/230/1`; `https://dspace.library.uvic.ca:8443/bitstream/handle/1828/3142/Random_Number_Generators.pdf?sequence=3`.

Marsaglia:1962:FPG

[280] G. Marsaglia, M. D. Maclaren, and T. A. Bray. A fast procedure for generating normal random variables. Mathematical note 282, Boeing Scientific Research Laboratories, Seattle, WA, USA, August 1962. URL `http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=AD0296195`.

Marsaglia:1962:IPM

[281] George Marsaglia. Improving the polar method for generating a pair of normal random variables. Technical report D1-82-0203, Boeing Scientific Research Laboratories, Seattle, WA, USA, September 1962.

Marsaglia:1962:RVC

[282] George Marsaglia. Random variables and computers. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, May 1962. ?? pp. URL `http://www.dtic.mil/docs/citations/AD0278358`.

Marsaglia:1962:SPG

[283] George Marsaglia and T. A. Bray. A small procedure for generating normal random variables. Mathematical note 283, Boeing Scientific Research Labs, Seattle, WA, USA, November 1962. ?? pp.

MendesFrance:1962:CMF

[284] M. Mendès France. Calcul des moyennes des fonctions aléatoires ou pseudo-aléatoires par échantillonnage. (French) [averaging functions of random or pseudo-random sampling]. *Publ. Inst. Statist. Univ. Paris*, 11 (??):225–256, ???? 1962. CODEN ???? ISSN ????

Pathria:1962:SSR

[285] R. K. Pathria. A statistical study of randomness among the first $10,000$ digits of π. *Mathematics of Computation*, 16(78):188–197, April 1962. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Richtmyer:1962:CFE

[286] R. D. Richtmyer, Marjorie Devaney, and N. Metropolis. Continued fraction expansions of algebraic numbers. *Numerische Mathematik*, 4:68–84, December 1962. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Scheuer:1962:GNR

[287] E. M. Scheuer and D. S. Stoller. On the generation of normal random vectors. *Technometrics*, 4(??):278–281, ???? 1962. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic).

Shanks:1962:CD

[288] Daniel Shanks and John W. Wrench, Jr. Calculation of π to 100,000 decimals. *Mathematics of Computation*, 16(77):76–99, January 1962. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Sibuya:1962:FCN

[289] Masaaki Sibuya. Further consideration on normal random variable generator. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 14(1): 159–165, December 1962. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/article/10.1007/BF02868636`.

Spanier:1962:UAM

[290] J. Spanier. A unified approach to Monte Carlo methods and an application to a multigroup calculation of absorption rates. *SIAM Review*, 4(2):115–134, April 1962. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2028365`.

Todd:1962:SNA

[291] John Todd, editor. *Survey of Numerical Analysis*. McGraw-Hill, New York, NY, USA, 1962. xvi + 589 pp. LCCN ????

Walsh:1962:HNS

[292] J. E. Walsh. *Handbook of Nonparametric Statistics*. Van Nostrand, Princeton, NJ, USA, 1962. xxvi + 549 pp. LCCN QA278.8 .W34.

Allard:1963:MCR

[293] J. L. Allard, A. R. Dobell, and T. E. Hull. Mixed congruential random number generators for decimal machines. *Journal of the ACM*, 10(2): 131–141, April 1963. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Anonymous:1963:BRBd

[294] Anonymous. Book review: *Random Variables and Probability Distributions* by H. Cramér. *Biometrika*, 50(1/2):232–233, June 1963. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2333784`.

Barnes:1963:CEG

[295] George H. Barnes. Comment on "An Electronic Generator of Random Numbers". *IEEE Transactions on Electronic Computers*, EC-12(1):22, February 1963. CODEN IEECA8. ISSN 0367-7508. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4037766`. See [271].

Bolshev:1963:APT

[296] L. N. Bol'shev. Asymptotically Pearson transformations. *Theory of Probability and its Applications*, 8(2):121–146, ???? 1963. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

DeMatteis:1963:SAP

[297] A. De Matteis and B. Faleschini. Some arithmetical properties in connection with pseudo-random numbers. *Bollettino della Unione matematica italiana*, 18(??):171–184, ???? 1963. CODEN BLUMAM. ISSN 0041-7084.

Firestone:1963:CNU

[298] C. D. Firestone and J. E. Hanson. Classroom notes: Uncorrelated Gaussian dependent random variables. *American Mathematical Monthly*, 70 (6):659–660, June/July 1963. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Fisher:1963:STB

[299] Sir Ronald Aylmer Fisher and Frank Yates. *Statistical Tables for Biological, Agricultural and Medical Research*. Oliver and Boyd, Edinburgh, UK; London, UK, sixth edition, 1963. ISBN 0-05-000872-2, 0-582-44525-6. x + 146 pp. LCCN QH324 .F52 1963.

Franklin:1963:DSR

[300] Joel N. Franklin. Deterministic simulation of random processes. *Mathematics of Computation*, 17(81):28–59, January 1963. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2003733`.

Gabai:1963:DCSa

[301] H. Gabai. On the discrepancy of certain sequences $\bmod 1$. *Nederl. Akad. Wetensch. Proc. Ser. A*, 66(??):603–605, ???? 1963. CODEN ???? ISSN ????

Gabai:1963:DCSb

[302] H. Gabai. On the discrepancy of certain sequences mod1. *Indagationes Mathematicæ*, 25(??):603–605, ???? 1963. CODEN IMTHBJ. ISSN 0019-3577, 0023-3358.

George:1963:ANR

[303] R. George. Algorithm 200: Normal random. *Communications of the ACM*, 6(8):444, August 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See also [364].

Gill:1963:WDP

[304] Arthur Gill. On a weight distribution problem, with application to the design of stochastic generators. *Journal of the ACM*, 10(1):110–122, January 1963. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Hoeffding:1963:PIS

[305] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, March 1963. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2282952`.

Jagerman:1963:AFS

[306] David L. Jagerman. The autocorrelation function of a sequence uniformly distributed modulo 1. *Annals of Mathematical Statistics*, 34(4):1243–1252, December 1963. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2238334`.

Kolmogorov:1963:TRN

[307] A. N. Kolmogorov. On tables of random numbers. *Sankhyā (Indian Journal of Statistics), Series A. Methods and Techniques*, 25(??):369–376, ???? 1963. CODEN SANABS. ISSN 0036-4452.

Laughlin:1963:RAR

[308] Donald L. Laughlin. Remark on Algorithm 133: Random. *Communications of the ACM*, 6(3):105, March 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

MacLaren:1963:FPG

[309] M. D. MacLaren, G. Marsaglia, and T. A. Bray. A fast procedure for generating exponential random variables. Report ??, Boeing Scientific Research Labs, Seattle, WA, USA, January 1963. ?? pp.

Magleby:1963:SNF

[310] K. B. Magleby. The synthesis of nonlinear feedback shift registers. Report TR 6207-1, Stanford Electronics Laboratory, Stanford, CA, USA, 1963.

Marsaglia:1963:GDR

[311] G. Marsaglia. Generating discrete random variables in a computer. *Communications of the ACM*, 6(1):37–38, January 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Marsaglia:1963:RNF

[312] George Marsaglia. Random numbers fall mainly in the planes. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, August 1963. 9 pp. URL `http://www.dtic.mil/docs/citations/AD0685578`.

Moses:1963:TRP

[313] Lincoln E. Moses and Robert V. Oakford. *Tables of random permutations*. Stanford University Press, Stanford, CA, USA, 1963. 233 pp. LCCN QA165 .M6.

Poore:1963:CAR

[314] Jesse H. Poore, Jr. Certification of Algorithm 133: Random. *Communications of the ACM*, 6(4):167, April 1963. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Tucker:1963:QCS

[315] Howard G. Tucker. Quasi-convergent series of independent random variables. *American Mathematical Monthly*, 70(7):718–722, August/September 1963. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Ahsanullah:1964:RVE

[316] Mohammad Ahsanullah. Record values of exponentially distributed random variables. *Statistical Papers*, 22(2):121–127, June 1964. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic). URL `http://link.springer.com/article/10.1007/BF02933548`.

Alanen:1964:TFF

[317] J. D. Alanen and Donald E. Knuth. Tables of finite fields. *Sankhyā (Indian Journal of Statistics), Series A. Methods and Techniques*, 26 (??):305–328, 1964. CODEN SANABS. ISSN 0036-4452.

Bekessy:1964:RBD

[318] András Békéssy. Remarks on beta distributed random numbers. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, 9:565–571, 1964.

Brillinger:1964:BRI

[319] David R. Brillinger. Book reviews: *Information and Information Stability of Random Variables and Processes*, by M. S. Pinsker and Amiel Feinstein. *Applied Statistics*, 13(2):134–135, 1964. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Chow:1964:RNG

[320] D. K. Chow. Random number generator test procedures applied to a modified, multiplicative, congruential generator method. Technical Report UIUCDCS-R-1964-612, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, 1964.

Durstenfeld:1964:ARP

[321] Richard Durstenfeld. Algorithm 235: Random permutation. *Communications of the ACM*, 7(7):420, July 1964. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Esmenjaud-Bonnardel:1964:PGN

[322] M. Esmenjaud-Bonnardel. Un procédé de génération de nombres 'pseudo-aléatoires' pour CAB 500. (French) [A procedure for the generation of pseudorandom numbers on the CAB 500]. *Chiffres: Revue de l'Association française de Calcul*, 7(??):185–197, ???? 1964. CODEN ???? ISSN 0245-9922.

Gebhardt:1964:GND

[323] Friedrich Gebhardt. Generating normally distributed random numbers by inverting the normal distribution function (in Technical Notes and Short Papers). *Mathematics of Computation*, 18(86):302–306, April 1964. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Halton:1964:ARI

[324] J. H. Halton. Algorithm 247: Radical-inverse quasi-random point sequence. *Communications of the ACM*, 7(12):701–702, December 1964. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hammer:1964:GRN

[325] C. Hammer and L. Green. Generation of random numbers. *Instruments and Control Systems*, 37(5):149–150, ???? 1964. CODEN INCSA7. ISSN 0020-4404.

Hammersley:1964:MCM

[326] J. M. Hammersley and D. C. Handscomb. *Monte Carlo methods*. Methuen's monographs on applied probability and statistics. Methuen, London, UK, 1964. vii + 178 pp. LCCN QA273 .H354 1964.

Hull:1964:MCR

[327] T. E. Hull and A. R. Dobell. Mixed congruential random number generators for binary machines. *Journal of the ACM*, 11(1):31–40, January 1964. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Jagerman:1964:AJD

[328] David L. Jagerman. The autocorrelation and joint distribution functions of the sequences $\left\{\frac{a}{m}j^2\right\}$, $\left\{\frac{a}{m}(j+\tau)^2\right\}$. *Mathematics of Computation*, 18 (86):211–232, April 1964. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Jansson:1964:ABP

[329] Birger Jansson. Autocorrelations between pseudo-random numbers. *Nordisk Tidskrift for Informationsbehandling*, 4(1):6–27, March 1964. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=4&issue=1&spage=6`.

Jansson:1964:GRB

[330] Birger Jansson. Generation of random bivariate normal deviates and computation of related integrals. *Nordisk Tidskrift for Informationsbehandling*, 4(4):205–212, December 1964. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=4&issue=4&spage=205`.

Johnk:1964:EBG

[331] M. D. Jöhnk. Erzeugung von betaverteilten und gammaverteilten Zufallszahlen. (German) [Production of beta- and gamma-distributed random numbers]. *Metrika. International Journal for Theoretical and Applied Statistics.*, 8(1):5–15, December 1964. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic). URL `http://link.springer.com/article/10.1007/BF02613706`.

Kronmal:1964:EPN

[332] Richard Kronmal. Evaluation of a pseudorandom normal number generator. *Journal of the ACM*, 11(3):357–363, July 1964. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Liu:1964:MFS

[333] R. Liu and J. Massey. Monotone feedback shift registers. In ????, editor, *Proceedings of the 2nd Allerton Conference on Circuit and System Theory. University of Illinois, Urbana, 1964*, pages 860–874. ????, ????, 1964. LCCN ????

MacLaren:1964:FPG

[334] M. D. MacLaren, G. Marsaglia, and T. A. Bray. A fast procedure for generating exponential random variables. *Communications of the ACM*, 7(5):298–300, May 1964. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Marsaglia:1964:CMG

[335] G. Marsaglia and T. A. Bray. A convenient method for generating normal variables. *SIAM Review*, 6(3):260–264, ???? 1964. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2027592`.

Marsaglia:1964:FPG

[336] G. Marsaglia, M. D. MacLaren, and T. A. Bray. A fast procedure for generating normal random variables. *Communications of the ACM*, 7 (1):4–10, January 1964. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Marsaglia:1964:MPR

[337] George Marsaglia. A method for producing random variables in a computer. Mathematical note 342, Boeing Scientific Research Laboratories, Seattle, WA, USA, February 1964. 13 pp.

Marsaglia:1964:RDA

[338] George Marsaglia. The radiation dose accumulated by blood diverted through a shunt. Mathematical note 357, Boeing Scientific Research Laboratories, Seattle, WA, USA, July 1964. 8 pp.

Marsaglia:1964:RNV

[339] George Marsaglia. Ratios of normal variables and ratios of sums of variables. Mathematical note D1-82-0348, Mathematics Re-

search Laboratory, Boeing Scientific Research Laboratories, Seattle, WA, USA, April 1964. iii + 13 + 3 pp. URL `http://www.dtic.mil/docs/citations/AD0600972`; `http://www.dtic.mil/dtic/tr/fulltext/u2/600972.pdf`; `http://www.dtic.mil/get-tr-doc/pdf?AD=AD0600972`.

Marsaglia:1964:RVC

[340] George Marsaglia. Random variables and computers. In Kožešník [4095], pages 499–512. LCCN ???? In memory of RNDr. Antonin Spacek.

Marsaglia:1964:SPIa

[341] George Marsaglia. Some problems involving circular and spherical targets. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, April 1964. 19 pp. URL `http://www.dtic.mil/docs/citations/AD0600566`.

Marsaglia:1964:SPIb

[342] George Marsaglia. Some problems involving circular and spherical targets. *Operations Research*, 13(1):18–27, January/February 1964. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://www.jstor.org/stable/167951`.

Onicescu:1964:NSA

[343] O. Onicescu. *Nombres et systèmes aléatoires. (French) [Random numbers and systems]*. Éditions Eyrolles, Paris, France, 1964. 280 pp. LCCN ????

Poore:1964:CPG

[344] Jesse H. Poore. *Computational procedures for generating and testing random numbers*. Division of Business and Economic Research, School of Business Administration, Louisiana Polytechnic Institute, Ruston, UK, 1964. 36 pp. LCCN QA273 .P78.

Sobol:1964:PPR

[345] I. M. Sobol'. Periods of pseudo-random sequences. *Teor. Verojatnost. i Primenen.*, 9:367–373, 1964. CODEN ???? ISSN 0040-361X.

Stockmal:1964:CPR

[346] Frank Stockmal. Calculations with pseudo-random numbers. *Journal of the ACM*, 11(1):41–52, January 1964. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Tocher:1964:AS

[347] K. D. Tocher. *The Art of Simulation*. Van Nostrand, Princeton, NJ, USA, 1964. viii + 184 pp. LCCN TA177 .T6.

Barker:1965:MCC

[348] A. A. Barker. Monte Carlo calculations of the radial distribution functions for a proton-electron plasma. *Australian Journal of Physics*, 18 (??):119–133, ???? 1965. CODEN AUJPAS. ISSN 0004-9506 (print), 1446-5582 (electronic).

Barnett:1965:RNE

[349] Vic D. Barnett. *Random negative exponential deviates; 2 pair-wise correlated sets of 10,000 observations: with facilities for the generation of random χ^2 deviates on any integral number of degrees of freedom*, volume 27 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1965. xxii + 89 pp. LCCN QA47 .T7 no. 27.

Franklin:1965:NSS

[350] Joel N. Franklin. Numerical simulation of stationary and non-stationary Gaussian random processes. *SIAM Review*, 7(1):68–80, ???? 1965. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Golenko:1965:MSA

[351] D. I. Golenko. *Modelirovanie i statisticheskii analiz psevdosluchainykh chisel na elektronnykh vychislitelnykh mashinakh. (Russian) [The method of statistical testing (The Monte Carlo method)]*. Izdatelstvo "Nauka", Moscow, USSR, 1965. 227 pp. LCCN ????

Greenberger:1965:MR

[352] Martin Greenberger. Method in randomness. *Communications of the ACM*, 8(3):177–179, March 1965. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hampton:1965:EUP

[353] Robert L. Hampton. Experiments using pseudo-random noise. *Simulation*, 4(4):246–254, April 1965. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/4/4/246.abstract`.

Hampton:1965:HAD

[354] R. L. T. Hampton. A hybrid analog-digital pseudo random noise generator. *Simulation*, 4(3):179–199, March 1965. CODEN SIMUA2. ISSN

0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/4/3/179.full.pdf+html`.

Jagerman:1965:STC

[355] D. L. Jagerman. Some theorems concerning pseudo-random numbers. *Mathematics of Computation*, 19(91):418–426, July 1965. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Jansson:1965:ASP

[356] B. Jansson. Analytical studies of pseudorandom number generators of the congruential type. In ????, editor, *Proceedings of the IFIP Congress*, pages 371–372. ????, ????, 1965. LCCN ????

Knuth:1965:CRS

[357] Donald E. Knuth. Construction of a random sequence. *Nordisk Tidskrift for Informationsbehandling*, 5(4):246–250, 1965. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic).

MacLaren:1965:URN

[358] M. Donald MacLaren and George Marsaglia. Uniform random number generators. *Journal of the ACM*, 12(1):83–89, January 1965. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Marsaglia:1965:SAM

[359] George Marsaglia. Still another method for producing normal variables in a computer. Mathematical note ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, January 1965. 8 pp.

Papoulis:1965:PRV

[360] Athanasios Papoulis. *Probability, random variables, and stochastic processes*. McGraw-Hill, New York, NY, USA, 1965. ISBN 0-07-048448-1, 0-07-085971-X. xi + 583 pp. LCCN QA273 .P2.

Pike:1965:AAP

[361] M. C. Pike and I. D. Hill. ACM Algorithm 266: Pseudo-random numbers. *Communications of the ACM*, 8(10):605–606, October 1965. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See certification [630].

Pike:1965:APR

[362] M. C. Pike and I. D. Hill. Algorithm 266: Pseudo-random numbers [G5]. *Communications of the ACM*, 8(10):605–606, October 1965. CODEN

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See certification [630] and remarks [380, 391].

Pike:1965:ARN

[363] M. C. Pike. Algorithm 267: Random normal deviate [G5]. *Communications of the ACM*, 8(10):606, October 1965. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Pike:1965:CAGb

[364] M. C. Pike. Certification of Algorithm 200 [G5]: Normal random. *Communications of the ACM*, 8(9):556, September 1965. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [303].

Potter:1965:CNS

[365] J. E. Potter. Classroom notes: Sets of Gaussian random variables. *American Mathematical Monthly*, 72(2):171–173, February 1965. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Pyke:1965:S

[366] R. Pyke. Spacings. *Journal of the Royal Statistical Society. Series B (Methodological)*, 27(??):395–434, ???? 1965. CODEN JSTBAJ. ISSN 0035-9246.

Reeves:1965:AUR

[367] C. M. Reeves. Algorithm 8: a uniform random number generator. *The Computer Bulletin*, 9(??):105–??, ???? 1965. CODEN COBUAH. ISSN 0010-4531 (print), 1464-357X (electronic).

Rosenberg:1965:CNN

[368] Lloyd Rosenberg. Classroom notes: Nonnormality of linear combinations of normally distributed random variables. *American Mathematical Monthly*, 72(8):888–890, October 1965. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Scheinok:1965:DFR

[369] P. Scheinok. The distribution functions of random variables in arithmetic domains modulo a. *American Mathematical Monthly*, 72(2):128–134, February 1965. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Seshadri:1965:RVW

[370] V. Seshadri. On random variables which have the same distribution as their reciprocals. *Canadian mathematical bulletin = Bulletin canadien*

de mathématiques, 8(??):819–824, ???? 1965. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Shapiro:1965:DAA

[371] Jesse M. Shapiro. Domains of attraction for absolute values of random variables. *Journal of the Society for Industrial and Applied Mathematics*, 13(1):129–135, March 1965. CODEN JSIMAV. ISSN 0368-4245 (print), 1095-712X (electronic).

Stoneham:1965:SDT

[372] R. G. Stoneham. A study of the 60,000 digits of the transcendental 'e'. *American Mathematical Monthly*, 72(4):483–506, April 1965. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Tausworthe:1965:RNG

[373] Robert C. Tausworthe. Random numbers generated by linear recurrence modulo two. *Mathematics of Computation*, 19(90):201–209, April 1965. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2003345`.

Teichroew:1965:HDS

[374] Daniel Teichroew. A history of distribution sampling prior to the era of the computer and its relevance to simulation. *Journal of the American Statistical Association*, 60(309):27–49, March 1965. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2283135`.

Chaitin:1966:LPC

[375] Gregory J. Chaitin. On the length of programs for computing finite binary sequences. *Journal of the ACM*, 13(4):547–569, October 1966. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Chiang:1966:ERR

[376] C. L. Chiang. On the expectation of the reciprocal of a random variable. *The American Statistician*, 20(4):28, October 1966. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2685960`.

Dyadkin:1966:SRE

[377] I. G. Dyad'kin. Simulation of the random energy of a gamma quantum scattered as a result of the Compton effect. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 6(2):274–276, ???? 1966.

CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/0041555366900772`. English translation of Russian original published in Zh. vychisl. Mat. mat. Fiz. **6**(2) 384–385, 1966.

Fleiss:1966:NER

[378] Joseph L. Fleiss. A note on the expectation of the reciprocal of a random variable. *The American Statistician*, 20(1):25, February 1966. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681673`.

Gorenstein:1966:APN

[379] S. Gorenstein. Another pseudorandom number generator. *Communications of the ACM*, 9(9):711, September 1966. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Hansson:1966:RAG

[380] L. Hansson. Remark on Algorithm 266 [G5]: Pseudo-random numbers. *Communications of the ACM*, 9(9):687, September 1966. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [362], remark [391], and certification [630].

Heyde:1966:SRS

[381] C. C. Heyde. Some results on small-deviation probability convergence rates for sums of independent random variables. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 18(??):656–665, ???? 1966. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Hutchinson:1966:NUP

[382] David W. Hutchinson. A new uniform pseudorandom number generator. *Communications of the ACM*, 9(6):432–433, June 1966. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Jansson:1966:RNG

[383] Birger Jansson. *Random number generators*. Almqvist & Wiksell, Stockholm, Sweden, 1966. 205 pp. LCCN QA276.5 .J3 1966.

Loveland:1966:NIM

[384] D. Loveland. A new interpretation of the von Mises concept of random sequence. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 12(??):279–294, ???? 1966. CODEN ZMLGAQ. ISSN 0044-3050.

Marsaglia:1966:GMP

[385] G. Marsaglia. A general method for producing random variables in a computer. In *Proceedings of the Fall Joint Computer Conference, San Francisco, November 1966*, pages 169–173. Spartan Books, Washington, DC, USA, 1966. LCCN TK7885.A1 J74 1966 Fall.

Martin-Lof:1966:CRS

[386] P. Martin-Löf. On the concept of a random sequence. *Theory of Probability and its Applications*, 11(??):177–179, ???? 1966. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Martin-Lof:1966:DRS

[387] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9(6):602–619, December 1966. CODEN IFCNA4. ISSN 0019-9958 (print), 1878-2981 (electronic).

Mckinney:1966:CNG

[388] E. H. Mckinney. Classroom notes: Generalized birthday problem. *American Mathematical Monthly*, 73(4):385–387, April 1966. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Miller:1966:BRB

[389] Irwin Miller. Book review: *Probability, Random Variables, and Stochastic Processes* by Anthanasios Papoulis. *Technometrics*, 8(2):378–380, May 1966. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/1266379`.

Murthy:1966:NER

[390] V. N. Murthy and C. S. Pillai. A note on the expectation of the reciprocal and square root of a random variable. *The American Statistician*, 20(5): 30, December 1966. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682640`.

Pike:1966:RAG

[391] M. C. Pike and I. D. Hill. Remark on Algorithm 266 [G5]: Pseudorandom numbers. *Communications of the ACM*, 9(9):687, September 1966. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [362], remark [380], and certification [630].

RAND:1966:MRD

[392] RAND Corporation. *A Million Random Digits With 100,000 Normal Deviates*. Free Press, New York, NY, USA, 1966. xxviii + 400 + 200 pp.

LCCN QA276.5 .R3. URL `http://www.rand.org/pubs/monograph_reports/MR1418.html`. Reprint of original edition [148]. Reprinted in 2001 [2647]. See also [9, 71, 89].

Shreider:1966:MCM

[393] I. A. (Ulii Anatol'evich) Shreider and N. P. (Nikolai Panteleimonovich) Buslenko, editors. *The Monte Carlo method; the method of statistical trials*, volume 87 of *International series of monographs in pure and applied mathematics*. Pergamon, New York, NY, USA, 1966. xii + 381 pp. LCCN QA273 .S5611.

Spitzer:1966:RPP

[394] Frank Spitzer. Recent publications and presentations: *Information and Information Stability of Random Variables and Processes*, by M. S. Pinsker. *American Mathematical Monthly*, 73(8):912–913, October 1966. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Springer:1966:DPI

[395] M. D. Springer and W. E. Thompson. The distribution of products of independent random variables. *SIAM Journal on Applied Mathematics*, 14(3):511–526, May 1966. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Stroud:1966:GQF

[396] A. H. Stroud and Don Secrest. *Gaussian Quadrature Formulas*. Prentice-Hall, Upper Saddle River, NJ, USA, 1966. ix + 374 pp. LCCN QA299.4.G3 S7 1966.

Watson:1962:PPM

[397] E. J. Watson. Primitive polynomials (mod 2). *Mathematics of Computation*, 16(79):368–369, July 1962. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Zaremba:1966:GLP

[398] S. C. Zaremba. Good lattice points, discrepancy, and numerical integration. *Annali di matematica pura ed applicata. Series 4*, 73(??):293–317, ???? 1966. CODEN ANLMAE. ISSN 0003-4622.

Albert:1967:CNN

[399] G. E. Albert and R. L. Tittle. Classroom notes: Nonnormality of linear combinations of normally distributed random variables. *American Mathematical Monthly*, 74(5):583–585, May 1967. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Azorin:1967:BRR

[400] F. Azorín. Book review: *Random Number Generators* by B. Jansson. *Revue de l'Institut international de statistique = Review of the International Statistical Institute*, 35(1):95–96, 1967. CODEN ISTRDP. ISSN 0373-1138 (print), 2212-1846 (electronic). URL `https://www.jstor.org/stable/1401645`. See [383].

Behboodian:1967:EAV

[401] Javad Behboodian. On the expectation of the absolute value of a random vector. *The American Statistician*, 21(4):25–26, October 1967. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682101`.

Canavos:1967:CAT

[402] G. C. Canavos. A comparative analysis of two concepts in the generation of uniform pseudorandom numbers. In ????, editor, *Proceedings of the 22nd Conference of the ACM*, pages 485–501. ACM Press, New York, NY 10036, USA, 1967. LCCN ????

Chambers:1967:RNG

[403] R. P. Chambers. Random-number generation on digital computers. *IEEE Spectrum*, 4(2):48–56, February 1967. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Coveyou:1967:FAU

[404] R. R. Coveyou and R. D. MacPherson. Fourier analysis of uniform random number generators. *Journal of the ACM*, 14(1):100–119, January 1967. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Csorgo:1967:NPS

[405] Miklós Csörgö. A new proof of some results of Rényi and the asymptotic distribution of the range of his Kolmogorov–Smirnov type random variables. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 19(??):550–558, ???? 1967. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

deBalbine:1967:NRP

[406] Guy de Balbine. Note on random permutations (in Technical Notes and Short Papers). *Mathematics of Computation*, 21(100):710–712, October 1967. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Downham:1967:MCP

[407] D. Y. Downham and F. D. K. Roberts. Multiplicative congruential pseudo-random number generators. *The Computer Journal*, 10 (1):74–77, May 1967. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_10/Issue_01/100074.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_10/Issue_01/tiff/74.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_10/Issue_01/tiff/75.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_10/Issue_01/tiff/76.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_10/Issue_01/tiff/77.tif`.

Gabai:1967:DCS

[408] H. Gabai. On the discrepancy of certain sequences mod1. *Illinois Journal of Mathematics*, 11(??):1–12, ???? 1967. CODEN IJMTAW. ISSN 0019-2082 (print), 1945-6581 (electronic).

Gebhardt:1967:GPR

[409] Friedrich Gebhardt. Generating pseudo-random numbers by shuffling a Fibonacci sequence (in Technical Notes and Short Papers). *Mathematics of Computation*, 21(100):708–709, October 1967. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Golomb:1967:SRS

[410] Solomon W. (Solomon Wolf) Golomb. *Shift Register Sequences*. Holden-Day series in information systems. Holden-Day, San Francisco, CA, USA, 1967. xiv + 224 pp. LCCN QA267.5.S4 G6. Portions co-authored by Lloyd R. Welch, Richard M. Goldstein and Alfred W. Hales.

Good:1967:GST

[411] I. J. Good and T. N. Gover. The generalized serial test and the binary expansion of $\sqrt{2}$. *Journal of the Royal Statistical Society. Series A (General)*, 130(1):102–107, ???? 1967. CODEN JSSAEF. ISSN 0035-9238. URL `http://www.jstor.org/stable/2344040`. See remark [442].

Gorenstein:1967:TRN

[412] Samuel Gorenstein. Testing a random number generator. *Communications of the ACM*, 10(2):111–118, February 1967. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Gurland:1967:ISE

[413] John Gurland. An inequality satisfied by the expectation of the reciprocal of a random variable. *The American Statistician*, 21(2):24–25, April 1967. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682610`.

Hemmerle:1967:SCD

[414] William J. Hemmerle. *Statistical Computations on a Digital Computer*. Blaisdell, Waltham, MA, USA, 1967. x + 230 pp. LCCN QA276 .H42.

Itzelsberger:1967:SEP

[415] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [4096], pages 64–68. LCCN QA76.5 D55 1965.

Marlow:1967:NLT

[416] N. A. Marlow. A normal limit theorem for power sums of independent random variables. *The Bell System Technical Journal*, 46(9):2081–2089, November 1967. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol46/bstj46-9-2081.pdf`; `http://www.alcatel-lucent.com/bstj/vol46-1967/articles/bstj46-9-2081.pdf`.

Mullen:1967:NRT

[417] Kenneth Mullen. A note on the ratio of two independent random variables. *The American Statistician*, 21(3):30–31, June 1967. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682042`.

Nasell:1967:SPP

[418] Ingemar Nasell. Some properties of power sums of truncated normal random variables. *The Bell System Technical Journal*, 46(9):2091–2110, November 1967. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol46/bstj46-9-2091.pdf`; `http://www.alcatel-lucent.com/bstj/vol46-1967/articles/bstj46-9-2091.pdf`.

Page:1967:GPR

[419] E. S. Page. The generation of pseudo-random numbers. In Hollingdale [4096], pages 55–63. LCCN QA76.5 D55 1965.

Ratz:1967:MPN

[420] Herbert C. Ratz and J. V. Hildebrand. Modified pseudorandom number generators. *IEEE Transactions on Electronic Computers*, EC-16(6):854–856, December 1967. CODEN IEECA8. ISSN 0367-7508. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4039202`.

Sclove:1967:FRE

[421] Stanley L. Sclove, Gordon Simons, and J. Van Ryzin. Further remarks on the expectation of the reciprocal of a positive random variable. *The American Statistician*, 21(4):33–34, October 1967. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682105`.

Serfling:1967:NCR

[422] R. J. Serfling. A note on the covariance of a random variable and its reciprocal. *The American Statistician*, 21(4):33, October 1967. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682104`.

Sobol:1967:DPC

[423] I. M. Sobol'. On the distribution of points in a cube and the approximate evaluation of integrals. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 7(4):86–112, ???? 1967. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/0041555367901449`. English translation of Russian original published in Zh. vychisl. Mat. mat. Fiz. **7**(4), 784–802, 1967.

Solomon:1967:RPD

[424] H. Solomon. Random packing density. In Lucien M. Le Cam and Jerzy Neyman, editors, *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability. Volume III. Physical Sciences*, volume 3, pages 119–134. University of California Press, Berkeley, CA, USA, 1967. LCCN QA276 .B4 v.3. URL `http://projecteuclid.org/euclid.bsmsp/1200513624`. Held at the Statistical Laboratory, University of California, June 21–July 18, 1965 and December 27, 1965–January 7, 1966.

Stein:1967:CPA

[425] Josef Stein. Computational problems associated with Racah algebra. *Journal of Computational Physics*, 1(3):397–405, February 1967. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999167900472`.

Strome:1967:AUR

[426] W. Murray Strome. Algorithm 294: Uniform random. *Communications of the ACM*, 10(1):40, January 1967. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

VanGelder:1967:SNR

[427] A. Van Gelder. Some new results in pseudo-random number generation. *Journal of the ACM*, 14(4):785–792, October 1967. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Westlake:1967:URN

[428] W. J. Westlake. A uniform random number generator based on the combination of two congruential generators. *Journal of the ACM*, 14 (2):337–340, April 1967. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

White:1967:EDC

[429] R. C. White. Experiments with digital computer simulations of pseudo-random noise generators. *IEEE Transactions on Electronic Computers*, EC-16(3):355–357, June 1967. CODEN IEECA8. ISSN 0367-7508. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4039076`.

Wyner:1967:RPC

[430] A. D. Wyner. Random packings and coverings of the unit n-sphere. *The Bell System Technical Journal*, 46(9):2111–2118, November 1967. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol46/bstj46-9-2111.pdf`; `http://www.alcatel-lucent.com/bstj/vol46-1967/articles/bstj46-9-2111.pdf`.

Adhikari:1968:DMS

[431] A. K. Adhikari and B. P. Sarkar. Distribution of most significant digit in certain functions whose arguments are random variables. *Sankhyā (Indian Journal of Statistics), Series B. Methodological*, 30(??):47–58, ???? 1968. CODEN SANBBV. ISSN 0976-8386 (print), 0976-8394 (electronic).

Anonymous:1968:GCM

[432] Anonymous. The generation of correlated multivariate samples for Monte Carlo simulation. *IEEE Spectrum*, 5(2):5, February 1968. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic).

Ayoub:1968:EEK

[433] F. Ayoub. Erratum: Encryption with keyed random permutations. *Electronics Letters*, 17(??):??, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4246020`.

Ayoub:1968:EKR

[434] F. Ayoub. Encryption with keyed random permutations. *Electronics Letters*, 17(??):583–585, February 1968. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4245887`.

Bell:1968:ANR

[435] James R. Bell. Algorithm 334: Normal random deviates [G5]. *Communications of the ACM*, 11(7):498, July 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See also [1051].

Berlekamp:1968:ACT

[436] Elwyn R. Berlekamp. *Algebraic coding theory*. McGraw-Hill series in systems science. McGraw-Hill, New York, NY, USA, 1968. xiv + 466 pp. LCCN QA268 .B46.

Bradley:1968:RTR

[437] J. V. Bradley. *Runs tests of randomness*. Prentice-Hall, Upper Saddle River, NJ, USA, 1968. ISBN ???? ???? pp. LCCN ????

David:1968:NCM

[438] F. N. (Florence Nightingale) David, editor. *Normal centroids, medians and scores for ordinal data*, volume 29 of *Tracts for Computers*. Cambridge University Press, Cambridge, UK, 1968. 201 pp. LCCN QA47 .T7 no. 29.

Dieter:1968:AME

[439] Ulrich Dieter. Autokorrelation multiplikativ erzeugter Pseudo-Zufallszahlen. (German) [Autocorrelation generated multiplicative pseudo-random numbers]. *Operations Research-Verfahren*, 6(??):69–85, ???? 1968. CODEN ORVEAI. ISSN 0078-5318.

Forsythe:1968:RNG

[440] A. B. Forsythe. Random number generators. *Computers and Biomedical Research*, 1(??):470–474, ???? 1968. CODEN CBMRB7. ISSN 0010-4809 (print), 1090-2368 (electronic).

Gardner:1968:MRS

[441] Martin Gardner. On the meaning of randomness and some ways of achieving it. *Scientific American*, ??(??):116–121, July 1968. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Good:1968:GST

[442] I. J. Good and T. N. Gover. The generalized serial test and the binary expansion of $\sqrt{2}$. *Journal of the Royal Statistical Society. Series A (General)*, 131(??):434, ???? 1968. CODEN JSSAEF. ISSN 0035-9238. See [411].

Good:1968:RHP

[443] I. J. Good and R. F. Churchhouse. The Riemann hypothesis and pseudo-random features of the Möbius sequence. *Mathematics of Computation*, 22(104):857–861, October 1968. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2004584.pdf`.

Green:1968:TRP

[444] J. W. (John William) Green. *Tables of random permutations*. Department of National Development, Forestry and Timber Bureau, Canberra, ACT, Australia, 1968. 161 pp. LCCN SD110 .A33 no. 44.

Gregory:1968:GRP

[445] G. Gregory and K. Sharpe. A generalization of the rejection procedure for the generation of random variables. *Australian Computer Journal*, 1 (3):169–172, 1968. CODEN ACMJB2. ISSN 0004-8917.

Kruskal:1968:NNC

[446] William Kruskal. Note on a note by C. S. Pillai. *The American Statistician*, 22(5):24–25, December 1968. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681837`. See [458].

Lindholm:1968:APR

[447] J. H. Lindholm. An analysis of the pseudo-randomness properties of subsequences of long m-sequences. *IEEE Transactions on Information Theory*, IT-14(4):569–576, 1968. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Marsaglia:1968:OLRa

[448] George Marsaglia and T. A. Bray. One-line random number generators and their use in combinations. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, March 1968. 12 pp. URL `http://www.dtic.mil/docs/citations/AD0667956`.

Marsaglia:1968:OLRb

[449] George Marsaglia and T. A. Bray. One-line random number generators and their use in combinations. *Communications of the ACM*, 11(11): 757–759, November 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Marsaglia:1968:QPR

[450] George Marsaglia. Query 27: Pseudo random normal numbers. *Technometrics*, 10(2):401–402, May 1968. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/1267057`.

Marsaglia:1968:RNF

[451] George Marsaglia. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences of the United States of America*, 61(1):25–28, September 15, 1968. CODEN PNASA6. ISSN 0027-8424 (print), 1091-6490 (electronic). A popularized account of this work appeared as "Are random numbers really random?" [Scientific Research (Philadelphia, PA), 3 (1968), 21–??]. This widely-cited paper describes the hyperplane problem that linear congruential generators suffer from, although careful choice of multipliers can minimize its importance: see [404, 2258, 2257, 2508].

Matthews:1968:GPN

[452] S. B. Matthews. Generation of pseudorandom noise having a Gaussian spectral density. *IEEE Transactions on Computers*, C-17(4):382–385, April 1968. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1687351`.

Meijer:1968:DASa

[453] H. G. Meijer. The discrepancy of a G-adic sequence. *Nederl. Akad. Wetensch, Proc. Ser. A*, 71(??):54–66, ???? 1968. CODEN ???? ISSN ????

Meijer:1968:DASb

[454] H. G. Meijer. The discrepancy of a g-adic sequence. *Indagationes Mathematicæ*, 30(??):54–66, ???? 1968. CODEN IMTHBJ. ISSN 0019-3577, 0023-3358.

Millenson:1968:HRN

[455] J. R. Millenson and G. D. Sullivan. A hardware random number generator for use with computer control of probabilistic contingencies. *Behavior Research Methods and Instrumentation*, 1(5):194–196, January 1968. CODEN BRMIAC. ISSN 0005-7878. URL `http://www.springerlink.com/content/l6q4517x00r56955/`.

Miller:1968:ACP

[456] J. C. P. Miller and M. J. Prentice. Additive congruential pseudorandom number generators. *The Computer Journal*, 11(3):341–346, November 1968. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/110341.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/341.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/342.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/343.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/344.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/345.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_11/Issue_03/tiff/346.tif`.

Muller:1968:RN

[457] M. E. Muller. Random numbers. In ????, editor, *International Encyclopedia of Social Sciences*, pages 307–313. ????, ????, 1968. LCCN ????

Pillai:1968:NEI

[458] C. S. Pillai. A note on the expectation of an irrational function of a random variable. *The American Statistician*, 22(3):31, June 1968. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681808`. See note [446].

Polljak:1968:APN

[459] Ju. G. Polljak. On the analysis of pseudorandom numbers. *Avtomat. i Vyčisl. Tehn.*, 5(??):31–35, ???? 1968. CODEN ???? ISSN 0132-4160.

Show:1968:AGR

[460] Richard H. Show. Algorithm 342: Generator of random numbers satisfying the Poisson distribution. *Communications of the ACM*, 11(12): 819–820, December 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Sibuya:1968:GDE

[461] M. Sibuya. Generating doubly exponential random numbers. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 5(??):1–7, 1968. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic).

Snow:1968:AGR

[462] R. H. Snow. Algorithm 342: Generator of random numbers satisfying the Poisson distribution [G5]. *Communications of the ACM*, 11(12):819–820, December 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Whittlesey:1968:CCB

[463] John R. B. Whittlesey. A comparison of the correlational behavior of random number generators for the IBM 360. *Communications of the ACM*, 11(9):641–644, September 1968. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See implementation [475].

Zaremba:1968:GLP

[464] S. C. Zaremba. Good lattice points in the sense of Hlawka and Monte Carlo integration. *Monatshefte für Mathematik*, 72(3):264–269, June 1968. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/j48m46451580607q/`.

Zaremba:1968:MBM

[465] S. K. Zaremba. The mathematical basis of Monte Carlo and quasi-Monte Carlo methods. *SIAM Review*, 10(3):303–314, July 1968. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2027655`.

Beasley:1969:DTS

[466] J. D. Beasley and K. Wilson. Design and testing of the System 4 random number generator. *The Computer Journal*, 12(4):368–372, November 1969. CODEN CMPJA6. ISSN 0010-4620 (print),

1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/120368.sgm.abs.html; http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/368.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/369.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/370.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/371.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/372.tif.

Bell:1969:DFT

[467] C. B. Bell and J. F. Donoghue. Distribution-free tests of randomness. *Sankhyā (Indian Journal of Statistics), Series A. Methods and Techniques*, 31(??):157–176, ???? 1969. CODEN SANABS. ISSN 0036-4452.

Chaitin:1969:LPC

[468] Gregory J. Chaitin. On the length of programs for computing finite binary sequences: Statistical considerations. *Journal of the ACM*, 16 (1):145–159, January 1969. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Coveyou:1969:RNG

[469] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [4098], pages 70–111. LCCN QA1 S565 v. 3.

Cunsolo:1969:CNP

[470] D. Cunsolo. Costruzione di numeri pseudorandom con periodo superiore alla base m. (Italian) [generation of pseudorandom numbers with period greater than the base m]. *Calcolo: a quarterly on numerical analysis and theory of computation*, 6(1):69–85, March 1969. CODEN CALOBK. ISSN 0008-0624 (print), 1126-5434 (electronic). URL http://www.springerlink.com/content/60u464k30851uj27/.

Deo:1969:APN

[471] N. Deo and D. Rubin. An additive pseudorandom number generator with semi-infinite sequence length. Report, NASA, ????, 1969. 4 pp. Document ID 19700050209.

Dieter:1969:AME

[472] Ulrich Dieter. Autokcorrelation multiplikativ erzeugter Pseudo-Zufallszahlen. (German) [Autocorrelation in multiplicatively-generated pseudorandom numbers]. *Operations Research-Verfahren*, 6(??):69–85, ???? 1969. CODEN ORVEAI. ISSN 0078-5318.

Donnelly:1969:STU

[473] T. Donnelly. Some techniques for using pseudorandom numbers in computer simulation. *Communications of the ACM*, 12(7):392–394, July 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Downham:1969:RT

[474] D. Y. Downham. The runs up and down test. *The Computer Journal*, 12(4):373–376, November 1969. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/120373.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/373.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/374.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/375.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_12/Issue_04/tiff/376.tif`.

Fellen:1969:LEI

[475] Bryna M. Fellen. Letter to the Editor: an implementation of the Tausworthe generator. *Communications of the ACM*, 12(7):413, July 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [463].

Good:1969:HRR

[476] I. J. Good. How random are random numbers? *The American Statistician*, 23(4):42–45, October 1969. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681742`.

Grosenbaugh:1969:MFR

[477] L. R. Grosenbaugh. More on Fortran random number generators. *Communications of the ACM*, 12(11):639, November 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Gubenko:1969:FPR

[478] V. S. Gubenko, N. E. Kirillov, K. A. Meškovskiĭ, and A. I. Čerkunov. Formation of pseudo-random uniformly distributed numbers from noise-like signals. *Izv. Akad. Nauk SSSR Tehn. Kibernet.*, 1(??):57–63, ???? 1969. CODEN ???? ISSN ????

Hemmerle:1969:GPN

[479] W. J. Hemmerle. Generating pseudorandom numbers on a two's complement machine such as the IBM 360. *Communications of the ACM*, 12(7):382–383, July 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Knop:1969:RAG

[480] R. Knop. Remark on Algorithm 334 [G5]: Normal random deviates. *Communications of the ACM*, 12(5):281, May 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Kruskal:1969:EPR

[481] J. B. Kruskal. Extremely portable random number generator. *Communications of the ACM*, 12(2):93–94, February 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Lee:1969:ECF

[482] W. C. Y. Lee. An extended correlation function of two random variables applied to mobile radio transmission. *The Bell System Technical Journal*, 48(10):3423–3440, December 1969. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol48/bstj48-10-3423.pdf`; `http://www.alcatel-lucent.com/bstj/vol48-1969/articles/bstj48-10-3423.pdf`. See erratum [498].

Lehmer:1969:BRR

[483] D. H. Lehmer. Book review: *Random number generators* by Birger Jansson. *Quarterly of Applied Mathematics*, 27(3):421, 1969. CODEN QAMAAY. ISSN 0033-569X (print), 1552-4485 (electronic). URL `http://www.jstor.org/stable/43636000`.

Lewis:1969:PNG

[484] P. A. W. Lewis, A. S. Goodman, and J. M. Miller. A pseudorandom number generator for the SYSTEM/360. *IBM Systems Journal*, 8(2): 136–146, 1969. CODEN IBMSA7. ISSN 0018-8670.

Marsaglia:1969:OSA

[485] George Marsaglia. One-sided approximations by linear combinations of functions. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, September 1969. 18 pp. URL `http://www.dtic.mil/docs/citations/AD0695796`.

Marsaglia:1969:RCR

[486] George Marsaglia. Regularities in congruential random number generators. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, May 1969. 8 pp. URL `http://www.dtic.mil/docs/citations/AD0689295`.

Martin-Lof:1969:AR

[487] P. Martin-Löf. Algorithms and randomness. *Revue de l'Institut international de statistique = Review of the International Statistical Institute*, 37(??):265–272, ???? 1969. CODEN ???? ISSN 0373-1138 (print), 2212-1846 (electronic).

Massey:1969:SRS

[488] J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, IT-15(1):122–127, January 1969. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Meyer:1969:MGR

[489] D. L. Meyer. Methods of generating random normal numbers. *Educational and Psychological Measurement*, 29(1):193–198, ???? 1969. CODEN EPMEAJ. ISSN 0013-1644 (print), 1552-3888 (electronic).

Naylor:1969:BSG

[490] T. H. Naylor. Bibliography 19: Simulation and gaming. *Computing Reviews*, 10(??):61–69, ???? 1969. CODEN CPGRA6. ISSN 0010-4884, 0149-1202.

Passaquindici:1969:MMC

[491] Maria Passaquindici. I metodi di Monte Carlo e la generazione dei numeri casuali. (Italian) [Monte Carlo methods and the generation of random numbers]. *Metron*, 27(3–4):88–112, i–viii. (2 foldouts), ???? 1969. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Payne:1969:CLP

[492] W. H. Payne, J. R. Rabung, and T. P. Bogyo. Coding the Lehmer pseudorandom number generator. *Communications of the ACM*, 12(2):85–86, February 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Seraphin:1969:NAF

[493] Dominic S. Seraphin. Numerical analysis: a fast random number generator for IBM 360. *Communications of the ACM*, 12(12):695, Decem-

ber 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Verdier:1969:RWS

[494] P. H. Verdier. Relations within sequences of congruential pseudorandom numbers. *Journal of Research of the National Bureau of Standards. Section B, Mathematics and Mathematical Physics*, 73(??):41–44, ???? 1969. CODEN JNBBAU. ISSN 0022-4340.

Whittlesey:1969:LEM

[495] John R. B. Whittlesey. Letter to the Editor: On the multidimensional uniformity of pseudorandom generators. *Communications of the ACM*, 12(5):247, May 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [451].

Zaremba:1969:MBM

[496] S. K. Zaremba. The mathematical basis of Monte Carlo and quasi-Monte Carlo methods. In Anonymous [4098], pages 1–12. LCCN QA1 S565 v. 3. See critical comments in [469, pages 108–110].

Ahrens:1970:PRN

[497] J. H. Ahrens, Ulrich Dieter, and A. Grube. Pseudo-random numbers. A new proposal for the choice of multiplicators. *Computing: Archiv für Informatik und Numerik*, 6(1–2):121–138, March 1970. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Anonymous:1970:EWC

[498] Anonymous. Erratum: W. C. Y. Lee, *An extended correlation function of two random variables applied to mobile radio transmission*, BSTJ **48**(10) 3423–3440 (1969). *The Bell System Technical Journal*, 49(2):320, February 1970. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol49/bstj49-2-320.pdf`; `http://www.alcatel-lucent.com/bstj/vol49-1970/articles/bstj49-2-320.pdf`. See [482].

Anonymous:1970:FVP

[499] Anonymous. A Fortran V package for testing and anaylsis of pseudorandom number generators. Technical report CP-700011, Computer Science/Operations Research Center, Institute of Technology, Southern Methodist University, Dallas, TX, USA, 1970. 32 pp.

Behboodian:1970:ERV

[500] Javad Behboodian. On the expectation of the random variable $(X^2 - Y^2)^{1/2}$. *The American Statistician*, 24(4):28–29, October 1970. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2681312`.

Blaisdell:1970:RSP

[501] B. E. Blaisdell and H. Solomon. On random sequential packing in the plane and a conjecture of Palásti. *Journal of Applied Probability*, 7(3): 667–689, December 1970. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL `http://www.jstor.org/stable/3211946`.

Butler:1970:AAG

[502] E. L. Butler. ACM Algorithm 370: General random number generator. *Communications of the ACM*, 13(1):49–52, January 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remark [620].

Cenacchi:1970:PRN

[503] G. Cenacchi and A. De Matteis. Pseudo-random numbers for comparative Monte Carlo calculations. *Numerische Mathematik*, 16(1):11–15, February 1970. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Dixon:1970:NSE

[504] J. Dixon. The number of steps in the Euclidean algorithm. *Journal of Number Theory*, 2(??):414–422, ???? 1970. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic).

Downham:1970:SAA

[505] D. Y. Downham. Statistical algorithms: Algorithm AS 29: The runs up and down test. *Applied Statistics*, 19(2):190–192, June 1970. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/29`. See [809].

Fuchs:1970:EDR

[506] E. A. Fuchs and P. E. Jackson. Estimates of distributions of random variables for certain computer communications traffic models. *Communications of the ACM*, 13(12):752–757, December 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Reproduced in Advances in Computer Commun., Chu, W. W., (Ed (1974), 2-7; in Computer Commun., Green, P. E., and Lucky, R. W. (Eds.), (1975), 577-582).

Good:1970:RPM

[507] Irving John Good. Review of Philip McShane, *Randomness, Statistics, and Emergence*, Gill and MacMillan, 1970. *Times Literary Supplement*, ??(??):1043, September 18, 1970. See book [524].

Gustavson:1970:FRN

[508] F. G. Gustavson and W. Liniger. A fast random number generator with good statistical properties. *Computing: Archiv für Informatik und Numerik*, 6(3–4):221–226, 1970. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Haber:1970:NEM

[509] Seymour Haber. Numerical evaluation of multiple integrals. *SIAM Review*, 12(4):481–526, October 1970. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2028488`.

Haber:1970:SNA

[510] Seymour Haber. Sequences of numbers that are approximately completely equidistributed. *Journal of the ACM*, 17(2):269–272, April 1970. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Halton:1970:RPS

[511] John H. Halton. A retrospective and prospective survey of the Monte Carlo method. *SIAM Review*, 12(1):1–63, ???? 1970. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Harris:1970:AFG

[512] V. C. Harris. An algorithm for finding the greatest common divisor. *Fibonacci Quarterly*, 8(1):102–103, February 1970. CODEN FIBQAU. ISSN 0015-0517. URL `http://www.fq.math.ca/Scanned/8-1/harris1.pdf`.

Hastings:1970:MCS

[513] W. K. Hastings. Monte Carlo sampling methods using Markov chains and their applications. *Biometrika*, 57(1):97–109, April 1970. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2334940`; `http://www.probability.ca/hastings/`. This paper introduces what is now known as the Metropolis–Hastings algorithm, a generalization of the work in [119]. See [2788, page 255].

Johnson:1970:CUD

[514] Norman Lloyd Johnson and Samuel Kotz. *Continuous univariate distributions*. Distributions in statistics. Hougton Mifflin, New York, NY, USA, 1970. xiv + 300 (vol. 1), xiii + 306 (vol. 2) pp. LCCN QA273.6 .J6.

Juncosa:1970:BRBb

[515] Mario Juncosa. Book review: *Random Number Generators* (Birger Jansson). *SIAM Review*, 12(2):310–311, ???? 1970. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://link.aip.org/link/?SIR/12/310/1`.

Kale:1970:CNN

[516] B. K. Kale. Classroom notes: Normality of linear combinations of non-normal random variables. *American Mathematical Monthly*, 77(9):992–995, November 1970. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Knop:1970:AAR

[517] R. E. Knop. ACM Algorithm 381: Random vectors uniform in solid angle. *Communications of the ACM*, 13(5):326, May 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remark [625].

Lempel:1970:HBG

[518] A. Lempel. On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers. *IEEE Transactions on Computers*, C-19(12):1204–1209, December 1970. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671452`.

Linder:1970:TTR

[519] Arthur Linder. Testing a table of random numbers. In Bose and Roy [4099], pages 469–478. ISBN 0-8078-1109-2. LCCN QA273 .E78.

Maritsas:1970:CSV

[520] D. G. Maritsas and M. G. Hartley. A case study of a versatile generator of repeatable non-Poisson sequences of pseudorandom pulses. *IEEE Transactions on Computers*, C-19(10):924–938, October 1970. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671393`.

Maritsas:1970:DCG

[521] D. G. Maritsas and M. G. Hartley. Design criteria for a generator of repeatable non-Poisson sequences of pseudorandom pulses. *IEEE Transactions on Computers*, C-19(9):812–817, September 1970. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671638`.

Marsaglia:1970:RCR

[522] George Marsaglia. Regularities in congruential random number generators. *Numerische Mathematik*, 16(1):8–10, February 1970. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Marsaglia:1970:RVI

[523] George Marsaglia. Random variables with independent binary digits. Report ??, Boeing Scientific Research Laboratories, Seattle, WA, USA, January 1970. 15 pp. URL `http://www.dtic.mil/docs/citations/AD0705642`.

McShane:1970:RSE

[524] P. McShane. *Randomness, Statistics and Emergence*. University of Notre Dame Press, South Bend, IN, USA, 1970. x + 268 pp. LCCN ????

Murry:1970:GAG

[525] Herschell F. Murry. A general approach for generating natural random variables. *IEEE Transactions on Computers*, C-19(12):1210–1213, December 1970. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671453`.

Payne:1970:FTP

[526] W. H. Payne. Fortran Tausworthe pseudorandom number generator. *Communications of the ACM*, 13(1):57, January 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Prasad:1970:PDA

[527] Ram D. Prasad. Probability distributions of algebraic functions of independent random variables. *SIAM Journal on Applied Mathematics*, 18(3):614–626, May 1970. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Rader:1970:FMG

[528] C. M. Rader, L. R. Rabiner, and R. W. Schafer. A fast method of generating digital random numbers. *The Bell System Technical*

Journal, 49(9):2303–2310, November 1970. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol49/bstj49-9-2303.pdf`.

Reader:1970:RDM

[529] A. V. Reader. Random digits by a mincing process. *The Computer Journal*, 13(1):118, February 1970. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/13/1/118.full.pdf+html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_13/Issue_01/130118.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_13/Issue_01/tiff/118.tif`.

Schaffer:1970:AAG

[530] H. E. Schaffer. ACM Algorithm 369: Generator of random numbers satisfying the Poisson distribution. *Communications of the ACM*, 13(1): 49, January 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Schmidt:1970:QMR

[531] H. Schmidt. Quantum-mechanical random-number generator. *Journal of Applied Physics*, 41(2):462–468, February 1, 1970. CODEN JAPIAU. ISSN 0021-8979 (print), 1089-7550 (electronic), 1520-8850.

Schnorr:1970:DEZa

[532] Claus-Peter Schnorr. Über die Definition von effektiven Zufallstests. Teil I. (German) [On the definition of effective random tests. Part I]. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 15(4): 297–312, ???? 1970. CODEN ZWVGAA. ISSN 0044-3719. URL `http://link.springer.com/article/10.1007/BF00533301`.

Schnorr:1970:DEZb

[533] Claus-Peter Schnorr. Über die Definition von effektiven Zufallstests. Teil II. (German) [On the definition of effective random tests. Part II]. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 15(4): 313–328, ???? 1970. CODEN ZWVGAA. ISSN 0044-3719. URL `http://link.springer.com/article/10.1007/BF00533302`.

Smith:1970:RN

[534] Robert E. (Robert Elijah) Smith. *Random numbers*. Control Data Corp., Minneapolis, MN, USA, 1970. 82 pp.

Springer:1970:DPB

[535] M. D. Springer and W. E. Thompson. The distribution of products of beta, gamma and Gaussian random variables. *SIAM Journal on Applied Mathematics*, 18(4):721–737, June 1970. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Stoneham:1970:NCM

[536] R. G. Stoneham. On a new class of multiplicative pseudo-random number generators. *BIT (Nordisk tidskrift for informationsbehandling)*, 10(4): 481–500, December 1970. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=10&issue=4&spage=481`.

Subrahmaniam:1970:SAM

[537] K. Subrahmaniam. On some applications of Mellin transforms to statistics: Dependent random variables. *SIAM Journal on Applied Mathematics*, 19(4):658–662, December 1970. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Vincent:1970:CGT

[538] C. H. Vincent. Corrigendum: The Generation of Truly Random Binary Numbers. *Journal of Physics. E: Scientific Instruments*, 3(10): 832, October 1970. CODEN JPSIAE. ISSN 0022-3735. URL `http://iopscience.iop.org/0022-3735/3/10/528/`. See [539].

Vincent:1970:GTR

[539] C. H. Vincent. The generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 3(8):594–598, August 1970. CODEN JPSIAE. ISSN 0022-3735. URL `http://iopscience.iop.org/0022-3735/3/8/303`. See corrigendum [538].

White:1970:FDC

[540] R. C. White, Jr. A fast digital computer method for recursive estimation of the mean. *IEEE Transactions on Computers*, C-19(9):847–850, September 1970. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671646`. See comments [603].

Zaremba:1970:DII

[541] S. K. Zaremba. La discrépance isotrope et l'intégration numérique. (French) [Isotropic discrepancy and numerical integration]. *Annali di*

matematica pura ed applicata. Series 4, 87(??):125–136, ???? 1970. CODEN ANLMAE. ISSN 0373-3114 (print), 1618-1891 (electronic).

Ashford:1971:BRG

[542] J. R. Ashford. Book reviews: *The Generation of Random Variates*, by T. G. Newman and P. L. Odell. *Applied Statistics*, 20(3):325, 1971. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Berman:1971:GGD

[543] M. B. Berman. Generating gamma distributed variates for computer simulation models. Report ??, RAND Corporation, Santa Monica, CA, USA, 1971. ?? pp.

Beyer:1971:LSM

[544] W. A. Beyer, R. B. Roof, and Dorothy Williamson. The lattice structure of multiplicative congruential pseudo-random vectors. *Mathematics of Computation*, 25(114):345–363, April 1971. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2004931.pdf`. See corrigenda [2149].

Brown:1971:LRA

[545] J. L. Brown, Jr. and R. L. Duncan. The least remainder algorithm. *Fibonacci Quarterly*, 9(4):347–350, October 1971. CODEN FIBQAU. ISSN 0015-0517. URL `http://www.fq.math.ca/Scanned/9-4/brown-a.pdf`.

Chen:1971:RNN

[546] Edwin H. Chen. A random normal number generator for 32-bit-word computers. *Journal of the American Statistical Association*, 66(334): 400–403, June 1971. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2283944`.

Cohn:1971:PRB

[547] Charles Erwin Cohn. The performance of random-bit generators. *Simulation*, 17(6):234–236, December 1971. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/17/6/234.full.pdf+html`.

Craddock:1971:TRM

[548] J. M. Craddock and Sheila A. Farmer. Two robust methods of random number generation. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 20(3):55–66, September 1971. CODEN ???? ISSN

0039-0526 (print), 1467-9884 (electronic). URL `http://www.jstor.org/stable/2986798`.

Davies:1971:PWO

[549] A. C. Davies. Properties of waveforms obtained by nonrecursive digital filtering of pseudorandom binary sequences. *IEEE Transactions on Computers*, C-20(3):270–281, March 1971. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1671824`.

Dieter:1971:EDS

[550] Ulrich Dieter and J. Ahrens. An exact determination of serial correlations of pseudo-random numbers. *Numerische Mathematik*, 17(2):101–123, April 1971. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Dieter:1971:PRN

[551] Ulrich Dieter. Pseudo-random numbers: The exact distribution of pairs. *Mathematics of Computation*, 25(116):855–883, October 1971. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Donn:1971:MDP

[552] E. S. Donn. Manipulating digital patterns with a new binary sequence generator. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 22(8):2–8, April 1971. CODEN HPJOAX. ISSN 0018-1153.

Dyadkin:1971:ANA

[553] I. G. Dyadkin. An analogue of von Neumann's algorithm for simulating a normal distribution. In *Monte Carlo methods and applications (Metody Monte-Karlo i ikh primeneniya USSR Academy of Sciences, Siberian Branch. Computing Center (VTs SO AN SSSR). Novosibirsk, 30 August–3 September 1971 (Vychislitelnyi Tsentr, Sibirskoye Otdelenie. Akademiia Nauk. SSSR))*, pages 53–54. Akademiia Nauk SSSR, Novosibirsk, USSR, 1971.

Friedman:1971:REG

[554] Jerome H. Friedman. Random event generation with preferred frequency distributions. *Journal of Computational Physics*, 7(2):201–218, April 1971. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999171900854`.

Gibbons:1971:NSI

[555] Jean Dickinson Gibbons. *Nonparametric Statistical Inference*. McGraw-Hill series in probability and statistics. McGraw-Hill, New York, NY, USA, 1971. ISBN 0-07-085250-2, 0-07-023166-4. xiv + 306 pp. LCCN QA278.8 .G5.

Good:1971:SRS

[556] I. J. Good and R. A. Gaskins. Some relationships satisfied by additive and multiplicative congruential sequences, with implications for pseudo-random number generation. In A. O. L. (Arthur O. L.) Atkin and B. J. (Bryan John) Birch, editors, *Computers in number theory: proceedings of the Science Research Council Atlas Symposium no. 2 held at Oxford, from 18–23 August, 1969*, pages 125–136. Academic Press, New York, NY, USA, 1971. ISBN 0-12-065750-3. LCCN QA241 .S35 1969.

Han:1971:DRV

[557] Chien-Pai Han. Dependence of random variables. *The American Statistician*, 25(4):35, October 1971. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2682925`.

Jackson:1971:PCC

[558] P. A. Jackson. PRBS cross-correlation measurements by hybrid computational techniques. *The Computer Journal*, 14(1):49–54, February 1971. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/140049.sgm.abs.html`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/49.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/50.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/51.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/52.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/53.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_14/Issue_01/tiff/54.tif`.

Kendall:1971:BRR

[559] David Kendall. Book review: *Random Variables and Probability Distributions* by H. Cramér. *Revue de l'Institut international de statistique = Review of the International Statistical Institute*, 39(2):240, 1971. CODEN ISTRDP. ISSN 0373-1138 (print), 2212-1846 (electronic). URL `https://www.jstor.org/stable/1402181`.

Kozlov:1971:DRN

[560] G. A. Kozlov. On the distribution of random numbers produced by sequential physical generators. *Theory of Probability and its Applications*, 16(2):369–378, ???? 1971. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Marsaglia:1971:RVI

[561] George Marsaglia. Random variables with independent binary digits. *Annals of Mathematical Statistics*, 42(6):1922–1929, December 1971. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://projecteuclid.org/euclid.aoms/1177693058`; `http://www.jstor.org/stable/2240118`.

Mitra:1971:PDS

[562] Samarendra Kumar Mitra. On the probability distribution of the sum of uniformly distributed random variables. *SIAM Journal on Applied Mathematics*, 20(2):195–198, March 1971. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Newman:1971:GRVa

[563] Thomas G. Newman and Patrick L. Odell. *The generation of random variates*, volume 29 of *Griffin's Statistical Monographs and Courses*. Charles Griffin & Co. Ltd., London, UK, 1971. ISBN 0-85264-194-X. viii + 88 pp. LCCN QA276.5 N55.

Newman:1971:GRVb

[564] Thomas G. Newman and Patrick L. Odell. *The generation of random variates*. Hafner, New York, NY, USA, 1971. ISBN ???? 88 (est.) pp. LCCN QA276.5 N55.

Payne:1971:CDS

[565] W. H. Payne and T. G. Lewis. Continuous distribution sampling: accuracy and speed. In Rice [4100], page ?? ISBN 0-12-587250-X. LCCN QA1 .M26. Based on the proceedings of the Mathematical Software Symposium held at Purdue University, Lafayette, Indiana, USA, April 1–3, 1970.

Philipp:1971:MSR

[566] Walter Philipp. *Mixing sequences of random variables and probablistic number theory*, volume 114 of *Memoirs of the American Mathematical Society*. American Mathematical Society, Providence, RI, USA, 1971. i + 102 pp. LCCN ????

Phillips:1971:PGG

[567] Don T. Phillips and Charles Beightler. Procedures for generating gamma variates with non-integer parameter sets. In *Proceedings of the 5th Conference on Winter Simulation — WSC '71*, pages 421–427. ACM Press, New York, NY 10036, USA, 1971.

Rizzi:1971:MGS

[568] Alfredo Rizzi. On a method for generating sequences of binary pseudo random numbers. *Metron*, 29(??):61–70, ???? 1971. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Schnorr:1971:UAD

[569] Claus-Peter Schnorr. A unified approach to the definition of random sequences. *Theory of Computing Systems*, 5(3):246–258, September 1971. CODEN TCSYFI. ISSN 1432-4350 (print), 1433-0490 (electronic). URL `http://www.springerlink.com/content/u08164t2503054rk/`.

Schnorr:1971:ZWA

[570] Claus Peter Schnorr. *Zufälligkeit und Wahrscheinlichkeit: Eine algorithmische Begründung der Wahrscheinlichkeitstheorie. (German) [Randomness and probability. An algorithmic foundation of probability theory]*, volume 218 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1971. CODEN LNMAA2. ISBN 3-540-05566-5 (print), 3-540-36883-3 (e-book). ISSN 0075-8434 (print), 1617-9692 (electronic). iv + 212 pp. URL `http://link.springer.com/book/10.1007/BFb0112458`; `http://www.springerlink.com/content/978-3-540-36883-0`.

Smith:1971:MPR

[571] C. S. Smith. Multiplicative pseudo-random number generators with prime modulus. *Journal of the ACM*, 18(4):586–593, October 1971. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Strawderman:1971:GTP

[572] W. E. Strawderman. Generation and testing of pseudo-random numbers. Technical Report 171, Department of Statistics, Stanford University, Stanford, CA, USA, ???? 1971.

Stroud:1971:ACM

[573] A. H. Stroud. *Approximate calculation of multiple integrals*. Prentice-Hall series in automatic computation. Prentice-Hall, Upper Saddle River, NJ, USA, 1971. ISBN 0-13-043893-6. xiii + 431 pp. LCCN QA311 .S85.

Tootill:1971:RPT

[574] J. P. R. Tootill, W. D. Robinson, and A. G. Adams. The runs up-and-down performance of Tausworthe pseudo-random number generators. *Journal of the ACM*, 18(3):381–399, July 1971. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Vincent:1971:PAG

[575] C. H. Vincent. Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 4(11): 825–828, ???? 1971. CODEN JPSIAE. ISSN 0022-3735. URL `http://iopscience.iop.org/0022-3735/4/11/007`. See corrigendum [631].

Voroncov:1971:UQS

[576] Ju. V. Voroncov and Ju. G. Polljak. On the use of quasirandom sequences in the direct probabilistic simulation of systems. *Avtomat. i Vyčisl. Tehn.*, 6(??):23–27, ???? 1971. CODEN ???? ISSN ????

Zinger:1971:LLC

[577] A. A. Zinger. Limit laws for cumulative sums of independent random variables with a finite number of distribution types. *Theory of Probability and its Applications*, 16(??):596–619, ???? 1971. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **16**, (1971), pp. 614–637.

Ahrens:1972:CMS

[578] Joachim H. Ahrens and Ulrich Dieter. Computer methods for sampling from the exponential and normal distributions. *Communications of the ACM*, 15(10):873–882, October 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Alam:1972:AVM

[579] Khursheed Alam. Asymptotic value of the mean of a function of a normal random variable. *SIAM Journal on Applied Mathematics*, 23(4):495–498, December 1972. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Barr:1972:CMN

[580] Donald R. Barr and Norman L. Sezak. A comparison of multivariate normal generators. *Communications of the ACM*, 15(12):1048–1049, December 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Basu:1972:ITF

[581] A. K. Basu. Invariance theorems for first passage time random variables. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 15(??):171–176, ???? 1972. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Behboodian:1972:CNS

[582] Javad Behboodian. Classroom notes: a simple example on some properties of normal random variables. *American Mathematical Monthly*, 79(6): 632–634, June/July 1972. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Beyer:1972:LSR

[583] W. A. Beyer. Lattice structure and reduced bases of random vectors generated by linear recurrences. In Zaremba [4101], pages 361–370. ISBN 0-12-775950-6. LCCN QA297 .A67.

Broemeling:1972:BPD

[584] L. D. Broemeling. Bayesian procedures for detecting a change in a sequence of random variables. *Metron*, 30(??):214–227, ???? 1972. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Cenacchi:1972:QRS

[585] G. Cenacchi and A. De Matteis. Quasi-random sequences by power residues. *Numerische Mathematik*, 20(1):54–63, February 1972. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Chang:1972:FSD

[586] R. W. Chang and E. Y. Ho. On fast start-up data communication systems using pseudo-random training sequences. *The Bell System Technical Journal*, 51(9):2013–2027, November 1972. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol51/bstj51-9-2013.pdf`; `http://www.alcatel-lucent.com/bstj/vol51-1972/articles/bstj51-9-2013.pdf`.

Dieter:1972:SIP

[587] U. Dieter. Statistical interdependence of pseudo-random numbers generated by the linear congruential method. In Zaremba [4101], pages 287–317. ISBN 0-12-775950-6. LCCN QA297 .A67.

Elias:1972:ECU

[588] P. Elias. The efficient construction of an unbiased random sequence. *Annals of Mathematical Statistics*, 43(3):865–870, June 1972. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL `http://www.jstor.org/stable/2240383`.

Ermakov:1972:NPSa

[589] S. M. Ermakov. Note on pseudorandom sequences. *Ž. Vyčisl. Mat. i Mat. Fiz.*, 12(??):??, ???? 1972. ISSN 1077-1082.

Ermakov:1972:NPSb

[590] S. M. Ermakov. Note on pseudorandom sequences. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 12(4):307–314, ???? 1972. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/004155537290136X`.

Everett:1972:MCS

[591] C. J. Everett and E. D. Cashwell. A Monte Carlo sampler. Informal Report LA-5061-MS, Los Alamos Scientific Laboratory, Los Alamos, NM, USA, 1972.

Falk:1972:EDT

[592] H. Falk. Entropy decomposition and transfer-matrix problems. *Journal of Mathematical Physics*, 13(5):608–609, May 1972. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v13/i5/p608_s1`.

Forsythe:1972:NCMa

[593] George E. Forsythe. Von Neumann's comparison method for random sampling from the normal and other distributions. Technical Report CS-TR-72-254, Stanford University, Department of Computer Science, Stanford, CA, USA, January 1972. 21 pp.

Forsythe:1972:NCMb

[594] George E. Forsythe. Von Neumann's comparison method for random sampling from the normal and other distributions. *Mathematics of Computation*, 26(120):817–826, October 1972. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Frazer:1972:BOM

[595] W. D. Frazer and B. T. Bennett. Bounds on optimal merge performance, and a strategy for optimality. *Journal of the ACM*, 19(4):641–648, Oc-

tober 1972. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Garside:1972:BRBa

[596] M. J. Garside. Book review: *The Generation of Random Variates*, by T. G. Newman; P. L. Odell. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 21(2):143, June 1972. CODEN ???? ISSN 0039-0526 (print), 1467-9884 (electronic). URL `http://www.jstor.org/stable/2987327`.

Heathcote:1972:TGF

[597] C. E. Heathcote. A test of goodness of fit for symmetric random variables. *Australian Journal of Statistics*, 14(2):172–181, August 1972. CODEN AUJSA3. ISSN 0004-9581.

Hurst:1972:AAG

[598] Rex L. Hurst and Robert E. Knop. ACM Algorithm 425: Generation of random correlated normal variables [G5]. *Communications of the ACM*, 15(5):355–357, May 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remark [700].

Kirschenmann:1972:CR

[599] P. Kirschenmann. Concepts of randomness. *Journal of Philosophical Logic*, 1(??):395–414, ???? 1972. CODEN JPLGA7. ISSN 0022-3611 (print), 1573-0433 (electronic).

Kral:1972:ENA

[600] J. Král. Erratum: "A new additive pseudorandom number generator for extremely short word-length". *Information Processing Letters*, 1(5):216, October 1972. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [601].

Kral:1972:NAP

[601] J. Král. A new additive pseudorandom number generator for extremely short word-length. *Information Processing Letters*, 1(4):164–167, June 1972. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See erratum [600].

Maddocks:1972:CAG

[602] R. S. Maddocks, S. Matthews, E. W. Walker, and C. H. Vincent. A compact and accurate generator for truly random binary digits. *Journal of Physics. E: Scientific Instruments*, 5(??):542–544, ???? 1972. CODEN

JPSIAE. ISSN 0022-3735. URL http://iopscience.iop.org/0022-3735/5/6/018.

Majithia:1972:CFD

[603] J. C. Majithia. Comments on "A Fast Digital Computer Method for Recursive Estimation of the Mean". *IEEE Transactions on Computers*, C-21(5):511–512, May 1972. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1672147. See [540].

Marsaglia:1972:CPS

[604] George Marsaglia. Choosing a point from the surface of a sphere. *Annals of Mathematical Statistics*, 43(2):645–646, April 1972. CODEN AASTAD. ISSN 0003-4851 (print), 2168-8990 (electronic). URL http://projecteuclid.org/euclid.aoms/1177692644; http://www.jstor.org/stable/2240001.

Marsaglia:1972:SLC

[605] George Marsaglia. The structure of linear congruential sequences. In Zaremba [4101], pages 249–285. ISBN 0-12-775950-6. LCCN QA297 .A67.

Mason:1972:LTN

[606] J. David Mason. Local theorems for nonidentically distributed lattice random variables. *SIAM Journal on Applied Mathematics*, 22(2):259–265, March 1972. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Meyer:1972:PCC

[607] C. H. Meyer and W. L. Tuchman. Pseudorandom codes can be cracked. *Electronic Design*, 20(23):74–76, November 9, 1972. CODEN ELODAW. ISSN 0013-4872 (print), 1944-9550 (electronic).

Mihram:1972:SV

[608] G. Arthur Mihram. *The Stochastic Variate*, volume 92 of *Mathematics in Science and Engineering*, chapter 2, pages 18–146. Academic Press, New York, NY, USA, June 1972. ISBN 0-12-495950-4. LCCN TA343 .M53. URL http://www.sciencedirect.com/science/article/pii/S0076539208613508.

Miyatake:1972:GUR

[609] O. Miyatake. Generation of uniform random numbers of good quality. *Mathematica Japonica*, 17(??):79–84, ???? 1972. CODEN MAJAA9. ISSN 0025-5513.

Nance:1972:BRN

[610] R. E. Nance and C. Overstreet, Jr. A bibliography on random number generation. *Computing Reviews*, 13(??):495–508, ???? 1972. CODEN CPGRA6. ISSN 0010-4884, 0149-1202.

Nance:1972:IFR

[611] Richard E. Nance and Claude Overstreet. Implementation of Fortran random number generators on the SRU 1108. Technical report CP-72022, Computer Science/Operations Research Center, Institute of Technology, Southern Methodist University, Dallas, TX, USA, 1972. 14 pp.

Neave:1972:CLW

[612] Henry R. Neave. A comparison of lag window generators. *Journal of the American Statistical Association*, 67(337):152–158, March 1972. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2284714`.

Neave:1972:RNP

[613] Henry R. Neave. A random number package. *Computer Applications in the Natural and Social Sciences*, 14:55, 1972. ISBN 0-85358-015-4. ISSN 0069-8105.

Niederreiter:1972:DCP

[614] Harald Niederreiter. Discrepancy and convex programming. *Annali di matematica pura ed applicata. Series 4*, 93(??):89–97, ???? 1972. CODEN ANLMAE. ISSN 0373-3114 (print), 1618-1891 (electronic).

Niederreiter:1972:DPR

[615] Harald Niederreiter. On the distribution of pseudo-random numbers generated by the linear congruential method. *Mathematics of Computation*, 26(119):793–795, July 1972. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2005109.pdf`.

Niederreiter:1972:MED

[616] Harald Niederreiter. Methods for estimating discrepancy. In Zaremba [4101], pages 203–236. ISBN 0-12-775950-6. LCCN QA297 .A67.

Norman:1972:CPG

[617] J. E. Norman and L. E. Cannon. A computer program for the generation of random variables from any discrete distribution. *Journal of Statistical Computation and Simulation*, 1(4):331–348, ???? 1972.

CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949657208810026`.

Overstreet:1972:FVP

[618] Claude Overstreet. A FORTRAN V package for testing and anaylsis of pseudorandom number generators. Technical report CP-72009, Computer Science/Operations Research Center, Institute of Technology, Southern Methodist University, Dallas, TX, USA, 1972. 7 + [24] pp.

Phillips:1972:PGG

[619] Don T. Phillips and Charles S. Beightler. Procedures for generating gamma variates with non-integer parameter sets. *Journal of Statistical Computation and Simulation*, 1(3):197–208, ???? 1972. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949657208810015`.

Proll:1972:RAA

[620] L. G. Proll. Remark on "ACM Algorithm 370: General random number generator [G5]". *Communications of the ACM*, 15(6):467–468, June 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [502].

Ramberg:1972:AMG

[621] John S. Ramberg and Bruce W. Schmeiser. Approximate method for generating symmetric random variables. *Communications of the ACM*, 15(11):987–990, November 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Rechtschaffen:1972:QSU

[622] R. N. Rechtschaffen. Queuing simulation using a random number generator. *IBM Systems Journal*, 11(3):255–271, 1972. CODEN IBMSA7. ISSN 0018-8670.

Relles:1972:SAG

[623] Daniel A. Relles. A simple algorithm for generating binomial random variables when N is large. *Journal of the American Statistical Association*, 67(339):612–613, September 1972. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2284449`.

Schincke:1972:EPS

[624] E. Schincke and J. Höpfner. Erzeugungen von Pseudozufallszahlenfolgen mit stückweise polygonaler Verteilung. (German) [Generation of pseudo random number sequences with piecemeal polynomial distribution]. *Computing: Archiv für Informatik und Numerik*, 9(1):63–68, March 1972. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Schrack:1972:RAR

[625] Günther F. Schrack. Remark on "Algorithm 381: Random vectors uniform in solid angle". *Communications of the ACM*, 15(6):468, June 1972. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [517].

Sobol:1972:DIG

[626] I. M. Sobol'. A deterministic interpretation of goodness-of-fit tests, and a test of pseudorandom numbers. In *Operations research and statistical modeling, No. 1 (Russian)*, pages 162–169. Izdat. Leningrad. Univ., Leningrad, 1972.

Sobol:1972:PEE

[627] I. M. Sobol'. A probabilistic estimate of the error for nonrandom integration nets. *Voprosy Vyçisl. i Prikl. Mat. (Taškent)*, 14(??):5–11, ???? 1972. CODEN ???? ISSN ????

Sokal:1972:OCN

[628] Nathan O. Sokal. Optimum choice of noise frequency band and sampling rate for generating random binary digits from clipped white noise. *IEEE Transactions on Computers*, C-21(6):614–615, June 1972. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5009023`.

Sowey:1972:CCB

[629] E. R. Sowey. A chronological and classified bibliography on random number generation and testing. *International Statistical Review = Revue Internationale de Statistique*, 40(3):355–371, December 1972. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL `http://www.jstor.org/stable/1402472`.

Sullins:1972:CAP

[630] Walter L. Sullins. Certification of "Algorithm 266: Pseudo-random numbers [G5]". *Communications of the ACM*, 15(12):1072–1073, 1972. CO-

DEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [362] and remarks [380, 391].

Vincent:1972:CPA

[631] C. H. Vincent. Corrigendum: Precautions for accuracy in the generation of truly random binary numbers. *Journal of Physics. E: Scientific Instruments*, 5(6):546, 1972. CODEN JPSIAE. ISSN 0022-3735. URL `http://stacks.iop.org/0022-3735/5/i=6/a=521`. See [575].

Ahrens:1973:EFM

[632] J. H. Ahrens and Ulrich Dieter. Extensions of Forsythe's method for random sampling from the normal distribution. *Mathematics of Computation*, 27(124):927–937, October 1973. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Ahrens:1973:NME

[633] J. H. Ahrens and Ulrich Dieter. Neuere Methoden zur Erzeugung von nicht-gleichverteilten Zufallsvariablen. (German) [Newer methods for the generation of nonuniformly distributed random variables]. *Zeitschrift für Angewandte Mathematik und Mechanik*, 53(12):T221–T223, ???? 1973. CODEN ZAMMAX. ISSN 0044-2267 (print), 1521-4001 (electronic). URL `http://onlinelibrary.wiley.com/doi/10.1002/zamm.197305312115/abstract`.

Burford:1973:BAC

[634] R. L. Burford. A better additive congruential random number generator. *Decision Sciences*, 4(??):190–193, ???? 1973. CODEN ???? ISSN 0011-7315.

Diaconis:1973:LMI

[635] Persi Diaconis. Limits of measures of the integers with applications to random number generators and the distribution of leading digits. Memorandum NS-211, Department of Statistics, Harvard University, Cambridge, MA, USA, March 22, 1973.

Dieter:1973:CMG

[636] Ulrich Dieter and J. H. Ahrens. A combinatorial method for the generation of normally distributed random numbers. *Computing: Archiv für Informatik und Numerik*, 11(2):137–146, June 1973. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Durbin:1973:DTT

[637] James Durbin. *Distribution Theory for Tests Based on the Sample Distribution Function*, volume 9 of *SIAM CBMS-NSF Regional Conference Series in applied mathematics*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1973. vi + 64 pp. LCCN QA276.7 .D87.

Fishman:1973:CMD

[638] George S. Fishman. *Concepts and Methods in Discrete Event Digital Simulation*. Wiley, New York, NY, USA, 1973. ISBN 0-471-26155-6. xiv + 385 pp. LCCN T57.62 .F57.

Geffe:1973:HPD

[639] P. Geffe. How to protect data with ciphers that are really hard to break. *Electronics*, 46(1):99–101, January 1973.

Good:1973:BRB

[640] I. J. Good. Book review: *The Generation of Random Variates* by T. G. Newman; P. L. Odell. *International Statistical Review = Revue Internationale de Statistique*, 41(1):139–140, April 1973. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL `http://www.jstor.org/stable/1402798`.

Grube:1973:MREa

[641] A. Grube. *Mehrfach rekursiv erzeugte Zahienfolgen (German) [Multiple sequences of numbers generated recursively]*. Dissertation, Fakultät für Mathematik, Universität Karlsruhe, Karlsruhe, West Germany, 1973.

Grube:1973:MREb

[642] A. Grube. Mehrfach rekursiv-erzeugte Pseudo-Zufallszahlen. (German) [Multiply recursive generation of pseudorandom numbers]. *Zeitschrift für Angewandte Mathematik und Mechanik*, 53(12):T223–T225, ???? 1973. CODEN ZAMMAX. ISSN 0044-2267 (print), 1521-4001 (electronic).

Gupta:1973:OSE

[643] Shanti S. Gupta, Klaus Nagel, and S. Panchapakesan. On the order statistics from equally correlated normal random variables. *Biometrika*, 60(2):403–413, August 1973. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2334554`.

Hader:1973:IMR

[644] R. J. Hader. An improper method of randomization in experimental design. *The American Statistician*, 27(2):82–84, April 1973. CODEN

ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683964`.

Hamming:1973:NMS

[645] R. W. Hamming. *Numerical Methods for Scientists and Engineers*. McGraw-Hill, New York, NY, USA, second edition, 1973. ISBN 0-07-025887-2. ix + 721 pp. LCCN QA297 .H28 1973.

Holland:1973:GAO

[646] John H. Holland. Genetic algorithms and the optimal allocation of trials. *SIAM Journal on Computing*, 2(2):88–105, April 1973. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). See erratum [690].

Knop:1973:AAR

[647] Robert E. Knop. ACM Algorithm 441: Random deviates from the dipole distribution [G5]. *Communications of the ACM*, 16(1):51, January 1973. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Kozlov:1973:EEM

[648] G. A. Kozlov. Estimation of the error of the method of statistical tests (Monte-Carlo) due to imperfections in the distribution of random numbers. *Theory of Probability and its Applications*, 17(3):493–509, ???? 1973. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Learmonth:1973:NPS

[649] G. P. Learmonth and P. A. W. Lewis. Naval Postgraduate School random number generator package LLRANDOM. Report NP555LW73061A, Naval Postgraduate School, Monterey, CA, USA, 1973. The shuffling algorithm proposed in this report does *not* lengthen the period, and only marginally reduces the lattice structure of linear congruential generators, despite the apparently tiny difference with the [757] algorithm: see [1493] for a comparison, both mathematical, and graphical.

Levin:1973:NRS

[650] L. A. Levin. On the notion of a random sequence. *Soviet Mathematics. Doklady*, 14(??):1413–1416, ???? 1973. CODEN ???? ISSN 0197-6788.

Lewis:1973:GFS

[651] T. G. Lewis and W. G. Payne. Generalized feedback shift register pseudorandom number algorithm. *Journal of the ACM*, 20(3):456–468, July

1973. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). See important errata, and algorithm and code improvements, in [1520].

Malcolm:1973:UUR

[652] Michael A. Malcolm and Cleve B. Moler. URAND: a universal random number generator. Technical Report STAN-CS-73-334, Computer Science Department, Stanford University, Stanford, CA, USA, 1973. 5 pp.

Maritsas:1973:AFT

[653] D. G. Maritsas. The autocorrelation function of the two feedback shift-register pseudorandom source. *IEEE Transactions on Computers*, C-22(10):962–964, October 1973. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1672219`.

Maritsas:1973:HSA

[654] Dimitris G. Maritsas. A high speed and accuracy digital Gaussian generator of pseudorandom numbers. *IEEE Transactions on Computers*, C-22 (7):629–634, July 1973. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5009127`.

Marsaglia:1973:HUM

[655] George Marsaglia, K. Ananthanarayanan, and A. Zaman. How to use the McGill random-number package SUPER-DUPER. Technical report, School of Computer Science, McGill University, Montreal, Quebec, Canada, 1973.

McGrath:1973:TEM

[656] E. J. McGrath and D. C. Irving. Techniques for efficient Monte Carlo simulation. Vol. II. Random number generation for selected probability distributions. Report ????, National Technical Information Service, Springfield, VA, USA, 1973.

Neave:1973:MUB

[657] Henry R. Neave. Miscellanea: On using the Box–Muller transformation with multiplicative congruential pseudo-random number generators. *Applied Statistics*, 22(1):92–97, 1973. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://www.jstor.org/stable/pdfplus/2346308.pdf`.

Neuman:1973:CSS

[658] Frank Neuman, Robert Merrick, and Clyde F. Martin. The correlation structure of several popular pseudorandom number generators. Report NASA-TM-X-62275, NASA Ames Research Center, ????, 1973. Document ID: 19730017891.

Niederreiter:1973:BEB

[659] H. Niederreiter and W. Philipp. Berry–Esseen bounds and a theorem of Erdős and Turán on uniform distribution mod1. *Duke Mathematical Journal*, 40(??):633–649, ???? 1973. CODEN DUMJAO. ISSN 0012-7094 (print), 1547-7398 (electronic).

Niederreiter:1973:MTD

[660] Harald Niederreiter. Metric theorems on the distribution of sequences. In ????, editor, *Analytic number theory (Proceedings of the Symposium on Pure Mathematics, St. Louis University, St. Louis, MO)*, volume XXIV, pages 195–212. American Mathematical Society, Providence, RI, USA, 1973. ISBN ???? LCCN ????

Overstreet:1973:QCM

[661] Claude Overstreet, Jr. *The Quadratic Congruential Method of Random Number Generation*. Ph.D. dissertation, Southern Methodist University, Dallas, TX, May 1973.

Overstreet:1973:RNG

[662] Claude Overstreet, Jr. and Richard E. Nance. A random number generator for small word-length computers. In Erwin E. Perlin and Thomas J. McConnell, Jr., editors, *ACM '73: Proceedings of the ACM annual conference*, pages 219–223. ACM Press, New York, NY 10036, USA, 1973. LCCN ???? URL `http://dl.acm.org/citation.cfm?id=805707`. See [601, 600].

Peskun:1973:OMC

[663] P. H. Peskun. Optimum Monte–Carlo sampling using Markov chains. *Biometrika*, 60(3):607–612, December 1973. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2335011`.

Philipp:1973:EDF

[664] W. Philipp. Empirical distribution functions and uniform distribution mod1. In C. F. Osgood, editor, *Diophantine Approximation and Its Applications*, pages 211–234. Academic Press, New York, NY, USA, 1973. ISBN ???? LCCN ????

Pohl:1973:MVM

[665] P. Pohl. The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and algebraic analysis. Report TRITA-NA-7307, The Royal Institute of Technology, Department of Information Processing and Computer Science, Stockholm, Sweden, 1973. 36 pp.

Polge:1973:GPR

[666] R. J. Polge, E. M. Holliday, and B. K. Bhagavan. Generation of a pseudo-random set with desired correlation and probability distribution. *Simulation*, 20(5):153–158, May 1973. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/20/5/153.full.pdf+html`.

Rice:1973:DRE

[667] S. O. Rice. Distribution of $\sum a_n/n$, a_n randomly equal to ± 1. *The Bell System Technical Journal*, 52(7):1097–1103, September 1973. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol52/bstj52-7-1097.pdf`; `http://www.alcatel-lucent.com/bstj/vol52-1973/articles/bstj52-7-1097.pdf`.

Schatte:1973:VMG

[668] Peter Schatte. Zur Verteilung der Mantisse in der Gleitkommadarstellung einer Zufallsgröße. (German) [distribution of the mantissa in the floating-point representation of a random variable]. *Zeitschrift für Angewandte Mathematik und Mechanik*, 53(??):553–565, ???? 1973. CODEN ZAMMAX. ISSN 0044-2267 (print), 1521-4001 (electronic).

Tootill:1973:ART

[669] J. P. R. Tootill, W. D. Robinson, and D. J. Eagle. An asymptotically random Tausworthe sequence. *Journal of the ACM*, 20(3):469–481, July 1973. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Tsuda:1973:NIF

[670] Takao Tsuda. Numerical integration of functions of very many variables. *Numerische Mathematik*, 20(5):377–391, October 1973. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Vincent:1973:RGT

[671] C. H. Vincent. Reply to "The generation of truly random binary digits". *Journal of Physics. E: Scientific Instruments*, 6(5):496, ???? 1973.

CODEN JPSIAE. ISSN 0022-3735. URL http://iopscience.iop.org/0022-3735/6/5/027.

Adam:1974:CLS

[672] Thomas L. Adam, K. Mani Chandy, and J. R. Dickson. A comparison of list schedules for parallel processing systems. *Communications of the ACM*, 17(12):685–690, December 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Ahrens:1974:CMS

[673] J. H. Ahrens and Ulrich Dieter. Computer methods for sampling from gamma, beta, Poisson and binomial distributions. *Computing: Archiv für Informatik und Numerik*, 12(3):223–246, September 1974. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). See note [896].

Alam:1974:SNT

[674] Khursheed Alam. Some nonparametric tests of randomness. *Journal of the American Statistical Association*, 69(347):738–739, September 1974. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL http://www.jstor.org/stable/2286010.

Beasley:1974:CSR

[675] J. D. Beasley. Correspondence: System 4 random number. *The Computer Journal*, 17(4):381, November 1974. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journal/hdb/Volume_17/Issue_04/tiff/381.tif.

Block:1974:CBE

[676] Henry W. Block and A. P. Basu. A continuous bivariate exponential extension. *Journal of the American Statistical Association*, 69(348):1031–1037, December 1974. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL http://www.jstor.org/stable/2286184.

Brent:1974:AAG

[677] Richard P. Brent. ACM Algorithm 488: a Gaussian pseudo-random number generator [G5]. *Communications of the ACM*, 17(12):704–706, December 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Chen:1974:GRV

[678] Hui-Chuan Chen and Yoshinori Asau. On generating random variates from an empirical distribution. *Transactions of the American Institute of Electrical Engineers*, 6(2):163–166, 1974. CODEN ???? ISSN ????

Cohn:1974:CRP

[679] Charles E. Cohn. Correlations in a random-pulse generator. *Simulation*, 23(4):128, October 1974. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/23/4/128.full.pdf+html`.

Coldwell:1974:CDS

[680] Robert Lynn Coldwell. Correlational defects in the standard IBM 360 random number generator and the classical ideal gas correlation function. *Journal of Computational Physics*, 14(2):223–226, February 1974. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999174900151`. See comment [816].

Collins:1974:CTE

[681] George E. Collins. The computing time of the Euclidean algorithm. *SIAM Journal on Computing*, 3(1):1–10, ???? 1974. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Dahlquist:1974:NM

[682] Germund Dahlquist, Åke Björck, and Ned Anderson. *Numerical Methods*. Prentice-Hall Series in Automatic Computation. Prentice-Hall, Upper Saddle River, NJ, USA, 1974. ISBN 0-13-627315-7. xviii + 573 pp. LCCN QA297 .D131 1969. Translated by Ned Anderson.

Dieter:1974:URN

[683] Ulrich Dieter and Joachim H. Ahrens. Uniform random numbers. Report, Institut für Mathematische Statistik, Technische Hochschule Graz, Graz, Austria, 1974.

Eggarter:1974:CRL

[684] T. P. Eggarter. On a complex representation of Lorentzian random variables. *Journal of Mathematical Physics*, 15(1):7–8, January 1974. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v15/i1/p7_s1`.

Good:1974:RTA

[685] Irving John Good. Random thoughts about randomness. In Schaffner and Cohen [4102], pages 117–135. ISBN 90-277-0408-2, 90-277-0409-0 (paperback). ISSN 0068-0346. LCCN Q175 .B7312. URL `https://link.springer.com/chapter/10.1007/978-94-010-2140-1_9`. Invited lecture in the symposium on the Concept of Randomness, dedicated to the memory of L. J. Savage, in the Biennial Meeting of the Philosophy of Science Association, Olds Plaza Hotel, Lansing, Michigan, October 27–29, 1972.

Greenwood:1974:FGG

[686] A. J. Greenwood. A fast generator for Gamma-distributed random variables. In G. Bruckman, F. Ferschl, and L. Schmetterer, editors, *COMPSTAT: Proceedings in Computational Statistics*, pages 17–27. Physica-Verlag, Vienna, Austria, 1974.

Handelsman:1974:AEL

[687] Richard A. Handelsman and John S. Lew. Asymptotic expansion of Laplace convolutions for large argument and tail densities for certain sums of random variables. *SIAM Journal on Mathematical Analysis*, 5 (3):425–451, May 1974. CODEN SJMAAH. ISSN 0036-1410 (print), 1095-7154 (electronic).

Harada:1974:OMS

[688] N. Harada. Optimal multipliers for the spectral test of uniform random number generators. *Information Processing in Japan*, 14(??):120–126, ???? 1974. CODEN ???? ISSN ????

Hoffmann-Jorgensen:1974:SIB

[689] J. Hoffmann-Jørgensen. Sums of independent Banach space valued random variables. *Studia Mathematica*, 52:159–186, 1974. CODEN SMATAZ. ISSN 0039-3223 (print), 1730-6337 (electronic).

Holland:1974:EGA

[690] John H. Holland. Erratum: Genetic algorithms and the optimal allocation of trials. *SIAM Journal on Computing*, 3(4):326, ???? 1974. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). See [646].

Kadota:1974:ISS

[691] T. T. Kadota. On the information stability of stationary ergodic processes. *SIAM Journal on Applied Mathematics*, 26(1):176–182, January 1974. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Kedem:1974:TGL

[692] Gershon Kedem and S. K. Zaremba. A table of good lattice points in three dimensions. *Numerische Mathematik*, 23(2):175–180, April 1974. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Kuipers:1974:UDS

[693] Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Pure and applied mathematics. Wiley, New York, NY, USA, 1974. ISBN 0-471-51045-9. xiv + 390 pp. LCCN QA292 .K84.

Lunow:1974:GRN

[694] W. Lünow. On the generation of random numbers with at choice distribution. *Computing: Archiv für Informatik und Numerik*, 13(1):21–31, March 1974. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Marsaglia:1974:APRa

[695] George Marsaglia. Acknowledgement of priority to: "Random variables with independent binary digits" (Ann. Math. Statist. **42** (1971), 1922–1929). *Annals of Probability*, 2(4):747, August 1974. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL `http://projecteuclid.org/euclid.aop/1176996619`.

Marsaglia:1974:APRb

[696] George Marsaglia. Acknowledgement of priority to: "Random variables with independent binary digits" (Ann. Math. Statist. **42** (1971), 1922–1929). *Annals of Statistics*, 2(4):848, 1974. CODEN ASTSC7. ISSN 0090-5364 (print), 2168-8966 (electronic). URL `http://projecteuclid.org/euclid.aos/1176342776`.

MendesFrance:1974:SNA

[697] Michel Mendès France. Suites de nombres au hasard (d'après Knuth). (French) [Sequences of random numbers (according to Knuth)]. *Sémin Théorie des Nombres*, 6(??):??, ???? 1974–1975. CODEN ???? ISSN ????

Niederreiter:1974:DPR

[698] Harald Niederreiter. On the distribution of pseudo-random numbers generated by the linear congruential method. II. *Mathematics of Computation*, 28(128):1117–1132, October 1974. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2005370.pdf`.

Odeh:1974:PPN

[699] R. E. Odeh and J. O. Evans. The percentage points of the normal distribution. *Applied Statistics*, 23(??):96–97, ???? 1974. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Page:1974:RAG

[700] R. L. Page. Remark on "Algorithm 425: Generation of random correlated normal variables". *Communications of the ACM*, 17(6):325, June 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [598].

Pollard:1974:TFP

[701] J. Pollard. Theorems on factorization and primality testing. *Proceedings of the Cambridge Philosophical Society. Mathematical and physical sciences*, 76:521–528, 1974. CODEN PCPSA4. ISSN 0008-1981.

Poole:1974:EDF

[702] W. Kenneth Poole. Estimation of the distribution function of a continuous type random variable through randomized response. *Journal of the American Statistical Association*, 69(348):1002–1005, December 1974. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2286179`.

Rabinowitz:1974:CVM

[703] M. Rabinowitz and M. L. Berenson. A comparison of various methods of obtaining random order statistics for Monte Carlo computations. *The American Statistician*, 28(1):27–29, February 1974. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683528`.

Ramberg:1974:AGG

[704] John S. Ramberg and P. R. Tadikamalla. An algorithm for generating gamma variates based on the Weibull distribution. *AIIE Transactions*, 6(3):257–260, ???? 1974.

Ramberg:1974:AMG

[705] John S. Ramberg and Bruce W. Schmeiser. An approximate method for generating asymmetric random variables. *Communications of the ACM*, 17(2):78–82, February 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Salfi:1974:LPR

[706] R. Salfi. A long-period random number generator with application to permutations. In Gerhart Bruckmann, Franz Ferschl, and Leopold Schmetterer, editors, *Compstat 1974: Proceedings of a Symposium on Computational Statistics, University of Vienna, 1974*, pages 28–35. Physica-Verlag, Vienna, Austria, 1974.

Santos:1974:QFS

[707] Emilio Santos. Quantumlike formulation of stochastic problems. *Journal of Mathematical Physics*, 15(11):1954–1962, November 1974. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v15/i11/p1954_s1`.

Sato:1974:PCP

[708] Masahiko Sato. On the periods of certain pseudorandom sequences. *Publ. Res. Inst. Math. Sci.*, 10(1):77–89, 1974–1975. ISSN 0034-5318.

Saunders:1974:FRV

[709] Sam C. Saunders. A family of random variables closed under reciprocation. *Journal of the American Statistical Association*, 69(346):533–539, June 1974. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2285692`.

Scherpenissea:1974:PRN

[710] J. Scherpenissea. A pseudo random number generator. *Interface*, 3(2): 187–190, ???? 1974. CODEN IFCEBC. ISSN 0929-8215 (print), 1744-5027 (electronic).

Schorr:1974:PLV

[711] B. Schorr. Programs for the Landau and the Vavilov distributions and the corresponding random numbers. *Computer Physics Communications*, 7(4):215–224, April 1974. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465574900915`.

Sobol:1974:PNC

[712] I. M. Sobol'. Pseudorandom numbers for the construction of discrete Markov chains by a Monte Carlo method. *Ž. Vyčisl. Mat. i Mat. Fiz.*, 14:36–44, 266, 1974. ISSN 0044-4669.

Walker:1974:FGU

[713] A. J. Walker. Fast generation of uniformly distributed pseudorandom numbers with floating-point representation. *Electronics Letters*, 10(25–26):533–534, December 12, 1974. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4245313`.

Walker:1974:NFM

[714] A. J. Walker. New fast method for generating discrete random numbers with arbitrary frequency distributions. *Electronics Letters*, 10(8):127–128, April 18, 1974. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4245054`.

Wallace:1974:CGG

[715] N. D. Wallace. Computer generation of gamma random variates with non-integral shape parameters. *Communications of the ACM*, 17(12):691–695, December 1974. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Whittaker:1974:MGG

[716] J. Whittaker. Miscellanea: Generating gamma and beta random variables with non-integral shape parameters. *Applied Statistics*, 23(2):210–214, 1974. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Akeda:1975:NTP

[717] Y. Akeda and M. Hori. Numerical test of Palásti's conjecture on two-dimensional random packing density. *Nature*, 254(5498):318–319, March 27, 1975. CODEN NATUAS. ISSN 0028-0836 (print), 1476-4687 (electronic). URL `http://www.nature.com/nature/journal/v254/n5498/pdf/254318a0.pdf`.

Beuerman:1975:LDS

[718] D. R. Beuerman. Limit distributions for sums of weighted random variables. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 18(??):291–294, ???? 1975. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Brooker:1975:SAA

[719] P. Brooker and M. J. P. Selby. Statistical algorithms: Algorithm AS 92: The sample size for a distribution-free tolerance interval. *Applied*

Statistics, 24(3):388–390, September 1975. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/92`.

Chaitin:1975:RMP

[720] G. J. Chaitin. Randomness and mathematical proof. *Scientific American*, 232(??):47–52, ???? 1975. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Chay:1975:MUB

[721] S. C. Chay, R. D. Fardo, and M. Mazumdar. Miscellanea: On using the Box–Muller transformation with multiplicative congruential pseudorandom number generators. *Applied Statistics*, 24(1):132–135, 1975. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://www.jstor.org/stable/pdfplus/2346711.pdf`.

Dieter:1975:HCS

[722] Ulrich Dieter. How to calculate shortest vectors in a lattice. *Mathematics of Computation*, 29(131):827–833, July 1975. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Dudewicz:1975:RNN

[723] E. J. Dudewicz. Random numbers: The need, the history, the generators. In Patil et al. [4103], page ?? ISBN 90-277-0609-3. LCCN QA273.6 .N37 1974. Reprinted in [1159].

Fellows:1975:CGF

[724] David Michael Fellows. Comments on "A general Fortran emulator for IBM 360/370 random number generator 'RANDU'". Technical report 6, School of Computer Science, University of New Brunswick, Fredericton, NB, Canada, 1975. b + [4] pp.

Franta:1975:NRV

[725] W. R. Franta. A note on random variate generators and antithetic sampling. *INFOR*, 13(??):112–117, ???? 1975. CODEN INFRCL. ISSN 0315-5986.

Fredericsson:1975:PPB

[726] S. A. Fredericsson. Pseudorandomness properties of binary shift register sequences. *IEEE Transactions on Information Theory*, IT-21(1):115–120, January 1975. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Frigerio:1975:RNS

[727] N. A. Frigerio and N. A. Clark. A random number set for Monte Carlo computations. *Transactions of the American Nuclear Society*, 22(??):283–284, ???? 1975. CODEN TANSAO. ISSN 0003-018X. URL `http://www.osti.gov/energycitations/product.biblio.jsp?osti_id=4072437`.

Gibbons:1975:VIM

[728] Jean D. Gibbons and John W. Pratt. P-values: Interpretation and methodology. *The American Statistician*, 29(1):20–25, February 1975. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683674`.

Harville:1975:ERW

[729] David A. Harville. Experimental randomization: Who needs it? *The American Statistician*, 29(1):27–31, February 1975. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683676`.

Kedem:1975:SGL

[730] G. Kedem. The search for good lattice points in N dimensions. Technical Report 1570, Mathematics Research Center, Madison, WI, USA, 1975.

Kemperman:1975:BDM

[731] J. H. B. Kemperman. Bounds on the discrepancy modulo 1 of a real random variable. *Bulletin — Institute of Mathematical Statistics*, 4(??): 138–??, ???? 1975. CODEN SMBCVA. ISSN 0146-3942. Abstract no. 75t-47.

Kleijnen:1975:AVC

[732] Jack P. C. Kleijnen. Antithetic variates, Common Random Numbers and optimal computer time allocation in simulation. *Management Science*, 21 (10):1176–1185, June 1975. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Levin:1975:UDSa

[733] M. B. Levin. On the uniform distribution of the sequence $\alpha\lambda$. *Mat. Sb. (N.S.)*, 98(??):??, ???? 1975. CODEN ???? ISSN ????

Levin:1975:UDSb

[734] M. B. Levin. On the uniform distribution of the sequence $\alpha\lambda$. *Math. USSR-Sb.*, 27(??):183–197, ???? 1975. CODEN ???? ISSN ????

Malcolm:1975:LVG

[735] Michael A. Malcolm and R. Bruce Simpson. Local versus global strategies for adaptive quadrature. *ACM Transactions on Mathematical Software*, 1(2):129–146, June 1975. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

MendesFrance:1975:SNA

[736] Michel Mendès France. Suites de nombres au hasard, d'après Knuth. (French) [Sequences of random numbers]. Technical report, Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence, France, 1975. 11 pp. Séminaire de Théorie des Nombres, 1974–1975 (Univ. Bordeaux I, Talence), Exp. No. 6.

Miyatake:1975:GPR

[737] O. Miyatake, H. Inoue, and Y. Yoshizawa. Generation of physical random numbers. *Mathematica Japonica*, 20(??):207–217, ???? 1975. CODEN MAJAA9. ISSN 0025-5513.

Monroe:1975:CIT

[738] James L. Monroe. Correlation inequalities for two-dimensional vector spin systems. *Journal of Mathematical Physics*, 16(9):1809–1812, September 1975. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v16/i9/p1809_s1`.

Nance:1975:IFR

[739] Richard E. Nance and Claude Overstreet, Jr. Implementation of Fortran random number generators on computers with one's complement arithmetic. *Journal of Statistical Computation and Simulation*, 4(3):235–243, ???? 1975. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949657508810126`.

Newman:1975:MIF

[740] Charles M. Newman. Moment inequalities for ferromagnetic Gibbs distributions. *Journal of Mathematical Physics*, 16(9):1956–1959, September 1975. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v16/i9/p1956_s1`.

Niederreiter:1975:DDM

[741] Harald Niederreiter and J. M. Wills. Diskrepanz und Distanz von Massen bezüglich konvexer und Jordanscher Mengen. (German) [Discrepancy

with respect to mass and distance of convex and Jordan sets]. *Mathematische Zeitschrift*, 144(??):125–134, ???? 1975. CODEN MAZEAX. ISSN 0025-5874 (print), 1432-1823 (electronic). See correction, volume 148, page 99.

Niederreiter:1975:QVR

[742] H. Niederreiter. Quantitative versions of a result of Hecke in the theory of uniform distribution mod1. *Acta Arithmetica*, 28(??):321–339, ???? 1975. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Pohl:1975:MFP

[743] Peter Pohl. MCV: a fast pseudo-random number generator with extremely good statistical properties. Report ??, The Royal Institute of Technology, Department of Information Processing and Computer Science, Stockholm, Sweden, 1975. 34 pp.

Pollard:1975:MCM

[744] J. M. Pollard. A Monte Carlo method for factorization. *BIT (Nordisk tidskrift for informationsbehandling)*, 15(3):331–334, September 1975. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=15&issue=3&spage=331`.

Rosenblatt:1975:MSS

[745] M. Rosenblatt. Multiply schemes and shuffling. *Mathematics of Computation*, 29(131):929–934, July 1975. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Schaufele:1975:API

[746] Ronald A. Schaufele. An application of pairwise independence of random variables to regression analysis. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 18(??):397–404, ???? 1975. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Schnurmann:1975:WRT

[747] H. D. Schnurmann, E. Lindbloom, and R. G. Carpenter. The weighted random test-pattern generator. *IEEE Transactions on Computers*, C-24 (7):695–700, July 1975. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1672883`.

Shapiro:1975:DAR

[748] Jesse M. Shapiro. Domains of attraction for reciprocals of powers of random variables. *SIAM Journal on Applied Mathematics*, 29(4):734–739, December 1975. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Stoneham:1975:NRD

[749] R. G. Stoneham. Normal recurring decimals, normal periodic systems, (j, ϵ) normality and normal numbers. *Acta Arithmetica*, 28(??):349–361, ???? 1975. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Tadikamalla:1975:AMG

[750] Pandu R. Tadikamalla and John S. Ramberg. An approximate method for generating gamma and other variates. *Journal of Statistical Computation and Simulation*, 3(3):275–282, 1975. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Wheeler:1975:ASG

[751] Donald J. Wheeler. An approximation for simulation of gamma distributions. *Journal of Statistical Computation and Simulation*, 3(3):225–232, 1975. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Witsenhausen:1975:SPD

[752] H. S. Witsenhausen. On sequences of pairs of dependent random variables. *SIAM Journal on Applied Mathematics*, 28(1):100–113, January 1975. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Yao:1975:ASA

[753] Andrew C. Yao and Donald E. Knuth. Analysis of the subtractive algorithm for greatest common divisors. *Proceedings of the National Academy of Sciences of the United States of America*, 72(12):4720–4722, December 1975. CODEN PNASA6. ISSN 0027-8424 (print), 1091-6490 (electronic).

Anderson:1976:PRR

[754] G. C. Anderson and G. T. Roberts. Pseudo-random and random test signals. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 28(??):??, ???? 1976. CODEN HPJOAX. ISSN 0018-1153.

Atkinson:1976:CGB

[755] A. C. Atkinson and M. C. Pearce. The computer generation of beta, gamma, and normal random variables. *Journal of the Royal Statistical Society. Series A (General)*, 139(??):431–448, ???? 1976. CODEN JSSAEF. ISSN 0035-9238.

Atkinson:1976:SAG

[756] A. C. Atkinson. A switching algorithm for the generation of beta random variables with at least one parameter less than 1. *Journal of the Royal Statistical Society. Series A (General)*, 139(??):462–467, ???? 1976. CODEN JSSAEF. ISSN 0035-9238.

Bays:1976:IPR

[757] Carter Bays and S. D. Durham. Improving a poor random number generator. *ACM Transactions on Mathematical Software*, 2(1):59–64, March 1976. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/355666.355670`. See also [649] for a slightly different, but inferior, shuffling algorithm, and [1493] for a comparison, both mathematical, and graphical, of the two algorithms. Reference [3] for IBM Report GC20-8011-0 is incorrectly given year 1969; the correct year is 1959.

Blood:1976:CPR

[758] F. A. Blood, Jr. Correlations in power residue generated random numbers. *Journal of Computational Physics*, 20(3):372–379, March 1976. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999176900899`.

Brent:1976:ABE

[759] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [4106], pages 321–355. ISBN 0-12-697540-X. LCCN QA76.6 .S9195 1976. URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.7959`. The complexity of the binary Euclidean algorithm for the greatest common denominator is shown to be $O(0.705 \lg N)$ for large $N = \max(|u|, |v|)$. See [2501] for an update, and a repair to an incorrect conjecture in this paper. See also [2424], where the worst case complexity is shown to be $O(\lg N)$, and the number of right shifts at most $2 \lg(N)$.

Chamayou:1976:DAG

[760] J. M. F. Chamayou. On a direct algorithm for the generation of lognormal pseudo-random numbers. *Computing: Archiv für Informatik und*

Numerik, 16(1–2):69–76, March 1976. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Chambers:1976:MSS

[761] J. M. Chambers, C. L. Mallows, and B. W. Stuck. A method for simulating stable random variables. *Journal of the American Statistical Association*, 71(354):340–344, June 1976. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2285309`. See correction [1273].

Claustriaux:1976:GCN

[762] J. J. Claustriaux. Génération et contrôle de nombres pseudo-aléatoires sur ordinateur à mots de 16 bits. (French). [generation and control of pseudorandom numbers on a 16-bit computer]. *Revue de statistique appliquée*, 24(2):75–88, ???? 1976. CODEN ???? ISSN ???? URL `http://archive.numdam.org/article/RSA_1976__24_2_75_0.pdf`.

Enison:1976:PTB

[763] R. L. Enison and H. S. Bright. Preliminary testing of a 64-bit Tausworthe–Lewis–Payne generator of Mersenne exponent degree. In Hoaglin and Welsch [4104], pages 208–211. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Fishman:1976:SGD

[764] George S. Fishman. Sampling from the Gamma-distribution on a computer. *Communications of the ACM*, 19(7):407–409, July 1976. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Fishman:1976:SPD

[765] G. S. Fishman. Sampling from the Poisson distribution on a computer. *Computing: Archiv für Informatik und Numerik*, 17(2):147–156, June 1976. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Fishman:1976:STR

[766] George S. Fishman. Some test results on the Simscript II.5 and SIMPL/1 pseudorandom number generators. *ACM Simuletter*, 8(1):79–84, October 1976. CODEN SIMUD5. ISSN 0163-6103. URL `http://www.or.unc.edu/research/temp/tech70b.html`.

Friday:1976:SGN

[767] Dennis S. Friday, G. P. Patil, and M. T. Boswell. A study of the generation of non-uniform random numbers on a computer. In Hoaglin and

Welsch [4104], pages 191–196. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Fuller:1976:PPR

[768] A. T. Fuller. The period of pseudo-random numbers generated by Lehmer's congruential method. *The Computer Journal*, 19(2): 173–177, May 1976. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_02/tiff/173.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_02/tiff/174.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_02/tiff/175.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_02/tiff/176.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_19/Issue_02/tiff/177.tif`.

Glaser:1976:RGM

[769] Ronald E. Glaser. The ratio of the geometric mean to the arithmetic mean for a random sample from a gamma distribution. *Journal of the American Statistical Association*, 71(354):480–487, June 1976. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2285338`.

Golder:1976:BMM

[770] E. R. Golder and J. G. Settle. The Box–Muller method for generating pseudo-random normal deviates. *Applied Statistics*, 25(1):12–20, 1976. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Golder:1976:SAA

[771] E. R. Golder. Statistical algorithms: Algorithm AS 98: The spectral test for the evaluation of congruential pseudo-random generators. *Applied Statistics*, 25(2):173–180, June 1976. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/98`; `http://www.jstor.org/stable/pdfplus/2346691.pdf`. See remark [772, 865].

Golder:1976:SAR

[772] E. R. Golder. Statistical algorithms: Remark AS R18: The spectral test for the evaluation of congruential pseudo-random generators. *Applied Statistics*, 25(3):324, 1976. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://www.jstor.org/stable/pdfplus/2347260.pdf`. See [771, 865].

Greenwood:1976:DTC

[773] J. A. Greenwood. The demands of trivial combinatorial problems on random number generators. In Hoaglin and Welsch [4104], pages 222–227. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Greenwood:1976:FMI

[774] J. A. Greenwood. A fast machine-independent long-period generator for 31-bit pseudorandom integers. In J. Gordesch and P. Naeve, editors, *Compstat 1976: Proceedings in Computational Statistics*, pages 30–37. Physica-Verlag, Vienna, Austria, 1976.

Greenwood:1976:MTG

[775] J. Arthur Greenwood. Moments of the time to generate random variables by rejection. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 28(3):399–401, ???? 1976. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic).

Guerra:1976:RNG

[776] V. O. Guerra, R. A. Tapia, and J. R. Thompson. A random number generator for continuous random variables based on an interpolation procedure of Akima. In Hoaglin and Welsch [4104], pages 228–230. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Heikes:1976:UCR

[777] Russell G. Heikes, Douglas C. Montgomery, and Ronald L. Rardin. Using Common Random Numbers in simulation experiments — an approach to statistical analysis. *Simulation*, 25(3):81–85, September 1976. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/27/3/81`.

Hoaglin:1976:TPC

[778] D. Hoaglin. Theoretical properties of congruential random-number generators: an empirical view. Memorandum NS-340, Department of Statistics, Harvard University, Cambridge, MA, USA, 1976.

Kinderman:1976:CGN

[779] A. J. Kinderman and J. G. Ramage. Computer generation of normal random variables. *Journal of the American Statistical Association*, 71(356): 893–896, December 1976. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2286857`. See corrections [1543, 2903].

Kinderman:1976:GRV

[780] A. J. Kinderman and J. F. Monahan. Generating random variables from the ratio of two uniform variates. In Hoaglin and Welsch [4104], pages 197–199. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Klauder:1976:CGR

[781] John R. Klauder. A characteristic glimpse of the renormalization group. *Journal of Mathematical Physics*, 17(5):826–830, May 1976. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v17/i5/p826_s1`.

Knuth:1976:CNR

[782] Donald E. Knuth and Andrew C. Yao. The complexity of nonuniform random number generation. In Traub [4106], pages 357–428. ISBN 0-12-697540-X. LCCN QA76.6 .S9195 1976. Russian translation by B. B. Pokhodzeĭ in *Kiberneticheskiĭ Sbornik* **19** (1983), 97–158.

Kounias:1976:BLB

[783] Stratis Kounias and Jacqueline Marin. Best linear Bonferroni bounds. *SIAM Journal on Applied Mathematics*, 30(2):307–323, March 1976. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Kuo:1976:SRI

[784] C. T. K. Kuo, T. W. Cadman, and R. J. Arsenault. Sequential random integer generator. *Computer Physics Communications*, 12(2):163–171, November 1976. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465576900655`.

Learmonth:1976:ETM

[785] G. P. Learmonth. Empirical tests of multipliers for the prime-modulus random number generator $X(I+1) = AX(I) \bmod 2^{31}1$. In Hoaglin and Welsch [4104], pages 178–183. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Levin:1976:UTR

[786] L. A. Levin. Uniform tests of randomness. *Soviet Mathematics*, 17(??): 337–340, ???? 1976. CODEN SVMDA8. ISSN 0038-5573.

Lewis:1976:SAN

[787] P. A. W. Lewis and G. S. Shedler. Statistical analysis of non-stationary series of events in a data base system. *IBM Journal of Research and*

Development, 20(5):465–482, September 1976. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Locks:1976:EAV

[788] M. O. Locks. Error analysis of various methods for generating beta and gamma variates. In Hoaglin and Welsch [4104], pages 184–188. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Lyness:1976:CNA

[789] J. N. Lyness and J. J. Kaganove. Comments on the nature of automatic quadrature routines. *ACM Transactions on Mathematical Software*, 2 (1):65–81, March 1976. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Margolin:1976:TKS

[790] Barry H. Margolin and Willi Maurer. Tests of the Kolmogorov–Smirnov type for exponential data with unknown scale, and related problems. *Biometrika*, 63(1):149–160, April 1976. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2335096`.

Marsaglia:1976:IFM

[791] G. Marsaglia, K. Ananthanarayanan, and N. J. Paul. Improvements on fast methods for generating normal random variables. *Information Processing Letters*, 5(2):27–30, June 1976. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Marsaglia:1976:RNG

[792] George Marsaglia. Random number generation. In Ralston and Meek [4105], pages 1192–1197. ISBN 0-88405-321-0. LCCN QA76.15 .E55 1976.

McArdle:1976:ETM

[793] J. McArdle. Empirical tests of multivariate generators. In Hoaglin and Welsch [4104], pages 263–267. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Michael:1976:GRV

[794] John R. Michael, William R. Schucany, and Roy W. Haas. Generating random variates using transformations with multiple roots. *The American Statistician*, 30(2):88–90, May 1976. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683801`.

Miklich:1976:HSN

[795] Donald R. Miklich and David J. Austin. A high-speed normal random number generator using table look-up. *Behavior Research Methods and Instrumentation*, 8(4):405, July 1976. CODEN BRMIAC. ISSN 0005-7878.

Mitchell:1976:EAD

[796] James Melvin Mitchell. Encryption algorithm for data security based on a polyalphabetic substitution scheme and a pseudo-random number generator. Thesis (M.S.), University of Tennessee, Knoxville, Knoxville, TN, USA, 1976. v + 83 pp.

Neuman:1976:APC

[797] F. Neuman and R. B. Merrick. Autocorrelation peaks in congruential pseudorandom number generators. *IEEE Transactions on Computers*, C-25(5):457–460, May 1976. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674632`.

Neuman:1976:AST

[798] F. Neuman and C. F. Martin. The autocorrelation structure of Tausworthe pseudorandom number generators. *IEEE Transactions on Computers*, C-25(5):460–464, May 1976. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674633`.

Niederreiter:1976:CSL

[799] Harald Niederreiter. On the cycle structure of linear recurring sequences. *Mathematica Scandinavica*, 38(??):53–77, ???? 1976. CODEN MTSCAN. ISSN 0025-5521 (print), 1903-1807 (electronic).

Niederreiter:1976:DPR

[800] Harald Niederreiter. On the distribution of pseudo-random numbers generated by the linear congruential method. III. *Mathematics of Computation*, 30(135):571–597, July 1976. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2005328.pdf`.

Niederreiter:1976:SIL

[801] Harald Niederreiter. Statistical independence of linear congruential pseudo-random numbers. *Bulletin of the American Mathematical Society*, 82(6):927–929, November 1976. CODEN BAMOAD. ISSN 0002-

9904 (print), 1936-881X (electronic). URL `http://projecteuclid.org/euclid.bams/1183538356`.

Niederreiter:1976:SNE

[802] Harald Niederreiter. Some new exponential sums with applications to pseudo-random numbers. *Colloquia Mathematica Societatis János Bolyai*, 13(??):209–232, ???? 1976. ISSN 0139-3383.

Pohl:1976:DMP

[803] Peter Pohl. Description of MCV, a pseudo-random number generator. *Scandinavian Actuarial Journal*, 1976(1):1–14, ???? 1976. CODEN SAJODI. ISSN 0346-1238 (print), 1651-2030 (electronic).

Rouault:1976:PAE

[804] Alain Rouault. Propriétés asymptotiques d'un n-échantillon d'une variable aléatoire dénombrable connues sous le nom de lois de Zipf. (French) [asymptotic properties of an n-sample of a denumerable random variable known under the name of Zipf's law]. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences. Séries A et B*, 283(6):Aiv, A379–A380, 1976. CODEN CHASAP. ISSN 0151-0509.

Rudolph:1976:RNG

[805] E. Rudolph and D. M. Hawkins. Random number generators in cyclic queuing applications. *Journal of Statistical Computation and Simulation*, 5(1):65–71, January 1976. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Sobol:1976:UDS

[806] I. M. Sobol'. Uniformly distributed sequences with an additional uniform property. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 16(5):236–242, ???? 1976. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/0041555376901543`.

vanDooren:1976:AAN

[807] Paul van Dooren and Luc de Ridder. An adaptive algorithm for numerical integration over an n-dimensional cube. *Journal of Computational and Applied Mathematics*, 2(3):207–217, September 1976. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0771050X7690005X`.

Wallace:1976:TRG

[808] C. S. Wallace. Transformed rejection generators for gamma and normal pseudo-random variables. *Australian Computer Journal*, 8(3):103–105, ???? 1976. CODEN ACMJB2. ISSN 0004-8917.

Wedderburn:1976:SAR

[809] R. W. M. Wedderburn. Statistical algorithms: Remark AS R16: a remark on Algorithm AS 29: "The Runs Up and Down Test". *Applied Statistics*, 25(2):193, 1976. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/29`. See [505].

Williams:1976:PRS

[810] F. J. Williams and N. J. A. Sloane. Pseudo-random sequences and arrays. *Proceedings of the IEEE*, 64(12):1715–1727, 1976. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic).

Witsenhausen:1976:VBC

[811] H. S. Witsenhausen. Values and bounds for the common information of two discrete random variables. *SIAM Journal on Applied Mathematics*, 31(2):313–333, September 1976. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Zakharov:1976:ECS

[812] V. V. Zakharov and V. I. Smirnova. Experimental comparison of some pseudorandom sequences. *Problems of Random Search, Zinatne, Riga*, 5 (??):185–190, ???? 1976.

Zucker:1976:TMT

[813] Steven W. Zucker. Toward a model of texture. *Computer Graphics and Image Processing*, 5(2):190–202, June 1976. CODEN CGIPBG. ISSN 0146-664x (print), 1557-9697 (electronic). ZUCKER76a.

Ahrens:1977:URN

[814] J. H. Ahrens and U. Dieter. Uniform random numbers. Technical Report ??, University of Graz, Graz, Austria, ???? 1977.

Akchurin:1977:RNG

[815] R. M. Akchurin. A random number generator. *Programming and Computer Software; translation of Programmirovaniye (Moscow, USSR) Plenum*, 3(??):392–395, ???? 1977. CODEN PCSODA. ISSN 0361-7688 (print), 1608-3261 (electronic).

Amadori:1977:CDS

[816] Rüdiger Amadori. Correlational defects in the standard IBM 360 random number generator and the classical ideal gas correlation function. *Journal of Computational Physics*, 24(4):450–454, August 1977. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002199917790033X`. See [680].

Atkinson:1977:EPA

[817] A. C. Atkinson. An easily programmed algorithm for generating gamma random variables. *Journal of the Royal Statistical Society. Series A (General)*, 140(2):232–234, ???? 1977. CODEN JSSAEF. ISSN 0035-9238. URL `http://www.jstor.org/stable/2344879`.

Beasley:1977:SAA

[818] J. D. Beasley and S. G. Springer. Statistical algorithms: Algorithm AS 111: The percentage points of the normal distribution. *Applied Statistics*, 26(1):118–121, March 1977. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/111`.

Bendat:1977:PAR

[819] Julius S. Bendat. *Principles and Applications of Random Noise Theory*. Robert E. Krieger Publishing Company, Huntington, NY, USA, 1977. ISBN 0-88275-556-0. xxi + 433 pp. LCCN TK5101 .B37 1978.

Bohrer:1977:SSR

[820] R. Bohrer and P. B. Imrey. Statistics, stationarity and random number generation. *ACM Simuletter*, 9(??):64–71, ???? 1977. CODEN SIMUD5. ISSN 0163-6103.

Camp:1977:IPN

[821] W. V. Camp and T. G. Lewis. Implementing a pseudorandom number generator on a minicomputer. *IEEE Transactions on Software Engineering*, SE-3(3):259–262, May/June 1977. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702434`.

Cheng:1977:MGG

[822] R. C. H. Cheng. Miscellanea: The generation of gamma variables with non-integral shape parameter. *Applied Statistics*, 26(1):71–75, 1977. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Fishman:1977:ETM

[823] George S. Fishman and Louis R. Moore. Empirical testing of multiplicative congruential generators with modulus $2^{31} - 1$. Technical Report 77-12, University of North Carolina at Chapel Hill, Chapel Hill, NC 27514, USA, October 1977. iv + 15 + ii pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a046149.pdf`.

Gait:1977:NNP

[824] J. Gait. A new nonlinear pseudorandom number generator. *IEEE Transactions on Software Engineering*, SE-3(5):359–363, September/October 1977. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1702460`.

Garling:1977:SBS

[825] D. J. H. Garling. Sums of Banach space valued random variables. Mimeographed lecture notes, 1977.

Gideon:1977:SAE

[826] Rudy A. Gideon and John Gurland. Some alternative expansions for the distribution function of a noncentral chi-square random variable. *SIAM Journal on Mathematical Analysis*, 8(1):100–110, February 1977. CODEN SJMAAH. ISSN 0036-1410 (print), 1095-7154 (electronic).

Jackson:1977:SGP

[827] D. Jackson. Software generation of pseudorandom sequences. *Electronic Engineering*, 49(??):55–58, December 1977. CODEN ELEGAP. ISSN 0013-4902.

Kinderman:1977:CGR

[828] A. J. Kinderman and J. F. Monahan. Computer generation of random variables using the ratio of uniform deviates. *ACM Transactions on Mathematical Software*, 3(3):257–260, September 1977. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kurita:1977:CPC

[829] Y. Kurita. Choosing parameters for congruential random number generators. In Barra et al. [4107], pages 697–704. ISBN 0-7204-0751-6. LCCN QA276.A1 E89 1976.

Landauer:1977:CCM

[830] Edwin G. Landauer. Computer corner: Methods of random number generation. *Two-Year College Mathematics Journal*, 8(5):296–303, Novem-

ber 1977. CODEN ???? ISSN 0049-4925 (print), 2325-9116 (electronic). URL `http://www.jstor.org/stable/3026786`; `http://www.tandfonline.com/doi/abs/10.1080/00494925.1977.11974532`.

Marsaglia:1977:SMG

[831] George Marsaglia. The squeeze method for generating gamma variates. *Computers and Mathematics and Applications*, 3(4):321–325, 1977. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Miller:1977:STD

[832] A. J. Miller, A. W. Brown, and P. Mars. A simple technique for the determination of delayed maximal length linear binary sequences. *IEEE Transactions on Computers*, C-26(8):808–811, August 1977. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674919`.

Miller:1977:TDD

[833] A. J. Miller and P. Mars. Theory and design of a digital stochastic computer random number generator. *Mathematics and Computers in Simulation*, 19(??):198–216, ???? 1977. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic).

Mitchell:1977:TLM

[834] R. L. Mitchell and C. R. Stone. Table-lookup methods for generating arbitrary random numbers. *IEEE Transactions on Computers*, C-26(10):1006–1008, October 1977. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674735`.

Mueller:1977:RNG

[835] R. A. Mueller, D. D. Georg, and G. R. Johnson. A random number generator for microprocessors. *Simulation*, 28(4):123–127, April 1977. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/28/4/123.abstract`.

Musyck:1977:SPG

[836] E. Musyck. Search for a perfect generator of random numbers. Working Paper BLG 516, Centre d'Étude de l'Énergie Nucléaire, Belgium, 1977.

Niederreiter:1977:PRN

[837] Harald Niederreiter. Pseudo-random numbers and optimal coefficients. *Advances in Mathematics*, 26(2):99–181, ???? 1977. CODEN ADMTA4. ISSN 0001-8708 (print), 1090-2082 (electronic).

Payne:1977:NRN

[838] W. H. Payne. Normal random numbers: Using machine analysis to choose the best algorithm. *ACM Transactions on Mathematical Software*, 3(4):346–358, December 1977. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/355759.355763`.

Peskun:1977:IAR

[839] P. Peskun. Improving the apparent randomness of pseudorandom numbers generated by the mixed congruential method. In D. Hogben and D. Fife, editors, *Proceedings of the 10th Annual Symposium on the Interface of Computer Science and Statistics*, pages 323–328. ????, ????, 1977. ISBN ???? LCCN ????

Pettitt:1977:KSG

[840] A. N. Pettitt and M. A. Stephens. The Kolmogorov–Smirnov goodness-of-fit statistic with discrete and grouped data. *Technometrics*, 19(??): 205–210, ???? 1977. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic).

Reeds:1977:CRN

[841] James A. Reeds. "Cracking" a random number generator. *Cryptologia*, 1(1):20–26, January 1977. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). Reprinted in [4134, pp. 509–515].

Reiser:1977:AAR

[842] John Fredrick Reiser. Analysis of additive random number generators. U.S. Government Report STAN-CS-77-601 (AD-A045652/5), Computer Science Department, School of Humanities and Sciences, Stanford University, Stanford, CA, USA, March 1977. 34 pp.

Roefs:1977:CPR

[843] H. F. A. Roefs and M. B. Pursley. Correlation parameters of random binary sequences. *Electronics Letters*, 13(16):488–489, August 4, 1977. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4240473`.

Schmeiser:1977:RMB

[844] Bruce W. Schmeiser and M. A. Shalaby. Rejection methods for beta variate generation. Technical Report 77014, Department of Operations Research and Engineering Management, Southern Methodist University, Dallas, TX 75275, USA, 1977.

Sheil:1977:SAA

[845] J. Sheil and I. O'Muircheartaigh. Statistical algorithms: Algorithm AS 106: The distribution of non-negative quadratic forms in normal variables. *Applied Statistics*, 26(1):92–98, March 1977. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/106`. See remark [1114].

Shepherd:1977:TLI

[846] W. L. Shepherd and J. N. Hynes. Table look-up and interpolation for a normal random number generator. In *Proceedings of the Twenty-Second Conference on the Design of Experiments in Army Research, Development, and Testing: sponsored by Army Mathematics Steering Committee, Host, Harry Diamond Laboratories, Adelphi, Maryland, 20–22 October 1976*, number 77-2 in ARO Report, pages 153–164. US Army Research Office, Research Triangle Park, NC, USA, 1977. ISBN ???? LCCN ????

Swick:1977:HRA

[847] D. A. Swick. Harmonic relationships among random variables. *SIAM Journal on Applied Mathematics*, 33(3):490–498, November 1977. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Tashiro:1977:MGU

[848] Yoshihiro Tashiro. On methods for generating uniform random points on the surface of a sphere. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 29(1):295–300, ???? 1977. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/article/10.1007/BF02532791`.

Vaduva:1977:CGG

[849] I. Väduva. On computer generation of gamma random variables by rejection and composition procedures. *Statistics (Berlin, DDR)*, 8(4):545–576, 1977. CODEN MOSSD5. ISSN 0323-3944.

Walker:1977:EMG

[850] Alastair J. Walker. An efficient method for generating discrete random variables with general distributions. *ACM Transactions on Mathematical Software*, 3(3):253–256, September 1977. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Yuen:1977:TRN

[851] Chung-Kwong Yuen. Testing random number generators by Walsh transform. *IEEE Transactions on Computers*, C-26(4):329–333, April

1977. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674842`.

Arvillias:1978:PPC

[852] A. C. Arvillias and D. G. Maritsas. Partitioning the period of a class of m-sequences and application to pseudorandom number generation. *Journal of the ACM*, 25(4):675–686, October 1978. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Best:1978:SAC

[853] D. J. Best. A simple algorithm for the computer generation of random samples from a Student's t or symmetric beta distribution. In L. C. A. (Leo Caspar Antoon) Corsten and J. Hermans, editors, *COMPSTAT 1978: Proceedings in Computational statistics: 3rd symposium held in Leiden 1978*, pages 341–347. Physica-Verlag, Vienna, Austria, 1978. ISBN 3-7908-0196-8 (paperback). LCCN QA276.4 .C192.

Castanie:1978:GRB

[854] F. Castanie. Generation of random bits with accurate and reproducible statistical properties. *Proceedings of the IEEE*, 66(7):865–870, July 1978. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic).

Cheng:1978:GBV

[855] R. C. H. Cheng. Generating beta variates with nonintegral shape parameters. *Communications of the ACM*, 21(4):317–322, April 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Dagpunar:1978:SVT

[856] J. S. Dagpunar. Sampling of variates from a truncated gamma distribution. *Journal of Statistical Computation and Simulation*, 8(1):59–64, 1978. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

DiDonato:1978:CBN

[857] A. R. DiDonato, M. P. Jarnagin, Jr., and R. K. Hageman. Computation of the bivariate normal distribution over convex polygons. Report NSWC/DL-TR-3886, Naval Surface Weapons Center, Dahlgren, VA 22448, USA, September 1978. v + 46 + 7 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a069406.pdf`.

Fishman:1978:PDE

[858] George S. Fishman. *Principles of Discrete Event Simulation*. Wiley series on systems engineering and analysis. Wiley, New York, NY, USA, 1978. ISBN 0-471-04395-8. xviii + 514 pp. LCCN T57.62 .F59.

Fishman:1978:SEM

[859] George S. Fishman and Louis R. Moore III. A statistical evaluation of multiplicative congruential generators with modulus $2^{-31} - 1$. Technical report 78-11, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, December 1978. v + 19 + 2 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a063858.pdf`; `http://www.or.unc.edu/research/temp/tech70b.html`.

Frigerio:1978:TTR

[860] N. A. Frigerio, N. Clark, and S. Tyler. Toward truly random numbers. Report ANL/ES-26 Part 4, Argonne National Laboratory, Argonne, IL, USA, 1978.

Galperin:1978:LPC

[861] E. A. Galperin. Loop properties and controllability of linear congruential sequences. *IEEE Transactions on Computers*, C-27(1):68–76, January 1978. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1674954`.

Garpman:1978:STP

[862] S. Garpman and J. Randrup. Statistical tests for pseudorandom number generators. *Computer Physics Communications*, 15(1–2):5–13, September 1978. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465578900802`.

Gaver:1978:PNA

[863] Donald P. Gaver. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Comment. *Journal of the American Statistical Association*, 73(363):522, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286593.pdf`. See [885].

Geller:1978:SEW

[864] Nancy L. Geller. Some examples of the weak and strong laws of large numbers for averages of mutually independent random variables. *The*

American Statistician, 32(1):34–36, February 1978. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683474`.

Hoaglin:1978:SAR

[865] David C. Hoaglin and Max L. King. Statistical algorithms: Remark AS R24: a remark on Algorithm AS 98: The spectral test for the evaluation of congruential pseudo-random generators. *Applied Statistics*, 27(3): 375–377, 1978. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/98`; `http://www.jstor.org/stable/pdfplus/2347183.pdf`. See [771, 772].

Hollander:1978:TDU

[866] Myles Hollander and Frank Proschan. Testing to determine the underlying distribution using randomly censored data. FSU Statistics Report M458, Department of Statistics, The Florida State University, Tallahassee, FL 32306, USA, April 1978. 18 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a054978.pdf`. Also issued as AFOSR Technical Report No. 6 and AFOSR Technical Report No. 79.

Holmlid:1978:UCP

[867] Leif Holmlid and Kjell Rynefors. Uniformity of congruential pseudorandom number generators. Dependence on length of number sequence and resolution. *Journal of Computational Physics*, 26(3):297–306, March 1978. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999178900724`.

Kemp:1978:CGB

[868] C. D. Kemp and S. Loukas. The computer generation of bivariate discrete random variables. *Journal of the Royal Statistical Society. Series A (General)*, 141(4):513–519, ???? 1978. CODEN JSSAEF. ISSN 0035-9238. URL `http://www.jstor.org/stable/2344486`.

Kiefer:1978:PNA

[869] J. Kiefer. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Comment. *Journal of the American Statistical Association*, 73(363):523–524, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286594.pdf`. See [885].

Kinderman:1978:RDC

[870] A. J. Kinderman and J. F. Monahen. Recent developments in the computer generation of Student s t and gamma random variables. Technical Report AMD-799, BNL-24679, Brookhaven National Laboratory, Long Island, NY, USA, 1978. ?? pp.

Li:1978:EMN

[871] T-Y. Li and J. A. Yorke. Ergodic maps on $[0, 1]$ and non-linear pseudorandom number generators. *Nonlinear Analysis, Theory, Methods and Applications*, 2(??):473–481, ???? 1978. CODEN NOANDD. ISSN 0362-546X (print), 1873-5215 (electronic).

Mallows:1978:PNA

[872] Colin L. Mallows. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Comment. *Journal of the American Statistical Association*, 73(363):520, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286591.pdf`. See [885].

Maritsas:1978:PSA

[873] D. G. Maritsas, A. C. Arvillias, and A. C. Bounas. Phase-shift analysis of linear feedback shift register structures generating pseudorandom sequences. *IEEE Transactions on Computers*, C-27(7):660–669, July 1978. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675166`.

Nance:1978:SEO

[874] Richard E. Nance and Claude Overstreet, Jr. Some experimental observations on the behavior of composite random number generators. *Operations Research*, 26(5):915–935, September/October 1978. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://www.jstor.org/stable/170084`.

Niederreiter:1978:EGL

[875] Harald Niederreiter. Existence of good lattice points in the sense of Hlawka. *Monatshefte für Mathematik*, 86(3):203–219, September 1978–1979. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Niederreiter:1978:QMC

[876] Harald Niederreiter. Quasi-Monte Carlo methods and pseudo-random numbers. *Bulletin of the American Mathematical Society*, 84(6):957–1041, November 1978. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic). URL `http://www.ams.org/bull/1978-84-06/S0002-9904-1978-14532-7/S0002-9904-1978-14532-7.pdf`.

Niederreiter:1978:STLa

[877] Harald Niederreiter. The serial test for linear congruential pseudo-random numbers. *Bulletin of the American Mathematical Society*, 84 (2):273–274, ???? 1978. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic).

Niederreiter:1978:STLb

[878] H. Niederreiter. Statistical tests for linear congruential pseudorandom numbers. In L. Corsten and J. Hermans, editors, *Proceedings of COMPSTAT 1978*, pages 398–404. Physica Verlag, ????, 1978. ISBN ???? LCCN ????

Padgett:1978:CCI

[879] W. J. Padgett. C21. Comment on inverse Gaussian random number generation. *Journal of Statistical Computation and Simulation*, 8(1):78–79, 1978. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Rivest:1978:MOD

[880] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). The basics of trap-door functions and the famous RSA public key cryptosystem are presented in this paper.

Romankevich:1978:MCN

[881] A. M. Romankevich. A method of construction of nonlinear generators of pseudorandom sequences. *Cybernetics*, 14(1):141–142, January 1978. CODEN CYBNAW. ISSN 0011-4235 (print), 2375-0189 (electronic). URL `http://link.springer.com/article/10.1007/BF01207141`.

Sakasegawa:1978:GNP

[882] Hirotaka Sakasegawa. On a generation of normal pseudo-random numbers. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 30

(1):271–279, ???? 1978. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/article/10.1007/BF02480218`.

Schmeiser:1978:GVD

[883] Bruce W. Schmeiser. Generation of variates from distribution tails. Technical Report 78008, Department of Operations Research and Engineering Management, Southern Methodist University, Dallas, TX 75275, USA, 1978. ?? pp.

Schmeiser:1978:SMG

[884] Bruce W. Schmeiser. Squeeze methods for generating gamma variates. Technical Report OREM-78009, Department of Operations Research and Engineering Management, Southern Methodist University, Dallas, TX 75275, USA, July 1978. 21 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a060388.pdf`.

Schruben:1978:PNAa

[885] Lee W. Schruben and Barry H. Margolin. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments. *Journal of the American Statistical Association*, 73 (363):504–520, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286590.pdf`. See discussion [863, 869, 872, 886, 887].

Schruben:1978:PNAb

[886] Lee W. Schruben and Barry H. Margolin. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Rejoinder. *Journal of the American Statistical Association*, 73(363):524–525, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286595.pdf`. See [885].

Simon:1978:PNA

[887] Gary A. Simon. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Comment. *Journal of the American Statistical Association*, 73(363):520–521, September 1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/pdfplus/2286592.pdf`. See [885].

Singh:1978:CPP

[888] Jagbir Singh. A characterization of positive Poisson distribution and its statistical application. *SIAM Journal on Applied Mathematics*, 34 (3):545–548, May 1978. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Sowey:1978:SCB

[889] E. R. Sowey. A second classified bibliography on random number generation and testing. *International Statistical Review = Revue Internationale de Statistique*, 46(1):89–102, April 1978. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL `http://www.jstor.org/stable/i261095`.

Starner:1978:EID

[890] J. W. Starner and W. L. Shepherd. Efficient inverse distribution type normal random number generator. *SIAM Review*, 20(3):635, ???? 1978. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Tadikamalla:1978:CGGa

[891] Pandu R. Tadikamalla. Computer generation of gamma random variables. *Communications of the ACM*, 21(5):419–422, May 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Tadikamalla:1978:CGGb

[892] Pandu R. Tadikamalla. Computer generation of gamma random variables — II. *Communications of the ACM*, 21(11):925–928, November 1978. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Whitmore:1978:NLT

[893] G. A. Whitmore and M. Yalovsky. A normalizing logarithmic transformation for inverse Gaussian random variables. *Technometrics*, 20(2): 207–208, May 1978. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/1268715`.

Zielinski:1978:EZP

[894] Ryszard Zieliński. *Erzeugung von Zufallszahlen: Programmierung und Test Digitalrechnern. (German) [Generation of random numbers: Programming and test digital computation]*. Ham Deutsch, Frankfurt, West Germany; Thun, Switzerland, 1978. ISBN 3-87144-404-9. xiii + 160 pp. LCCN ????

Anonymous:1979:BRT

[895] Anonymous. Book reviews: Tables of Random Times, by I. D. Hill and P. A. Hill. *Applied Statistics*, 28(1):72, 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Apostolopoulos:1979:IAN

[896] N. Apostolopoulos and G. Schuff. Initializing algorithms: a note to the article: "Computer methods for sampling from gamma, beta, Poisson and binomial distributions" [Computing **12** (1974), no. 3, 223–246; MR **52** #15949] by J. H. Ahrens and Ulrich Dieter. *Computing: Archiv für Informatik und Numerik*, 22(2):185–189, June 1979. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). See [673].

Atkinson:1979:CGP

[897] A. C. Atkinson. The computer generation of Poisson random variables. *Applied Statistics*, 28(??):29–35, ???? 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Atkinson:1979:FSA

[898] A. C. Atkinson. A family of switching algorithms for the computer generation of beta random variables. *Biometrika*, 66(1):141–145, April 1979. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL `http://www.jstor.org/stable/2335253`.

Atkinson:1979:RDC

[899] A. C. Atkinson. Recent developments in the computer generation of Poisson random variables. *Applied Statistics*, 28(??):260–263, ???? 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Atkinson:1979:SAA

[900] A. C. Atkinson and J. Whittaker. Statistical algorithms: Algorithm AS 134: The generation of beta random variables with one parameter greater than and one parameter less than 1. *Applied Statistics*, 28(1):90–93, March 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/134`.

Atkinson:1979:SGI

[901] A. C. (Anthony Curtis) Atkinson. *The simulation of generalised inverse Gaussian, generalised hyperbolic, gamma, and related random variables.* Research reports — Department of Theoretical Statistics, University of

Aarhus; no. 52. Department of Theoretical Statistics, Institute of Mathematics, University of Aarhus, Århus, Denmark, 1979. 48 (various) pp. LCCN QA273.6 .A84.

Bache:1979:APP

[902] Niels Bache. Approximate percentage points for the distribution of a product of independent positive random variables. *Applied Statistics*, 28 (2):158–162, 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Bentley:1979:AGS

[903] J. L. Bentley and J. B. Saxe. Algorithm: Generating sorted lists of randoms. Report CMU-CS-79-113, Department of Computer Science, Carnegie-Mellon University, Pittsburgh, PA, USA, March 1979. Published in [949].

Best:1979:SEP

[904] D. J. Best. Some easily programmed pseudo-random normal generators. *Australian Computer Journal*, 11(2):60–62, 1979. CODEN ACMJB2. ISSN 0004-8917.

Braaten:1979:ILD

[905] Eric Braaten and George Weller. An improved low-discrepancy sequence for multidimensional quasi-Monte Carlo integration. *Journal of Computational Physics*, 33(2):249–258, November 1979. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999179900196`. See improvements in [3346].

Bright:1979:QRN

[906] Herbert S. Bright and Richard L. Enison. Quasi-random number sequences from a long-period TLP generator with remarks on application to cryptography. *ACM Computing Surveys*, 11(4):357–370, December 1979. CODEN CMSVAN. ISSN 0010-4892.

Brown:1979:CPNa

[907] Mark Brown and Herbert Solomon. On combining pseudorandom number generators. In Anonymous, editor, *Proceedings of the Twenty-Fourth Conference on the Design of Experiments, Mathematics Research Center, University of Wisconsin, Madison, Wisconsin, 4–6 October 1978*, volume 79-2, pages 133–142. U.S. Army Research Office, P.0. Box 12211, Research Triangle Park, NC, USA, June 1979. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a070840.pdf`.

Brown:1979:CPNb

[908] Mark Brown and Herbert Solomon. On combining pseudorandom number generators. *Annals of Statistics*, 7(3):691–695, May 1979. CODEN ASTSC7. ISSN 0090-5364 (print), 2168-8966 (electronic). URL `http://www.jstor.org/stable/2958754`.

Burford:1979:AVM

[909] R. L. Burford. Additive vs multiplicative uniform pseudo-random number generators in the generation of Erlang variates. *ACM Simuletter*, 10 (3):75–82, 1979. CODEN SIMUD5. ISSN 0163-6103.

Cheng:1979:SSG

[910] R. C. H. Cheng and G. M. Feast. Some simple gamma variate generators. *Applied Statistics*, 28(3):290–295, 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

delJunco:1979:HLV

[911] A. del Junco and J. Michael Steele. Hammersley's Law for the Van Der Corput sequence: An instance of probability theory for pseudorandom numbers. *Annals of Probability*, 7(2):267–275, April 1979. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL `http://projecteuclid.org/euclid.aop/1176995087`; `http://www.jstor.org/stable/pdfplus/2242879.pdf`.

Edgell:1979:SCD

[912] Stephen E. Edgell. A statistical check of the DECsystem-10 FORTRAN pseudorandom number generator. *Behavior Research Methods and Instrumentation*, 11(5):529–530, September 1979. CODEN BRMIAC. ISSN 0005-7878. URL `http://www.springerlink.com/content/ah71321478333g10/`.

Good:1979:CCR

[913] I. J. Good. C52: The clustering of random variables. *Journal of Statistical Computation and Simulation*, 9(3):241–243, ???? 1979. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Hammersley:1979:MCM

[914] J. M. (John Michael) Hammersley and D. C. (David Christopher) Handscomb. *Monte Carlo methods*. Monographs on statistics and applied probability. Chapman and Hall, Ltd., London, UK, 1979. ISBN 0-412-15870-1. vii + 178 pp. LCCN QA298 .H354 1964. Reprint of [326].

Heidelberger:1979:CSS

[915] Philip Heidelberger and Donald L. Iglehart. Comparing stochastic systems using regenerative simulation with Common Random Numbers. *Advances in Applied Probability*, 11(4):804–819, December 1979. CODEN AAPBBD. ISSN 0001-8678 (print), 1475-6064 (electronic). URL `http://www.jstor.org/stable/1426860`.

Hellman:1979:MPK

[916] Martin E. Hellman. The mathematics of public-key cryptography. *Scientific American*, 241(2):146–?? (Intl. ed. 130–139), August 1979. CODEN SCAMAC. ISSN 0036-8733 (print), 1946-7087 (electronic).

Hill:1979:CPP

[917] G. W. Hill. Cyclic properties of pseudo-random sequences of Mersenne prime residues. *The Computer Journal*, 22(1):80–85, February 1979. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/80.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/81.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/82.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/83.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/84.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_22/Issue_01/tiff/85.tif`.

Iglehart:1979:RSI

[918] Donald L. Iglehart and Peter A. W. Lewis. Regenerative simulation with internal controls. *Journal of the ACM*, 26(2):271–282, April 1979. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Kahaner:1979:EAD

[919] David K. Kahaner and Mark B. Wells. An experimental algorithm for N-dimensional adaptive quadrature. *ACM Transactions on Mathematical Software*, 5(1):86–96, March 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kirby:1979:MFC

[920] William H. Kirby. Machine-independent FORTRAN coding of Lehmer random number generators. Open-file series 80- 004, U.S. Geological Survey, Reston, VA, USA, 1979. [i] + 11 pp.

Kleijnen:1979:ASC

[921] J. P. C. Kleijnen. Analysis of simulation with Common Random Numbers: a note on Heikes et al. *Simulette*, 11(??):7–13, ???? 1979. CODEN ???? ISSN ????

Kronmal:1979:AMG

[922] Richard A. Kronmal and Arthur V. Peterson, Jr. On the alias method for generating random variables from a discrete distribution. *The American Statistician*, 33(4):214–218, ???? 1979. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Lee:1979:DRC

[923] Ru Ying Lee, Burt S. Holland, and John A. Flueck. Distribution of a ratio of correlated gamma random variables. *SIAM Journal on Applied Mathematics*, 36(2):304–320, April 1979. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Monahan:1979:ENM

[924] John F. Monahan. Extensions of von Neumann's method for generating random variables. *Mathematics of Computation*, 33(147):1065–1069, July 1979. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Moore:1979:RNG

[925] J. L. Moore and F. H. Thomas. A random number generator for BASIC programs. *Computer Education*, 33(??):13–16, ???? 1979. CODEN ???? ISSN ????

Nadas:1979:PP

[926] Arthur Nadas. Probabilistic PERT. *IBM Journal of Research and Development*, 23(3):339–347, May 1979. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Niki:1979:CMF

[927] Naoto Niki. Corrections to "Multi-folding the normal distribution and mutual transformation between uniform and normal random variables". *Annals of the Institute of Statistical Mathematics (Tokyo)*, 31(1):349, ???? 1979. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/BF02480292`. See [928].

Niki:1979:MFN

[928] Naoto Niki. Multi-folding the normal distribution and mutual transformation between uniform and normal random variables. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 31(1):125–140, ???? 1979. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/article/10.1007/BF02480270`. See corrections [927].

Pangratz:1979:PRN

[929] H. Pangratz and H. Weinrichter. Pseudo-random number generator based on binary and quinary maximal-length sequences. *IEEE Transactions on Computers*, C-28(9):637–642, September 1979. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1675431`.

Pavlov:1979:PNG

[930] A. I. Pavlov and B. B. Pokhodzei. Pseudorandom numbers generated by linear recurrence relations over a finite field. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 19(4):38–44, ???? 1979. CODEN CMMPA9. ISSN 0041-5553 (print), 1878-2930 (electronic). URL `http://www.sciencedirect.com/science/article/pii/004155537990154X`.

Reeds:1979:CMC

[931] James A. Reeds. Cracking a multiplicative congruential encryption algorithm. In Wang [4108], pages 467–472. ISBN 0-12-734250-8. LCCN TA329 .W67 1978.

Ripley:1979:TRS

[932] B. D. Ripley. Tests of randomness for spatial point patterns. *Journal of the Royal Statistical Society. Series B (Methodological)*, 41(??):368–374, ???? 1979. CODEN JSTBAJ. ISSN 0035-9246.

Roberts:1979:ITN

[933] C. S. Roberts. Implementing and testing new versions of a good 48-bit pseudo-random number generator. Report 1453 (TM 79-1353-5), AT&T Bell Laboratories, Murray Hill, NJ, USA, September 4, 1979. ?? pp.

Rubin:1979:SCB

[934] Frank Rubin. Solving a cipher based on multiple random number streams. *Cryptologia*, 3(3):155–157, July 1979. CODEN CRYPE6.

ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902796~db=all~order=page.

Sahai:1979:SSB

[935] Hardeo Sahai. A supplement to Sowey's bibliography on random number generation and related topics. *Journal of Statistical Computation and Simulation*, 10(1):31–52, December 1979. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949657908810345.

Schrage:1979:MPF

[936] Linus Schrage. A more portable Fortran random number generator. *ACM Transactions on Mathematical Software*, 5(2):132–138, June 1979. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL http://doi.acm.org/10.1145/355826.355828.

Sobol:1979:ESS

[937] I. M. Sobol'. Erratum: "On the Systematic Search in a Hypercube" [SIAM J. Numer. Anal. **16** (1979), no. 5, 790–793, MR 80f:65072]. *SIAM Journal on Numerical Analysis*, 16(6):1080, December 1979. CODEN SJNAAM. ISSN 0036-1429 (print), 1095-7170 (electronic). See [938].

Sobol:1979:SSH

[938] I. M. Sobol'. On the systematic search in a hypercube. *SIAM Journal on Numerical Analysis*, 16(5):790–793, October 1979. CODEN SJNAAM. ISSN 0036-1429 (print), 1095-7170 (electronic). See erratum [937].

Tanemura:1979:RCP

[939] M. Tanemura. On random complete packing by discs. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 31(Part B):351–365, ???? 1979. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic).

Tripathi:1979:RFI

[940] V. S. Tripathi. RANTEST — a Fortran IV program for testing randomness of uniform pseudorandom numbers. *Computers and Geosciences*, 5 (??):251–268, ???? 1979. CODEN CGEODT, CGOSDN. ISSN 0098-3004 (print), 1873-7803 (electronic).

vanLint:1979:PRA

[941] J. H. van Lint, F. J. MacWilliams, and N. J. A. Sloane. On pseudorandom arrays. *SIAM Journal on Applied Mathematics*, 36(1):62–72,

February 1979. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic). URL `http://www.jstor.org/stable/2100768`.

Wang:1979:MND

[942] Y. H. Wang. Mathematical notes: Dependent random variables with independent subsets. *American Mathematical Monthly*, 86(4):290–292, April 1979. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Williams:1979:SPF

[943] H. C. Williams and E. Seah. Some primes of the form $(a^n - 1)/(a - 1)$. *Mathematics of Computation*, 33(148):1337–1342, October 1979. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Wright:1979:ECR

[944] R. D. Wright and T. E. Ramsay, Jr. On the effectiveness of Common Random Numbers. *Management Science*, 25(7):649–656, July 1979. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Ahrens:1980:SBP

[945] J. H. Ahrens and Ulrich Dieter. Sampling from binomial and Poisson distributions: a method with bounded computation times. *Computing: Archiv für Informatik und Numerik*, 25(3):193–208, September 1980. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Atkinson:1980:TPR

[946] A. C. Atkinson. Tests of pseudo-random numbers. *Applied Statistics*, 29(2):164–171, 1980. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Basu:1980:RAEa

[947] D. Basu. Randomization analysis of experimental data: The Fisher randomization test. *Journal of the American Statistical Association*, 75 (371):575–582, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287648`.

Basu:1980:RAEb

[948] D. Basu. Randomization analysis of experimental data: The Fisher randomization test rejoinder. *Journal of the American Statistical Association*, 75(371):593–595, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287654`.

Bentley:1980:GSL

[949] Jon Louis Bentley and James B. Saxe. Generating sorted lists of random numbers. *ACM Transactions on Mathematical Software*, 6(3):359–364, September 1980. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/355900.355907`.

Brown:1980:GFG

[950] T. Brown. General fast generation of random variables for discrete distribution. *ACM Simuletter*, 11, 4:73–75, 1980. CODEN SIMUD5. ISSN 0163-6103.

Davies:1980:SAA

[951] Robert B. Davies. Statistical algorithms: Algorithm AS 155: The distribution of a linear combination of χ^2 random variables. *Applied Statistics*, 29(3):323–333, September 1980. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/155`. See remark [1114].

Dempster:1980:CEA

[952] M. A. H. Dempster and A. Papagaki-Papoulias. Computational experience with an approximate method for the distribution problem. In Dempster [4109], pages xiii + 573. ISBN 0-12-208250-8. LCCN T57.79 .I54 1974. US$97.00.

Edgington:1980:RT

[953] Eugene S. Edgington. *Randomization tests*, volume 31 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, 1980. ISBN 0-8247-6878-7. xii + 287 pp. LCCN QA277 .E32.

Farebrother:1980:SAA

[954] R. W. Farebrother. Statistical algorithms: Algorithm AS 153: Pan's procedure for the tail probabilities of the Durbin–Watson statistic. *Applied Statistics*, 29(2):224–227, June 1980. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/153`. See remark [1113, 1114].

Fishman:1980:NLR

[955] G. S. Fishman. Notes on linear recurrence generators modulo 2. Technical report, University of North Carolina, Chapel Hill, NC, USA, 1980.

Fishman:1980:SCM

[956] George S. Fishman and Louis R. Moore III. In search of correlation in multiplicative congruential generators with modulus $2^{-31} - 1$. Technical

report 80-05, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, September 1980. URL http://www.or.unc.edu/research/temp/tech80a.html#1980.

Gardenes:1980:FSI

[957] E. Gardenes and A. Trepat. Fundamentals of Sigla, an interval computing system over the completed set of intervals. *Computing: Archiv für Informatik und Numerik*, 24(2–3):161–179, June 1980. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Good:1980:CFD

[958] I. J. Good. C77. Functions of distinct random variables having identical distributions. *Journal of Statistical Computation and Simulation*, 12(1): 68–70, ???? 1980. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Hassner:1980:UMR

[959] Martin Hassner and Jack Sklansky. The use of Markov random fields as models of texture. *Computer Graphics and Image Processing*, 12(4):357–370, April 1980. CODEN CGIPBG. ISSN 0146-664x (print), 1557-9697 (electronic). HASSNER80.

Hinkley:1980:RAE

[960] David V. Hinkley. Randomization analysis of experimental data: The Fisher randomization test comment. *Journal of the American Statistical Association*, 75(371):582–584, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL http://www.jstor.org/stable/2287649.

James:1980:MCT

[961] F. James. Monte Carlo theory and practice. *Reports on Progress in Physics*, 43(9):1145–1189, September 1980. CODEN RPPHAG. ISSN 0034-4885 (print), 1361-6633 (electronic). URL http://iopscience.iop.org/0034-4885/43/9/002.

Johnson:1980:RPS

[962] Dudley Paul Johnson. The ruin problem for sums of dependent random variables. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 23(??):333–338, ???? 1980. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Kempthorne:1980:RAE

[963] Oscar Kempthorne. Randomization analysis of experimental data: The Fisher randomization test comment. *Journal of the American Statistical Association*, 75(371):584–587, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287650`.

Kennedy:1980:SC

[964] William J. Kennedy, Jr. and James E. Gentle. *Statistical Computing*, volume 33 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, 1980. ISBN 0-8247-6898-1. xi + 591 pp. LCCN QA276.4 .K46. URL `http://lccn.loc.gov/80010976`.

Kinderman:1980:NMG

[965] A. J. Kinderman and J. F. Monahan. New methods for generating Student's t and gamma variables. *Computing: Archiv für Informatik und Numerik*, 25(4):369–377, December 1980. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Knuth:1980:DLC

[966] Donald E. Knuth. Deciphering a linear congruential encryption. Report 024800, Department of Computer Science, Stanford University, Stanford, CA, USA, 1980.

Lam:1980:RTD

[967] Simon S. Lam and A. Udaya Shankar. Response time distributions for a multi-class queue with feedback. *ACM SIGMETRICS Performance Evaluation Review*, 9(2):225–234, Summer 1980. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Lane:1980:RAE

[968] David A. Lane. Randomization analysis of experimental data: The Fisher randomization test comment. *Journal of the American Statistical Association*, 75(371):587–589, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287651`.

Lindley:1980:RAE

[969] D. V. Lindley. Randomization analysis of experimental data: The Fisher randomization test comment. *Journal of the American Statistical Association*, 75(371):589–590, September 1980. CODEN JSTNAL. ISSN

0162-1459 (print), 1537-274X (electronic). URL http://www.jstor.org/stable/2287652.

Marsaglia:1980:GRV

[970] George Marsaglia. Generating random variables with a t-distribution. *Mathematics of Computation*, 34(149):235–236, January 1980. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

OBrien:1980:PIR

[971] G. L. O'Brien. Pairwise independent random variables. *Annals of Probability*, 8(1):170–175, February 1980. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL http://projecteuclid.org/euclid.aop/1176994834.

Peskun:1980:TTC

[972] Peter H. Peskun. Theoretical tests for choosing the parameters of the general mixed linear congruential pseudorandom number generator. *Journal of Statistical Computation and Simulation*, 11(3–4):281–305, ???? 1980. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949658008810415.

Petkovic:1980:RRV

[973] M. S. Petkovic. A representation of random variables by the probable intervals. Freiburger Intervall-Ber. 80/10, Universität Freiburg, Freiburg, Germany, 1980. 12–20 pp.

Ribeiro:1980:MOS

[974] C. A. Ribeiro. Method for obtaining small sets of pseudo random numbers with uniform distribution. *Computer Physics Communications*, 19 (3):305–307, July/August 1980. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/0010465580900855.

Rice:1980:DQF

[975] S. O. Rice. Distribution of quadratic forms in normal random variables—evaluation by numerical integration. *SIAM Journal on Scientific and Statistical Computing*, 1(4):438–448, December 1980. CODEN SIJCD4. ISSN 0196-5204. See comment [1071].

Rubin:1980:RAE

[976] Donald B. Rubin. Randomization analysis of experimental data: The Fisher randomization test comment. *Journal of the American Statistical*

Association, 75(371):591–593, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287653`.

Sahai:1980:SSB

[977] Hardeo Sahai. A supplement to Sowey's bibliography on random number generation and related topics. *Biometrical Journal*, 22(5):447–461, ???? 1980. CODEN BIJODN. ISSN 0323-3847. URL `http://onlinelibrary.wiley.com/doi/10.1002/bimj.4710220509`.

Sampson:1980:NCD

[978] Allan R. Sampson. Nonnegative Cholesky decomposition and its application to association of random variables. *SIAM Journal on Algebraic and Discrete Methods*, 1(3):284–291, 1980. CODEN SJAMDU. ISSN 0196-5212 (print), 2168-345X (electronic).

Schmeiser:1980:ARM

[979] Bruce W. Schmeiser and Mohamed A. Shalaby. Acceptance/rejection methods for beta variate generation. *Journal of the American Statistical Association*, 75(371):673–678, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287667`.

Schmeiser:1980:BVG

[980] B. W. Schmeiser and A. J. G. Babu. Beta variate generation via exponential majorizing functions. *Operations Research*, 28(??):917–926, ???? 1980. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Schmeiser:1980:GVD

[981] B. W. Schmeiser. Generation of variates from distribution tails. *Operations Research*, 28(??):1012–1017, ???? 1980. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Schmeiser:1980:RVGa

[982] B. W. Schmeiser. Random variate generation: a survey. Technical report, School of Industrial Engineering, Purdue University, West Lafayette, IN, USA, June 1980. ii + 26 + 1 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a091343.pdf`.

Schmeiser:1980:RVGb

[983] B. W. Schmeiser. Random variate generation: a survey. In Ören et al. [4110], pages 79–104. ISBN ???? LCCN QA76.5 W78 1980.

Schmeiser:1980:SMG

[984] Bruce W. Schmeiser and Ram Lal. Squeeze methods for generating gamma variates. *Journal of the American Statistical Association*, 75 (371):679–682, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287668`.

Shedler:1980:RTS

[985] G. S. Shedler. Response-time simulation of multivariate point process models for multiprogrammed jobstreams. *International Journal of Computer and Information Sciences*, 9(2):73–91, April 1980. CODEN IJCIAH. ISSN 0091-7036.

Simmons:1980:RNG

[986] R. E. Simmons. Random number generator. U.S. Patent No. 4,183,088., January 8, 1980.

Soulis:1980:RDL

[987] A. Soulis. *Recent developments in linear congruential and other methods for pseudorandom number generation*. Ph.D. thesis, Chelsea College, University of London, London, UK, 1980.

Tadikamalla:1980:RSE

[988] Pandu R. Tadikamalla. Random sampling from the exponential power distribution. *Journal of the American Statistical Association*, 75(371): 683–686, September 1980. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287669`.

Tsay:1980:SST

[989] H. Tsay. *Stringent statistical tests for randomness and random number generators*. Ph.D. thesis, Washington State University, Pullman, WA, USA, 1980.

Ahrens:1981:CME

[990] J. H. Ahrens and K. D. Kohrt. Computer methods for efficient sampling from largely arbitrary statistical distributions. *Computing: Archiv für Informatik und Numerik*, 26(1):19–31, March 1981. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Battaglia:1981:RDA

[991] F. Battaglia. Riproduzione delle autocorrelazioni nei metodi di generazione di numeri pseudo-casuali normali. (Italian) [Reproduction of

autocorrelations in the generation of pseudorandom normal numbers]. *Metron*, 39(3):187–208, ???? 1981. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695x (electronic).

Becker:1981:LSD

[992] Richard A. Becker and John M. Chambers. *S: a Language and System for Data Analysis*. AT&T Bell Laboratories, Murray Hill, NJ, USA, January 1981. 405 pp. URL `https://drive.google.com/drive/folders/14ijVPw1DihydXFqTzj-wgl3C5LYEJdKX`.

Calo:1981:DAT

[993] S. B. Calo. Delay analysis of a two-queue, nonuniform message channel. *IBM Journal of Research and Development*, 25(6):915–929, November 1981. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Deak:1981:EMR

[994] I. Deák. An economical method for random number generation and a normal generator. *Computing: Archiv für Informatik und Numerik*, 27 (2):113–121, June 1981. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Devroye:1981:CGP

[995] Luc Devroye. The computer generation of Poisson random variables. *Computing: Archiv für Informatik und Numerik*, 26(3):197–207, September 1981. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Devroye:1981:CGR

[996] Luc Devroye. On the computer generation of random variables with a given characteristic function. *Computers and Mathematics and Applications*, 7(6):547–552, ???? 1981. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122181900389`.

Diaconis:1981:GRP

[997] Persi Diaconis and Mehrdad Shahshahani. Generating a random permutation with random transpositions. *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, 57(2):159–179, ???? 1981. CODEN ZWVGAA. ISSN 0044-3719. URL `http://link.springer.com/article/10.1007/BF00535487`.

Dudewicz:1981:EBT

[998] Edward J. Dudewicz and Edward C. van der Meulen. Entropy-based tests of uniformity. *Journal of the American Statistical Association*, 76(376): 967–974, December 1981. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287597`.

Dudewicz:1981:HRN

[999] Edward J. Dudewicz and Thomas G. Ralley. *The handbook of random number generation and testing with TESTRAND computer code*, volume 4 of *American series in mathematical and management sciences*. American Sciences Press, Columbus, OH, USA, 1981. ISBN 0-935950-01-X (paperback). xi + 634 pp. LCCN QA298 .D8.

Fishman:1981:SCM

[1000] George S. Fishman and Louis R. Moore III. In search of correlation in multiplicative congruential generators with modulus $2^{31} - 1$. In W. F. Eddy, editor, *Computer Science and Statistics: Proc. of the 13th Symposium on the Interface*, page ?? Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1981. ISBN ???? LCCN ????

Friedman:1981:NPP

[1001] Jerome H. Friedman and Margaret H. Wright. A nested partitioning procedure for numerical multiple integration. *ACM Transactions on Mathematical Software*, 7(1):76–92, March 1981. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Gentle:1981:PCR

[1002] James E. Gentle. Portability considerations for random number generators. In Eddy [4111], pages 158–164. ISBN 3-540-90633-9. LCCN QA276.4. .C58 1981.

Grafton:1981:SAA

[1003] R. G. T. Grafton. Statistical algorithms: Algorithm AS 157: The runs-up and runs-down tests. *Applied Statistics*, 30(1):81–85, March 1981. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/157`.

Green:1981:BRBa

[1004] Bert F. Green. Book review: *Randomization Tests*, by Eugene S. Edgington. *Journal of the American Statistical Association*, 76(374):495, June 1981. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287866`.

Greenwood:1981:PFA

[1005] J. Arthur Greenwood. A portable formulation of the alias method for random numbers with discrete distributions. *Communications in Statistics: Simulation and Computation*, 10(6):649–655, 1981. CODEN CSSCDB. ISSN 0361-0918.

Ide:1981:EZM

[1006] H. D. Ide and J. Sägebarth. Zur Erzeugung von Zufallszahlen mittels linearer Rekursion. (German) [Generation of random numbers using linear recursion]. Technical report, Lehrstuhl für Elektronische Systeme und Vermittlungstechnik, Universität Dortmund, Dortmund, West Germany, 1981. 21 pp.

Kaplan:1981:ERS

[1007] Howard L. Kaplan. Effective random seeding of random number generators. *Behavior Research Methods and Instrumentation*, 13(2):283–289, January 1981. CODEN BRMIAC. ISSN 0005-7878. URL `http://www.springerlink.com/content/0146m73q44251315/`.

Kemp:1981:EGL

[1008] A. W. Kemp. Efficient generation of logarithmically distributed pseudorandom variables. *Applied Statistics*, 30(3):249–253, 1981. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Kirkpatrick:1981:VFS

[1009] S. Kirkpatrick and E. Stoll. A very fast shift-register sequence random number generator. *Journal of Computational Physics*, 40(2):517–526, April 1981. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999181902278`.

Kozlov:1981:ECI

[1010] G. A. Kozlov. The error in calculating an integral by the Monte–Carlo method using a random code generator with independent digits. *Theory of Probability and its Applications*, 25(2):401–408, ???? 1981. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Kronmal:1981:VAR

[1011] Richard A. Kronmal and Arthur V. Peterson, Jr. A variant of the acceptance-rejection method for computer generation of random variables. *Journal of the American Statistical Association*, 76(374):446–451,

June 1981. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287848`. See corrigendum [1039].

Lakhan:1981:GAP

[1012] V. Chris Lakhan. Generating autocorrelated pseudo-random numbers with specific distributions. *Journal of Statistical Computation and Simulation*, 12(3–4):303–309, ???? 1981. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949658108810463`.

Landauer:1981:RNF

[1013] Edwin G. Landauer. Random numbers: finding a good, low cost generator. *International Journal of Mathematical Education in Science and Technology*, 12(1):1–8, ???? 1981. CODEN IJMEBM. ISSN 0020-739X (print), 1464-5211 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/0020739810120102`.

Menzefricke:1981:BAC

[1014] Ulrich Menzefricke. A Bayesian analysis of a change in the precision of a sequence of independent normal random variables at an unknown time point. *Applied Statistics*, 30(2):141–146, 1981. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Nekrutkin:1981:JSM

[1015] V. V. Nekrutkin. Justification of the selection method for a multiplicative pseudorandom number generator. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 21(5):25–33, ???? 1981. CODEN ???? ISSN 0041-5553 (print), 1878-2930 (electronic).

Preece:1981:DFD

[1016] D. A. Preece. Distributions of final digits in data. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 30(1):31–60, March 1981. CODEN ???? ISSN 0039-0526 (print), 1467-9884 (electronic). URL `http://www.jstor.org/stable/2987702`.

Rubinstein:1981:RNG

[1017] Reuven Y. Rubinstein. Random number generation. In *Simulation and the Monte Carlo method* [4112], page ?? ISBN 0-470-31651-9, 0-470-31722-1 (e-book). LCCN QA298 .R8. URL `http://onlinelibrary.wiley.com/doi/10.1002/9780470316511.ch2/summary`.

Schatte:1981:RVL

[1018] P. Schatte. On random variables with logarithmic mantissa distribution relative to several bases. *Elektronische Informationsverarbeitung und Kybernetik (EIK)*, 17(??):293–295, ???? 1981. CODEN EIVKAX. ISSN 0013-5712.

Schmeiser:1981:PRV

[1019] B. W. Schmeiser and V. Kachitvichyanukul. Poisson random variate generation. Research Memorandum 81-4, School of Industrial Engineering, Purdue University, West Lafayette, IN, USA, 1981.

Tadikamalla:1981:CGG

[1020] P. R. Tadikamalla and M. E. Johnson. A complete guide to gamma variate generation. *American Journal of Mathematical and Management Sciences*, 1(??):78–95, ???? 1981. CODEN AMMSDX. ISSN 0196-6324.

Tadikamalla:1981:FDO

[1021] Pandu R. Tadikamalla. On a family of distributions obtained by the transformation of the gamma distribution. *Journal of Statistical Computation and Simulation*, 13(3–4):209–214, 1981. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Ahrens:1982:CGP

[1022] J. H. Ahrens and U. Dieter. Computer generation of Poisson deviates from modified normal distributions. *ACM Transactions on Mathematical Software*, 8(2):163–179, June 1982. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Ahrens:1982:GGV

[1023] J. H. Ahrens and Ulrich Dieter. Generating Gamma variates by a modified rejection technique. *Communications of the ACM*, 25(1):47–54, January 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Atkinson:1982:SGI

[1024] A. C. Atkinson. The simulation of generalized inverse Gaussian and hyperbolic random variables. *SIAM Journal on Scientific and Statistical Computing*, 3(4):502–515, December 1982. CODEN SIJCD4. ISSN 0196-5204.

Baccelli:1982:DBR

[1025] F. Baccelli and E. G. Coffman. A data base replication analysis using an M/M/m queue with service interruptions. *ACM SIGMETRICS Per-*

formance Evaluation Review, 11(4):102–107, December 1982. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Bartels:1982:RVN

[1026] Robert Bartels. The rank version of von Neumann's ratio test for randomness. *Journal of the American Statistical Association*, 77(377):40–46, March 1982. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287767`.

Blum:1982:HGC

[1027] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. In IEEE [4114], pages 112–117. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog number 82CH1806-9. IEEE Computer Society order number 440.

Crigler:1982:RCP

[1028] J. R. Crigler. RANDOM: a computer program for evaluating pseudo-uniform random number generators. U.S. Government Report AD-A 118412/6, Naval Surface Weapons Center (K 106), Dahlgren, VA 22448, USA, August 1982. v + 41 + 3 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a118412.pdf`.

Devroye:1982:NAR

[1029] Luc Devroye. A note on approximations in random variate generation. *Journal of Statistical Computation and Simulation*, 14(2):149–158, ???? 1982. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

DiDonato:1982:FSP

[1030] A. R. DiDonato. Five statistical programs in Basic for desktop computers. Report NSWC TR 83-13, Naval Surface Weapons Center (Code K104), Dahlgren, VA 22448, USA, November 1982. vi + 96 + 4 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a158111.pdf`.

Dykstra:1982:MLE

[1031] Richard L. Dykstra. Maximum likelihood estimation of the survival functions of stochastically ordered random variables. *Journal of the American Statistical Association*, 77(379):621–628, September 1982. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287725`.

Faure:1982:DSA

[1032] H. Faure. Discrépance des suites associées à un système de numération en dimension S. (French) [Discrepancy of sequences associated with a numeration system in dimension S]. *Acta Arithmetica*, 61(??):337–351, ???? 1982. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Fishman:1982:SEM

[1033] George S. Fishman and Louis R. Moore. A statistical evaluation of multiplicative congruential random number generators with modulus $2^{31} - 1$. *Journal of the American Statistical Association*, 77(377):129–136, March 1982. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://links.jstor.org/sici?sici=0162-1459%28198203%2977%3A377%3C129%3AASEOMC%3E2.0.CO%3B2-Q; http://www.jstor.org/stable/2287778`.

Fredricksen:1982:SFL

[1034] Harold Fredricksen. A survey of full length nonlinear shift register cycle algorithms. *SIAM Review*, 24(2):195–221, April 1982. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2029360`.

Gabriel:1982:VPI

[1035] Richard Gabriel. Verschlüsselungsabbildungen mit Pseudo-Inversen, Zufallsgeneratoren und Täfelungen. (German) [Encryption mapping with pseudoinverses, random generators and tilings]. *Kybernetika (Prague)*, 18(6):485–504, 1982. CODEN KYBNAI. ISSN 0023-5954.

Golomb:1982:SRS

[1036] Solomon W. (Solomon Wolf) Golomb. *Shift register sequences*. Aegean Park Press, Laguna Hills, CA, USA, revised edition, 1982. ISBN 0-89412-048-4 (paperback). xvi + 247 pp. LCCN QA267.5.S4 G6 1982. Portions co-authored by Lloyd R. Welch, Richard M. Goldstein and Alfred W. Hales.

Houle:1982:CGD

[1037] P. A. Houle. Comment on gamma deviate generation. *Communications of the ACM*, 25(10):747–748, October 1982. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Kashiwagi:1982:SPT

[1038] H. Kashiwagi. On some properties of TLP random numbers generated by m-sequence. *Transactions of the Society of Instrument and Control*

Engineers, 18(??):828–832, ???? 1982. CODEN TSICA9. ISSN 0453-4654.

Kronmal:1982:CVA

[1039] Richard A. Kronmal and Arthur V. Peterson, Jr. Corrigendum: "A variant of the acceptance-rejection method for computer generation of random variables" [J. Amer. Statist. Assoc. **76** (1981), no. 374, 446–451, MR 82h:62037]. *Journal of the American Statistical Association*, 77 (380):954, December 1982. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2287364`. See [1011].

Law:1982:SMA

[1040] Averill M. Law and W. David Kelton. *Simulation modeling and analysis*. McGraw-Hill series in industrial engineering and management science. McGraw-Hill, New York, NY, USA, 1982. ISBN 0-07-036696-9. xiv + 400 pp. LCCN QA76.9.C65 L38.

Lenstra:1982:FPR

[1041] Arjen K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, December 1982. CODEN MAANA3. ISSN 0025-5831 (print), 1432-1807 (electronic). URL `http://www.springerlink.com/content/lh1m24436431g068/`.

Marsaglia:1982:CSA

[1042] J. C. Marsaglia. Computer studies of the Anderson–Darling statistic. Technical Report CS-82-096, Computer Science Department, Washington State University, Pullman, WA, USA, ???? 1982.

Meyers:1982:CDR

[1043] M. H. Meyers. Computing the distribution of a random variable via Gaussian quadrature rules. *The Bell System Technical Journal*, 61(9):2245–2261, November 1982. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol61/bstj61-9-2245.pdf`; `http://www.alcatel-lucent.com/bstj/vol61-1982/articles/bstj61-9-2245.pdf`.

Niederreiter:1982:STT

[1044] H. Niederreiter. Statistical tests for Tausworthe pseudorandom numbers. In Grossmann et al. [4113], pages 265–274. ISBN 90-277-1427-4. LCCN QA276.A1 P36 1981.

Peterson:1982:MMC

[1045] Arthur V. Peterson, Jr. and Richard A. Kronmal. On mixture methods for the computer generation of random variables. *The American Statistician*, 36(3):184–191, August 1982. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Plumstead:1982:ISG

[1046] Joan Boyar Plumstead. Inferring a sequence generated by a linear congruence. In IEEE [4114], pages 153–159. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog number 82CH1806-9. IEEE Computer Society order number 440.

Rizzi:1982:GPB

[1047] Alfredo Rizzi. The generation of pseudorandom binary digits by primitive polynomes. *Statistica (Bologna)*, 42(??):193–207, ???? 1982. CODEN ???? ISSN 0390-590X (print), 1973-2201 (electronic).

Roberts:1982:ITN

[1048] C. S. Roberts. Implementing and testing new versions of a good, 48-bit, pseudo-random number generator. *The Bell System Technical Journal*, 61(8):2053–2063, October 1982. CODEN BSTJAN. ISSN 0005-8580. URL `http://bstj.bell-labs.com/BSTJ/images/Vol61/bstj61-8-2053.pdf`; `http://www.alcatel-lucent.com/bstj/vol61-1982/articles/bstj61-8-2053.pdf`.

Schmeiser:1982:BGR

[1049] B. W. Schmeiser and R. Lal. Bivariate gamma random vectors. *Operations Research*, 30(2):355–374, March/April 1982. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Shen:1982:FAD

[1050] A. Shen. Frequency approach to the definition of the notion of random sequence. *Semiotika i Informatika*, 18(??):14–42, ???? 1982. CODEN ???? ISSN 0259-4269.

Tracht:1982:RAN

[1051] Allen E. Tracht. Remark on "Algorithm 334: Normal Random Deviates". *ACM Transactions on Mathematical Software*, 8(1):89, March 1982. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). See [435].

Vahle:1982:BPR

[1052] M. O. Vahle and L. F. Tolendino. Breaking a pseudo random number based cryptographic algorithm. *Cryptologia*, 6(4):319–328, October 1982. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903089~db=all~order=page`.

Wichmann:1982:SAA

[1053] B. A. Wichmann and I. D. Hill. Statistical algorithms: Algorithm AS 183: An efficient and portable pseudo-random number generator. *Applied Statistics*, 31(2):188–190, June 1982. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/183`. See correction [1147] and remarks [1187, 1262, 2254, 2480]. Reprinted in [1169, pages 238–242]. See also the extended 32-bit generator in [3069].

Yao:1982:TAT

[1054] A. Yao. Theory and applications of trapdoor functions. In IEEE [4114], pages 80–91. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog number 82CH1806-9. IEEE Computer Society order number 440.

Afflerbach:1983:LKG

[1055] Lothar Afflerbach. *Lineare Kongruenz-Generatoren zur Erzeugung von Pseudo-Zufallszafflen und ibre Gitterstruktur. (German) [Linear congruential generators for generating pseudorandom numbers and their lattice structure]*. Dissertation, Fachbereich Mathematik, Technische Hochschule Darmstadt, Darmstadt, West Germany, 1983.

Barel:1983:FHR

[1056] M. Barel. Fast hardware random number generator for the Tausworthe sequence. In *Proceedings of the 16th Annual Simulation Symposium, Florida*, pages 121–135. ????, ????, 1983.

Barel:1983:UGG

[1057] Mair Barel and Bernd Jobes. Untersuchungen an Generatoren für gleichverteilte Zufallszahlen. (German) [Testing of uniform random number generators]. *Angewandte Informatik (Elektron. Datenverarbeitung)*, 25 (9):404–409, ???? 1983. CODEN AWIFA7. ISSN 0013-5704.

Best:1983:NGV

[1058] D. J. Best. A note on gamma variate generators with shape parameter less than unity. *Computing: Archiv für Informatik und Numerik*, 30

(2):185–188, June 1983. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Blum:1983:CTP

[1059] Lenore Blum, Manuel Blum, and Michael Shub. Comparison of two pseudorandom number generators. In Chaum et al. [4115], pages 61–78. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982. See also final version of paper with proofs in [1208].

Borosh:1983:OMP

[1060] Itshak Borosh and Harald Niederreiter. Optimal multipliers for pseudorandom number generation by the linear congruential method. *BIT (Nordisk tidskrift for informationsbehandling)*, 23(1):65–74, March 1983. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=23&issue=1&spage=65`.

Bratley:1983:GS

[1061] Paul Bratley, Bennett L. Fox, and Linus E. Schrage. *A Guide to Simulation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1983. ISBN 0-387-90820-X. xviii + 383 pp. LCCN QA76.9.C65 B73 1983.

Brillhart:1983:FHP

[1062] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, volume 22 of *Contemporary mathematics*. American Mathematical Society, Providence, RI, USA, 1983. ISBN 0-8218-5021-0 (paperback). ISSN 0271-4132 (print), 1098-3627 (electronic). lxvii + 178 pp. LCCN QA161.F3 F33 1983.

Chen:1983:SSR

[1063] Robert Chen and Larry A. Shepp. On the sum of symmetric random variables. *The American Statistician*, 37(3):237, ???? 1983. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Devroye:1983:MIR

[1064] Luc Devroye. Moment inequalities for random variables in computational geometry. *Computing: Archiv für Informatik und Numerik*, 30(2):111–119, June 1983. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Dudewicz:1983:TRN

[1065] Edward J. Dudewicz and Thomas G. Ralley. TESTRAND: a random number generation and testing library. *The American Statistician*, 37 (2):169–170, May 1983. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2685882`.

Erber:1983:SRP

[1066] T. Erber, T. M. Rynne, W. F. Darsow, and M. J. Frank. The simulation of random processes on digital computers: Unavoidable order. *Journal of Computational Physics*, 49(3):394–419, March 1983. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999183901377`.

Fushimi:1983:DGF

[1067] Masanori Fushimi and Shu Tezuka. The k-distribution of Generalized Feedback Shift Register pseudorandom numbers. *Communications of the ACM*, 26(7):516–523, July 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Fushimi:1983:IOE

[1068] Masanori Fushimi. Increasing the orders of equidistribution of the leading bits of the Tausworthe sequence. *Information Processing Letters*, 16(4): 189–192, May 13, 1983. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Fushimi:1983:RTR

[1069] Masanori Fushimi. A reciprocity theorem on the random number generation based on m-sequences and its applications. *Transactions of the Information Processing Society of Japan*, 24(??):576–579, ???? 1983. CODEN JSGRD5. ISSN 0387-5806.

Gokhale:1983:EBG

[1070] D. V. Gokhale. On entropy-based goodness-of-fit tests. *Computational Statistics & Data Analysis*, 1(1):157–165, March 1983. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic).

Helstrom:1983:CDQ

[1071] Carl W. Helstrom. Comment: "Distribution of quadratic forms in normal random variables—evaluation by numerical integration" [SIAM J. Sci. Statist. Comput. **1** (1980), no. 4, 438–448, MR 82g:62037] by S. O. Rice. *SIAM Journal on Scientific and Statistical Computing*, 4(2): 353–356, June 1983. CODEN SIJCD4. ISSN 0196-5204. See [975].

Hopkins:1983:SAAb

[1072] T. R. Hopkins. Statistical algorithms: Algorithm AS 193: a revised algorithm for the spectral test. *Applied Statistics*, 32(3):328–335, September 1983. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/193`. See remark [1173].

Hora:1983:EIF

[1073] Stephen C. Hora. Estimation of the inverse function for random variate generation. *Communications of the ACM*, 26(5):590–594, May 1983. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Inoue:1983:RNG

[1074] H. Inoue, H. Kumahora, Y. Yoshizawa, M. Ichimura, and O. Miyatake. Random numbers generated by a physical device. *Applied Statistics*, 32 (2):115–120, 1983. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://www.jstor.org/stable/2347290`.

Jennergren:1983:AMR

[1075] L. Peter Jennergren. Another method for random number generation on microcomputers. *Simulation*, 41(2):79, ???? 1983. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/41/2/79.abstract`.

Kac:1983:WR

[1076] M. Kac. What is randomness? *American Scientist*, 71(??):405–406, August 1983. CODEN AMSCAC. ISSN 0003-0996 (print), 1545-2786 (electronic). URL `http://www.americanscientist.org/issues/past.aspx`.

Kachitvichyanukul:1983:DUR

[1077] V. Kachitvichyanukul. Discrete univariate random variate generation. In Roberts et al. [4119], pages 179–187. ISBN ???? LCCN QA76.9.C65 W56 1983.

Keefer:1983:TPA

[1078] D. L. Keefer and S. E. Bodily. Three-point approximations for continuous random variables. *Management Science*, 29(??):595–609, ???? 1983. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Lawrance:1983:SDP

[1079] A. J. Lawrance and P. A. W. Lewis. Simple dependent pairs of exponential and uniform random variables. *Operations Research*, 31(6):1179–

1197, November/December 1983. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Marsaglia:1983:RNG

[1080] George Marsaglia. Random number generation. In Ralston and Reilly, Jr. [4118], pages 1260–1264. ISBN 0-442-24496-7. LCCN QA76.15 .E48 1983.

Marsaglia:1983:RVI

[1081] George Marsaglia. Random variables with independent binary digits. *Kibern. Sb., Nov. Ser.*, 20:216–224, 1983. CODEN ???? ISSN 0453-8382.

Marse:1983:IPF

[1082] Ken Marse and Stephen D. Roberts. Implementing a portable FORTRAN uniform $(0, 1)$ generator. *Simulation*, 41(4):135–139, October 1983. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic).

Miyatake:1983:MAR

[1083] Osamu Miyatake, Minoru Ichimura, Yasukazu Yoshizawa, and Hikaru Inoue. Mathematical analysis of random number generator using gamma-rays. I. *Mathematica Japonica*, 28(4):399–414, ???? 1983. CODEN MAJAA9. ISSN 0025-5513. See also part II [1237].

Muller:1983:BRB

[1084] Mervin E. Muller. Book review: *The Handbook of Random Number Generation and Testing with TESTRAND Computer Code* by Edward J. Dudewicz; Thomas G. Ralley. *Technometrics*, 25(2):207–208, May 1983. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/1268561`.

Pearson:1983:APR

[1085] Robert B. Pearson. An algorithm for pseudo random number generation suitable for large scale integrations. *Journal of Computational Physics*, 49(3):478–489, March 1983. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999183901420`.

Peterson:1983:ACT

[1086] Arthur V. Peterson, Jr. and Richard A. Kronmal. Analytic comparison of three general-purpose methods for the computer generation of discrete random variables. *Applied Statistics*, 32(3):276–286, 1983. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Plumstead:1983:ISPa

[1087] Joan Boyar Plumstead. *Inferring Sequences Produced by Pseudo-Random Number Generators*. Ph.D. dissertation, Department of Computer Science, University of California, Berkeley, Berkeley, CA, USA, June 1983. ii + 56 pp.

Plumstead:1983:ISPb

[1088] Joan B. Plumstead. Inferring a sequence produced by a linear congruence. In R. L. Rivest, A. Sherman, and D. Chaum, editors, *CRYPTO82*, pages 317–319. Plenum Press, New York, NY, USA; London, UK, 1983.

Pokhodzei:1983:OMM

[1089] B. B. Pokhodzeĭ. Optimality of the Marsaglia method for simulating discrete distributions. *Vestnik Leningrad. Univ. Mat. Mekh. Astronom.*, 4:105–107, 1983. CODEN VMMAA3. ISSN 0024-0850.

Purdy:1983:CFA

[1090] George B. Purdy. A carry-free algorithm for finding the greatest common divisor of two integers. *Computers and Mathematics and Applications*, 9(2):311–316, 1983. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122183901335`. Purdy's extended binary algorithm for the gcd runs in $O(n^2)$ time, where n is the number of bits in the inputs; see [1269] for an $O(n)$ algorithm.

Ripley:1983:CGR

[1091] B. D. Ripley. Computer generation of random variables: a tutorial. *International Statistical Review = Revue Internationale de Statistique*, 51(??):301–319, ???? 1983. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic).

Ripley:1983:LSP

[1092] B. D. Ripley. The lattice structure of pseudorandom number generators. *Proceedings of the Royal Society of London. Series A, Mathematical and physical sciences*, 389(1796):197–204, September 1983. CODEN PRLAAZ. ISSN 0080-4630 (print), 2053-9169 (electronic). URL `http://www.jstor.org/stable/2397327`.

Rosenbaum:1983:RNG

[1093] W. Rosenbaum, J. Syrotuik, and R. Gordon. Random number generators for microcomputers. *Computer Programs in Biomedicine*, 16(??):235–240, ???? 1983. CODEN COPMBU. ISSN 0010-468X (print), 1878-3139 (electronic).

Sakasegawa:1983:SRS

[1094] H. Sakasegawa. Stratified rejection and squeeze method for generating beta random numbers. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 35B(??):291–302, 1983. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic).

Savir:1983:NET

[1095] J. Savir. A new empirical test for the quality of random integer generators. *IEEE Transactions on Computers*, C-32(10):960–961, October 1983. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676142`.

Schmeiser:1983:RAG

[1096] B. W. Schmeiser. Recent advances in generating observations from discrete random variables. In Gentle [4116], pages 154–160. ISBN 0-444-86688-4. LCCN QA276.4 .S95 1983.

Shamir:1983:GCS

[1097] Adi Shamir. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1):38–44, February 1983. CODEN ACSYEC. ISSN 0734-2071 (print), 1557-7333 (electronic).

VanEs:1983:RNG

[1098] A. J. Van Es, R. D. Gill, and C. Van Putten. Random number generators for a pocket calculator. *Statistica Neerlandica. Journal of the Netherlands Society for Statistics and Operations Research*, 37(??):95–102, ???? 1983. CODEN ???? ISSN 0039-0402 (print), 1467-9574 (electronic).

Vazirani:1983:TPR

[1099] Umesh V. Vazirani and Vijay V. Vazirani. Trapdoor pseudo-random number generators, with applications to protocol design. In IEEE [4117], pages 23–30. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. LCCN QA76.6 .S95 1983. IEEE catalog number 83CH1938-0.

Banks:1984:DES

[1100] Jerry Banks and John S. Carson II. *Discrete-Event System Simulation*. Prentice-Hall international series in industrial and systems engineering. Prentice-Hall, Upper Saddle River, NJ, USA, 1984. ISBN 0-13-215582-6. xiv + 514 pp. LCCN T57.62 .B35 1984.

Blum:1984:HGC

[1101] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, ???? 1984. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Also published in [1027].

Blum:1984:IUC

[1102] Manuel Blum. Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. In IEEE [4120], pages 425–433. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog number 84CH2085-9.

Brody:1984:RNG

[1103] T. A. Brody. A random-number generator. *Computer Physics Communications*, 34(1–2):39–46, November/December 1984. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465584901577`.

Brown:1984:ETS

[1104] Morton B. Brown and Judith Bromberg. An efficient two-stage procedure for generating random variates from the multinomial distribution. *The American Statistician*, 38(3):216–219, August 1984. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683660`.

Cheng:1984:GIG

[1105] Russell C. H. Cheng. Generation of inverse Gaussian variates with given sample mean and dispersion. *Applied Statistics*, 33(3):309–316, 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Devroye:1984:MGR

[1106] Luc Devroye. Methods for generating random variates with Polya characteristic functions. *Statistics & Probability Letters*, 2(5):257–261, October 1984. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Devroye:1984:RVG

[1107] Luc Devroye. Random variate generation for unimodal and monotone densities. *Computing: Archiv für Informatik und Numerik*, 32(1):43–68, March 1984. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Devroye:1984:SAG

[1108] Luc Devroye. A simple algorithm for generating random variates with a log-concave density. *Computing: Archiv für Informatik und Numerik*, 33(3–4):247–257, September 1984. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Devroye:1984:UPI

[1109] Luc Devroye. The use of probability inequalities in random variate generation. *Journal of Statistical Computation and Simulation*, 20(2):91–100, ???? 1984. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949658408810759`.

Downing:1984:PDP

[1110] C. P. Downing. Proposal for a digital pseudorandom number generator. *Electronics Letters*, 20(11):435–436, May 24, 1984. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4248756`.

Etzion:1984:AGF

[1111] T. Etzion and A. Lempel. Algorithms for the generation of full-length shift-register sequences. *IEEE Transactions on Information Theory*, IT-30(3):480–484, ???? 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Farebrother:1984:SAA

[1112] R. W. Farebrother. Statistical algorithms: Algorithm AS 204: The distribution of a positive linear combination of χ^2 random variables. *Applied Statistics*, 33(3):332–339, September 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/204`.

Farebrother:1984:SARa

[1113] R. W. Farebrother. Statistical algorithms: Remark AS R52: The distribution of a linear combination of central χ^2 random variables: a remark on AS 153: Pan's procedure for the tail probabilities of the Durbin-Watson statistic. *Applied Statistics*, 33(3):363–366, 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). See [954, 1114].

Farebrother:1984:SARb

[1114] R. W. Farebrother. Statistical algorithms: Remark AS R53: a remark on algorithms AS 106, AS 153 and AS 155: The distribution of a linear

combination of χ^2 random variables. *Applied Statistics*, 33(3):366–369, 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). See [845, 954, 951, 1113].

Fishman:1984:EAM

[1115] George S. Fishman and Louis R. Moore III. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{32} - 1$. Technical report 84-05, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, June 1984. ii + 44 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a143085.pdf`; `http://www.or.unc.edu/research/temp/tech80a.html#1984`.

Fishman:1984:SDD

[1116] George S. Fishman and Louis R. Moore III. Sampling from a discrete distribution while preserving monotonicity. *The American Statistician*, 38(??):219–223, ???? 1984. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Frederickson:1984:PRT

[1117] P. Frederickson, R. Hiromoto, T. L. Jordan, B. Smith, and T. Warnock. Pseudo-random trees in Monte Carlo. *Parallel Computing*, 1(2):175–180, December 1984. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Frieze:1984:LCG

[1118] A. M. Frieze, R. Kannan, and J. C. Lagarias. Linear congruential generators do not produce random sequences. In IEEE [4120], pages 480–484. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog number 84CH2085-9.

Gal:1984:OEC

[1119] S. Gal, R. Y. Rubinstein, and A. Ziv. On the optimality and efficiency of Common Random Numbers. *Mathematics and Computers in Simulation*, 26(??):502–512, ???? 1984. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic).

Guinier:1984:RNS

[1120] Daniel Guinier. Random numbers for stochastic simulation. *ACM SIGBIO Newsletter*, 6(4):5–6, March 1984. CODEN SINWDG. ISSN 0163-5697 (print), 1557-9506 (electronic).

Hamedani:1984:NLC

[1121] G. G. Hamedani. Nonnormality of linear combinations of normal random variables. *The American Statistician*, 38(4):295–296, ???? 1984. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Heth:1984:PVP

[1122] C. D. Heth. A Pascal version of a pseudorandom number generator. *Behavior Research Methods, Instruments, and Computers*, 16(6):548–550, ???? 1984. CODEN BRMCEW. ISSN 0743-3808 (print), 1532-5970 (electronic).

Kalle:1984:PRN

[1123] Claus Kalle and Stephan Wansleben. Problems with the random number generator RANF implemented on the CDC Cyber 205. *Computer Physics Communications*, 33(4):343–346, October 1984. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465584901395`.

Kannan:1984:SPA

[1124] R. Kannan, G. Miller, and L. Rudolph. Sublinear parallel algorithm for computing the greatest common divisor of two integers. In IEEE [4120], pages 7–11. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog number 84CH2085-9.

Kronmal:1984:ACA

[1125] Richard A. Kronmal and Arthur V. Peterson, Jr. An acceptance-complement analogue of the mixture-plus-acceptance-rejection method for generating random variables. *ACM Transactions on Mathematical Software*, 10(3):271–281, September 1984. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Kuo:1984:SRI

[1126] C. T. K. Kuo, T. W. Cadman, and R. J. Arsenault. Sequential random integer generator. *Computer Physics Communications*, 35(1–3): C–394, ???? 1984. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465584826053`.

Landauer:1984:ERN

[1127] Edwin G. Landauer. The effect of random number generators on an application. *Computers & Industrial Engineering*, 8(1):65–72, 1984. CODEN

CINDDL. ISSN 0360-8352 (print), 1879-0550 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0360835284900226`.

Lugannani:1984:DRQ

[1128] R. Lugannani and S. O. Rice. Distribution of the ratio of quadratic forms in normal variables—numerical methods. *SIAM Journal on Scientific and Statistical Computing*, 5(2):476–488, June 1984. CODEN SIJCD4. ISSN 0196-5204.

Marsaglia:1984:EAM

[1129] George Marsaglia. The exact-approximation method for generating random variables in a computer. *Journal of the American Statistical Association*, 79(385):218–221, March 1984. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2288360`.

Marsaglia:1984:FEI

[1130] George Marsaglia and Wai Wan Tsang. A fast, easily implemented method for sampling from decreasing or symmetric unimodal density functions. *SIAM Journal on Scientific and Statistical Computing*, 5(2):349–359, June 1984. CODEN SIJCD4. ISSN 0196-5204.

Marsaglia:1984:GCM

[1131] George Marsaglia and Ingram Olkin. Generating correlation matrices. *SIAM Journal on Scientific and Statistical Computing*, 5(2):470–475, June 1984. CODEN SIJCD4. ISSN 0196-5204.

Modianos:1984:RNG

[1132] D. T. Modianos, R. C. Scott, and L. W. Cornwell. Random number generation on microcomputers. *Interfaces*, 14(2):81–87, March/April 1984. CODEN INFAC4. ISSN 0092-2102 (print), 1526-551X (electronic).

Niederreiter:1984:PSP

[1133] Harald Niederreiter. The performance of k-step pseudorandom number generators under the uniformity test. *SIAM Journal on Scientific and Statistical Computing*, 5(4):798–810, December 1984. CODEN SIJCD4. ISSN 0196-5204.

Papoulis:1984:PRV

[1134] Athanasios Papoulis. *Probability, random variables, and stochastic processes*. McGraw-Hill series in electrical engineering. Communications and information theory. McGraw-Hill, New York, NY, USA, second edition, 1984. ISBN 0-07-048468-6. xv + 576 pp. LCCN QA273 .P2 1984.

Paulsen:1984:IRN

[1135] Jostein Paulsen. Impact of random number generators in time series Monte Carlo simulation. *Journal of Statistical Computation and Simulation*, 19(1):23–33, ???? 1984. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949658408810711`.

Porter:1984:CNS

[1136] Sig Porter. Cryptology and number sequences: Pseudorandom, random, and perfectly random. *Computers & Security*, 3(1):43–44, February 1984. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/0167404884900257`.

Rasmussen:1984:FPS

[1137] Jeffrey Lee Rasmussen. A Fortran program for statistical evaluation of pseudorandom number generators. *Behavior Research Methods, Instruments, and Computers*, 16(1):63–64, January 1984. CODEN BRMCEW. ISSN 0743-3808 (print), 1532-5970 (electronic). URL `http://www.springerlink.com/content/a25j12g243u6566n/`.

Ronse:1984:FSR

[1138] Christian Ronse. *Feedback shift registers*, volume 169 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1984. CODEN LNCSD9. ISBN 0-387-13330-5 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). 145 pp. LCCN TK7895.S54 R66 1984. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0169.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=169`.

Scholtz:1984:GS

[1139] Robert A. Scholtz and Lloyd R. Welch. GMW sequences. *IEEE Transactions on Information Theory*, IT-30(3):548–553, May 1984. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). See [276].

Schorr:1984:PLV

[1140] B. Schorr. Programs for the Landau and the Vavilov distributions and the corresponding random numbers. *Computer Physics Communications*, 35(1–3):C–239–C–240, ???? 1984. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465584824789`.

Smith:1984:EMC

[1141] Robert L. Smith. Efficient Monte Carlo procedures for generating points uniformly distributed over bounded regions. *Operations Research*, 32(6): 1296–1308, 1984. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Thesen:1984:SER

[1142] A. Thesen, Z. Sun, and T. J. Wang. Some efficient random number generators for micro-computers. In Sheppard et al. [4121], pages 187–196. ISBN 0-911801-04-9 (SCS), 0-444-87605-7 (North Holland). LCCN QA76.9.C65 W56 1984. IEEE order number 84CH2098-2.

Tolleth:1984:SSM

[1143] David W. Tolleth. System sparing for minicomputer-based operations systems. *AT&T Bell Laboratories Technical Journal*, 63(6 part 2):1029–1047, 1984. CODEN ABLJER. ISSN 0748-612X (print), 2376-7162 (electronic).

Ulrich:1984:CGD

[1144] Gary Ulrich. Computer generation of distributions on the m-sphere. *Applied Statistics*, 33(2):158–163, 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Vazirani:1984:ESP

[1145] U. V. Vazirani and V. V. Vazirani. Efficient and secure pseudo-random number generation. In IEEE [4120], pages 458–463. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog number 84CH2085-9.

Whitney:1984:GTP

[1146] C. A. Whitney. Generating and testing pseudorandom numbers. *BYTE Magazine*, 9(11):128–129, November 1984. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Wichmann:1984:SAC

[1147] B. A. Wichmann and I. D. Hill. Statistical algorithms: Correction: Algorithm AS 183: An efficient and portable pseudo-random number generator. *Applied Statistics*, 33(1):123, 1984. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Afflerbach:1985:CMR

[1148] L. Afflerbach and H. Grothe. Calculation of Minkowski-reduced lattice bases. *Computing: Archiv für Informatik und Numerik*, 35(3–4):269–276, September 1985. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Afflerbach:1985:PRN

[1149] L. Afflerbach. The pseudo-random number generators in Commodore and Apple microcomputers. *Statistical Papers = Statistische Hefte*, 26 (1):321–333, December 1985. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic).

Ahrens:1985:SRS

[1150] J. H. Ahrens and Ulrich Dieter. Sequential random sampling. *ACM Transactions on Mathematical Software*, 11(2):157–169, June 1985. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/214392.214402`; `http://www.acm.org/pubs/citations/journals/toms/1985-11-2/p157-ahrens/`.

Akl:1985:FPR

[1151] Selim G. Akl and Henk Meijer. A fast pseudo random permutation generator with applications to cryptology. In Blakley and Chaum [4125], pages 269–275. CODEN LNCSD9. ISBN 0-387-15658-5, 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=269`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Berry:1985:RPD

[1152] Keith Berry and Cliff J. Huang. Random pseudo-disturbance generators in a stochastic simulation of an econometric model. *Journal of Statistical Computation and Simulation*, 22(3–4):285–302, ???? 1985. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949658508810851`.

Blom:1985:SPE

[1153] Gunnar Blom. A simple property of exchangeable random variables. *American Mathematical Monthly*, 92(7):491–492, ???? 1985. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Bounas:1985:DDS

[1154] Adam C. Bounas. Direct determination of a "seed" binary matrix. *Information Processing Letters*, 20(1):47–50, January 2, 1985. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Burks:1985:CEM

[1155] Arthur W. Burks, Alston S. Householder, N. Metropolis, and S. M. Ulam. Comments on early Monte Carlo computations and scientific meetings. *Annals of the History of Computing*, 7(2):147–148, April/June 1985. CODEN AHCOE5. ISSN 0164-1239. URL `http://dlib.computer.org/an/books/an1985/pdf/a2141.pdf`; `http://www.computer.org/annals/an1985/a2141abs.htm`.

Clark:1985:PNG

[1156] R. N. Clark. A pseudorandom number generator. *Simulation*, 45(5): 252–255, November 1985. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). See criticism and response [1236].

Dowdy:1985:AUM

[1157] Lawrence W. Dowdy and Manvinder S. Chopra. On the applicability of using multiprogramming level distributions. *ACM SIGMETRICS Performance Evaluation Review*, 13(2):116–127, August 1985. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Dudewicz:1985:RNG

[1158] E. J. Dudewicz, Z. A. Karian, and R. J. Marshall, III. Random number generation on microcomputers. In ????, editor, *Modeling and Simulation on Microcomputers: 1985*, pages 9–14. Society for Computer Simulation, San Diego, CA, USA, 1985. ISBN ???? LCCN ????

Dudewicz:1985:TMD

[1159] Edward J. Dudewicz and Zaven A. Karian. *Tutorial: Modern Design and Analysis of Discrete-Event Computer Simulations*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1985. ISBN 0-8186-0597-9 (paperback), 0-8186-4597-0. ix + 475 pp. LCCN QA76.9.C65 D83 1985.

Dyadkin:1985:AMN

[1160] I. G. Dyad'kin. An algorithm for modelling a normal distribution. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 25

(4):91–93, ???? 1985. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/004155538590148X`. English translation of Russian original published in Zh. vychisl. Mat. mat. Fiz., **25**(7), 1102–1104, 1985.

Fairfield:1985:LRN

[1161] R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An LSI random number generator (RNG). In Blakley and Chaum [4125], pages 203–230. CODEN LNCSD9. ISBN 0-387-15658-5, 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=203`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Feltz:1985:MLE

[1162] Carol J. Feltz and Richard L. Dykstra. Maximum likelihood estimation of the survival functions of N stochastically ordered random variables. *Journal of the American Statistical Association*, 80(392):1012–1019, December 1985. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2288568`.

Figiel:1985:NLP

[1163] K. D. Figiel and D. R. Sule. New lagged product test for random number generators. *Computers & Industrial Engineering*, 9(3):287–296, March 1985. CODEN CINDDL. ISSN 0360-8352 (print), 1879-0550 (electronic).

Fincke:1985:IMC

[1164] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*, 44(170):463–471, April 1985. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Gibbons:1985:NSI

[1165] Jean Dickinson Gibbons. *Nonparametric Statistical Inference*, volume 65 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, second edition, 1985. ISBN 0-8247-7327-6. xv + 408 pp. LCCN QA278.8 .G5 1985.

Gleser:1985:EPG

[1166] Leon Jay Gleser. Exact power of goodness-of-fit tests of Kolmogorov type for discontinuous distributions. *Journal of the American Statistical Association*, 80(392):954–958, December 1985. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2288560`.

Goldreich:1985:CAR

[1167] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptographic applications of random functions (extended abstract). In Blakley and Chaum [4125], pages 276–288. CODEN LNCSD9. ISBN 0-387-15658-5, 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=276`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Gordon:1985:SSB

[1168] T. F. Gordon. Statistical simulations on the BBC microcomputer: significance tests of the pseudo-random number generator. *Journal of Applied Statistics*, 12(2):147–155, 1985. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/02664768500000020`.

Griffiths:1985:ASA

[1169] Paul Griffiths and Ian David Hill, editors. *Applied statistics algorithms*. Ellis Horwood series in mathematics and its applications. Ellis Horwood, New York, NY, USA, 1985. ISBN 0-85312-772-7 (UK), 0-470-20184-3 (US). 307 pp. LCCN QA276.4 .A57 1985. Published for the Royal Statistical Society.

Haastad:1985:CST

[1170] J. Håstad and A. Shamir. The cryptographic security of truncated linearly related variables. In ACM [4122], pages 356–362. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. URL `http://www.acm.org/pubs/articles/proceedings/stoc/22145/p356-hastad/p356-hastad.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/22145/p356-hastad/`. ACM order number 508850.

Helfrich:1985:ACMa

[1171] B. Helfrich. An algorithm to construct Minkowski-reduced lattice-bases. In Mehlhorn [4126], pages 173–179. CODEN LNCSD9. ISBN 0-387-13912-5 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.182. URL http://link.springer-ny.com/link/service/series/0558/tocs/t0182.htm; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=182.

Helfrich:1985:ACMb

[1172] B. Helfrich. Algorithms to construct Minkowski reduced and Hermite reduced lattice bases. *Theoretical Computer Science*, 41(2-3):125–139, ???? 1985. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Hill:1985:SAR

[1173] I. D. Hill. Statistical algorithms: Remark AS R57: a remark on Algorithm AS 193: a revised algorithm for the spectral test. *Applied Statistics*, 34(1):102–103, 1985. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL http://lib.stat.cmu.edu/apstat/193. See [1072].

Hurd:1985:NEM

[1174] Cuthbert C. Hurd. A note on early Monte Carlo computations and scientific meetings. *Annals of the History of Computing*, 7(2): 141–155, April/June 1985. CODEN AHCOE5. ISSN 0164-1239. URL http://dlib.computer.org/an/books/an1985/pdf/a2141.pdf; http://www.computer.org/annals/an1985/a2141abs.htm.

Imai:1985:PNG

[1175] T. Imai and Masanori Fushimi. Pseudorandom number generators whose subsequences are multidimensionally equidistributed. *Transactions of the Information Processing Society of Japan*, 26:454–458, ???? 1985. CODEN JSGRD5. ISSN 0387-5806.

Jodrey:1985:CSC

[1176] W. S. Jodrey and E. M. Tory. Computer simulation of close random packing of equal spheres. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 32(4):2347–2351, October 1985. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL http://link.aps.org/doi/10.1103/PhysRevA.32.2347.

Kachitvichyanukul:1985:CGH

[1177] Voratas Kachitvichyanukul and Burce Schmeiser. Computer generation of hypergeometric random variates. *Journal of Statistical Computation and Simulation*, 22(2):127–145, 1985. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Kallenberg:1985:NCC

[1178] W. C. M. Kallenberg, J. Oosterhoff, and B. F. Schriever. The number of classes in chi-squared goodness-of-fit tests. *Journal of the American Statistical Association*, 80(392):959–968, December 1985. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2288561`.

Knuth:1985:DLC

[1179] Donald E. Knuth. Deciphering a linear congruential encryption. *IEEE Transactions on Information Theory*, IT-31(1):49–52, January 1985. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic). Russian translation, to appear.

Lambrou:1985:DPR

[1180] L. Lambrou, V. C. Bhavsar, and U. G. Gujar. On the discrepancy of pseudo-random number sequences generated by the linear congruential method. In *Proceedings of the Annual APICS Computer Science Seminar*, pages 53–68. Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax, NS, Canada, ????, ????, November 1985.

Leemis:1985:RVG

[1181] L. Leemis and B. W. Schmeiser. Random variate generation for Monte Carlo experiments. *IEEE Transactions on Reliability*, R-34(1):81–85, April 1985. CODEN IEERAJ. ISSN 0018-9529 (print), 1558-1721 (electronic).

Lenstra:1985:FMP

[1182] Arjen K. Lenstra. Factoring multivariate polynomials over finite fields. *Journal of Computer and System Sciences*, 30(2):235–248, April 1985. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0022000085900169`.

Levin:1985:OWF

[1183] L. A. Levin. One-way functions and pseudorandom generators. In ACM [4122], pages 363–365. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6

A13 1985. URL http://www.acm.org/pubs/articles/proceedings/stoc/22145/p363-levin/p363-levin.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/22145/p363-levin/. ACM order number 508850.

Marsaglia:1985:CVR

[1184] George Marsaglia. A current view of random number generators. In Billard [4124], pages 3–10. ISBN 0-444-87725-8. LCCN QA276.4 .S95 1984. URL http://stat.fsu.edu/pub/diehard/; http://www.evensen.org/marsaglia/keynote.ps.

Marsaglia:1985:MSR

[1185] George Marsaglia and Liang-Huei Tsay. Matrices and the structure of random number sequences. *Linear Algebra and its Applications*, 67:147–156, 1985. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic).

Marsaglia:1985:NPT

[1186] George Marsaglia. Note on a proposed test for random number generators. *IEEE Transactions on Computers*, C-34(8):756–758, August 1985. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676623.

McLeod:1985:SAR

[1187] A. Ian McLeod. Statistical algorithms: Remark AS R58: a remark on Algorithm AS 183. an efficient and portable pseudo-random number generator. *Applied Statistics*, 34(2):198–200, 1985. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL http://lib.stat.cmu.edu/apstat/183. See [1053, 1262].

Monahan:1985:ARN

[1188] John F. Monahan. Accuracy in random number generation. *Mathematics of Computation*, 45(172):559–568, October 1985. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Montgomery:1985:MMT

[1189] Peter L. Montgomery. Modular multiplication without trial division. *Mathematics of Computation*, 44(170):519–521, April 1985. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Niederreiter:1985:STP

[1190] Harald Niederreiter. The serial test for pseudo-random numbers generated by the linear congruential method. *Numerische Mathematik*, 46

(1):51–68, March 1985. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Norton:1985:EBG

[1191] G. Norton. Extending the binary GCD algorithm. *Lecture Notes in Computer Science*, 229:363–372, 1985. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Percus:1985:PBS

[1192] Ora E. Percus and Jerome K. Percus. Probability bounds on the sum of independent nonidentically distributed binomial random variables. *SIAM Journal on Applied Mathematics*, 45(4):621–640, August 1985. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Pierchala:1985:IMU

[1193] Carl D. Pierchala. An improvement for the McGill University Random Number Package. *Computational Statistics & Data Analysis*, 2(4):317–322, February 1985. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic).

Reichert:1985:LLT

[1194] P. Reichert and R. Schilling. A local limit theorem for strongly dependent random variables and its application to a chaotic configuration of atoms. *Journal of Mathematical Physics*, 26(6):1165–1172, June 1985. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v26/i6/p1165_s1`.

Riesel:1985:PNC

[1195] Hans Riesel. *Prime numbers and computer methods for factorization*, volume 57 of *Progress in mathematics*. Birkhäuser Boston Inc., Cambridge, MA, USA, 1985. ISBN 0-8176-3291-3. xvi + 463 pp. LCCN QA246 .R54 1985.

Saito:1985:HSS

[1196] T. Saito, Masanori Fushimi, and T. Imai. High-speed M-sequence random number generation based on the primitive polynomials with many terms. *Transactions of the Information Processing Society of Japan*, 26 (??):148–152, ???? 1985. CODEN JSGRD5. ISSN 0387-5806.

Sawitzki:1985:ARN

[1197] G. Sawitzki. Another random number generator which should be avoided. *Statistical Software Newsletter*, 11(2):81–82, ???? 1985. CODEN SSNEEX. ISSN 0173-5896.

Shanthikumar:1985:DRV

[1198] J. G. Shanthikumar. Discrete random variate generation using uniformization. *European Journal of Operational Research*, 21(3):387–398, September 1985. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic).

Smith:1985:VHP

[1199] K. A. Smith, S. F. Reddaway, and D. M. Scott. Very high performance pseudo-random number generation on DAP. *Computer Physics Communications*, 37(1–3):239–244, July 1985. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465585901584`.

Thesen:1985:EGU

[1200] Arne Thesen. An efficient generator of uniformly distributed random variates between zero and one. *Simulation*, 44(1):17–22, January 1985. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/44/1/17`.

Vazirani:1985:ESP

[1201] Umesh V. Vazirani and Vijay V. Vazirani. Efficient and secure pseudo-random number generation (extended abstract). In Blakley and Chaum [4125], pages 193–202. CODEN LNCSD9. ISBN 0-387-15658-5, 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://www.springerlink.com/openurl.asp?genre=article&issn=????&volume=0&issue=0&spage=193`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Vitter:1985:RSR

[1202] Jeffrey Scott Vitter. Random sampling with a reservoir. *ACM Transactions on Mathematical Software*, 11(1):37–57, March 1985. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/3147.3165`; `http://www.acm.org/pubs/citations/journals/toms/1985-11-1/p37-vitter/`.

Yashchin:1985:ADC

[1203] Emmanuel Yashchin. On the analysis and design of Cusum-Shewhart control schemes. *IBM Journal of Research and Development*, 29(4):377–391, July 1985. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Afflerbach:1986:SLS

[1204] L. Afflerbach. The sub-lattice structure of linear congruential random number generators. *Manuscripta Mathematica*, 55(??):455–465, ???? 1986. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Anderson:1986:MMC

[1205] Herbert L. Anderson. Metropolis, Monte Carlo, and the MANIAC. *Los Alamos Science*, 14:96–108, Fall 1986. CODEN LASCDI. ISSN 0273-7116. URL `http://library.lanl.gov/cgi-bin/getfile?00326886.pdf; http://library.lanl.gov/cgi-bin/getfile?number14.htm; http://www.osti.gov/energycitations/product.biblio.jsp?osti_id=5697932&query_id=0`. Report LA-UR-85-1202;CONF-8504110-3.

Anon:1986:IRN

[1206] Anon. Integer random number generator. *IBM Technical Disclosure Bulletin*, 28(11):4869–??, April 1986. CODEN IBMTAA. ISSN 0018-8689.

Blum:1986:IUC

[1207] M. Blum. Independent unbiased coin flips from a correlated biased source — a finite state Markov chain. *Combinatorica*, 6(2):97–108, ???? 1986. CODEN COMBDI. ISSN 0209-9683 (print), 1439-6912 (electronic).

Blum:1986:SUP

[1208] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15(2):364–383, ???? 1986. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Bowman:1986:SRN

[1209] K. O. Bowman and M. T. Robinson. Studies of random number generators for parallel processing. In Heath [4130], pages 445–453. ISBN 0-89871-215-7. LCCN QA76.5 .C61921 1986.

Brown:1986:DFP

[1210] Robert H. Brown. The distribution function of positive definite quadratic forms in normal random variables. *SIAM Journal on Scientific and Statistical Computing*, 7(2):689–695, April 1986. CODEN SIJCD4. ISSN 0196-5204.

Celmaster:1986:MVR

[1211] William Celmaster and K. J. M. Moriarty. A method for vectorized random number generators. *Journal of Computational Physics*, 64(1):

271–275, May 1986. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002199918690032X`.

Chandrasekaran:1986:IAR

[1212] U. Chandrasekaran and S. Sheppard. Implementation and analysis of random variate generators in Ada. *Journal of Pascal, Ada and Modula-2*, 5(??):27–39, July/August 1986. CODEN JOPAD5. ISSN 0735-1232.

Chernoff:1986:NSB

[1213] Herman Chernoff and A. John Petkau. Numerical solutions for Bayes sequential decision problems. *SIAM Journal on Scientific and Statistical Computing*, 7(1):46–59, January 1986. CODEN SIJCD4. ISSN 0196-5204.

Clark:1986:BSP

[1214] G. M. Clark and W. Yang. A Bonferroni selection procedure when using common random numbers with unknown variances. In Wilson et al. [4131], pages 313–315. ISBN 0-911801-11-1. LCCN QA76.9.C65 W56 1986. URL `http://www.acm.org/pubs/contents/proceedings/simulation/318242/`.

Collings:1986:IGF

[1215] Bruce Jay Collings and G. Barry Hembree. Initializing generalized feedback shift register pseudorandom number generators. *Journal of the ACM*, 33(4):706–711, October 1986. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/6493.html`. See also [1335].

Deak:1986:EMG

[1216] I. Deak. The economical method for generating random samples from discrete distributions. *ACM Transactions on Mathematical Software*, 12(1):34–36, March 1986. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/5960.214321; http://www.acm.org/pubs/citations/journals/toms/1986-12-1/p34-deak/`.

Devroye:1986:AMG

[1217] Luc Devroye. An automatic method for generating random variates with a given characteristic function. *SIAM Journal on Applied Mathematics*, 46(4):698–719, August 1986. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Devroye:1986:GMS

[1218] Luc Devroye. Grid methods in simulation and random variate generation. *Computing: Archiv für Informatik und Numerik*, 37(1):71–84, March 1986. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Devroye:1986:NUR

[1219] Luc Devroye. *Non-uniform random variate generation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. ISBN 0-387-96305-7. xvi + 843 pp. LCCN QA274 .D48 1986. US$54.00.

Dyadkin:1986:EAM

[1220] I. G. Dyad'kin. On efficient algorithms for the modelling of neutron and γ-quanta transport events by the Monte-Carlo method. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 26(1): 134–140, ???? 1986. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/0041555386901977`. English translation of Russian original published in Zh. vychisl. Mat. mat. Fiz., **26**(2), 220–229, 1986.

Edgeman:1986:GPS

[1221] Rick L. Edgeman and Robert C. Scott. GENERATOR: a program for simulating nonuniform random variates. *The American Statistician*, 40 (1):54, February 1986. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2683125`.

Ehrhardt:1986:GPN

[1222] J. C. Ehrhardt. Generation of pseudorandom numbers. *Medical Physics (Woodbury)*, 13(2):240–241, ???? 1986. ISSN 0094-2405 (print), 1522-8541 (electronic).

Eichenauer:1986:NLC

[1223] Jürgen Eichenauer and Jürgen Lehn. A non-linear congruential pseudo random number generator. *Statistical Papers = Statistische Hefte*, 27(1): 315–326, September 1986. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic).

Eremin:1986:DIM

[1224] I. I. Eremin and A. A. Vatolin. Duality in improper mathematical programming problems under uncertainty. In Arkin et al. [4128], pages x + 754. ISBN 0-387-16659-9. LCCN QA402.3.S778 1986.

Fishman:1986:EAM

[1225] George S. Fishman and Louis R. Moore III. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM Journal on Scientific and Statistical Computing*, 7(1): 24–45, January 1986. CODEN SIJCD4. ISSN 0196-5204. URL `http://link.aip.org/link/?SCE/7/24/1`. See erratum [1226].

Fishman:1986:EEA

[1226] George S. Fishman and Louis R. Moore III. Erratum: "An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$". *SIAM Journal on Scientific and Statistical Computing*, 7(3):1058, July 1986. CODEN SIJCD4. ISSN 0196-5204. URL `http://epubs.siam.org/sisc/resource/1/sjoce3/v7/i3/p1058_s1`; `http://link.aip.org/link/?SCE/7/1058/1`. See [1225].

Flury:1986:SRV

[1227] Bernhard K. Flury. On sums of random variables and independence. *The American Statistician*, 40(3):214–215, ???? 1986. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Fox:1986:AIR

[1228] Bennett L. Fox. Algorithm 647: Implementation and relative efficiency of quasirandom sequence generators. *ACM Transactions on Mathematical Software*, 12(4):362–376, December 1986. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Friedman:1986:CSA

[1229] Linda Weiser Friedman and Hershey H. Friedman. Comparing simulated alternatives using a distribution-free statistic with blocking by random number stream. *Simulation*, 47(2):68–70, August 1986. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/47/2/68.abstract`.

Fushimi:1986:STE

[1230] Masanori Fushimi. Statistical tests of eight hundred million pseudorandom numbers based on an M-sequence. *Japan J. Appl. Statist.*, 15(??): 147–162, ???? 1986. CODEN ???? ISSN ????

Gleason:1986:TLF

[1231] John R. Gleason. TURBO_RAND: a library for fast Monte Carlo sampling and simulation on microcomputers. *The American Statistician*,

40(3):233, August 1986. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2684551`.

Goldreich:1986:HCR

[1232] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/6503.html`. A computational complexity measure of the randomness of functions is introduced, and, assuming the existence of one-way functions, a pseudo-random function generator is presented.

Grothe:1986:MEG

[1233] H. Grothe. Matrixgeneratoren zur Erzeugung gleichverteilter Zufallsvektoren. (German) [Matrix generators for generating uniformly distributed random vectors]. In Lothar Afflerbach and Jürgen Lehn, editors, *Kolloquium über Zufallszahlen und Simulationen: Darmstadt, 21. März, 1986. (German) [Conference on random numbers and simulation. Darmstadt, 21 March 1986]*, pages 29–34. Teubner, Stuttgart, Germany; Leipzig, Germany, 1986. ISBN 3-519-02624-4. LCCN QA274.A1 K65 1986.

Hamming:1986:NMS

[1234] R. W. (Richard Wesley) Hamming. *Numerical methods for scientists and engineers*. Dover Publications, Inc., New York, NY, USA, second edition, 1986. ISBN 0-486-65241-6 (paperback). ix + 721 pp. LCCN QA297 .H28 1986. US$14.95. URL `http://www.loc.gov/catdir/description/dover032/86016226.html`.

Hosack:1986:UCM

[1235] John M. Hosack. The use of Čebyšev mixing to generate pseudo-random numbers. *Journal of Computational Physics*, 67(2):482–486, December 1986. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999186902743`.

Hultquist:1986:LST

[1236] Paul F. Hultquist and R. N. Clark. Letter: Statistical tests of a random number generator. *Simulation*, 47(2):72–74, August 1986. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/47/2/72.full.pdf+html`. See [1156].

Inoue:1986:MAR

[1237] Hikaru Inoue, Naoki Furukawa, Yasukazu Yoshizawa, Minoru Ichimura, and Osamu Miyatake. Mathematical analysis of random number generator using gamma rays. II. *Mathematica Japonica*, 31(2):287–300, 1986. CODEN MAJAA9. ISSN 0025-5513. See also part I [1083].

Kahaner:1986:MSB

[1238] David K. Kahaner, Jeffrey Horlick, and Debra K. Foer. Mathematical software in BASIC: RV, generation of uniform and normal random variables. *IEEE Micro*, 6(3):52–60, May/June 1986. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

Kalos:1986:MCM

[1239] Malvin H. Kalos and Paula A. Whitlock. *Monte Carlo methods*. Wiley, New York, NY, USA, 1986. ISBN 0-471-89839-2. ix + 186 pp. LCCN QA298 .K35 1986. URL `http://www.loc.gov/catdir/enhancements/fy0607/86011009-b.html`; `http://www.loc.gov/catdir/enhancements/fy0607/86011009-d.html`; `http://www.loc.gov/catdir/toc/onix05/86011009.html`.

Kleijnen:1986:SRN

[1240] Jack P. C. Kleijnen. Selecting random number seeds in practice. *Simulation*, 47(1):15–17, July 1986. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/47/1/15.abstract`.

Ko:1986:NIP

[1241] K.-I. Ko. On the notion of infinite pseudorandom sequences. *Theoretical Computer Science*, 48(1):9–33, ???? 1986. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

LEcuyer:1986:EPB

[1242] P. L'Ecuyer. Efficient and portable 32-bit random variate generators. In Wilson et al. [4131], pages 275–277. ISBN 0-911801-11-1. LCCN QA76.9.C65 W56 1986. URL `http://www.acm.org/pubs/contents/proceedings/simulation/318242/`.

Lidl:1986:IFF

[1243] Rudolph Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, UK, 1986. ISBN 0-521-30706-6. viii + 407 pp. LCCN QA247.3L54 1986.

Loukas:1986:CGB

[1244] S. Loukas and C. D. Kemp. The computer generation of bivariate binomial and negative binomial random variables. *Communications in Statistics: Simulation and Computation*, 15(1):15–25, 1986. CODEN CSSCDB. ISSN 0361-0918.

Luby:1986:PRP

[1245] M. Luby and C. Rackoff. Pseudo-random permutation generators and cryptographic composition. In ACM [4127], pages 356–363. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. URL `http://www.acm.org/pubs/articles/proceedings/stoc/12130/p356-luby/p356-luby.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/12130/p356-luby/`. ACM order number 508860.

Malik:1986:PDF

[1246] Henrick J. Malik and Roger Trudel. Probability density function of the product and quotient of two correlated exponential random variables. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 29(??):413–418, ???? 1986. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Marsaglia:1986:IFC

[1247] George Marsaglia. The incomplete Γ function as a continuous Poisson distribution. *Computers and Mathematics with Applications. Part B*, 12 (5–6):1187–1190, September/December 1986. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Nicola:1986:QAF

[1248] Victor F. Nicola, V. G. Kulkarni, and Kishor S. Trivedi. Queueing analysis of fault-tolerant computer systems (extended abstract). *ACM SIGMETRICS Performance Evaluation Review*, 14(1):203, May 1986. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Niederreiter:1986:DFS

[1249] Harald Niederreiter. Dyadic fractions with small partial quotients. *Monatshefte für Mathematik*, 101(4):309–315, December 1986. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/q87291681r81t782/`.

Niederreiter:1986:LDP

[1250] Harald Niederreiter. Low-discrepancy point sets. *Monatshefte für Mathematik*, 102(2):155–167, June 1986. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Niederreiter:1986:MNI

[1251] Harald Niederreiter. Multidimensional numerical integration using pseudorandom numbers. *Mathematical Programming Study*, 27(??):17–38, ???? 1986. CODEN MPSTDF. ISSN 0303-3929. Stochastic programming 84. I.

Niederreiter:1986:PVG

[1252] H. Niederreiter. A pseudorandom vector generator based on finite field arithmetic. *Mathematica Japonica*, 31(5):759–774, ???? 1986. CODEN MAJAA9. ISSN 0025-5513.

Panny:1986:NHM

[1253] Wolfgang Panny. A note on the higher moments of the expected behavior of straight insertion sort. *Information Processing Letters*, 22(4):175–177, April 17, 1986. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Santha:1986:GQR

[1254] Miklos Santha and Umesh V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75–87, August 1986. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0022000086900449`.

Shore:1986:AID

[1255] Haim Shore. An approximation for the inverse distribution function of a combination of random variables, with an application to operating theatres. *Journal of Statistical Computation and Simulation*, 23(3):157–181, 1986. CODEN JSCSAJ. ISSN 0094-9655 (print), 1563-5163 (electronic).

Shore:1986:SGA

[1256] H. Shore. Simple general approximations for a random variable and its inverse distribution function based on linear transformations of a nonskewed variate. *SIAM Journal on Scientific and Statistical Computing*, 7(1):1–23, January 1986. CODEN SIJCD4. ISSN 0196-5204.

Sowey:1986:TCB

[1257] Eric R. Sowey. A third classified bibliography on random number generation and testing. *Journal of the Royal Statistical Society. Series A (General)*, 149(1):83–107, ???? 1986. CODEN JSSAEF. ISSN 0035-9238. URL `http://www.jstor.org/stable/2981887`.

Stephens:1986:TBE

[1258] M. S. Stephens. Tests based on EDF statistics. In D'Agostino and Stephens [4129], page ?? ISBN 0-8247-7487-6. LCCN QA277 .G645 1986.

Stephens:1986:TUD

[1259] M. S. Stephens. Tests for the uniform distribution. In D'Agostino and Stephens [4129], page ?? ISBN 0-8247-7487-6. LCCN QA277 .G645 1986.

Wolfram:1986:RSG

[1260] Stephen Wolfram. Random sequence generation by cellular automata. *Advances in Applied Mathematics*, 7(2):123–169, June 1986. CODEN ???? ISSN 0196-8858 (print), 1090-2074 (electronic). URL `http://www.sciencedirect.com/science/article/pii/019688588690028X`.

Wolfram:1986:TAC

[1261] Stephen Wolfram, editor. *Theory and applications of cellular automata: including selected papers, 1983–1986*, volume 1 of *Advanced series on complex systems*. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1986. ISBN 9971-5-0123-6, 9971-5-0124-4 (paperback). ix + 560 pp. LCCN QA267.5.C45 T48 1986.

Zeisel:1986:SAR

[1262] H. Zeisel. Statistical algorithms: Remark ASR 61: a remark on Algorithm AS 183. an efficient and portable pseudo-random number generator. *Applied Statistics*, 35(1):89, 1986. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://lib.stat.cmu.edu/apstat/183`; `http://www.jstor.org/stable/2347876`. See [1053, 1187].

Zielinski:1986:QRN

[1263] Ryszard Zieliński. A quasi-random number generator with infinite period. *Statistics & Probability Letters*, 4(5):259, August 1986. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Agnew:1987:RSC

[1264] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [4133], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Aldridge:1987:CRR

[1265] James W. Aldridge. Cautions regarding random number generation on the Apple II. *Behavior Research Methods, Instruments, and Computers*, 19(4):397–399, July 1987. CODEN BRMCEW. ISSN 0743-3808 (print), 1532-5970 (electronic). URL `http://www.springerlink.com/content/x612304327m6jm52/`.

Allender:1987:SCE

[1266] E. Allender. Some consequences of the existence of pseudorandom generators. In ACM [4132], pages 151–159. ISBN 0-89791-221-7 (paperback). LCCN QA 76.6 A13 1987. URL `http://www.acm.org/pubs/articles/proceedings/stoc/28395/p151-allender/p151-allender.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/28395/p151-allender/`. ACM order number 508870.

Anderson:1987:GRO

[1267] T. W. Anderson, I. Olkin, and L. G. Underhill. Generation of random orthogonal matrices. *SIAM Journal on Scientific and Statistical Computing*, 8(4):625–629, July 1987. CODEN SIJCD4. ISSN 0196-5204.

Barbu:1987:NFM

[1268] Gh. Barbu. A new fast method for computer generation of gamma and beta random variables by transformations of uniform variables. *Statistics: a Journal of Theoretical and Applied Statistics*, 18(3):453–464, 1987. CODEN MOSSD5. ISSN 0233-1888 (print), 1029-4910 (electronic).

Bojanczyk:1987:SAE

[1269] Adam W. Bojanczyk and Richard P. Brent. A systolic algorithm for extended GCD computation. *Computers and Mathematics and Applications*, 14(4):233–238, 1987. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Boncelet:1987:ACO

[1270] Charles G. Boncelet, Jr. Algorithms to computer order statistic distributions. *SIAM Journal on Scientific and Statistical Computing*, 8(5):868–876, September 1987. CODEN SIJCD4. ISSN 0196-5204.

Bratley:1987:GS

[1271] Paul Bratley, Bennett L. Fox, and Linus E. Schrage. *A Guide to Simulation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 1987. ISBN 0-387-96467-3. xx + 397 pp. LCCN QA76.9.C65 B73 1987.

Burton:1987:CLT

[1272] Robert Burton and Manfred Denker. On the Central Limit Theorem for dynamical systems. *Transactions of the American Mathematical Society*, 302(2):715–726, 1987. CODEN TAMTAM. ISSN 0002-9947 (print), 1088-6850 (electronic). See [2119].

Chambers:1987:CMS

[1273] J. M. Chambers, C. L. Mallows, and B. W. Stuck. Correction to: "A method for simulating stable random variables" [J. Amer. Statist. Assoc. **71** (1976), no. 354, 340–344, MR 54 #4059]. *Journal of the American Statistical Association*, 82(398):704, June 1987. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2289515`. See [761].

Chin:1987:TLP

[1274] Cary K. Chin and Edward J. McCluskey. Test length for pseudorandom testing. *IEEE Transactions on Computers*, C-36(2):252–256, February 1987. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1676892; http://www.mendeley.com/research/test-length-pseudorandom-testing/`.

Chiu:1987:SRS

[1275] Ting-Wai Chiu and Tian-Shin Guu. A shift-register sequence random number generator implemented on the microcomputers with 8088/8086 and 8087. *Computer Physics Communications*, 47(1):129–137, October 1987. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465587900725`.

Chung:1987:RWA

[1276] F. R. K. Chung, Persi Diaconis, and R. L. Graham. Random walks arising in random number generation. *Annals of Probability*, 15(3):1148–1165, July 1987. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL `http://projecteuclid.org/euclid.aop/1176992088; http://www.jstor.org/stable/2244046`.

Collings:1987:CRN

[1277] Bruce Jay Collings. Compound random number generators. *Journal of the American Statistical Association*, 82(398):525–527, June 1987. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2289456`.

Compagner:1987:MLS

[1278] A. Compagner and A. Hoogland. Maximum-length sequences, cellular automata, and random numbers. *Journal of Computational Physics*, 71(2):391–428, August 1987. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999187900374`.

Dagpunar:1987:NMS

[1279] J. S. Dagpunar. Nomograms for the manual sampling of random variates from gamma, normal and associated distributions. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 36(1):31–36, ???? 1987. CODEN ???? ISSN 0039-0526 (print), 1467-9884 (electronic). URL `http://www.jstor.org/stable/2988272`.

Diaconis:1987:SAG

[1280] Persi Diaconis and Mehrdad Shahshahani. The subgroup algorithm for generating uniform random variables. *Probability in the Engineering and Informational Sciences*, 1(1):15–32, January 1987. CODEN ???? ISSN 0269-9648 (print), 1469-8951 (electronic). URL `https://www.cambridge.org/core/product/5F15097B60994F362F6926689FA8A465`.

Doolen:1987:MCW

[1281] Gary D. Doolen and John Hendricks. Monte Carlo at work: MCNP and the Metropolis method. *Los Alamos Science*, 15 (Special Issue, Stanisław Ulam 1909–1984):142–143, 1987. CODEN LASCDI. ISSN 0273-7116. URL `http://library.lanl.gov/cgi-bin/getfile?00326867.pdf`; `http://library.lanl.gov/cgi-bin/getfile?15-12.pdf`.

Edgington:1987:RT

[1282] Eugene S. Edgington. *Randomization tests*, volume 77 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, second edition, 1987. ISBN 0-8247-7656-9. xvii + 341 pp. LCCN QA277 .E32 1987.

Eichenauer:1987:MRN

[1283] Jürgen Eichenauer, Holger Grothe, Jürgen Lehn, and Alev Topuzoğlu. A multiple recursive non-linear congruential pseudo random number generator. *Manuscripta Mathematica*, 59(??):331–346, ???? 1987. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Eichenauer:1987:SQC

[1284] J. Eichenauer and J. Lehn. On the structure of quadratic congruential sequences. *Manuscripta Mathematica*, 58(??):129–140, ???? 1987. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Federickson:1987:PMC

[1285] P. Federickson, R. Hiromoto, and J. Larson. A parallel Monte Carlo transport algorithm using a pseudo-random tree to guarantee reproducibility. *Parallel Computing*, 4(3):281–290, June 1987. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Fullerton:1987:NPN

[1286] James Fullerton. Note on a pseudorandom number generator. *ACM SIGNUM Newsletter*, 22(4):3–5, October 1987. CODEN SNEWD6. ISSN 0163-5778 (print), 1558-0237 (electronic).

Fushimi:1987:MAP

[1287] Masanori Fushimi. On misunderstandings about pseudorandom number generation by linear recurrence modulo two. In ????, editor, *First IASC (Internat. Assoc. Statist. Computing) World Conference on Computational Statistics and Data Analysis, Shizuoka, Japan, 1987*, page ?? ????, ????, 1987. ISBN ???? LCCN ????

Greenberg:1987:SAS

[1288] Irwin Greenberg. A simple approximation for the simulation of continuous random variables. *Simulation*, 49(1):32–33, July 1987. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/49/1/32.abstract`.

Grothe:1987:MGP

[1289] Holger Grothe. Matrix generators for pseudo-random vectors generation. *Statistical Papers = Statistische Hefte*, 28(1):233–238, December 1987. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic).

Haas:1987:MPR

[1290] Alexander Haas. The multiple prime random number generator. *ACM Transactions on Mathematical Software*, 13(4):368–381, December 1987. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/35078.214349`; `http://www.acm.org/pubs/citations/journals/toms/1987-13-4/p368-haas/`.

Johnson:1987:MSS

[1291] Mark E. Johnson. *Multivariate statistical simulation*. Wiley series in probability and mathematical statistics. Applied probability and statistics. Wiley, New York, NY, USA, 1987. ISBN 0-471-82290-6. ix + 230 pp. LCCN QA278 .J62 1987. URL `http://www.loc.gov/catdir/description/wiley031/86022469.html`; `http://www.loc.gov/catdir/toc/onix01/86022469.html`.

Kabaya:1987:SUD

[1292] K. Kabaya and Masoa Iri. Sum of uniformly distributed random variables and family of nonanalytic C^∞-functions. *Japan Journal of Applied Mathematics*, 4(??):1–22, 1987. CODEN ???? ISSN ????

Kaliski:1987:PBG

[1293] B. Kaliski. A pseudorandom bit generator based on elliptic logarithms. In Odlyzko [4136], pages 84–103. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Kannan:1987:SPA

[1294] Ravindran Kannan, Gary Miller, and Larry Rudolph. Sublinear parallel algorithm for computing the greatest common divisor of two integers. *SIAM Journal on Computing*, 16(1):7–16, February 1987. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

LEcuyer:1987:PRN

[1295] P. L'Ecuyer. A portable random number generator for 16-bit computers. In Paul Hogan, editor, *Modeling and Simulation on Microcomputers 1987: Proceedings of the Conference on Modeling and Simulation on Microcomputers, 14–16 January 1987, San Diego, California*, pages 45–49. Society for Computer Simulation, San Diego, CA, USA, 1987. ISBN 9997784952. ISSN 0735-6773. LCCN ????

Lenstra:1987:FIE

[1296] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987. CODEN ANMAAH. ISSN 0003-486X (print), 1939-8980 (electronic). URL `http://www.jstor.org/stable/1971363`.

Levin:1987:OWF

[1297] L. A. Levin. One-way functions and pseudorandom generators. *Combinatorica*, 7(4):357–363, December 1987. CODEN COMBDI. ISSN 0209-9683 (print), 1439-6912 (electronic).

Michener:1987:UCN

[1298] John R. Michener. The use of complete, nonlinear, block codes for nonlinear, noninvertible mixing of pseudorandom sequences. *Cryptologia*, 11(2):108–111, April 1987. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741903012~db=all~order=page`.

Modianos:1987:TIR

[1299] D. T. Modianos, R. C. Scott, and L. W. Cornwell. Testing intrinsic random number generators. *BYTE Magazine*, 12(1):175–178, 1987. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Monahan:1987:AGC

[1300] John F. Monahan. An algorithm for generating chi random variables. *ACM Transactions on Mathematical Software*, 13(2):168–172, June 1987. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). See corrigendum [1384].

Mullen:1987:OCP

[1301] G. L. Mullen and H. Niederreiter. Optimal characteristic polynomials for digital multistep pseudorandom numbers. *Computing: Archiv für Informatik und Numerik*, 39(2):155–163, June 1987. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Nelsen:1987:CMP

[1302] Roger B. Nelsen. Consequences of the memoryless property for random variables. *American Mathematical Monthly*, 94(10):981–984, ???? 1987. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).

Niederreiter:1987:PSS

[1303] Harald Niederreiter. Point sets and sequences with small discrepancy. *Monatshefte für Mathematik*, 104(4):273–337, December 1987. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Niederreiter:1987:SAG

[1304] Harald Niederreiter. A statistical analysis of generalized feedback shift register pseudorandom number generators. *SIAM Journal on Scientific*

and Statistical Computing, 8(6):1035–1051, November 1987. CODEN SIJCD4. ISSN 0196-5204.

Norton:1987:SRG

[1305] G. Norton. A shift-remainder GCD algorithm. *Lecture Notes in Computer Science*, 356:350–356, 1987. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Percus:1987:RNG

[1306] O. E. Percus and M. H. Kalos. Rand number generators for ultracomputers. NYU Ultracomputer Note 114, New York University, New York, NY, USA, 1987.

Pierre:1987:NRN

[1307] L. Pierre, T. Giamarchi, and H. J. Schulz. A new random-number generator for multispin Monte Carlo algorithms. *Journal of Statistical Physics*, 48(1–2):135–149, July 1987. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL `http://link.springer.com/article/10.1007/BF01010404`.

Ripley:1987:SS

[1308] Brian D. Ripley. *Stochastic Simulation*. Wiley series in probability and mathematical statistics. Applied probability and statistics. Wiley, New York, NY, USA, 1987. ISBN 0-471-81884-4. ISSN 0271-6356. xi + 237 pp. LCCN QA76.9.C65 R57 1987. US$29.95. URL `http://www.loc.gov/catdir/description/wiley032/86015728.html`; `http://www.loc.gov/catdir/toc/onix03/86015728.html`.

Salvat:1987:ARS

[1309] Francesc Salvat. Algorithms for random sampling from single-variate distributions. *Computer Physics Communications*, 46(3):427–436, September 1987. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465587900968`.

Schmidt:1987:VGF

[1310] K. E. Schmidt. Variational and Green's function Monte Carlo calculations of few-body systems. In L. S. Ferreira, A. C. Fonseca, and L. Streit, editors, *Models and Methods in Few-Body Physics: proceedings of the 8th Autumn School on Models and Methods in Few-Body Physics, held in Lisboa, Portugal, October 13–18, 1986*, volume 273 of *Lecture Notes in Physics*, pages 363–407. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-17647-0. LCCN QC174.17.P7 M63 1987.

Steele:1987:BRB

[1311] J. Michael Steele. Book review: *Non-Uniform Random Variate Generation* (Luc Devroye). *SIAM Review*, 29(4):675–676, ???? 1987. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Stern:1987:SLC

[1312] J. Stern. Secret linear congruential generators are not cryptographically secure. In IEEE [4135], pages 421–426. CODEN ASFPDV. ISBN 0-8186-0807-2, 0-8186-4807-4 (microfiche), 0-8186-8807-6 (casebound). ISSN 0272-5428. LCCN QA 76 S979 1987. IEEE Catalog no. 87CH2471-1. Computer Society order number 807.

Tezuka:1987:DGP

[1313] Shu Tezuka. On the discrepancy of GFSR pseudorandom numbers. *Journal of the ACM*, 34(4):939–949, October 1987. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/31848.html`.

Tezuka:1987:WST

[1314] Shu Tezuka. Walsh-spectral test for GFSR pseudorandom numbers. *Communications of the ACM*, 30(8):731–735, August 1987. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/27657.html`.

Tsang:1987:DTA

[1315] Wai Wan Tsang and George Marsaglia. A decision tree algorithm for squaring histograms in random number generation. *Ars Combinatoria. The Canadian Journal of Combinatorics*, 23A:291–301, 1987. CODEN ???? ISSN 0381-7032.

Ulrich:1987:MCG

[1316] Gary Ulrich and Layne T. Watson. A method for computer generation of variates from arbitrary continuous distributions. *SIAM Journal on Scientific and Statistical Computing*, 8(2):185–197, March 1987. CODEN SIJCD4. ISSN 0196-5204.

Vaziranni:1987:SCC

[1317] U. V. Vaziranni. Strong communication complexity or generating quasi-random sequences from two communicating semi-random sources. *Combinatorica*, 7(4):375–392, ???? 1987. CODEN COMBDI. ISSN 0209-9683 (print), 1439-6912 (electronic).

Warnock:1987:RNG

[1318] Tony Warnock. Random-number generators. *Los Alamos Science*, 15 (Special Issue, Stanisław Ulam 1909–1984):137–141, 1987. CODEN LASCDI. ISSN 0273-7116. URL http://library.lanl.gov/cgi-bin/getfile?00326867.pdf; http://library.lanl.gov/cgi-bin/getfile?15-12.pdf.

Wichmann:1987:BRN

[1319] Brian A. Wichmann and I. D. Hill. Building a random-number generator: A Pascal routine for very-long-cycle random-number sequences. *BYTE Magazine*, 12(3):127–128, ???? 1987. CODEN BYTEDJ. ISSN 0360-5280 (print), 1082-7838 (electronic).

Afflerbach:1988:LSP

[1320] Lothar Afflerbach and Holger Grothe. The lattice structure of pseudo-random vectors generated by matrix generators. *Journal of Computational and Applied Mathematics*, 23(1):127–131, July 1988. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/037704278890338X.

Afflerbach:1988:NRN

[1321] Lothar Afflerbach and Klaus Wenzel. Normal random numbers lying on spirals and clubs. *Statistical Papers = Statistische Hefte*, 29(1): 237–244, December 1988. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic). URL http://www.springerlink.com/content/q7885421202m6565/.

Afflerbach:1988:UDA

[1322] Lothar Afflerbach and Rainer Weilbächer. On using discrepancy for the assessment of pseudo-random number generators. Report, Fachbereich Mathematik, Technische Hochschule Darmstadt, Darmstadt, West Germany, 1988.

Agnew:1988:RSC

[1323] G. B. Agnew. Random sources for cryptographic systems. In Chaum and Price [4133], pages 77–81. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Ahrens:1988:ETF

[1324] Joachim H. Ahrens and Ulrich Dieter. Efficient table-free sampling methods for the exponential, Cauchy, and normal distributions. *Communications of the ACM*, 31(11):1330–1337, November 1988. CODEN

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/50094.html`.

Alexi:1988:RRF

[1325] Werner Alexi, Benny Chor, Oded Goldreich, and Claus-P. Schnorr. RSA and Rabin functions: certain parts are as hard as the whole. *SIAM Journal on Computing*, 17(2):194–209, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Altman:1988:BWB

[1326] N. S. Altman. Bit-wise behavior of random number generators. *SIAM Journal on Scientific and Statistical Computing*, 9(5):941–949, September 1988. CODEN SIJCD4. ISSN 0196-5204.

Bach:1988:HGF

[1327] Eric Bach. How to generate factored random numbers. *SIAM Journal on Computing*, 17(2):179–193, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Bakry:1988:PFG

[1328] S. H. Bakry and M. Shatila. Pascal functions for the generation of random numbers. *Computers and Mathematics and Applications*, 15(11):969–973, ???? 1988. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122188900429`.

Beauchemin:1988:GRN

[1329] Pierre Beauchemin, Gilles Brassard, Claude Crépeau, Claude Goutier, and Carl Pomerance. The generation of random numbers that are probably prime. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):53–64, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Binder:1988:MCS

[1330] K. (Kurt) Binder and Dieter W. Heermann. *Monte Carlo simulation in statistical physics: an introduction*, volume 80 of *Springer series in solid-state sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. ISBN 0-387-19107-0. viii + 127 pp. LCCN QC174.85.M64 B56 1988.

Bratley:1988:AIS

[1331] Paul Bratley and Bennett L. Fox. Algorithm 659: Implementing Sobol's quasirandom sequence generator. *ACM Transactions on Mathematical*

Software, 14(1):88–100, March 1988. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1988-14-1/p88-bratley/`.

Brickell:1988:CSR

[1332] Ernest F. Brickell and Andrew M. Odlyzko. Cryptanalysis: a survey of recent results. *Proceedings of the IEEE*, 76(5):578–593, May 1988. CODEN IEEPAD. ISSN 0018-9219 (print), 1558-2256 (electronic).

Brillhart:1988:FHP

[1333] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, volume 22 of *Contemporary mathematics*. American Mathematical Society, Providence, RI, USA, second edition, 1988. ISBN 0-8218-5078-4. ISSN 0271-4132 (print), 1098-3627 (electronic). xcv + 236 pp. LCCN QA161.F3 F33 1988.

Chor:1988:UBS

[1334] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Collings:1988:AIG

[1335] Bruce Jay Collings and G. Barry Hembree. Addendum to "Initializing generalized feedback shift register pseudorandom number generators". *Journal of the ACM*, 35(4):1001, October 1988. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). See [1215].

Dagpunar:1988:CGR

[1336] J. S. Dagpunar. Computer generation of random variates from the tail of t and normal distributions. *Communications in Statistics: Simulation and Computation*, 17(2):653–661, 1988. CODEN CSSCDB. ISSN 0361-0918.

Dagpunar:1988:PRV

[1337] John Dagpunar. *Principles of Random Variate Generation*. Clarendon Press, New York, NY, USA, 1988. ISBN 0-19-852202-9. xv + 228 pp. LCCN QA273 .D24 1988. US$45.00 (U.S.). URL `http://www.loc.gov/catdir/enhancements/fy0638/88003212-d.html`; `http://www.loc.gov/catdir/enhancements/fy0638/88003212-t.html`.

DeAngelis:1988:CDP

[1338] A. De Angelis. A class of N-dimensional probability density functions suitable for random generation. *Computer Physics Communications*, 52(1):61–64, December 1988. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465588901725`.

DeMatteis:1988:PRN

[1339] A. De Matteis and S. Pagnutti. Parallelization of random number generators and long-range correlations. *Numerische Mathematik*, 53(5):595–608, August 1988. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Deng:1988:RSS

[1340] Lih-Yuan Deng. Robustness study of some random variate generators. In Wegman et al. [4141], pages 624–626. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf`.

Denzer:1988:OML

[1341] V. Denzer and A. Ecker. Optimal multipliers for linear congruential pseudo-random number generators with prime moduli. *BIT (Nordisk tidskrift for informationsbehandling)*, 28(4):803–808, December 1988. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=28&issue=4&spage=803`.

Dudewicz:1988:TVF

[1342] Edward J. Dudewicz and Zaven A. Karian. TESTRAND for the VAX-11 family of computers: a random-number generation and testing library. *The American Statistician*, 42(3):228, August 1988. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2685018`.

Durst:1988:TPR

[1343] Mark J. Durst. Testing parallel random number generators. In Wegman et al. [4141], pages 228–231. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf`.

Edwards:1988:CAM

[1344] Lynne K. Edwards. On comparative accuracy of multivariate nonnormal random number generators. In Wegman et al. [4141], pages 618–623. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf`.

Eichenauer:1988:MLTb

[1345] Jürgen Eichenauer and Harald Niederreiter. On Marsaglia's lattice test for pseudorandom numbers. *Manuscripta Mathematica*, 62(2):245–248, 1988. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Eichenauer:1988:MLTc

[1346] Jürgen Eichenauer, Holger Grothe, and Jürgen Lehn. Marsaglia's lattice test and non-linear congruential pseudo-random number generators. *Metrika. International Journal for Theoretical and Applied Statistics.*, 35(3/4):241–250, 1988. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic).

Eichenauer:1988:NCP

[1347] Jürgen Eichenauer, Jürgen Lehn, and Alev Topuzoğlu. A nonlinear congruential pseudorandom number generator with power of two modulus. *Mathematics of Computation*, 51(184):757–759, October 1988. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008776.pdf`.

Fishman:1988:MCR

[1348] G. S. Fishman. Multiplicative congruential random number generators with modulus 2^β: An exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$. Technical Report UNC/OR/TR-87/10, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA, 1988.

Frieze:1988:RTI

[1349] Alan M. Frieze, Johan Håstad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM Journal on Computing*, 17(2):262–280, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Fushimi:1988:DUR

[1350] Masanori Fushimi. Designing a uniform random number generator whose subsequences are k-distributed. *SIAM Journal on Computing*, 17(1):89–99, February 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Fushimi:1988:STP

[1351] Masanori Fushimi. Statistical tests of pseudorandom numbers generated by a linear recurrence modulo two. In ????, editor, *First APORS (Assoc.*

Asian-Pacific Oper. Res. Soc. IFORS) Conf, Seoul, Korea, 1988, page ?? ????, ????, 1988. ISBN ???? LCCN ????

Gifford:1988:NRN

[1352] David K. Gifford. Natural random numbers. Report MIT/LCS/TM-371, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA, September 1988. URL `http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TM-371.pdf`.

Gleason:1988:IPS

[1353] John M. Gleason. The importance of proper seeding of the Applesoft pseudorandom number generator. *Computer Methods and Programs in Biomedicine*, 26(3):229–232, May/June 1988. CODEN CMPBEK. ISSN 0169-2607 (print), 1872-7565 (electronic).

Gleick:1988:QTR

[1354] J. Gleick. The quest for true randomness finally appears successful. *New York Times*, ??(??):C1, C8, April 19, 1988. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095.

Goldreich:1988:EPG

[1355] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. In IEEE [4140], pages 12–24. CODEN ASFPDV. ISBN 0-8186-0877-3 (paperback), 0-8186-4877-5 (microfiche), 0-8186-8877-7 (hard). ISSN 0272-5428. LCCN QA 76 S979 1988. IEEE catalog number 88CH2652-6. Computer Society order no. 877.

Greiner:1988:NIS

[1356] A. Greiner, W. Strittmatter, and J. Honerkamp. Numerical integration of stochastic differential equations. *Journal of Statistical Physics*, 51 (1–2):95–108, April 1988. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL `http://link.springer.com/article/10.1007/BF01015322`; `http://www.springerlink.com/content/k655227v66316102/`.

Grothe:1988:MEG

[1357] H. Grothe. *Matrixgeneratoren zur erzeugung gleichverteilter pseudozufallsvektoren. (German) [Matrix generators for the generation of equally distributed pseudo-random vectors]*. Dissertation, Technische Hochschule Darmstadt, Darmstadt, Germany, 1988.

Guinier:1988:FPU

[1358] D. Guinier. A fast and portable uniform quasi-random generator of very large period based on a generalized multi-moduli congruential method. *ACM Simuletter*, 19(3):27–33, 1988. CODEN SIMUD5. ISSN 0163-6103.

Gunther:1988:ASG

[1359] C. G. Günther. Alternating step generators controlled by de Bruijn sequences. In D. Chaum and W. L. Price, editors, *Advances in Cryptology — EUROCRYPT 87*, volume 304 of *Lecture Notes in Computer Science*, pages 5–14. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1988. URL `https://scispace.com/pdf/alternating-step-generators-controlled-by-de-bruijn-2fg3dor74t.pdf`.

Haberman:1988:WUC

[1360] Shelby J. Haberman. A warning on the use of chi-squared statistics with frequency tables with small expected cell counts. *Journal of the American Statistical Association*, 83(402):555–560, June 1988. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2288877`.

Hallin:1988:RBT

[1361] Marc Hallin and Guy Mélard. Rank-based tests for randomness against first-order serial dependence. *Journal of the American Statistical Association*, 83(404):1117–1128, December 1988. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2290144`.

Harmon:1988:AIM

[1362] Marion G. Harmon and Ted P. Baker. An Ada implementation of Marsaglia's "Universal" random number generator. *ACM SIGADA Ada Letters*, 8(2):110–112, March/April 1988. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Heidelberger:1988:DES

[1363] Philip Heidelberger. Discrete event simulations and parallel processing: statistical properties. *SIAM Journal on Scientific and Statistical Computing*, 9(6):1114–1132, November 1988. CODEN SIJCD4. ISSN 0196-5204.

Hong:1988:LGA

[1364] J. Hong, X. Tan, and M. Chen. From local to global: an analysis of nearest neighbor balancing on hypercube. *ACM SIGMETRICS Performance*

Evaluation Review, 16(1):73–82, May 1988. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Izumi:1988:FGW

[1365] T. Izumi. Fast generation of a white and normal random signal. *IEEE Transactions on Instrumentation and Measurement*, 37(2):316–318, 1988. CODEN IEIMAO. ISSN 0018-9456 (print), 1557-9662 (electronic).

Kachitvichyanukul:1988:AHS

[1366] Voratas Kachitvichyanukul and Bruce W. Schmeiser. Algorithm 668: H2PEC: Sampling from the hypergeometric distribution. *ACM Transactions on Mathematical Software*, 14(4):397–398, December 1988. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/50063.214387; http://www.acm.org/pubs/citations/journals/toms/1988-14-4/p397-kachitvichyanukul/`.

Kachitvichyanukul:1988:BRV

[1367] Voratas Kachitvichyanukul and Bruce W. Schmeiser. Binomial random variate generation. *Communications of the ACM*, 31(2): 216–222, February 1988. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/214994.html; http://www.acm.org/pubs/toc/Abstracts/0001-0782/42381.html`.

Kannan:1988:PFN

[1368] R. Kannan, Arjen K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Mathematics of Computation*, 50(181):235–250, January 1988. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Karloff:1988:RAP

[1369] Howard Karloff and Prabhakar Raghavan. Randomized algorithms and pseudorandom numbers. In ACM [4138], pages 310–321. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. URL `http://www.acm.org/pubs/articles/proceedings/stoc/62212/p310-karloff/p310-karloff.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/62212/p310-karloff/`. ACM order number 508880.

Kleijnen:1988:ASE

[1370] Jack P. C. Kleijnen. Analyzing simulation experiments with Common Random Numbers. *Management Science*, 34(1):65–74, January 1988. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Kolmogorov:1988:AR

[1371] A. N. Kolmogorov and V. A. Uspenskii. Algorithms and randomness. *Theory of Probability and its Applications*, 32(3):389–412, ???? 1988. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/tvp/resource/1/tprbau/v32/i3/p389_s1`.

Korin:1988:TRM

[1372] Basil P. Korin. Turbo Rand: Monte Carlo sampling and simulations. *Computational Statistics & Data Analysis*, 6(2):185–188, March 1988. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0167947388900497`.

Kurosawa:1988:CSP

[1373] K. Kurosawa and K. Matsu. Cryptographically secure pseudorandom sequence generator based on reciprocal number cryptosystem. *Electronics Letters*, 24(1):16–17, January 7, 1988. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8134`.

Lagarias:1988:UEP

[1374] Jeffrey C. Lagarias and James A. Reeds. Unique extrapolation of polynomial recurrences. *SIAM Journal on Computing*, 17(2):342–362, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

LEcuyer:1988:BLP

[1375] Pierre L'Ecuyer and François Blouin. BonGCL, un logiciel pour la recherche de bons générateurs à congruence linéaire. (French) [BonGCL, software for the search for good linear congruential generators]. Technical Report DIUL-RT-8803, Computer Science Department, Laval University, Ste-Foy, Québec, Canada, 1988.

LEcuyer:1988:EPC

[1376] Pierre L'Ecuyer. Efficient and portable combined random number generators. *Communications of the ACM*, 31(6):742–749, 774, June 1988.

CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/62969.html`.

LEcuyer:1988:GLC

[1377] Pierre L'Ecuyer and François Blouin. Generalized linear congruential generators. Report DIUL-RT-8814, Computer Science Department, Laval University, Ste-Foy, Québec, Canada, 1988. Also presented at ORSA/TIMS St-Louis, 1987.

LEcuyer:1988:LCG

[1378] Pierre L'Ecuyer and François Blouin. Linear congruential generators of order $k > 1$. In Abrams et al. [4137], pages 432–439. ISBN 0-911801-42-1. LCCN QA76.9.C65 W56 1988. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5817`. IEEE catalog number 88CH2659-1.

Levitan:1988:QSN

[1379] Yu. L. Levitan, N. I. Markovich, S. G. Rozin, and I. M. Sobol'. On quasirandom sequences for numerical computations. *U.S.S.R. Computational Mathematics and Mathematical Physics*, 28(3):88–92, ???? 1988. CODEN CMMPA9. ISSN 0041-5553, 0502-9902. URL `http://www.sciencedirect.com/science/article/pii/0041555388901814`.

Luby:1988:HCP

[1380] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Mactutus:1988:CSN

[1381] C. F. Mactutus and R. M. Booze. Computer simulations in neuroscience pseudo-random numbers. *Society for Neuroscience Abstracts*, 14(2):863, ???? 1988. ISSN 0190-5295.

Matsumoto:1988:FPS

[1382] M. Matsumoto and Y. Kurita. The fixed point of an m-sequence and local non-randomness. Report 88-027, Department of Information Science, University of Tokyo, Tokyo, Japan, 1988.

Minh:1988:GGV

[1383] Do Le Minh. Generating gamma variates. *ACM Transactions on Mathematical Software*, 14(3):261–266, September 1988. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1988-14-3/p261-minh/`.

Monahan:1988:CAG

[1384] John F. Monahan. Corrigendum: "An algorithm for generating chi random variables". *ACM Transactions on Mathematical Software*, 14(1): 111, March 1988. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). See [1300].

Niederreiter:1988:LDL

[1385] Harald Niederreiter. Low-discrepancy and low-dispersion sequences. *Journal of Number Theory*, 30(1):51–70, 1988. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic).

Niederreiter:1988:RNC

[1386] Harald Niederreiter. Remarks on nonlinear congruential pseudorandom numbers. *Metrika. International Journal for Theoretical and Applied Statistics.*, 35(??):321–328, ???? 1988. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic).

Niederreiter:1988:SIN

[1387] Harald Niederreiter. Statistical independence of nonlinear congruential pseudorandom numbers. *Monatshefte für Mathematik*, 106(2): 149–159, June 1988. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/x6g636675406h964/`.

Niederreiter:1988:SNC

[1388] Harald Niederreiter. Some new cryptosystems based on feedback shift register sequences. *Math. J. Okayama Univ.*, 30:121–149, 1988. CODEN MJOKAP. ISSN 0030-1566.

Niederreiter:1988:STD

[1389] Harald Niederreiter. The serial test for digital k-step pseudorandom numbers. *Math. J. Okayama Univ.*, 30(??):93–119, ???? 1988. CODEN MJOKAP. ISSN 0030-1566.

Ore:1988:NTH

[1390] Øystein Øre. *Number theory and its history.* Dover classics of science and mathematics. Dover Publications, Inc., New York, NY, USA, 1988. ISBN 0-486-65620-9 (paperback). x + 370 pp. LCCN QA241 .O7 1988. URL `http://www.loc.gov/catdir/enhancements/fy0707/88000372-d.htm`.

Panton:1988:PPS

[1391] Don B. Panton. A PASCAL program for simulating stable random variates. *Communications in Statistics: Simulation and Computation*, 17(3): 837–842, 1988. CODEN CSSCDB. ISSN 0361-0918.

Park:1988:RNG

[1392] Stephen K. Park and Keith W. Miller. Random number generators: Good ones are hard to find. *Communications of the ACM*, 31(10):1192–1201, October 1988. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/63042.html`.

Percus:1988:LRC

[1393] Ora E. Percus and Jerome K. Percus. Long range correlations in linear congruential generators. *Journal of Computational Physics*, 77(1): 267–269, 1988. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic).

Petersen:1988:SVR

[1394] W. P. Petersen. Some vectorized random number generators for uniform, normal, and Poisson distributions for CRAY X-MP. *The Journal of Supercomputing*, 1(3):327–335, April 1988. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=1&issue=3&spage=327`.

Reif:1988:EPP

[1395] J. H. Reif and J. D. Tygar. Efficient parallel pseudorandom number generation. *SIAM Journal on Computing*, 17(2):404–411, April 1988. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). Special issue on cryptography.

Ripley:1988:UAS

[1396] B. D. Ripley. Uses and abuses of statistical simulation. *Mathematical Programming*, 42(??):53–68, ???? 1988. CODEN MHPGA4. ISSN 0025-5610.

Rockower:1988:IIR

[1397] Edward B. Rockower. Integral identities for random variables. *The American Statistician*, 42(1):68–72, ???? 1988. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Sezgin:1988:MOP

[1398] Fatin Sezgin. A method of obtaining portable random number generators. In Edwards and Raun [4139], pages 41–42. ISBN 3-7908-0411-8. LCCN QA276.4 .C57 1988. URL http://catalog.hathitrust.org/api/volumes/oclc/19564603.html.

Shi:1988:SRP

[1399] Wen-Hong Shi and Jin-Guang Chen. Study on the recurrences of pseudorandom array. *Electronics Letters*, 24(8):499–500, April 14, 1988. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8260.

Tezuka:1988:OGP

[1400] Shu Tezuka. On optimal GFSR pseudorandom number generators. *Mathematics of Computation*, 50(182):531–533, April 1988. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.jstor.org/stable/pdfplus/2008621.pdf.

Young:1988:RUM

[1401] Dean M. Young, Danny W. Turner, and John W. Seaman, Jr. A ratio-of-uniforms method for generating exponential power variates. In Wegman et al. [4141], pages 627–629. URL http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf.

Afflerbach:1989:CAR

[1402] L. Afflerbach. Criteria for the assessment of random number generators. Technical Report 1205, Fachbereich Mathematik, Technische Hochschule Darmstadt, Darmstadt, Germany, 1989.

Afflerbach:1989:EDR

[1403] Lothar Afflerbach and Rainer Weilbächer. The exact determination of rectangle discrepancy for linear congruential pseudorandom numbers. *Mathematics of Computation*, 53(187):343–354, July 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.jstor.org/stable/pdfplus/2008367.pdf.

Ahrens:1989:AMS

[1404] J. H. Ahrens and U. Dieter. An alias method for sampling from the normal distribution. *Computing: Archiv für Informatik und Numerik*, 42 (2–3):159–170, June 1989. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Ahrens:1989:HAL

[1405] J. H. Ahrens. How to avoid logarithms in comparisons with uniform random variables. *Computing: Archiv für Informatik und Numerik*, 41 (1–2):163–166, March 1989. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Ahrens:1989:NUR

[1406] J. H. Ahrens and E. Stadlober. Non-uniform random number generation: a survey and tutorial. In MacNair et al. [4147], page 50. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/iel4/5823/15520/00718661.pdf`. IEEE order number 89CH2778-9.

Aiello:1989:HIG

[1407] G. R. Aiello, M. Budinich, and E. Milotti. Hardware implementation of a GFSR pseudo-random number generator. *Computer Physics Communications*, 56(2):135–139, December 1, 1989. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465589900143`.

Allender:1989:SCE

[1408] Eric W. Allender. Some consequences of the existence of pseudorandom generators. *Journal of Computer and System Sciences*, 39(1):101–124, August 1989. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0022000089900214`.

Babai:1989:MPL

[1409] L. Babai and N. Nisan. Multiparty protocols and logspace-hard pseudorandom sequences. In ACM [4143], pages 1–11. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL `http://www.acm.org/pubs/articles/proceedings/stoc/73007/p1-babai/p1-babai.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/73007/p1-babai/`. ACM order number 508890.

Baccelli:1989:AFJ

[1410] François Baccelli, William A. Massey, and Don Towsley. Acyclic fork-join queueing networks. *Journal of the ACM*, 36(3):615–642, July 1989. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/65957.html`.

Bardin:1989:IUI

[1411] B. Bardin, C. Colket, and D. Smith. Implementation of unsigned integers in Ada. *Ada Letters*, 9(1):47–70, January–February 1989. CODEN AALEE5. ISSN 1094-3641 (print), 1557-9476 (electronic).

Benichou:1989:DMI

[1412] Jacques Benichou and Mitchell H. Gail. A delta method for implicitly defined random variables. *The American Statistician*, 43(1):41–44, ???? 1989. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Bethmann:1989:LFT

[1413] J. Bethmann. The Lindberg–Feller theorem for sums of a random number of independent random variables in a triangular array. *Theory of Probability and its Applications*, 33(2):334–339, ???? 1989. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **33**(2), (1988), pp. 354–359.

Black:1989:GRN

[1414] S. C. Black and A. D. Kennedy. Gaussian random number generators on a CYBER-205. *Computers in Physics*, 3(3):59–??, May 1989. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.168326`.

Booth:1989:ZVS

[1415] Thomas E. Booth. Zero-variance solutions for linear Monte Carlo. *Nuclear Science and Engineering*, 102(4):332–340, August 1989. CODEN NSENAO. ISSN 0029-5639 (print), 1943-748X (electronic). URL `http://www.ans.org/pubs/journals/nse/a_23646`.

Boyar:1989:ISPa

[1416] Joan Boyar. Inferring sequences produced by pseudo-random number generators. *Journal of the ACM*, 36(1):129–141, January 1989. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/59305.html`; `http://www.imada.sdu.dk/~joan/`.

Boyar:1989:ISPb

[1417] Joan Boyar. Inferring sequences produced by a linear congruential generator missing low-order bits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3):177–184, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brody:1989:RNG

[1418] T. A. Brody. Random-number generation for parallel processors. *Computer Physics Communications*, 56(2):147–153, December 1, 1989. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465589900167`.

Butler:1989:RBG

[1419] David A. Butler. A random-bit generator for use in simulating the reliability of a coherent system. *Probability in the Engineering and Informational Sciences*, 3(1):141–147, January 1989. CODEN ???? ISSN 0269-9648 (print), 1469-8951 (electronic). URL `https://www.cambridge.org/core/product/2C2964E730008624C67C1262123E0D36`.

Chassaing:1989:ORN

[1420] Philippe Chassaing. An optimal random number generator on Z_p. *Statistics & Probability Letters*, 7(4):307–309, February 1989. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Dagpunar:1989:CPP

[1421] J. S. Dagpunar. A compact and portable Poisson random variate generator. *Journal of Applied Statistics*, 16(3):391–393, 1989. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic).

Danilowicz:1989:DDP

[1422] Ronald L. Danilowicz. Demonstrating the dangers of pseudo-random numbers. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 21(2):46–48, June 1989. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Deak:1989:URN

[1423] I. Deak. Uniform random number generators for parallel computers. Report 89-1, Department of Industrial Engineering, University of Wisconsin-Madison, Madison, WI, USA, 1989.

Devroye:1989:RVG

[1424] Luc Devroye. Random variate generators for the Poisson–Poisson and related distributions. *Computational Statistics & Data Analysis*, 8 (3):247–278, November 1989. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0167947389900443`.

Durst:1989:ULC

[1425] M. J. Durst. Using linear congruential generators for parallel random number generation. In MacNair et al. [4147], pages 462–466. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

Edgeman:1989:RNG

[1426] Rick L. Edgeman, Paul W. Abrahams, Francis M. Sand, and James Crawford, Jr. Random number generators and the minimal standard. *Communications of the ACM*, 32(8):1020–1024, August 1989. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Eichenauer-Herrmann:1989:PLP

[1427] Jürgen Eichenauer-Herrmann, Holger Grothe, and Jürgen Lehn. On the period length of pseudorandom vector sequences generated by matrix generators. *Mathematics of Computation*, 52(185):145–148, January 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008659.pdf`.

Eichenauer-Herrmann:1989:RLR

[1428] Jürgen Eichenauer-Herrmann and Holger Grothe. A remark on long-range correlations in multiplicative congruential pseudo random number generators. *Numerische Mathematik*, 56(6):609–611, December 1989. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Evans:1989:PRN

[1429] W. Evans and B. Sulga. Parallel random number generation. In Anonymous [4144], pages 415–420. ISBN ???? LCCN QA76.5.C619215 1989. Two volumes.

Flajolet:1989:RMS

[1430] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *EUROCRYPT 1989: Advances in Cryptology — EUROCRYPT '89: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, volume 434 of *Lecture Notes in Computer Science*, pages 329–354. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1989.

Fushimi:1989:ERB

[1431] M. Fushimi. An equivalence relation between Tausworthe and GFSR sequences and applications. *Applied Mathematics Letters*, 2(2):135–137,

???? 1989. CODEN AMLEEL. ISSN 0893-9659 (print), 1873-5452 (electronic).

Fushimi:1989:RNG

[1432] M. Fushimi. Random number generation on parallel processors. In MacNair et al. [4147], pages 459–461. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

Gilmore:1989:RSP

[1433] J. Barnard Gilmore. Randomness and the search for PSI. *Journal of Parapsychology*, 53(4):309–340, December 1989. CODEN JPRPAU. ISSN 0022-3387. URL `http://www.rhine.org/journalarchive.htm`.

Gleason:1989:STI

[1434] John M. Gleason. Statistical tests of the IBM PC pseudorandom number generator. *Computer Methods and Programs in Biomedicine*, 30(1):43–46, October 1989. CODEN CMPBEK. ISSN 0169-2607 (print), 1872-7565 (electronic).

Gordon:1989:FMI

[1435] J. Gordon. Fast multiplicative inverse in modular arithmetic. In Beker and Piper [4145], pages 269–279. ISBN 0-19-853623-2. LCCN QA268.C74 1989. UK£35.00, US$52.00. Held in December 1986. Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester on 15th–17th December 1986.

Grzesik:1989:NRT

[1436] J. A. Grzesik. Von Neumann's rejection technique reexamined. *SIAM Review*, 31(3):486–489, September 1989. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Guinier:1989:FUA

[1437] Daniel Guinier. A fast uniform 'astronomical' random number generator. *SIGSAC Review*, 7(1):1–13, Spring 1989. CODEN SSARE7. ISSN 0277-920X (print), 1558-0261 (electronic).

Halton:1989:PRT

[1438] John H. Halton. Pseudo-random trees: Multiple independent sequence generators for parallel and branching computations. *Journal of Computational Physics*, 84(1):1–56, September 1989. CODEN JCTPAH.

ISSN 0021-9991 (print), 1090-2716 (electronic). URL http://www.sciencedirect.com/science/article/pii/0021999189901800.

Herring:1989:RNG

[1439] C. Herring and J. I. Palmore. Random number generators are chaotic. *ACM SIGPLAN Notices*, 24(11):76–79, November 1989. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Hortensius:1989:CAB

[1440] P. D. Hortensius, R. D. McLeod, W. Pries, D. M. Miller, and H. C. Card. Cellular automata-based pseudorandom number generators for built-in self-test. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 8(8):842–859, ???? 1989. CODEN ITCSDI. ISSN 0278-0070 (print), 1937-4151 (electronic).

Hortensius:1989:PRN

[1441] P. D. Hortensius, R. D. McLeod, and H. C. Card. Parallel random number generation for VLSI systems using cellular automata. *IEEE Transactions on Computers*, 38(10):1466–1473, October 1989. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=35843.

Impagliazzo:1989:ECS

[1442] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. In IEEE [4146], pages 236–241. CODEN ASFPDV. ISBN 0-8186-1982-1. ISSN 0272-5428. LCCN QA 76 S979 1989. IEEE catalog number 89CH2808-4.

Impagliazzo:1989:HRR

[1443] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In IEEE [4146], pages 248–253. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989; TK7885.A1 S92 1989. Formerly called the Annual Symposium on Switching and Automata Theory. IEEE catalog number 89CH2808-4. Computer Society order number 1982.

Impagliazzo:1989:PRG

[1444] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions (extended abstract). In ACM [4143], pages 12–24. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. URL http://www.acm.org/pubs/articles/proceedings/stoc/73007/p12-impagliazzo/p12-impagliazzo.pdf; http://www.acm.

org/pubs/citations/proceedings/stoc/73007/p12-impagliazzo/. ACM order number 508890.

Kachitvichyanukul:1989:ABS

[1445] Voratas Kachitvichyanukul and Bruce W. Schmeiser. Algorithm 678: BTPEC: Sampling from the binomial distribution. *ACM Transactions on Mathematical Software*, 15(4):394–397, December 1989. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL http://doi.acm.org/10.1145/76909.76916; http://www.acm.org/pubs/citations/journals/toms/1989-15-4/p394-kachitvichyanukul/.

Kahaner:1989:NMS

[1446] David Kahaner, Cleve Moler, and Stephen Nash. *Numerical Methods and Software*. Prentice-Hall series in computational mathematics. Prentice-Hall, Upper Saddle River, NJ, USA, 1989. ISBN 0-13-627258-4. xii + 495 pp. LCCN TA345 .K341 1989. US$50.

Kamps:1989:CPL

[1447] U. Kamps. Chebyshev polynomials and least squares estimation based on one-dependent random variables. *Linear Algebra and its Applications*, 112(??):217–230, January 1989. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). URL http://www.sciencedirect.com/science/article/pii/0024379589905971.

Kao:1989:RNG

[1448] Chiang Kao. A random number generator for microcomputers. *OR: the journal of the Operational Research Society*, 40(7):687–691, July 1989. CODEN OPRQAK. ISSN 0160-5682 (print), 1476-9360 (electronic). URL http://www.jstor.org/stable/2582978. See comments [1538, 1581, 1609, 1633].

Kelton:1989:RIM

[1449] W. D. Kelton. Random initialization methods in simulation. *IIE Transactions*, 21(4):355–367, ???? 1989. CODEN IIETDM. ISSN 0740-817X (print), 1573-9724 (electronic).

Kharitonov:1989:LBP

[1450] M. Kharitonov, A. V. Goldberg, and M. Yung. Lower bounds for pseudorandom number generators. In IEEE [4146], pages 242–247. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989; TK7885.A1 S92 1989. Formerly called the Annual Symposium on Switching and Automata The-

ory. IEEE catalog number 89CH2808-4. Computer Society order number 1982.

Kim:1989:PRP

[1451] Su Hee Kim and Carl Pomerance. The probability that a random probable prime is composite. *Mathematics of Computation*, 53(188):721–741, October 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Kleijnen:1989:PNG

[1452] J. Kleijnen. Pseudorandom number generation on supercomputers. *Supercomputer*, 6(6):34–40, November 1989. CODEN SPCOEL. ISSN 0168-7875.

Komo:1989:MLP

[1453] J. J. Komo and W. J. Park, Jr. Maximal-length pseudorandom number generator. In ????, editor, *Proceedings. Twenty-First Southeastern Symposium on System Theory, 1989*, page ?? ????, ????, 1989. ISBN ???? LCCN ????

Koniges:1989:PPR

[1454] A. E. Koniges and C. E. Leith. Parallel processing of random number generation for Monte Carlo turbulence simulation. *Journal of Computational Physics*, 81(1):230–235, March 1989. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999189900727`.

Korolev:1989:ANA

[1455] V. Yu. Korolev. On the accuracy of normal approximation for the distributions of sums of a random number of independent random variables. *Theory of Probability and its Applications*, 33(3):540–544, ???? 1989. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **33**(3), (1988), pp. 577–581.

Kuo:1989:DSF

[1456] Y. S. Kuo, S.-Y. Hwang, and H. F. Hu. Data structure for fast region searches. *IEEE Design & Test of Computers*, 6(5):20–28, October 1989. CODEN IDTCEC. ISSN 0740-7475 (print), 1558-1918 (electronic).

Lecot:1989:AGL

[1457] C. Lecot. An algorithm for generating low discrepancy sequences on vector computers. *Parallel Computing*, 11(1):113–116, July 1989. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

LEcuyer:1989:APT

[1458] Pierre L'Ecuyer and R. Proulx. About polynomial-time "unpredictable" generators. In MacNair et al. [4147], pages 467–476. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

LEcuyer:1989:TUV

[1459] Pierre L'Ecuyer. A tutorial on uniform variate generation. In MacNair et al. [4147], pages 40–49. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

Lilja:1989:EGP

[1460] David J. Lilja. Efficient generation of Poisson distributed random variables. Technical Report CSRD 900, University of Illinois at Urbana-Champaign, Center for Supercomputing Research and Development, Urbana, IL 61801, USA, July 31, 1989. 15 pp.

Luby:1989:SPS

[1461] Michael Luby and Charles Rackoff. A study of password security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3):151–158, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maclaren:1989:GMI

[1462] N. M. Maclaren. The generation of multiple independent sequences of pseudorandom numbers. *Applied Statistics*, 38(2):351–359, 1989. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL `http://www.jstor.org/stable/2348065`.

Manas:1989:PCI

[1463] G. J. Manas and D. H. Meyer. On a problem of coin identification. *SIAM Review*, 31(1):114–117, March 1989. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Marsaglia:1989:RVS

[1464] George Marsaglia. Random variables for supercomputers. In Wegman [4142], page 103. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a205068.pdf`. Abstract only.

Martin:1989:AMM

[1465] R. Douglas Martin and Ruben H. Zamar. Asymptotically min-max bias robust M-estimates of scale for positive random variables. *Journal of the*

American Statistical Association, 84(406):494–501, June 1989. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2289935`.

McIntosh:1989:RAE

[1466] David McIntosh. Random Atari: Enhancing the number generator. *ANTIC*, 7(11):12–??, 1989. CODEN ???? ISSN 0113-1141. URL `http://www.atarimagazines.com/v7n11/randomatari.html`.

Meer:1989:SIP

[1467] Peter Meer. Stochastic image pyramids. *Computer Vision, Graphics, and Image Processing*, 45(3):269–294, March 1989. CODEN CVGPDB. ISSN 0734-189x (print), 1557-895x (electronic).

Meier:1989:FCA

[1468] Willi Meier and Othmar Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3):159–176, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Mertsch:1989:PAS

[1469] M. K. Mertsch. *On Performance Analysis and Selection Criteria of Random Number Generators for Simulations*. Dissertation, Institute for Electronic Systems and Switching, University of Dortmund, Dortmund, Germany, 1989.

Niederreiter:1989:STC

[1470] Harald Niederreiter. The serial test for congruential pseudorandom numbers generated by inversions. *Mathematics of Computation*, 52(185): 135–144, January 1989. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008658.pdf`.

Paul:1989:IRN

[1471] W. Paul, Dieter W. Heermann, and Rashmi C. Desai. Implementation of a random number generator in OCCAM. *Journal of Computational Physics*, 82(2):487–491, June 1989. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999189900594`.

Percus:1989:RNG

[1472] Ora E. Percus and Malvin H. Kalos. Random number generators for MIMD parallel processors. *Journal of Parallel and Distributed Com-*

puting, 6(3):477–497, June 1989. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic).

Pickover:1989:PRG

[1473] Clifford A. Pickover. Picturing randomness on a graphics supercomputer. Research report RC 14468 (#64759), IBM T.J. Watson Research Center, Yorktown Heights, NY, USA, 1989. iii + 8 pp.

Press:1989:QSR

[1474] William H. Press and Saul A. Teukolsky. Quasi- (that is, sub-) random numbers. *Computers in Physics*, 3(6):76–??, November 1989. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.4822879`.

Reber:1989:PNG

[1475] James C. Reber. Pseudorandom number generators in a four-bit computer system. *College Mathematics Journal*, 20(1):54–55, January 1989. CODEN ???? ISSN 0746-8342 (print), 1931-1346 (electronic). URL `http://www.jstor.org/stable/pdfplus/2686821.pdf`; `http://www.tandfonline.com/doi/abs/10.1080/07468342.1989.11973205`.

Rhee:1989:OPIa

[1476] Wansoo T. Rhee and Michel Talagrand. Optimal bin packing with items of random sizes. II. *SIAM Journal on Computing*, 18(1):139–151, February 1989. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Richards:1989:GRP

[1477] T. Richards. Graphical representation of pseudorandom sequences. *Computers and Graphics*, 13(2):261–262, 1989. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

Sezgin:1989:EPC

[1478] Fatin Sezgin. On efficient and portable combined random number generators. *Communications of the ACM*, 32(8):1019–1020, August 1989. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Tezuka:1989:ALC

[1479] Shu Tezuka. Analysis of L'Ecuyer's combined random number generator. Report RT-5014, IBM Research, Tokyo Research Laboratory, Tokyo, Japan, November 1989.

Tezuka:1989:RNG

[1480] Shu Tezuka. Random number generation based on the polynomial arithmetic modulo two. Report, IBM Research, Tokyo Research Laboratory, Tokyo, Japan, 1989.

Thomas:1989:SNL

[1481] Marlin A. Thomas, Gary W. Gemmill, and John R. Crigler. STATLIB: NSWC library of statistical programs and subroutines. Technical Report NSWC TR 89-97, Naval Surface Warfare Center, Dahlgren, VA 22448-5000, USA and Silver Spring, MD 20903-5000, USA, August 1989. viii + 280 pp. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a221538.pdf`.

Wang:1989:SMR

[1482] Mei-Cheng Wang. A semiparametric model for randomly truncated data. *Journal of the American Statistical Association*, 84(407):742–748, September 1989. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2289656`.

Wikramaratna:1989:ANM

[1483] Roy S. Wikramaratna. ACORN — a new method for generating sequences of uniformly distributed pseudo-random numbers. *Journal of Computational Physics*, 83(1):16–31, July 1989. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999189902210`.

Yang:1989:OUC

[1484] W.-N. Yang and B. L. Nelson. Optimization using Common Random Numbers, control variates and multiple comparisons with the best. In MacNair et al. [4147], pages 444–449. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

Afflerbach:1990:CAR

[1485] Lothar Afflerbach. Criteria for the assessment of random number generators. *Journal of Computational and Applied Mathematics*, 31(1):3–10, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903303`.

Alon:1990:SCA

[1486] N. Alon, O. Goldreich, J. Håstad, and R. Peralta. Simple construction of almost k-wise independent random variables. In IEEE [4152], pages 544–

553. CODEN ASFPDV. ISBN 0-8186-2082-X (paperback), 0-8186-6082-1 (microfiche), 0-8186-9082-8 (case). ISSN 0272-5428. LCCN TK7885.A1 S92 1990. Formerly called the Annual Symposium on Switching and Automata Theory. IEEE catalog number 90CH29256. Computer Society order number 2082.

Anderson:1990:RNG

[1487] Stuart L. Anderson. Random number generators on vector supercomputers and other advanced architectures. *SIAM Review*, 32(2):221–251, June 1990. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://www.jstor.org/stable/2030521`.

Anderson:1990:SCS

[1488] Ross J. Anderson. Solving a class of stream ciphers. *Cryptologia*, 14(3):285–288, July 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902650~db=all~order=page`. keystream sequences; linear feedback shift registers; multiplexor; consistency check; observed keystream; address information.

Andre:1990:FMD

[1489] Debra A. André, Gary L. Mullen, and Harald Niederreiter. Figures of merit for digital multistep pseudorandom numbers. *Mathematics of Computation*, 54(190):737–748, April 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008509.pdf`.

Asada:1990:GCH

[1490] Y. Asada, N. Kobayashi, T. Hayashi, M. Suzuki, N. Hidaka, K. Odani, K. Kondo, T. Mimura, and M. Abe. A gigahertz cryogenic HEMT pseudorandom number generator chip set. In ????, editor, *Digest of Technical Papers. IEEE International 37th ISSCC Solid-State Circuits Conference, 16–16 February 1990, San Francisco, CA, USA*, pages 186–187. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN ???? LCCN ????

Ascheid:1990:GWD

[1491] G. Ascheid. On the generation of WMC-distributed random numbers. *IEEE Transactions on Communications*, 38(12):2117–2118, December 1990. CODEN IECMBT. ISSN 0090-6778 (print), 1558-0857 (electronic).

Baccelli:1990:EPP

[1492] François Baccelli and Zhen Liu. On the execution of parallel programs on multiprocessor systems — a queuing theory approach. *Journal of the*

ACM, 37(2):373–414, April 1990. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/77622.html`.

Bays:1990:CIR

[1493] Carter Bays. C364. Improving a random number generator: a comparison between two shuffling methods. *Journal of Statistical Computation and Simulation*, 36(1):57–59, May 1990. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659008811264`. See [649, 757] for the two nearly identical shuffling algorithms. This paper explains why the first does not lengthen the generator period, or much reduce the lattice structure of linear congruential generators, but the second improves both dramatically.

Behboodian:1990:EUD

[1494] Javad Behboodian. Examples of uncorrelated dependent random variables using a bivariate mixture. *The American Statistician*, 44(3):218, August 1990. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Bernstein:1990:SRN

[1495] G. M. Bernstein and M. A. Lieberman. Secure random number generation using chaotic circuits. *IEEE Transactions on Circuits and Systems*, 37(9):1157–1164, September 1990. CODEN ICSYBT. ISSN 0098-4094 (print), 1558-1276 (electronic).

Beth:1990:CPR

[1496] Thomas Beth and Zong-Duo Dai. On the complexity of pseudo-random sequences — or: If you can describe a sequence it can't be random. *Lecture Notes in Computer Science*, 434:533–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340533.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340533.pdf`.

Bhavsar:1990:EDL

[1497] Virendra C. Bhavsar, Uday G. Gujar, Joseph D. Horton, and Lambros A. Lambrou. Evaluation of the discrepancy of the linear congruential pseudo-random number sequences. *BIT (Nordisk tidskrift for informationsbehandling)*, 30(2):257–267, June 1990. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (elec-

tronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=30&issue=2&spage=257.

Bralic:1990:AGR

[1498] N. Bralić, R. Espinosa, and C. Saavedra. An algorithm for the generation of random numbers with density $C\exp(-\lambda|x|^{\nu})$. *Journal of Computational Physics*, 88(2):484–489, June 1990. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL http://www.sciencedirect.com/science/article/pii/0021999190901913.

Burford:1990:RNG

[1499] Roger L. Burford. Random number generators for microcomputers. *Communications in Statistics: Simulation and Computation*, 19(2):649–662, ???? 1990. CODEN CSSCDB. ISSN 0361-0918. URL http://www.tandfonline.com/doi/abs/10.1080/03610919008812880.

Carta:1990:TFI

[1500] David G. Carta. Two fast implementations of the "minimal standard" random number generator. *Communications of the ACM*, 33(1):87–88, January 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/76379.html. See criticism and errata [1779], and further criticism in [1870]. The latter point out that Carta's implementation does not correspond to their proposal.

Dagpunar:1990:SMD

[1501] J. S. Dagpunar. Sampling from the von Mises distribution via a comparison of random numbers. *Journal of Applied Statistics*, 17(1):165–168, 1990. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic).

Deak:1990:RNG

[1502] István Deák. *Random number generators and simulation*, volume 4 of *Mathematical methods of operations research*. Akadémiai Kiadó, Budapest, Hungary, 1990. ISBN 963-05-5316-3. 341 pp. LCCN QA298 .D4313 1990.

Deak:1990:URN

[1503] István Deák. Uniform random number generators for parallel computers. *Parallel Computing*, 15(1–3):155–164, September 1990. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

DeArman:1990:IRN

[1504] James DeArman. Improving random number generators on microcomputers. *Computers and Operations Research*, 17(3):283–295, ????

1990. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/030505489090005R`.

DeMatteis:1990:CPR

[1505] A. De Matteis and S. Pagnutti. A class of parallel random number generators. *Parallel Computing*, 13(2):193–198, February 1990. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

DeMatteis:1990:LRC

[1506] A. De Matteis and S. Pagnutti. Long-range correlations in linear and nonlinear random number generators. *Parallel Computing*, 14(2):207–210, June 1990. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Deng:1990:GUV

[1507] Lih-Yuan Deng and E. Olusegun George. Generation of uniform variates from several nearly uniformly distributed variables. *Communications in Statistics: Simulation and Computation*, 19(1):145–154, ???? 1990. CODEN CSSCDB. ISSN 0361-0918.

Doring:1990:ENZ

[1508] H. Döring. Erzeugung normalverteilter Zufallsszahlen mit 16-bit-PC. (German) [Generation of normally-distributed random numbers on an 16-bit PC]. *Nachrichtentechnik Elektronik*, 40(8):306–309, 1990. CODEN NTELAP. ISSN 0323-4657.

Eddy:1990:RNG

[1509] William F. Eddy. Random number generators for parallel processors. *Journal of Computational and Applied Mathematics*, 31(1):63–71, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090336X`. See [358, 1277] for combined generators.

Eichenauer-Herrmann:1990:LSN

[1510] J. Eichenauer-Herrmann, H. Grothe, H. Niederreiter, and A. Topuzoğlu. On the lattice structure of a nonlinear generator with modulus 2^α. *Journal of Computational and Applied Mathematics*, 31(1):81–85, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090338Z`.

Eichenauer-Herrmann:1990:PLC

[1511] J. Eichenauer-Herrmann and A. Topuzoğlu. On the period length of congruential pseudorandom number sequences generated by inversions. *Journal of Computational and Applied Mathematics*, 31(1):87–96, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903392`.

Eichenauer-Herrmann:1990:UBB

[1512] J. Eichenauer-Herrmann and H. Grothe. Upper bounds for the Beyer ratios of linear congruential generators. *Journal of Computational and Applied Mathematics*, 31(1):73–80, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090337Y`. Random numbers and simulation (Lambrecht, 1988).

Ermakov:1990:LTT

[1513] S. M. Ermakov and V. V. Dovgal. Limit theorems for the Tausworthe randomizer. *Vestnik Leningradskogo Universiteta. Matematika*, 23(1): 105–106, ???? 1990. CODEN ???? ISSN 0024-0850.

Etzion:1990:PRA

[1514] T. Etzion. On pseudo-random arrays constructed from patterns with distinct differences. In Capocelli [4150], pages 195–207. ISBN 3-540-97186-6 (Berlin), 0-387-97186-6 (New York). LCCN QA292 A38 1988.

Faure:1990:UPR

[1515] H. Faure. Using permutations to reduce discrepancy. *Journal of Computational and Applied Mathematics*, 31(1):97–103, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903406`.

Filippone:1990:VLS

[1516] Salvatore Filippone, Paolo Santangelo, and Marcello Vitaletti. A vectorized long-period shift-register random number generator. In IEEE [4153], pages 676–684. ISBN 0-8186-2056-0 (paperback) (IEEE Computer Society), 0-89791-412-0 (paperback) (ACM). LCCN QA 76.88 S87 1990. ACM order number 415903. IEEE Computer Society Press order number 2056. IEEE catalog number 90CH2916-5.

Fishman:1990:MCR

[1517] George S. Fishman. Multiplicative congruential random number generators with modulus 2^β: An exhaustive analysis for $\beta \simeq 32$ and a partial

analysis for $\beta \simeq 48$. *Mathematics of Computation*, 54(189):331–344, January 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2008698`.

Flury:1990:ARS

[1518] Bernard D. Flury. Acceptance-rejection sampling made easy. *SIAM Review*, 32(3):474–476, September 1990. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Fruit:1990:PRN

[1519] Robert Fruit. A pseudo-random number generator. *C Users Journal*, 8 (5):83–??, May 1990. CODEN ???? ISSN 0898-9788.

Fushimi:1990:RNG

[1520] Masanori Fushimi. Random number generation with the recursion $X_t = X_{t-3p} \oplus X_{t-3q}$. *Journal of Computational and Applied Mathematics*, 31(1):105–118, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090341V`.

Gentle:1990:CIR

[1521] James E. Gentle. Computer implementation of random number generators. *Journal of Computational and Applied Mathematics*, 31(1):119–125, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090342W`. See comments [1779].

Gleason:1990:ETI

[1522] John M. Gleason. Empirical tests of the intrinsic pseudorandom number generator on IBM-compatible microcomputers. *Computer Methods and Programs in Biomedicine*, 33(3):171–174, December 1990. CODEN CMPBEK. ISSN 0169-2607 (print), 1872-7565 (electronic).

Goldreich:1990:NCI

[1523] Oded Goldreich. A note on computational indistinguishability. *Information Processing Letters*, 34(6):277–281, May 28, 1990. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Goldreich:1990:SPD

[1524] Oded Goldreich and Hugo Krawczyk. Sparse pseudorandom distributions (extended abstract). *Lecture Notes in Computer Science*, 435:113–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350113.htm; http://link.springer-ny.com/link/service/series/0558/papers/0435/04350113.pdf.

Golland:1990:BRB

[1525] Ronald W. Golland. Book review: *Principles of Random Variate Generation* by John Dagpunar. *Technometrics*, 32(2):226–227, May 1990. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL http://www.jstor.org/stable/1268875.

Granville:1990:NTR

[1526] V. Granville and J.-P. Rasson. A new type of random permutations generator to simulate random images. *Computational Statistics Quarterly*, 6(1):55–64, 1990. CODEN CSQUEM. ISSN 0723-712X.

Haastad:1990:PRG

[1527] J. Håstad. Pseudo-random generators under uniform assumptions. In ACM [4148], pages 395–404. ISBN 0-89791-361-2. LCCN QA76.A15 1990. URL http://www.acm.org/pubs/citations/proceedings/stoc/100216/p395-hastad/. ACM order number 508900.

Hildebrand:1990:RCS

[1528] M. Hildebrand. *Rates of convergence of some random processes on finite groups*. Ph.D. dissertation, Department of Mathematics, Harvard University, Cambridge, MA, USA, 1990.

Hormann:1990:AMG

[1529] Wolfgang Hörmann and Gerhard Derflinger. The ACR method for generating normal random variables. *OR Spektrum: Quantitative approaches in management*, 12(??):181–185, ???? 1990. ISSN 0171-6468 (print), 1436-6304 (electronic).

Hortensius:1990:CAC

[1530] P. D. Hortensius, R. D. McLeod, and B. W. Podaima. Cellular automata circuits for built-in self-test. *IBM Journal of Research and Development*, 34(2/3):389–405, March/May 1990. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Ito:1990:MCS

[1531] N. Ito and Y. Kanada. Monte Carlo simulation of the Ising model and random number generation on the vector processor. In IEEE [4153], pages 753–763. ISBN 0-8186-2056-0 (paperback) (IEEE Computer Society), 0-89791-412-0 (paperback) (ACM). LCCN QA 76.88 S87 1990.

ACM order number 415903. IEEE Computer Society Press order number 2056. IEEE catalog number 90CH2916-5.

Ito:1990:RNG

[1532] N. Ito and Y. Kanada. Random number generation on a vector processor. *Supercomputer*, 7(1):29–35, January 1990. CODEN SPCOEL. ISSN 0168-7875.

James:1990:RPN

[1533] F. James. A review of pseudorandom number generators. *Computer Physics Communications*, 60(3):329–344, October 1990. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559090032V`.

Jansen:1990:SFS

[1534] Cees J. A. Jansen and Dick E. Boekee. The shortest feedback shift register that can generate a given sequence. *Lecture Notes in Computer Science*, 435:90–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350090.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0435/04350090.pdf`.

Joe:1990:RLR

[1535] S. Joe. Randomization of lattice rules for numerical multiple integration. *Journal of Computational and Applied Mathematics*, 31(2):299–304, August 31, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090172V`.

Johnson:1990:SDC

[1536] Bruce R. Johnson and David J. Leeming. A study of the digits of π, e, and certain other irrational numbers. *Sankhyā (Indian Journal of Statistics), Series B. Methodological*, 52(2):183–189, ???? 1990. CODEN SANBBV. ISSN 0976-8386 (print), 0976-8394 (electronic).

Just:1990:IRA

[1537] Bettina Just. Integer relations among algebraic numbers. *Mathematics of Computation*, 54(189):467–477, January 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Kao:1990:RNG

[1538] Chiang Kao. On a random-number generator for microcomputers: Reply. *OR: the journal of the Operational Research Society*, 41(12):1193,

December 1990. CODEN OPRQAK. ISSN 0160-5682 (print), 1476-9360 (electronic). URL `http://www.jstor.org/stable/2583127`. See [1448, 1581, 1609, 1633].

Kelton:1990:BRB

[1539] W. David Kelton. Book review: *Principles of Random Variate Generation* (John Dagpunar). *SIAM Review*, 32(3):508–511, ???? 1990. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Kemp:1990:BRB

[1540] C. David Kemp. Book review: *Principles of Random Variate Generation*, by J. Dagpunar. *Journal of the Royal Statistical Society. Series D (The Statistician)*, 39(4):472–473, ???? 1990. CODEN ???? ISSN 0039-0526 (print), 1467-9884 (electronic). URL `http://www.jstor.org/stable/2349098`.

Kemp:1990:NAG

[1541] C. D. Kemp. New algorithms for generating Poisson variates. *Journal of Computational and Applied Mathematics*, 31(1):133–137, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090344Y`.

Kemp:1990:PRA

[1542] A. W. Kemp. Patchwork rejection algorithms. *Journal of Computational and Applied Mathematics*, 31(1):127–131, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090343X`.

Kinderman:1990:CCG

[1543] A. J. Kinderman and J. G. Ramage. Correction: Computer generation of normal random variables. *Journal of the American Statistical Association*, 85(409):272, March 1990. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2289582`. See [779] and further correction [2903].

Korolev:1990:ADR

[1544] V. Yu. Korolev. Approximation of distributions of random sums of independent random variables by mixtures of normal laws. *Theory of Probability and its Applications*, 34(3):523–531, ???? 1990. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **34**(3), (1989), pp. 581–588.

Koutras:1990:TCN

[1545] M. Koutras. Two classes of numbers appearing in the convolution of binomial-truncated Poisson and Poisson-truncated binomial random variables. *Fibonacci Quarterly*, 28(4):321–333, November 1990. CODEN FIBQAU. ISSN 0015-0517. URL `http://www.fq.math.ca/Scanned/28-4/koutras.pdf`.

Krawczyk:1990:HPC

[1546] Hugo Krawczyk. How to predict congruential generators. *Lecture Notes in Computer Science*, 435:138–153, 1990. CODEN LNCSD9. ISBN 0-387-97317-6 (NY), 3-540-97317-6 (Berlin). ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350138.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0435/04350138.pdf`.

Lagarias:1990:PNG

[1547] J. C. Lagarias. Pseudorandom number generators in cryptography and number theory. In Pomerance and Goldwasser [4154], pages 115–143. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Abridged and revised version of [1547].

LEcuyer:1990:RNS

[1548] Pierre L'Ecuyer. Random numbers for simulation. *Communications of the ACM*, 33(10):85–97, October 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/84555.html`.

LEcuyer:1990:UVW

[1549] P. L'Ecuyer. A unified view of the WA, SF, and LR gradient estimation techniques. *Management Science*, 36(??):1364–1383, ???? 1990. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Levitan:1990:PNG

[1550] Yu. L. Levitan and I. M. Sobol. On a pseudorandom number generator for personal computers. *Matematicheskoe Modelirovanie*, 2(8):119–126, ???? 1990. CODEN ???? ISSN 0234-0879.

Lutz:1990:PSB

[1551] Jack H. Lutz. Pseudorandom sources for BPP. *Journal of Computer and System Sciences*, 41(3):307–320, December 1990. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002200009090023E`.

Macomber:1990:DUR

[1552] James H. Macomber and Charles S. White. An n-dimensional uniform random number generator suitable for IBM-compatible microcomputers. *Interfaces*, 20(3):49–59, 1990. CODEN INFAC4. ISSN 0092-2102 (print), 1526-551X (electronic).

Marsaglia:1990:DBR

[1553] George Marsaglia, B. Narasimhan, and Arif Zaman. The distance between random points in rectangles. *Communications in Statistics: Theory and Methods*, 19(11):4199–4212, 1990. CODEN CSTMDC. ISSN 0361-0926 (print), 1532-415X (electronic).

Marsaglia:1990:RNG

[1554] George Marsaglia, B. Narasimhan, and Arif Zaman. A random number generator for PC's. *Computer Physics Communications*, 60(3):345–349, October 1990. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559090033W`.

Marsaglia:1990:TUR

[1555] George Marsaglia, Arif Zaman, and Wai Wan Tsang. Toward a universal random number generator. *Statistics & Probability Letters*, 9(1):35–39, 1990. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Maurer:1990:PLR

[1556] Ueli M. Maurer and James L. Massey. Perfect local randomness in pseudo-random sequences. *Lecture Notes in Computer Science*, 435:100–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350100.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0435/04350100.pdf`.

Micali:1990:EPR

[1557] Silvio Micali and Claus-Peter Schnorr. Efficient, perfect random number generators. In Goldwasser [4151], pages 173–198. CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403`.

Mitchell:1990:EEA

[1558] Ricardo A. Mitchell. Error estimates arising from certain pseudorandom sequences in a quasi-random search method. *Mathematics of Computation*, 55(191):289–297, July 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008806.pdf`.

Mitchell:1990:NKG

[1559] Douglas W. Mitchell. Nonlinear key generators. *Cryptologia*, 14(4):350–354, October 1990. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). key generators; nonlinear generation; key sequences; chaos-based approach; simulations; desirable properties.

Morris:1990:NLM

[1560] Alfred H. Morris, Jr. NSWC library of mathematics subroutines. Report NSWC TR 90-21, Naval Surface Warfare Center, Dahlgren, VA 22448-5000, USA; Silver Spring, MD 20903-5000, USA, January 1990. xii + 492 + 9 pp. URL `https://apps.dtic.mil/sti/citations/ADA476840`; `https://apps.dtic.mil/sti/pdfs/ADA476840.pdf`; `https://people.math.sc.edu/Burkardt/f_src/nswc/nswc.f90`; `https://people.math.sc.edu/Burkardt/f_src/nswc/nswc.html`. See also later edition [1861].

Naor:1990:BCU

[1561] Moni Naor. Bit commitment using pseudo-randomness (extended abstract). *Lecture Notes in Computer Science*, 435:128–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350128.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0435/04350128.pdf`.

Naor:1990:SPS

[1562] Joseph Naor and Moni Naor. Small-bias probability spaces. efficient constructions and applications. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (May 14–16 1990: Baltimore, MD, USA)*, pages 213–223. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN QA75.5 .A14.

Niederreiter:1990:CAP

[1563] Harald Niederreiter. Combinatorial approach to probabilistic results on the linear-complexity profile of random sequences. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2

(2):105–112, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Niederreiter:1990:LBD

[1564] Harald Niederreiter. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Mathematics of Computation*, 55 (191):277–287, July 1990. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2008805.pdf`.

Niederreiter:1990:PNG

[1565] Harald Niederreiter. Pseudorandom numbers generated from shift register sequences. *Lecture Notes in Mathematics*, 1452:165–177, 1990. CODEN LNMAA2. ISBN 3-540-53408-3 (print), 3-540-46864-1 (e-book). ISSN 0075-8434 (print), 1617-9692 (electronic). URL `http://link.springer.com/chapter/10.1007/BFb0096988/`.

Niederreiter:1990:SIP

[1566] H. Niederreiter. Statistical independence properties of pseudorandom vectors produced by matrix generators. *Journal of Computational and Applied Mathematics*, 31(1):139–151, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903 45Z`.

Nisan:1990:PGS

[1567] N. Nisan. Pseudorandom generators for space-bounded computations. In ACM [4148], pages 204–212. ISBN 0-89791-361-2. LCCN QA76.A15 1990. URL `http://www.acm.org/pubs/citations/proceedings/stoc/100216/p204-nisan/`. ACM order number 508900.

Norton:1990:AAE

[1568] G. H. Norton. On the asymptotic analysis of the Euclidean algorithm. *Journal of Symbolic Computation*, 10(1):53–58, July 1990. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Oommen:1990:GRP

[1569] B. J. Oommen and D. T. H. Ng. On generating random permutations with arbitrary distributions. *The Computer Journal*, 33(4): 368–374, August 1990. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/368.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/369.tif`; `http://www3.oup.co.uk/computer_journal/hdb/Volume_33/`

Issue_04/tiff/370.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/371.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/372.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/373.tif; http://www3.oup.co.uk/computer_journal/hdb/Volume_33/Issue_04/tiff/374.tif.

Oyanagi:1990:SPR

[1570] Yoshio Oyanagi, Eiichi Goto, and N. Yoshida. Supercomputing pseudo random numbers: proposals on hardware and software. Technical report 90-012, University of Tokyo, Faculty of Science, Dept. of Information Science, Tokyo, Japan, April 1990. 6 pp.

Palmore:1990:CAC

[1571] J. Palmore and C. Herring. Computer arithmetic, chaos and fractals. *Physica D, Nonlinear phenomena*, 42(1–3):99–110, June 1990. CODEN PDNPDT. ISSN 0167-2789 (print), 1872-8022 (electronic). Ninth Annual International Conference of the Center for Nonlinear Studies on Self-Organizing, Collective and Cooperative Phenomena in Natural and Artificial Networks.

Parrish:1990:GRD

[1572] Rudolph S. Parrish. Generating random deviates from multivariate Pearson distributions. *Computational Statistics & Data Analysis*, 9(3):283–295, May 1990. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL http://www.sciencedirect.com/science/article/pii/0167947390901104.

Ripley:1990:TPN

[1573] B. D. Ripley. Thoughts on pseudorandom number generators. *Journal of Computational and Applied Mathematics*, 31(1):153–163, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/0377042790903462.

Roggeman:1990:VFS

[1574] Yves Roggeman. Varying feedback shift registers. *Lecture Notes in Computer Science*, 434:670–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340670.htm; http://link.springer-ny.com/link/service/series/0558/papers/0434/04340670.pdf.

Rozovskii:1990:PLD

[1575] L. V. Rozovskiĭ. Probabilities of large deviations of sums of independent random variables with common distribution function in the domain of attraction of the normal law. *Theory of Probability and its Applications*, 34(4):625–644, ???? 1990. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **34**(4), (1989), pp. 686–705.

Rueppel:1990:SSP

[1576] Rainer A. Rueppel. On the security of Schnorr's pseudo random generator. *Lecture Notes in Computer Science*, 434:423–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340423.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0434/04340423.pdf`.

Sarno:1990:GDR

[1577] R. Sarno, V. C. Bhavsar, and E. M. A. Hussein. Generation of discrete random variables on vector computers for Monte Carlo simulations. *International Journal of High Speed Computing (IJHSC)*, 2(4):335–350, December 1990. CODEN IHSCEZ. ISSN 0129-0533.

Schmeiser:1990:NCI

[1578] Bruce Schmeiser and Vorats Kachitvichyanukul. Noninverse correlation induction: guidelines for algorithm development. *Journal of Computational and Applied Mathematics*, 31(1):173–180, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic).

Schnorr:1990:EPR

[1579] C. P. Schnorr S. Micali. Efficient perfect random number generators. In Goldwasser [4151], pages 173–?? CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403`.

Sezgin:1990:FPU

[1580] Fatin Sezgin. On a fast and portable uniform quasi-random number generator. *ACM SIGSIM Simulation Digest*, 21(2):30–36, December 1990. ISSN 0163-6103 (print), 2330-9083 (electronic). URL `http://doi.acm.org/10.1145/382264.382434`.

Sezgin:1990:RNG

[1581] Fatin Sezgin. On a random-number generator for microcomputers. *OR: the journal of the Operational Research Society*, 41(12):1191–1193, December 1990. CODEN OPRQAK. ISSN 0160-5682 (print), 1476-9360 (electronic). URL `http://www.jstor.org/stable/2583126`. See [1448, 1538, 1609, 1633].

Sherif:1990:DNC

[1582] Y. S. Sherif and R. G. Dear. Development of a new composite pseudorandom number generator. *Microelectronics and Reliability*, 30(??):545–553, ???? 1990. CODEN MCRLAS. ISSN 0026-2714 (print), 1872-941X (electronic).

Sobol:1990:QMC

[1583] I. M. Sobol'. Quasi-Monte Carlo methods. *Progress in Nuclear Energy*, 24(??):55–61, ???? 1990. CODEN PNENDE. ISSN 0149-1970 (print), 1878-4224 (electronic).

Stadlober:1990:RUA

[1584] Ernst Stadlober. The ratio of uniforms approach for generating discrete random variates. *Journal of Computational and Applied Mathematics*, 31(1):181–189, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903495`.

Tezuka:1990:LSP

[1585] Shu Tezuka. Lattice structure of pseudorandom sequences from shift-register generators. In Balci et al. [4149], pages 266–269. ISBN 0-911801-72-3. LCCN QA76.5.W56 1990.

Tezuka:1990:NFL

[1586] S. Tezuka. A new family of low-discrepancy point sets. Report RT-0031, IBM Research, Tokyo Research Laboratory, Tokyo, Japan, January 1990.

Tichy:1990:RPC

[1587] Robert F. Tichy. Random points in the cube and on the sphere with applications to numerical analysis. *Journal of Computational and Applied Mathematics*, 31(1):191–197, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042790903509`.

Tindo:1990:ACA

[1588] G. Tindo. *Automates cellulaires: applications à la modélisation de certains systèmes discrets et à la conception d'une architecture parallèle pour la génération de suites pseudo-aléatoires. (French) [Cellular automata: applications to the modeling of certain discrete systems and toward the design of a parallel architecture for generation of random sequences]*. Dissertation (thesis), Université de Nantes, Nantes, France, 1990.

Traub:1990:MCA

[1589] J. F. Traub and H. Wozniakowski. The Monte Carlo algorithm with a pseudo-random generator. Technical Report TR-90-039, International Computer Science Institute, Berkeley, CA, August 1990.

vanderSteen:1990:PPG

[1590] A. van der Steen. Portable parallel generation of random numbers. *Supercomputer*, 7(1):18–20, January 1990. CODEN SPCOEL. ISSN 0168-7875.

Velizhanin:1990:MCS

[1591] V. A. Velizhanin, I. G. Dyadkin, F. Kh. Enikeeva, B. K. Zhuravlyov, B. E. Lukhminsky, and R. T. Khanatdinov. Monte Carlo simulation in nuclear geophysics — 1. Features of Monte Carlo algorithmic techniques for solving problems in borehole nuclear geophysics. *Nuclear Geophysics*, 4(B12):425–435, 2376, ???? 1990. ISSN 0969-8086 (print), 1878-6383 (electronic).

Vinogradova:1990:ECF

[1592] T. R. Vinogradova. Estimation of characteristic functions of functionals of multidimensional Gaussian random variables. *Theory of Probability and its Applications*, 34(2):318–321, ???? 1990. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **34**(2), (1989), pp. 360–364.

Wallace:1990:PRG

[1593] C. S. Wallace. Physically random generator. *Computer Systems Science and Engineering*, 5(2):82–88, April 1990. CODEN CSSEEI. ISSN 0267-6192.

Wang:1990:DRV

[1594] Y. H. Wang. Dependent random variables with independent subsets. II. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 33(??):24–28, ???? 1990. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Wang:1990:VDC

[1595] C. C. Wang and D. Pei. A VLSI design for computing exponentiations in GF(2^m) and its application to generate pseudorandom number sequences. *IEEE Transactions on Computers*, 39(2):258–262, February 1990. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=45211`.

Williamson:1990:PAN

[1596] R. C. Williamson and T. Downs. Probabilistic arithmetic. I. numerical methods for calculating convolutions and dependency bounds. *International Journal of Approximate Reasoning*, 4(2):89–158, March 1990. CODEN IJARE4. ISSN 0888-613x (print), 1873-4731 (electronic).

Wolff:1990:AFM

[1597] Ulli Wolff. Asymptotic freedom and mass generation in the O(3) nonlinear σ-model. *Nuclear Physics B*, 334(3):581–610, April 23, 1990. CODEN NUPBBO. ISSN 0550-3213 (print), 1873-1562 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0550321390903133`.

Wong:1990:RNG

[1598] P. W. Wong. Random number generation without multiplication. In *Ninth Annual International Phoenix Conference on Computers and Communications, March 21–23, 1990. Proceedings*, pages 217–221. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2030-7 (paperback), 0-8186-6030-9 (microfiche), 0-8186-9030-5 (case). LCCN TK7885.A1 I567 1990. IEEE catalog number 90CH2799-5. IEEE Computer Society order number 2030.

Yeh:1990:ODT

[1599] Hsiaw-Chan Yeh. One discrete time series model for fat-tailed integer random variables: Zipf process. *Bull. Inst. Math. Acad. Sinica*, 18(1):19–33, 1990. CODEN BIMSDG. ISSN 0304-9825.

Zielinski:1990:APN

[1600] Ryszard Zieliński. An aperiodic pseudorandom number generator. *Journal of Computational and Applied Mathematics*, 31(1):205–210, July 24, 1990. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279090352Z`.

Akopov:1991:MGP

[1601] N. Z. Akopov, G. K. Savvidy, and N. G. Ter-Arutyunyan-Savvidy. Matrix generator of pseudorandom numbers. *Journal of Computational Physics*, 97(2):573–579, December 1991. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002199919190016E`.

Anastasio:1991:OCL

[1602] Thomas A. Anastasio and William W. Carlson. An observation on the C library procedure `random()`. Technical report SRC-TR-91-044, Supercomputing Research Center: IDA, Lanham, MD, USA, September 25, 1991. 6 pp.

Arno:1991:SDR

[1603] Steven Arno and Ferrell S. Wheeler. Signed digit representations of minimal Hamming weight. Technical report SRC-TR-91-046, Supercomputing Research Center: IDA, Lanham, MD, USA, July 1991. 18 pp.

Bays:1991:GRN

[1604] Carter Bays and W. E. Sharp. Generating random numbers in the field. *Mathematical Geology*, 23(??):541–548, ???? 1991. CODEN MATGED. ISSN 0882-8121 (print), 1573-8868 (electronic).

Berblinger:1991:MCI

[1605] Michael Berblinger and Christoph Schlier. Monte Carlo integration with quasi-random numbers: some experience. *Computer Physics Communications*, 66(2–3):157–166, September/October 1991. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559190064R`.

Berdnicov:1991:MCS

[1606] A. S. Berdnicov and S. B. Turtia. Monte-Carlo simulation artefacts in physical modeling due to pseudo-random generators. *International Journal of Modern Physics C [Physics and Computers]*, 2(1): 244–249, April 1991. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/02/0201/S0129183191000263.html`.

Bittner:1991:NSP

[1607] Leonhard Bittner. A numerical sampling problem and the Weyl pseudorandom numbers. *Numerische Mathematik*, 59(7):637–645, October 1991. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).

Chambers:1991:SEM

[1608] W. G. Chambers and Z. D. Dai. Simple but effective modification to a multiplicative congruential random-number generator. *IEE proceedings, E: Computers and digital techniques*, 138(3):121–122, May 1991. CODEN IPETD3. ISSN 0143-7062.

Clementson:1991:CRN

[1609] Alan T. Clementson. A comment on a random-number generator for microcomputers. *OR: the journal of the Operational Research Society*, 42(2):193, February 1991. CODEN OPRQAK. ISSN 0160-5682 (print), 1476-9360 (electronic). URL `http://www.jstor.org/stable/2583193`. See [1448, 1581, 1538, 1633].

Compagner:1991:DR

[1610] Aaldert Compagner. Definitions of randomness. *American Journal of Physics*, 59(8):700–705, August 1991. CODEN AJPIAS. ISSN 0002-9505 (print), 1943-2909 (electronic). URL `http://m.ajp.aapt.org/resource/1/ajpias/v59/i8/p700_s1`.

Compagner:1991:HCR

[1611] Aaldert Compagner. The hierarchy of correlations in random binary sequences. *Journal of Statistical Physics*, 63(5–6):883–896, June 1991. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL `http://link.springer.com/article/10.1007/BF01029989`.

Deng:1991:CRN

[1612] Lih-Yuan Deng and Yu-Chao Chu. Combining random number generators. In Nelson et al. [4158], pages 1043–1046. CODEN WSCPDK. ISBN 0-7803-0181-1. ISSN 0275-0708, 0743-1902. LCCN QA 76.9 C65 W56 1991. IEEE catalog number 91CH3050-2.

Deng:1991:RDR

[1613] L. Y. Deng and C. Rousseau. Recent development in random number generation. In Day [4156], pages 89–94. ISBN 0-89791-388-4. LCCN ????

Devroye:1991:AGD

[1614] Luc Devroye. Algorithms for generating discrete random variables with a given generating function or a given moment sequence. *SIAM Journal on Scientific and Statistical Computing*, 12(1):107–126, January 1991. CODEN SIJCD4. ISSN 0196-5204.

Devroye:1991:ETA

[1615] Luc Devroye. Expected time analysis of a simple recursive Poisson random variate generator. *Computing: Archiv für Informatik und Numerik*, 46(2):165–173, June 1991. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Dohmann:1991:RNG

[1616] Birgit Dohmann, Michael Falk, and Karin Lessenich. The random number generators of the Turbo Pascal family. *Computational Statistics & Data Analysis*, 12(1):129–132, August 1991. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/016794739190108E`.

Dunweg:1991:BDS

[1617] Burkhard Dünweg and Wolfgang Paul. Brownian dynamics simulations without Gaussian random numbers. *International Journal of Modern Physics C [Physics and Computers]*, 2(3):817–827, September 1991. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/02/0203/S0129183191001037.html`.

Eichenauer-Herrmann:1991:ASI

[1618] J. Eichenauer-Herrmann. On the autocorrelation structure of inversive congruential pseudorandom number sequences. Technical Report 1384, Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Germany, 1991. 9 pp.

Eichenauer-Herrmann:1991:CCP

[1619] J. Eichenauer-Herrmann. Cubic congruential pseudorandom numbers for simulation. Technical Report 1399, Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Germany, 1991. 13 pp.

Eichenauer-Herrmann:1991:CIC

[1620] Jürgen Eichenauer-Herrmann. Construction of inversive congruential pseudorandom number generators with maximal period length. Technical Report 1363, Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Germany, 1991. 10 pp.

Eichenauer-Herrmann:1991:DIC

[1621] Jürgen Eichenauer-Herrmann. On the discrepancy of inversive congruential pseudorandom numbers with prime power modulus. *Manuscripta Mathematica*, 71(2):153–161, 1991. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Eichenauer-Herrmann:1991:DQC

[1622] Jürgen Eichenauer-Herrmann and Harald Niederreiter. On the discrepancy of quadratic congruential pseudorandom numbers. *Journal of Computational and Applied Mathematics*, 34(2):243–249, April 4, 1991. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279190046M`.

Eichenauer-Herrmann:1991:ICPa

[1623] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. Technical Report 1405, Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Germany, 1991. 21 pp.

Eichenauer-Herrmann:1991:ICPb

[1624] Jürgen Eichenauer-Herrmann. Inversive congruential pseudorandom numbers avoid the planes. *Mathematics of Computation*, 56(193):297–301, January 1991. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2008543`.

Eichenauer-Herrmann:1991:NIC

[1625] J. Eichenauer-Herrmann and H. Grothe. A new inversive congruential pseudorandom number generator with power of two modulus. Technical Report 1392, Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Germany, 1991. 13 pp.

Geers:1991:HEB

[1626] N. Geers and W. Walde. Highly efficient basic numerical software for supercomputers. *Supercomputer*, 8(6):136–145, November 1991. CODEN SPCOEL. ISSN 0168-7875.

Gerasimov:1991:NOH

[1627] V. A. Gerasimov, B. S. Dobronets, and M. Yu. Shustrov. Numerical operations of histogram arithmetic and their applications. *Automation and Remote Control*, 52(2):83–88, February 1991. CODEN AVTEAI. ISSN 0005-2310 (print), 2413-9777 (electronic).

Gupta:1991:PAT

[1628] Anurag Gupta, Ian Akyildiz, and Richard M. Fujimoto. Performance analysis of Time Warp with homogeneous processors and exponential task times. *ACM SIGMETRICS Performance Evaluation Review*, 19 (1):101–110, May 1991. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Hultquist:1991:GRN

[1629] Paul F. Hultquist. A good random number generator for microcomputers. *Simulation*, 57(4):258–259, ???? 1991. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/57/4/258`.

Ito:1991:PEU

[1630] N. Ito and Y. Kanada. Performance evaluation using random number generator and Ising Monte Carlo simulation — the application-based benchmark Test(AbBT). In Anonymous [4155], pages 253–257. ISBN 4-87378-284-8. LCCN QA76.88.I1991.

Jumarie:1991:QEN

[1631] Guy Jumarie. Quantum entropies of nonprobabilistic matrices. *Journal of Mathematical Physics*, 32(11):2967–2971, November 1991. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v32/i11/p2967_s1`.

Kaliski:1991:OWP

[1632] Burton S. Kaliski, Jr. One-way permutations on elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3):187–199, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kao:1991:CRN

[1633] Chiang Kao. A comment on a random-number generator for microcomputers: Response. *OR: the journal of the Operational Research Society*, 42(2):193, February 1991. CODEN OPRQAK. ISSN 0160-5682 (print), 1476-9360 (electronic). URL `http://www.jstor.org/stable/2583194`. See [1448, 1581, 1609].

Kemp:1991:PRV

[1634] C. D. Kemp and Adrienne W. Kemp. Poisson random variate generation. *Applied Statistics*, 40(1):143–158, 1991. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Koen:1991:ACB

[1635] Chris Koen. Approximate confidence bounds for Ripley's statistic for random points in a square. *Biometrical Journal*, 33(2):173–177, ???? 1991. CODEN BIJODN. ISSN 0323-3847. URL `http://onlinelibrary.wiley.com/doi/10.1002/bimj.4710330206/abstract`. See correction [3081].

Komo:1991:DPR

[1636] John J. Komo and William J. Park, Jr. Decimal pseudo-random number generator. *Simulation*, 57(4):228–230, October 1991. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/57/4/228.abstract`.

Lai:1991:PNB

[1637] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In *Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990)*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1991. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0473/04730389.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0473/04730389.pdf`. See [3443] for proofs of requirements on the number of rounds.

Law:1991:SMA

[1638] Averill M. Law and W. David Kelton. *Simulation modeling and analysis*. McGraw-Hill series in industrial engineering and management science. McGraw-Hill, New York, NY, USA, second edition, 1991. ISBN 0-07-100803-9, 0-07-036698-5. xxii + 759 + 2 pp. LCCN QA76.9.C65 L38 1991. URL `http://www.loc.gov/catdir/enhancements/fy0602/90042969-b.html`; `http://www.loc.gov/catdir/enhancements/fy0602/90042969-d.html`; `http://www.loc.gov/catdir/enhancements/fy0602/90042969-t.html`.

LEcuyer:1991:IRN

[1639] Pierre L'Ecuyer and Serge Côté. Implementing a random number package with splitting facilities. *ACM Transactions on Mathematical Software*, 17(1):98–111, March 1991. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/103147.103158`; `http://www.acm.org/pubs/citations/journals/toms/1991-17-1/p98-lecuyer/`.

LEcuyer:1991:SPT

[1640] Pierre L'Ecuyer and Shu Tezuka. Structural properties for two classes of combined random number generators. *Mathematics of Computation*, 57(196):735–746, October 1991. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Luby:1991:PRG

[1641] Michael Luby. Pseudo-random generators from one-way functions (invited abstract). *Lecture Notes in Computer Science*, 576:300–??,

1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760300.htm; http://link.springer-ny.com/link/service/series/0558/papers/0576/05760300.pdf.

Maier:1991:FPR

[1642] William L. Maier. A fast pseudo random number generator. *Dr. Dobb's Journal of Software Tools*, 16(5):152, 154–157, May 1991. CODEN DDJOEB. ISSN 1044-789X.

Makino:1991:GSR

[1643] Jun Makino and Osamu Miyamura. Generation of shift register random numbers on vector processors. *Computer Physics Communications*, 64(3):363–368, June 1991. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/0010465591901325.

Marsaglia:1991:NCR

[1644] George Marsaglia and Arif Zaman. A new class of random number generators. *Annals of Applied Probability*, 1(3):462–480, August 1991. CODEN ???? ISSN 1050-5164 (print), 2168-8737 (electronic). URL http://projecteuclid.org/euclid.aoap/1177005878. See popular description in [1660]. See remarks in [2046, 1883] about the extremely bad lattice structure in high dimensions of the generators proposed in this paper.

Marsaglia:1991:NGR

[1645] George Marsaglia. Normal (Gaussian) random variables for supercomputers. *The Journal of Supercomputing*, 5(1):49–55, June 1991. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=5&issue=1&spage=49.

Matus:1991:AFD

[1646] F. Matus. Abstract functional dependency structures. *Theoretical Computer Science*, 81(1):117–126, April 22, 1991. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Maurer:1991:LRP

[1647] U. M. Maurer and J. L. Massey. Local randomness in pseudorandom sequences. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2):135–149, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1991:UST

[1648] Ueli M. Maurer. A universal statistical test for random bit generators. *Lecture Notes in Computer Science*, 537:409–420, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0537/05370409.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0537/05370409.pdf`.

McInnes:1991:IPK

[1649] J. L. McInnes and B. Pinkas. On the impossibility of private key cryptography with weakly random keys. *Lecture Notes in Computer Science*, 537:421–??, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Melamed:1991:TCM

[1650] Benjamin Melamed. TES: A class of methods for generating autocorrelated uniform variates. *ORSA Journal on Computing*, 3(4):317–329, 1991. CODEN OJCOE3. ISSN 0899-1499 (print), 2326-3245 (electronic).

Micali:1991:EPP

[1651] Silvio Micali and Claus-Peter Schnorr. Efficient, perfect polynomial random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3):157–172, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Mulmuley:1991:FPP

[1652] Ketan Mulmuley. A fast planar partition algorithm, II. *Journal of the ACM*, 38(1):74–103, January 1991. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/102785.html`.

Naor:1991:BCU

[1653] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2):151–158, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Niederreiter:1991:FFT

[1654] Harald Niederreiter. Finite fields and their applications. In Dorninger [4157], pages 251–264. ISBN 3-209-01380-2 (HPT), 3-519-02766-6 (Teubner). LCCN QA150 .C666 1991.

Niederreiter:1991:RTR

[1655] Harald Niederreiter. Recent trends in random number and random vector generation. *Annals of Operations Research*, 31(??):323–345, ???? 1991. CODEN AOREEV. ISSN 0254-5330 (print), 1572-9338 (electronic).

Oyanagi:1991:SPR

[1656] Y. Oyanagi, E. Goto, and N. Yoshida. Supercomputing pseudo random numbers — proposals on hardware and software. In Anonymous [4155], pages 97–98. ISBN 4-87378-284-8. LCCN QA76.88.I1991.

Papoulis:1991:PRV

[1657] Athanasios Papoulis. *Probability, random variables, and stochastic processes*. McGraw-Hill series in electrical engineering. Communications and signal processing. McGraw-Hill, New York, NY, USA, third edition, 1991. ISBN 0-07-048477-5. xvii + 666 pp. LCCN QA273 .P2 1991. US$54.95. URL `http://www.loc.gov/catdir/description/mh022/90023127.html`; `http://www.loc.gov/catdir/toc/mh021/90023127.html`.

Pardalos:1991:CTP

[1658] Panos M. Pardalos. Construction of test problems in quadratic bivalent programming. *ACM Transactions on Mathematical Software*, 17 (1):74–87, March 1991. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1991-17-1/p74-pardalos/`.

Patarin:1991:NRP

[1659] Jacques Patarin. New results on pseudorandom permutation generators based on the DES scheme. *Lecture Notes in Computer Science*, 576:301–213, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0576/05760301.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0576/05760301.pdf`.

Peterson:1991:NRN

[1660] Ivars Peterson. Numbers at random: Number theory supplies a superior random-number generator. *Science News (Washington, DC)*, 140(19): 300–301, November 9, 1991. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic). URL `http://www.jstor.org/stable/3975915`.

Pickover:1991:PRG

[1661] C. A. Pickover. Picturing randomness on a graphics supercomputer. *IBM Journal of Research and Development*, 35(1/2):227–230, January/March 1991. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Revello:1991:CEC

[1662] Timothy E. Revello. A combination of exponentiation ciphers and the data encryption standard as a pseudorandom number generator. Thesis (M.S.), Rensselaer Polytechnic Institute at The Hartford Graduate Center, Troy, NY, USA, 1991. viii + 68 pp.

Ritter:1991:EGC

[1663] Terry Ritter. The efficient generation of cryptographic confusion sequences. *Cryptologia*, 15(2):81–139, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://fizz.sys.uea.ac.uk/~rs/ritter.html`; `http://www.ciphersbyritter.com/ARTS/CRNG2ART.HTM`; `http://www.informaworld.com/smpp/content~content=a741902748~db=all~order=page`. cryptographic confusion sequences; pseudo-random sequence; random number generators; cryptographic applications; random sequences; incompleteness theorem; deterministic implementation; external analysis; RNG comparison; chaos; Čebyšev mixing; cellular automata; linear congruential; linear feedback shift register; nonlinear shift register; generalized feedback shift register; additive types; isolator mechanisms; one-way functions; combined sequences; random permutations; primitive mod 2 polynomials; empirical state-trajectory approach; RNG design analysis; GFSR.

Saarinen:1991:VIT

[1664] J. Saarinen, J. Tomberg, L. Vehmanen, and K. Kaski. VLSI implementation of Tausworthe random number generator for parallel processing environment. *IEE proceedings, E: Computers and digital techniques*, 138 (3):138–146, 1991. CODEN IPETD3. ISSN 0143-7062. URL `http://link.aip.org/link/?PET/138/138/1`.

Sadeghiyan:1991:COW

[1665] Babak Sadeghiyan and Józef P. Pieprzyk. A construction for one way hash functions and pseudorandom bit generators. *Lecture Notes in Computer Science*, 547:431–445, 1991. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0547/05470431.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0547/05470431.pdf`.

Savvidy:1991:MCS

[1666] G. K. Savvidy and N. G. Ter-Arutyunyan-Savvidy. On the Monte Carlo simulation of physical systems. *Journal of Computational Physics*, 97(2):566–572, December 1991. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002199919190015D`.

Schwartz:1991:NGM

[1667] Charles Schwartz. A new graphical method for encryption of computer data. *Cryptologia*, 15(1):43–46, January 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902742~db=all~order=page`. pseudorandom number generator; decryption; graphical method; encryption; computer data; text; pictures; binary files; graphically generated inversions; bit pattern; uncrackability.

Sezgin:1991:FPU

[1668] Fatin Sezgin. On a fast and portable uniform quasi-random number generator. *ACM Simuletter*, 21(2):30–36, 1991. CODEN SIMUD5. ISSN 0163-6103.

Tezuka:1991:EPC

[1669] Shu Tezuka and Pierre L'Ecuyer. Efficient and portable combined Tausworthe random number generators. *ACM Transactions on Modeling and Computer Simulation*, 1(2):99–112, April 1991. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Tonkin:1991:SB

[1670] Bruce W. Tonkin. Speedy buffering. *Dr. Dobb's Journal of Software Tools*, 16(3):52–53, March 1991. CODEN DDJOEB. ISSN 1044-789X.

Tsalides:1991:PNG

[1671] Ph. Tsalides, T. A. York, and A. Thanailakis. Pseudorandom number generators for VLSI systems based on linear cellular automata. *IEE proceedings, E: Computers and digital techniques*, 138(4):241–249, July 1991. CODEN IPETD3. ISSN 0143-7062.

Tyurin:1991:TRN

[1672] Yu. N. Tyurin and V. E. Figurnov. On the testing of random number generators. *Theory of Probability and its Applications*, 35(1):180–184, ???? 1991. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Ugrin-Sparac:1991:SIP

[1673] G. Ugrin-Šparac. Stochastic investigations of pseudo-random number generators. *Computing: Archiv für Informatik und Numerik*, 46(1):53–65, March 1991. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Vose:1991:LAG

[1674] Michael D. Vose. A linear algorithm for generating random numbers with a given distribution. *IEEE Transactions on Software Engineering*, 17(9):972–975, September 1991. CODEN IESEDJ. ISSN 0098-5589 (print), 1939-3520 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=92917`.

Wakefield:1991:EGR

[1675] J. C. Wakefield, A. E. Gelfand, and A. F. M. Smith. Efficient generation of random variates via the ratio-of-uniforms method. *Statistics and Computing*, 1(2):129–133, December 1991. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF01889987`; `http://www.springerlink.com/content/w1vt431r722p17j8/`.

Walsh:1991:MFR

[1676] John F. Walsh. Microsoft's FORTRAN 5.0 random number generator: be aware. *Perceptual and Motor Skills*, 72(1):257–??, February 1991. CODEN PMOSAZ. ISSN 0031-5125 (print), 1558-688x (electronic).

Wheeler:1991:PMN

[1677] Daniel D. Wheeler. Problems with Mitchell's nonlinear key generators. *Cryptologia*, 15(4):355–363, October 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902768~db=all~order=page`. pseudo random numbers; successive differences; nonlinear key generators; probable-word attack.

Wheeler:1991:SIC

[1678] Daniel D. Wheeler and Robert A. J. Matthews. Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, 15(2):140–152, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a741902749~db=all~order=page`. chaotic encryption algorithm; nonlinear pseudo-random number generator; chaos the-

ory; cycling keys; low-precision arithmetic; numerical investigation; Cray Y-MP machine; cycling problem.

Yamamoto:1991:NEM

[1679] H. Yamamoto. Note on the efficiency of methods to generate quasi-random sequences. *Systems and computers in Japan*, 22(??):385–365, ???? 1991. CODEN SCJAEP. ISSN 0882-1666 (print), 1520-684X (electronic).

Yang:1991:UCR

[1680] W.-N. Yang and B. L. Nelson. Using Common Random Numbers and control variates in multiple-comparison procedures. *Operations Research*, 39(??):583–591, ???? 1991. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

Zeng:1991:PBG

[1681] Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei, and T. R. N. Rao. Pseudorandom bit generators in stream-cipher cryptography. *Computer*, 24(2):8–17, February 1991. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Agrawal:1992:PAS

[1682] V. D. Agrawal and S. T. Chakradhar. Performance analysis of synchronized iterative algorithms on multiprocessor systems. *IEEE Transactions on Parallel and Distributed Systems*, 3(6):739–746, November 1992. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Aluru:1992:RNG

[1683] Srinivas Aluru, G. M. Prabhu, and John Gustafson. A random number generator for parallel computers. *Parallel Computing*, 18(8):839–847, August 1992. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Anastasio:1992:OCL

[1684] Thomas A. Anastasio and William W. Carlson. An observation on the C library procedure `random()`. *ACM SIGPLAN Notices*, 27(3):71–74, March 1992. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Anderson:1992:CRN

[1685] Ross Anderson. Chaos and random numbers. *Cryptologia*, 16(3):226, July 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Arno:1992:PSC

[1686] Steven Arno and Ken Iobst. The PETASYS supercomputer and a class of pseudo-random number generators. Technical report SRC-TR-92-069, Supercomputing Research Center: IDA, Lanham, MD, USA, April 1992. 29 pp.

Atkinson:1992:GBT

[1687] M. D. Atkinson and J. R. Sack. Generating binary trees at random. *Information Processing Letters*, 41(1):21–23, January 21, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Babai:1992:MPP

[1688] László Babai, Noam Nisant, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space tradeoffs. *Journal of Computer and System Sciences*, 45(2):204–232, October 1992. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/002200009290047M`.

Baker:1992:PPT

[1689] B. M. Baker and D. E. Handelman. Positive polynomials and time dependent integer-valued random variables. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 44(1):3–41, February 1992. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Bays:1992:IRN

[1690] Carter Bays and W. E. Sharp. Improved random numbers for your personal computer or workstation. *Geobyte*, 7(2):25–32, April 1992. ISSN 0885-6362.

Bellido:1992:SBR

[1691] M. J. Bellido, A. J. Acosta, M. Valencia, A. Barriga, and J. L. Huertas. Simple binary random number generator. *Electronics Letters*, 28(6):617–618, March 26, 1992. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=133026`.

Berdnikov:1992:RNG

[1692] A. S. Berdnikov, S. B. Tunia, and A. Compagner. Random-number generators: testing procedures and comparison of RNG algorithms. In Robert A. de Groot and Jaroslav Nadrhal, editors, *Physics computing*

'92: proceedings of the 4th international conference, Prague, Czechoslovakia, August 24–28, 1992, pages 264–265. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1992. ISBN 981-02-1245-3. LCCN QC20 .I45 1992.

Binder:1992:MCS

[1693] K. (Kurt) Binder and Dieter W. Heermann. *Monte Carlo simulation in statistical physics: an introduction*, volume 80 of *Springer series in solid state sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 1992. ISBN 3-540-55729-6 (Berlin), 0-387-55729-6 (New York). viii + 129 pp. LCCN QC174.85.M64 B55 1992.

Bratley:1992:ITL

[1694] Paul Bratley, Bennett L. Fox, and Harald Niederreiter. Implementation and tests of low-discrepancy sequences. *ACM Transactions on Modeling and Computer Simulation*, 2(3):195–213, July 1992. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Brenner:1992:PRL

[1695] N. Brenner and S. Fishman. Pseudo-randomness and localization. *Nonlinearity (Bristol)*, 5(1):211, 1992. CODEN NONLE5. ISSN 0951-7715 (print), 1361-6544 (electronic). URL `http://stacks.iop.org/0951-7715/5/i=1/a=009`.

Brent:1992:URN

[1696] R. P. Brent. Uniform random number generators for supercomputers. In ????, editor, *Supercomputing, the competitive advantage: proceedings of the Fifth Australian Supercomputing Conference, 5ASC Organising Committee, Melbourne, 1992*, pages 95–104. ????, ????, 1992. ISBN 0-86444-270-X. URL `http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pd/rpb132.pdf`.

Brickell:1992:CSR

[1697] E. F. Brickell and A. M. Odlyzko. Cryptanalysis: a survey of recent results. In Simmons [4164], pages 501–540. ISBN 0-87942-277-7. LCCN QA76.9.A25 C6678 1992. US$79.95. URL `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.pdf`; `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.ps`; `http://www.research.att.com/~amo/doc/arch/cryptanalysis.surv.tex`. IEEE order number: PC0271-7.

Brightwell:1992:TSP

[1698] Graham Brightwell, Teunis J. Ott, and Peter Winkler. Target shooting with programmed random variables. In ACM [4159], pages 691–698. ISBN 0-89791-511-9. LCCN QA76.A15 1992. URL http://www.acm.org/pubs/articles/proceedings/stoc/129712/p691-brightwell/p691-brightwell.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/129712/p691-brightwell/. ACM order number 508920.

Burgess:1992:FLC

[1699] N. Burgess and K. V. Lever. Fast linear congruential pseudorandom number generators using the Messerschmitt pipelining transformation. *IEE proceedings, E: Computers and digital techniques*, 139(2):131–133, 1992. CODEN IPETD3. ISSN 0143-7062.

Burton:1992:DRN

[1700] F. Warren Burton and Rex L. Page. Distributed random number generation. *Journal of Functional Programming*, 2(2):203–212, April 1992. CODEN JFPRES. ISSN 0956-7968 (print), 1469-7653 (electronic). URL https://www.cambridge.org/core/product/6D10F1D0A2FB7E66D5F746F6D0822D78.

Canfield:1992:RARa

[1701] E. H. Canfield, Jr. and J. A. Viecelli. Random access to a random number sequence. *Journal of Computational Physics*, 98(2):349, February 1992. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL http://www.sciencedirect.com/science/article/pii/002199919290164T.

Canfield:1992:RARb

[1702] E. H. Canfield, Jr. and J. A. Viecelli. Random access to a random number sequence. *Journal of Computational Physics*, 99(1):176–178, March 1992. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL http://www.sciencedirect.com/science/article/pii/0021999192902857.

Carroll:1992:CCE

[1703] John M. Carroll, Jeff Verhagen, and Perry T. Wong. Chaos in cryptography: The escape from the strange attractor. *Cryptologia*, 16(1):52–72, January 1992. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a741902824~db=all~order=page. cryptography; random characteristics; cipher system; pseudo-random number gen-

erators; random generators; Lorenz attractor; chaotic nature; strange attractor; key management; authentication protocols.

Collins:1992:RNG

[1704] J. J. Collins, M. Fanciulli, R. G. Hohlfeld, D. C. Finch, G. v. H. Sandri, and E. S. Shtatland. A random number generator based on the logit transform of the logistic variable. *Computers in Physics*, 6(6):630–??, November 1992. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.168442`.

Dai:1992:BSD

[1705] Zong Duo Dai. Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(3):193–207, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

DalleMolle:1992:HOC

[1706] J. W. Dalle Molle, M. J. Hinich, and D. J. Morrice. Higher-order cumulant spectral based statistical tests of pseudo random variate generators. In Swain [4166], pages 618–625. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

DeMatteis:1992:CCD

[1707] A. De Matteis, J. Eichenauer-Herrmann, and H. Grothe. Computation of critical distances within multiplicative congruential pseudorandom number sequences. *Journal of Computational and Applied Mathematics*, 39(1):49–55, February 28, 1992. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279290221I`.

DeMatteis:1992:CDP

[1708] A. De Matteis and S. Pagnutti. Critical distances in pseudorandom sequences generated with composite moduli. *International Journal of Computer Mathematics*, 43(??):189–196, ???? 1992. CODEN IJCMAT. ISSN 0020-7160.

Deng:1992:GLT

[1709] L.-Y. Deng, C. Rousseau, and Y. Yuan. Generalized Lehmer–Tausworthe random number generators. In Vouk et al. [4167], pages 108–115. ISBN 0-89791-506-2. LCCN QA75.5 .S69a 1992.

Deng:1992:RSN

[1710] L. Y. Deng and R. S. Chhikara. Robustness of some non-uniform random variate generators. *Statistica Neerlandica. Journal of the Netherlands Society for Statistics and Operations Research*, 46(2–3):195–207, July 1992. CODEN ???? ISSN 0039-0402 (print), 1467-9574 (electronic).

Deng:1992:SCU

[1711] Lih-Yuan Deng and E. Olusegun George. Some characterizations of the uniform distribution with applications to random number generation. *Annals of the Institute of Statistical Mathematics (Tokyo)*, 44 (2):379–385, June 1992. CODEN AISXAD. ISSN 0020-3157 (print), 1572-9052 (electronic). URL `http://link.springer.com/article/10.1007/BF00058647`.

Devroye:1992:BPM

[1712] Luc Devroye. A branching process method in Lagrange random variate generation. *Communications in Statistics: Simulation and Computation*, 21(1):1–14, 1992. CODEN CSSCDB. ISSN 0361-0918.

Devroye:1992:RVG

[1713] Luc Devroye. Random variate generation for the digamma and trigamma distributions. *Journal of Statistical Computation and Simulation*, 43(3–4):197–216, ???? 1992. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659208811438`.

Dougherty:1992:OMSa

[1714] Edward R. Dougherty. Optimal mean-square N-observation digital morphological filters. I. Optimal binary filters. *Computer Vision, Graphics, and Image Processing. Image Understanding*, 55(1):36–54, January 1992. CODEN CIUNEJ. ISSN 1049-9660 (print), 1557-7635 (electronic).

Dougherty:1992:OMSb

[1715] Edward R. Dougherty. Optimal mean-square N-observation digital morphological filters. II. Optimal gray-scale filters. *Computer Vision, Graphics, and Image Processing. Image Understanding*, 55(1):55–72, January 1992. CODEN CIUNEJ. ISSN 1049-9660 (print), 1557-7635 (electronic).

Ehrenfeucht:1992:PSH

[1716] Andrzej Ehrenfeucht and Jan Mycielski. A pseudorandom sequence–how random is it? *American Mathematical Monthly*, 99(4):373–375, April 1992. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972

(electronic). URL http://www.jstor.org/stable/pdfplus/2324917.pdf.

Eichenauer-Herrmann:1992:ASI

[1717] J. Eichenauer-Herrmann. On the autocorrelation structure of inversive congruential pseudorandom number sequences. *Statistical Papers = Statistische Hefte*, 33(1):261–268, December 1992. CODEN STPAE4. ISSN 0932-5026 (print), 1613-9798 (electronic).

Eichenauer-Herrmann:1992:CIC

[1718] Jürgen Eichenauer-Herrmann. Construction of inversive congruential pseudorandom number generators with maximal period length. *Journal of Computational and Applied Mathematics*, 40(3):345–349, July 24, 1992. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/0377042792901909.

Eichenauer-Herrmann:1992:ICP

[1719] Jürgen Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. *International Statistical Review = Revue Internationale de Statistique*, 60(2):167–176, August 1992. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL http://www.jstor.org/stable/1403647.

Eichenauer-Herrmann:1992:LBD

[1720] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus. *Mathematics of Computation*, 58(198):775–779, April 1992. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.jstor.org/stable/pdfplus/2153216.pdf.

Eichenauer-Herrmann:1992:NIC

[1721] Jürgen Eichenauer-Herrmann and Holger Grothe. A new inversive congruential pseudorandom number generator with power of two modulus. *ACM Transactions on Modeling and Computer Simulation*, 2(1):1–11, January 1992. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Eichenauer-Herrmann:1992:RDQ

[1722] Jürgen Eichenauer-Herrmann. A remark on the discrepancy of quadratic congruential pseudorandom numbers. *Journal of Computational and Applied Mathematics*, 43(3):383–387, December 2, 1992. CODEN JCAMDI.

ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279290023Q`.

Engel:1992:RRP

[1723] Eduardo Engel. *A road to randomness in physical systems*, volume 71 of *Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 0-387-97740-6 (New York), 3-540-97740-6 (Berlin). viii + 155 pp. LCCN QC20.7.P7 E54 1992.

Faure:1992:GPE

[1724] Henri Faure. Good permutations for extreme discrepancy. *Journal of Number Theory*, 42(1):47–56, September 1992. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic).

Ferrenberg:1992:MCS

[1725] Alan M. Ferrenberg, D. P. Landau, and Y. Joanna Wong. Monte Carlo simulations: Hidden errors from 'good' random number generators. *Physical Review Letters*, 69(23):3382–3384, December 7, 1992. CODEN PRLTAO. ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145. URL `http://prl.aps.org/abstract/PRL/v69/i23/p3382_1`. See also [1824].

Gavelek:1992:SII

[1726] D. Gavelek and T. Erber. Shadowing and iterative interpolation for Čebyšev mixing transformations. *Journal of Computational Physics*, 101 (1):25–50, July 1992. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0021999192900406`.

Gibbons:1992:NSI

[1727] Jean Dickinson Gibbons and Subhabrata Chakraborti. *Nonparametric Statistical Inference*, volume 131 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, third edition, 1992. ISBN 0-8247-8661-0. xix + 544 pp. LCCN QA278.8 .G5 1992.

Glasserman:1992:SGG

[1728] Paul Glasserman and David D. Yao. Some guidelines and guarantees for Common Random Numbers. *Management Science*, 38(6):884–908, June 1992. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Graham:1992:CFP

[1729] W. N. Graham. A comparison of four pseudo random number generators implemented in Ada. *ACM Simuletter*, 22(2):3–18, Fall 1992. CODEN SIMUD5. ISSN 0163-6103.

Guha:1992:RCB

[1730] A. Guha and L. L. Kinney. Relating the cyclic behavior of linear and intrainverted feedback shift registers. *IEEE Transactions on Computers*, 41(9):1088–1100, September 1992. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=165391`.

Heringa:1992:NPT

[1731] J. R. Heringa, H. W. J. Blöte, and A. Compagner. New primitive trinomials of Mersenne-exponent degrees for random-number generation. *International Journal of Modern Physics C [Physics and Computers]*, 3 (3):561–564, 1992. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic).

Impagliazzo:1992:PGP

[1732] Russell Graham Impagliazzo. *Pseudo-random generators for probabilistic algorithms and for cryptography*. Thesis (Ph.D. in mathematics), Department of Mathematics, University of California, Berkeley, Berkeley, CA, USA, December 1992. 105 pp.

Ishikawa:1992:MHS

[1733] T. Ishikawa, P. Y. Wang, K. Wakui, and T. Yabe. A method for the high-speed generation of random numbers with arbitrary distributions. *Computer Physics Communications*, 70(3):501–509, July 1992. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559290112C`.

Kleijnen:1992:PNG

[1734] J. P. C. Kleijnen and B. Annink. Pseudorandom number generators for supercomputers and classical computers: a practical introduction. *European Journal of Operational Research*, 63(1):76–85, November 25, 1992. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic).

Kleijnen:1992:RMS

[1735] Jack P. C. Kleijnen. Regression metamodels for simulation with common random numbers: Comparison of validation tests and confidence intervals. *Management Science*, 38(8):1164–1185, August 1992. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Ko:1992:GPB

[1736] Chun Wa Ko and Frank Ruskey. Generating permutations of a bag by interchanges. *Information Processing Letters*, 41(5):263–269, April 3, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kolonko:1992:GUD

[1737] M. Kolonko. Generating uniformly distributed random numbers without floating point operations. *Probability in the Engineering and Informational Sciences*, 6(1):139–145, January 1992. CODEN ???? ISSN 0269-9648 (print), 1469-8951 (electronic). URL `https://www.cambridge.org/core/product/4C1B47A0C509ECB109FC6000F69F7D18`.

Krawczyk:1992:HPC

[1738] Hugo Krawczyk. How to predict congruential generators. *Journal of Algorithms*, 13(4):527–545, December 1992. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `http://www.sciencedirect.com/science/article/pii/019667749290054G`.

Lagarias:1992:PN

[1739] Jeffrey C. Lagarias. Pseudorandom numbers. In Steele and Eddy [4165], chapter 6, pages 65–86. ISBN 0-309-04776-5. LCCN QA273.P7953 1992. URL `http://site.ebrary.com/lib/stanford/Doc?id=10056784`; `http://www.nap.edu/books/0309047765/html/`.

Lawrance:1992:UDF

[1740] A. J. Lawrance. Uniformly distributed first-order autoregressive time series models and multiplicative congruential random number generators. *Journal of Applied Probability*, 29(4):896–903, December 1992. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL `http://www.jstor.org/stable/pdfplus/3214722.pdf`.

LEcuyer:1992:TRN

[1741] Pierre L'Ecuyer. Testing random number generators. In Swain [4166], pages 305–313. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

Lehn:1992:PNG

[1742] J. Lehn. Pseudorandom number generators. In Gritzmann et al. [4161], pages 9–13. ISBN 0-387-91431-5 (New York), 3-7908-0608-0 (Heidelberg). LCCN T57.6 .S95 1991.

Leva:1992:ANR

[1743] Joseph L. Leva. Algorithm 712: a normal random number generator. *ACM Transactions on Mathematical Software*, 18(4):454–455, December 1992. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/138351.138367; http://www.acm.org/pubs/citations/journals/toms/1992-18-4/p454-leva/`.

Leva:1992:FNR

[1744] Joseph L. Leva. A fast normal random number generator. *ACM Transactions on Mathematical Software*, 18(4):449–453, December 1992. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/138351.138364; http://www.acm.org/pubs/citations/journals/toms/1992-18-4/p449-leva/`.

Lloyd:1992:CBF

[1745] Sheelagh Lloyd. Counting binary functions with certain cryptographic properties. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):107–131, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lo:1992:FCA

[1746] K. C. Lo and A. Purvis. Fast computational algorithm in parallel random sampling. *Electronics Letters*, 28(12):1115–1117, June 1992. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=141150`.

Louchard:1992:DAD

[1747] G. Louchard, B. Randrianarimanana, and R. Schott. Dynamic algorithms in D. E. Knuth's model: a probabilistic analysis. *Theoretical Computer Science*, 93(2):201–225, February 17, 1992. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Maclaren:1992:LUL

[1748] N. M. Maclaren. A limit on the usable length of a pseudorandom sequence. *Journal of Statistical Computation and Simulation*, 42(1–2):47–54, ???? 1992. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659208811409`.

Makino:1992:GSR

[1749] Jun Makino, Tetsuya Takaishi, and Osamu Miyamura. Generation of shift register random numbers on distributed memory multiprocessors.

Computer Physics Communications, 70(3):495–500, July 1992. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559290111B`.

Marsaglia:1992:MRN

[1750] George Marsaglia. The mathematics of random number generators. In Burr [4160], pages 73–90. ISBN 0-8218-5501-8. LCCN QA241 .U67 1992.

Mason:1992:ACA

[1751] William K. Mason. Art from cellular automata and symmetrized dot-patterns. *Computers and Graphics*, 16(4):439–441, Winter 1992. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

Matsumoto:1992:TGG

[1752] Makoto Matsumoto and Yoshiharu Kurita. Twisted GFSR generators. *ACM Transactions on Modeling and Computer Simulation*, 2(3):179–194, July 1992. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Maurer:1992:UST

[1753] Ueli M. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):89–105, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Meier:1992:CPC

[1754] Willi Meier and Othmar Staffelbach. Correlation properties of combiners with memory in stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1):67–86, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Mertsch:1992:MBB

[1755] Michael Mertsch. *Methoden zur Bestimmung und Begrenzung des Einflusses algorithmischer Zufallszahlengeneratoren auf simulative Untersuchungen. (German) [Methods for determining and limiting the influence of algorithmic random number generators on experimental investigations]*, volume 199 of *Fortschritt-Berichte VDI: Reihe 10*. VDI-Verlag, Düsseldorf, Germany, 1992. ISBN 3-18-149910-2. x + 206 pp. LCCN ???? URL `http://www.ub.tu-dortmund.de/katalog/titel/477670`.

Mode:1992:BRB

[1756] Charles J. Mode. Book review: *Random Number Generators and Simulation*, by István Deák. *SIAM Review*, 34(2):338–341, June 1992. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). See [1502].

Morii:1992:PSP

[1757] Masakatu Morii and Masao Kasahara. Perfect staircase profile of linear complexity for finite sequences. *Information Processing Letters*, 44(2): 85–89, November 19, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Mulmuley:1992:RGA

[1758] K. Mulmuley. Randomized geometric algorithms and pseudo-random generators. In IEEE [4162], pages 90–100. CODEN ASFPDV. ISBN 0-8186-2901-0 (microfiche), 0-8186-2900-2 (paperback). ISSN 0272-5428. LCCN QA 76 S979 1992. IEEE Catalog Number 92CH3188-0. IEEE Computer Society Press Order Number 2900.

Nelson:1992:CRN

[1759] B. L. Nelson. Common random numbers and multiple comparisons in simulation analysis. In G. Klutke, D. A. Mitta, B. O. Nnaji, and L. M. Seiford, editors, *Proceedings of the 1st Industrial Engineering Research Conference*, pages 463–466. ????, ????, 1992.

Niederreiter:1992:CLD

[1760] H. Niederreiter. Constructions of low-discrepancy point sets and sequences. In *Colloquia Mathematica Societatis János Bolyai, 60. Sets, Graphs and Numbers, Budapest, 1991*, volume 60 of *Colloq. Math. Soc. János Bolyai*, pages 529–559. North-Holland, Amsterdam, The Netherlands, 1992.

Niederreiter:1992:LDP

[1761] Harald Niederreiter. Low-discrepancy point sets obtained by digital constructions over finite fields. *Czechoslovak mathematical journal = Chekhoslovatskii matematicheskii zhurnal*, 42(117)(1):143–166, 1992. CODEN CZMJAE. ISSN 0011-4642.

Niederreiter:1992:NMPa

[1762] Harald Niederreiter. New methods for pseudorandom number and pseudorandom vector generation. In Swain [4166], pages 264–269. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

Niederreiter:1992:NMPb

[1763] Harald Niederreiter. Nonlinear methods for pseudorandom number and vector generation. In Pflug and Dieter [4163], pages 145–153. ISBN 3-540-54980-3 (Berlin), 0-387-54980-3 (New York). LCCN QA402.5 .I525 1990.

Niederreiter:1992:RNG

[1764] Harald Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*, volume 63. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1992. ISBN 0-89871-295-5. vi + 241 pp. LCCN QA298 .N54 1992.

Nisan:1992:PGS

[1765] N. Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, December 1992. CODEN COMBDI. ISSN 0209-9683 (print), 1439-6912 (electronic). See comments [3543].

Nisan:1992:UHP

[1766] Noam Nisan. *Using hard problems to create pseudorandom generators*, volume 1990 of *ACM distinguished dissertations*. MIT Press, Cambridge, MA, USA, 1992. ISBN 0-262-14051-9. vi + 43 pp. LCCN QA298 .N57 1992.

Novak:1992:DMR

[1767] S. Yu. Novak. On the distribution of the maximum of a random number of random variables. *Theory of Probability and its Applications*, 36(4): 714–721, December 1992. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Percus:1992:ESC

[1768] Ora Engelberg Percus and Jerome K. Percus. An expanded set of correlation tests for linear congruential random number generators. *Combinatorics, Probability and Computing*, 1(2):161–168, June 1992. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Percus:1992:IRS

[1769] Ora E. Percus and J. K. Percus. Intrinsic relations in the structure of linear congruential generators modulo 2^β. *Statistics & Probability Letters*, 15(5):381–383, 1992. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Peres:1992:INP

[1770] Yuval Peres. Iterating von Neumann's procedure for extracting random bits. *Annals of Statistics*, 20(1):590–197, March 1992. CODEN ASTSC7. ISSN 0090-5364 (print), 2168-8966 (electronic). URL `http://www.jstor.org/stable/2242181`.

Peterson:1992:MCP

[1771] I. Peterson. Monte Carlo physics: a cautionary lesson. *Science News (Washington, DC)*, 142(25–26):422, December 19, 1992. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic). URL `http://www.jstor.org/stable/4018020`. Comment on negative experience with the Marsaglia–Zaman generator reported in [1725]. See response [1852].

Plimpton:1992:PSE

[1772] S. J. Plimpton, J. R. Michael, and A. D. Romig, Jr. Parallel simulation of electron-solid interactions for electron microscopy modeling. *The Journal of Supercomputing*, 6(2):139–151, June 1992. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0920-8542&volume=6&issue=2&spage=139`.

Press:1992:NRF

[1773] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical Recipes in FORTRAN: The Art of Scientific Computing*. Cambridge University Press, Cambridge, UK, second edition, 1992. ISBN 0-521-43064-X (book), 0-521-43721-0 (example book) 0-521-43717-2 (diskette), 0-521-43719-9 (diskette), 0-521-43716-4 (diskette). xxvi + 963 pp. LCCN QA76.73.C15 N865 1992.

Press:1992:PRN

[1774] William H. Press and Saul A. Teukolsky. Portable random number generators. *Computers in Physics*, 6(5):522–524, September/October 1992. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `https://aip.scitation.org/doi/10.1063/1.4823101`.

Ressler:1992:RLP

[1775] Eugene K. Ressler. Random list permutations in place. *Information Processing Letters*, 43(5):271–275, October 5, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Savir:1992:MSL

[1776] J. Savir and W. H. McAnney. A multiple seed linear feedback shift register. *IEEE Transactions on Computers*, 41(2):250–252, February 1992. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=123404`.

Schneier:1992:PRS

[1777] Bruce Schneier. Pseudo-random sequence generator for 32-bit CPUs. *Dr. Dobb's Journal of Software Tools*, 17(2):34, 37–38, 40, February 1992. CODEN DDJOEB. ISSN 1044-789X.

Sedgewick:1992:AC

[1778] Robert Sedgewick. *Algorithms in C++*. Addison-Wesley, Reading, MA, USA, 1992. ISBN 0-201-36118-3, 0-201-51059-6. xiv + 656 pp. LCCN QA76.73.C153 S38 1992.

Sezgin:1992:SCC

[1779] Fatin Sezgin. Some comments on computer implementation of random number generators. *Journal of Computational and Applied Mathematics*, 39(3):383–386, May 8, 1992. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037704279290212G`. See [1500, 1521].

Sharp:1992:RPR

[1780] W. E. Sharp and Carter Bays. A review of portable random number generators. *Computers and Geosciences*, 18(1):79–87, January 1992. CODEN CGEODT, CGOSDN. ISSN 0098-3004 (print), 1873-7803 (electronic).

Sobol:1992:QSG

[1781] I. M. Sobol', V. I. Turchaninov, Yu. L. Levitan, and B. V. Shukhinan. Quasirandom sequence generators. *Keldysh Inst. Appl. Math., Rus. Acad. Sci.*, ??(??):??, ???? 1992.

Sprugnoli:1992:GBT

[1782] Renzo Sprugnoli. The generation of binary trees as a numerical problem. *Journal of the ACM*, 39(2):317–327, April 1992. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/128753.html`.

Szyszkowicz:1992:GRP

[1783] Mieczyslaw Szyszkowicz. Graphical representation of pseudorandom numbers. *Computers and Graphics*, 16(2):237–??, Summer 1992. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic).

Tang:1992:SDA

[1784] Hui-Chin Tang. Simulated division with approximate factoring for the multiple recursive generator with both unrestricted multiplier and non-Mersenne prime modulus. *Computers and Mathematics and Applications*, 40(3):1173–1181, July 24, 1992. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122103902094`.

Tezuka:1992:AAC

[1785] S. Tezuka and P. L'Ecuyer. An analysis of add-with-carry and subtract-with-borrow generators. In Swain [4166], pages 443–447. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

Tezuka:1992:FGL

[1786] S. Tezuka and M. Fushimi. Fast generation of low discrepancy points based on Fibonacci polynomials. In Swain [4166], pages 433–437. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

Traub:1992:MCA

[1787] J. F. Traub and H. Woźniakowski. The Monte Carlo algorithm with a pseudorandom generator. *Mathematics of Computation*, 58(197):323–339, January 1992. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153037.pdf`.

Tsai:1992:AFT

[1788] Li-Hui Tsai. An algorithm for flow time minimization and its asymptotic makespan properties. *Information Processing Letters*, 43(1):41–46, August 10, 1992. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

vonHanxleden:1992:CDP

[1789] R. von Hanxleden and L. R. Scott. Correctness and determinism of Parallel Monte Carlo Processes. *Parallel Computing*, 18(2):121–132, February 1992. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Warford:1992:GPR

[1790] J. S. Warford. Good pedagogical random number generators. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 24(1):142–146, March 1992. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Wikramaratna:1992:TBA

[1791] Roy S. Wikramaratna. Theoretical background for the ACORN random number generator. Report AEA-APS-0244, AEA Technology, Winfrith, Dorset, UK, 1992.

Wollan:1992:PRN

[1792] Peter C. Wollan. A portable random number generator for parallel computers. *Communications in Statistics: Simulation and Computation*, 21 (4):1247–1254, ???? 1992. CODEN CSSCDB. ISSN 0361-0918.

Won:1992:USN

[1793] Chee Sun Won and Haluk Derin. Unsupervised segmentation of noisy and textured images using Markov random fields. *Computer Vision, Graphics, and Image Processing. Graphical Models and Image Processing*, 54 (4):308–328, July 1992. CODEN CGMPE5. ISSN 1049-9652 (print), 1557-7643 (electronic).

Anderson:1993:CCB

[1794] N. H. Anderson and D. M. Titterington. Cross-correlation between simultaneously generated sequences of pseudo-random uniform deviates. *Statistics and Computing*, 3(2):61–65, June 1993. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00153064`.

Atkinson:1993:UGR

[1795] M. D. Atkinson. Uniform generation of rooted ordered trees with prescribed degrees. *The Computer Journal*, 36(6):593–594, December 1993. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_36/Issue_06/Vol36_06.body.html#AbstractAtkinson`.

Belisle:1993:HRA

[1796] Claude J. P. Bélisle, H. Edwin Romeijn, and Robert L. Smith. Hit-and-run algorithms for generating multivariate distributions. *Mathematics of Operations Research*, 18(2):255–266, 1993. CODEN MOREDQ. ISSN 0364-765X (print), 1526-5471 (electronic).

Brickell:1993:SRI

[1797] Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman. SKIPJACK review: Interim report: The SKIPJACK algorithm. Technical report, Georgetown University, Washington, DC, USA, July 28, 1993. URL `http://www.cs.georgetown.edu/~denning/crypto/clipper/SKIPJACK.txt`.

Browne:1993:CTC

[1798] Malcolm W. Browne. Coin-tossing computers found to show subtle bias. *New York Times*, ??(??):??, January 12, 1993. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095. Section C; Page 1; Column 4; Science Desk.

Bshouty:1993:CFR

[1799] Nader H. Bshouty. On the complexity of functions for random access machines. *Journal of the ACM*, 40(2):211–223, April 1993. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/151262.html`.

Bundschuh:1993:MEC

[1800] Peter Bundschuh and Yaochen Zhu. A method for exact calculation of the discrepancy of low-dimensional finite point sets I. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 63(??):115–133, ???? 1993. CODEN AMHAAJ. ISSN 0025-5858 (print), 1865-8784 (electronic).

Cerecedo:1993:NIG

[1801] M. Cerecedo, T. Matsumoto, and H. Imai. Non-interactive generation of shared pseudorandom sequences. *Lecture Notes in Computer Science*, 718:385–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chen:1993:PGH

[1802] Ming-Hui Chen and Bruce Schmeiser. Performance of the Gibbs, hit-and-run, and Metropolis samplers. *Journal of Computational and Graphical Statistics*, 2(3):251–272, September 1993. CODEN ???? ISSN 1061-8600 (print), 1537-2715 (electronic).

Couture:1993:DDV

[1803] Raymond Couture, Pierre L'Ecuyer, and Shu Tezuka. On the distribution of k-dimensional vectors for simple and combined Tausworthe sequences. *Mathematics of Computation*, 60(202):749–761, S11–S16, April

1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Damgaard:1993:ACE

[1804] Ivan Damgård, Peter Landrock, and Carl Pomerance. Average case error estimates for the strong probable prime test. *Mathematics of Computation*, 61(203):177–194, July 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

DeMatteis:1993:LRC

[1805] A. De Matteis and S. Pagnutti. Long-range correlation analysis of the Wichmann–Hill random number generator. *Statistics and Computing*, 3(2):67–70, June 1993. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00153065`.

Devroye:1993:GRI

[1806] Luc Devroye, Peter Epstein, and Jörg-Rüdiger Sack. On generating random intervals and hyperrectangles. *Journal of Computational and Graphical Statistics*, 2(3):291–307, September 1993. CODEN ???? ISSN 1061-8600 (print), 1537-2715 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/10618600.1993.10474613`.

Devroye:1993:RVG

[1807] Luc Devroye. On random variate generation for the generalized hyperbolic secant distributions. *Statistics and Computing*, 3(3):125–134, September 1993. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00147775`.

Dobkin:1993:CD

[1808] David P. Dobkin and David Eppstein. Computing the discrepancy. In ACM, editor, *SCG '93: Proceedings of the ninth annual Symposium on Computational Geometry, San Diego, California, May 19–21, 1993*, pages 47–52. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-582-8, 0-89791-583-6. LCCN QA448.D38 S96 1993.

Dufour:1993:IEB

[1809] Jean-Marie Dufour and Marc Hallin. Improved Eaton bounds for linear combinations of bounded random variables, with statistical applications. *Journal of the American Statistical Association*, 88(423):1026–1033, September 1993. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL `http://www.jstor.org/stable/2290795`.

Eichenauer-Herrmann:1993:DIC

[1810] Jürgen Eichenauer-Herrmann. On the discrepancy of inversive congruential pseudorandom numbers with prime power modulus. II. *Manuscripta Mathematica*, 79(3–4):239–246, 1993. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (electronic).

Eichenauer-Herrmann:1993:EIC

[1811] J. Eichenauer-Herrmann. Explicit inversive congruential pseudorandom numbers: the compound approach. *Computing: Archiv für Informatik und Numerik*, 51(2):175–182, June 1993. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Eichenauer-Herrmann:1993:EPN

[1812] Jürgen Eichenauer-Herrmann. Equidistribution properties of nonlinear congruential pseudorandom numbers. *Metrika. International Journal for Theoretical and Applied Statistics.*, 40(??):333–338, ???? 1993. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic).

Eichenauer-Herrmann:1993:ICP

[1813] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers. *Zeitschrift für Angewandte Mathematik und Mechanik*, 73(7–8):T644–T647, 1993. CODEN ZAMMAX. ISSN 0044-2267 (print), 1521-4001 (electronic). Bericht über die Wissenschaftliche Jahrestagung der GAMM (Leipzig, 1992).

Eichenauer-Herrmann:1993:KTS

[1814] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Kloosterman-type sums and the discrepancy of nonoverlapping pairs of inversive congruential pseudorandom numbers. *Acta Arithmetica*, 65(2):185–194, 1993. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Eichenauer-Herrmann:1993:LSN

[1815] J. Eichenauer-Herrmann. The lattice structure of nonlinear congruential pseudorandom numbers. *Metrika. International Journal for Theoretical and Applied Statistics.*, 40(??):115–120, ???? 1993. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic).

Eichenauer-Herrmann:1993:SIN

[1816] Jürgen Eichenauer-Herrmann. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Mathematics of Computation*, 60(201):375–384, January 1993. CODEN MCMPAF. ISSN

0025-5718 (print), 1088-6842 (electronic). URL http://www.jstor.org/stable/2153174.

Erdmann:1993:CMT

[1817] Eva Diane Erdmann. *Complexity measures for testing binary keystreams*. Ph.D. thesis, Department of Operations Research, Stanford University, Stanford, CA, USA, June 1993. xi + 105 pp. URL http://search.proquest.com/docview/304081057.

Fisher:1993:OOR

[1818] Joseph A. Fisher. Object oriented random number generators. *Computers & Industrial Engineering*, 25(1–4):561–563, September 1993. CODEN CINDDL. ISSN 0360-8352 (print), 1879-0550 (electronic). URL http://www.sciencedirect.com/science/article/pii/036083529390344W.

Flahive:1993:ICG

[1819] Mary Flahive and Harald Niederreiter. On inversive congruential generators for pseudorandom numbers. In Mullen and Shiue [4172], pages 75–80. ISBN 0-8247-8805-2. LCCN QA247.3 .F56 1993. URL http://www.loc.gov/catdir/enhancements/fy0745/92023503-d.html. Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing held at the University of Nevada, Las Vegas, August 7–10, 1991.

Galway:1993:ESCb

[1820] Lionel Galway. On the edge: Statistics and computing: John von Neumann and the origin of pseudo-random number generators. *Chance*, 6 (3):57–59, 1993. CODEN CNDCE4. ISSN 0933-2480 (print), 1867-2280 (electronic).

Ganzha:1993:PSM

[1821] V. G. Ganzha and E. V. Vorozhtsov. A probabilistic symbolic-numerical method for the stability analyses of difference schemes for PDEs. In Bronstein [4169], pages 9–13. ISBN 0-89791-604-2. LCCN QA 76.95 I59 1993. URL http://www.acm.org:80/pubs/citations/proceedings/issac/164081/p9-ganzha/. ACM order number: 505930.

Gokhale:1993:DBC

[1822] Maya B. Gokhale and Judith D. Schlesinger. A data-parallel bit-serial C (dbC). Technical report SRC-TR-93-096, Supercomputing Research Center: IDA, Lanham, MD, USA, May 1993. 14 pp.

Goldreich:1993:EPG

[1823] Oded Goldreich, Hugo Krawczyk, and Michael Luby. On the existence of pseudorandom generators. *SIAM Journal on Computing*, 22(6):1163–1175, December 1993. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Grassberger:1993:CGR

[1824] Peter Grassberger. On correlations in "good" random number generators. *Physics Letters A*, 181(1):43–46, September 27, 1993. CODEN PYLAAG. ISSN 0375-9601 (print), 1873-2429 (electronic). URL `http://www.sciencedirect.com/science/article/pii/037596019391122L`. See [1725].

Grassberger:1993:MCS

[1825] Peter Grassberger. Monte Carlo simulations of 3D self-avoiding walks. *Journal of Physics A (Mathematical and General)*, 26(12):2769–2776, June 21, 1993. CODEN JPHAC5. ISSN 0305-4470 (print), 1361-6447 (electronic).

Hamilton:1993:PNGa

[1826] Kenneth G. Hamilton. Pseudorandom number generators for personal computers. *Computer Physics Communications*, 75(1–2):105–117, April 1993. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559390168C`.

Hamilton:1993:PNGb

[1827] Kenneth G. Hamilton. Pseudorandom number generators for personal computers II. *Computer Physics Communications*, 78(1–2):172–180, December 1993. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465593901523`.

Hansen:1993:GPC

[1828] Tom Hansen, Gary L. Mullen, and Harald Niederreiter. Good parameters for a class of node sets in quasi-Monte Carlo integration. *Mathematics of Computation*, 61(203):225–234, July 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Hayes:1993:WF

[1829] Brian Hayes. The wheel of fortune. *American Scientist*, 81(2):114–118, March/April 1993. CODEN AMSCAC. ISSN 0003-0996 (print), 1545-2786 (electronic).

Hildebrand:1993:RPF

[1830] Martin Hildebrand. Random processes of the form $X_{n+1} = a_n X_n + b_n \pmod{p}$. *Annals of Probability*, 21(2):710–720, April 1993. CODEN APBYAE. ISSN 0091-1798 (print), 2168-894X (electronic). URL `http://projecteuclid.org/euclid.aop/1176989264`; `http://www.jstor.org/stable/2244672`.

Hormann:1993:GBR

[1831] Wolfgang Hörmann. The generation of binomial random variates. *Journal of Statistical Computation and Simulation*, 46(1–2):101–110, ???? 1993. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659308811496`.

Hormann:1993:PRN

[1832] Wolfgang Hörmann and G. Deflinger. A portable random number generator well suited for the rejection method. *ACM Transactions on Mathematical Software*, 19(4):489–495, December 1993. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/168173.168414`; `http://www.acm.org/pubs/citations/journals/toms/1993-19-4/p489-hormann/`.

Hormann:1993:QNU

[1833] Wolfgang Hörmann. The quality of non-uniform random numbers. Preprint Series 7, Department of Applied Statistics and Data Processing, Wirtschaftsuniversität Wien, Vienna, Austria, September 1993. 8 pp.

Hormann:1993:TRM

[1834] W. Hörmann. The transformed rejection method for generating Poisson random variables. *Insurance, Mathematics and Economics*, 12(1):39–45, February 1993. CODEN IMECDX. ISSN 0167-6687 (print), 1873-5959 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0167668793909974`.

Jebelean:1993:CSG

[1835] T. Jebelean. Comparing several GCD algorithms. In Swartzlander, Jr. et al. [4175], pages 180–185. ISBN 0-7803-1401-8 (soft-

bound), 0-8186-3862-1 (casebound), 0-8186-3861-3 (microfiche). ISSN 0018-9340 (print), 1557-9956 (electronic). LCCN QA 76.9 C62 S95 1993. URL `http://www.acsel-lab.com/arithmetic/arith11/papers/ARITH11_Jebelean.pdf`. IEEE Transactions on Computers **43(8)**, 1994.

Kalkuhl:1993:PDC

[1836] Christoph Kalkuhl. Pulse/data channel extends programmable pulse generator applications. *Hewlett-Packard Journal: technical information from the laboratories of Hewlett-Packard Company*, 44(2):56–59, April 1993. CODEN HPJOAX. ISSN 0018-1153.

Kanellakis:1993:IDM

[1837] Paris C. Kanellakis, Sridhar Ramaswamy, Darren E. Vengroff, and Jeffrey S. Vitter. Indexing for data models with constraints and classes (extended abstract). In ACM [4168], pages 233–243. ISBN 0-89791-593-3. LCCN QA 76.9 D3 A26 1993. URL `http://www.acm.org/pubs/articles/proceedings/pods/153850/p233-kanellakis/p233-kanellakis.pdf`; `http://www.acm.org/pubs/citations/proceedings/pods/153850/p233-kanellakis/`; `http://www.acm.org:80/pubs/citations/proceedings/pods/153850/p233-kanellakis/`.

Kankaala:1993:BLC

[1838] K. Kankaala, T. Ala-Nissila, and I. Vattulainen. Bit-level correlations in some pseudorandom number generators. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 48 (6):R4211–R4214, December 1993. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.48.R4211`.

Karloff:1993:FAA

[1839] Howard Karloff. Fast algorithms for approximately counting mismatches. *Information Processing Letters*, 48(2):53–60, November 8, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Karloff:1993:RAP

[1840] Howard J. Karloff and Prabhakar Raghavan. Randomized algorithms and pseudorandom numbers. *Journal of the ACM*, 40(3):454–476, July 1993. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/174132.html`.

Keppler:1993:RVM

[1841] Karl Keppler. Random variables made simply. *Computer Language Magazine*, 10(6):67–??, June 1993. CODEN COMLEF. ISSN 0749-2839.

Korsh:1993:CRG

[1842] James F. Korsh. Counting and randomly generating binary trees. *Information Processing Letters*, 45(6):291–294, April 16, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Kumar:1993:PAS

[1843] Anurag Kumar and Rajeev Shorey. Performance analysis and scheduling of stochastic fork-join jobs in a multicomputer system. *IEEE Transactions on Parallel and Distributed Systems*, 4(10):1147–1164, October 1993. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Lagarias:1993:PN

[1844] J. Lagarias. Pseudorandom numbers. *Statistical Science*, 8(1):31–39, February 1993. CODEN STSCEP. ISSN 0883-4237 (print), 2168-8745 (electronic). URL `http://www.jstor.org/stable/pdfplus/2246038.pdf`.

Laud:1993:RVG

[1845] Purushottam W. Laud, Paul Ramgopal, and Adrian F. M. Smith. Random variate generation from D-distributions. *Statistics and Computing*, 3 (3):109–112, September 1993. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00147773`.

LEcuyer:1993:SGM

[1846] Pierre L'Ecuyer, François Blouin, and Raymond Couture. A search for good multiple recursive random number generators. *ACM Transactions on Modeling and Computer Simulation*, 3(2):87–98, April 1993. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Lee:1993:GRB

[1847] A. J. Lee. Generating random binary deviates having fixed marginal distributions and specified degrees of association. *The American Statistician*, 47(3):209–215, August 1993. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2684980`.

Li:1993:IKC

[1848] Ming Li and P. M. B. (Paul Michael Béla) Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*. Texts and monographs in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 0-387-94053-7 (New York), 3-540-94053-7 (Berlin). xx + 546 pp. LCCN QA267.7 .L5 1993. URL `http://www.gbv.de/dms/bowker/toc/9780387940533.pdf`; `http://www.zentralblatt-math.org/zmath/en/search/?an=0805.68063`.

Lin:1993:NCP

[1849] T. Lin and L. O. Chua. A new class of pseudo-random number generator based on chaos in digital filters. *International Journal of Circuit Theory and Applications*, 21(5):473–480, September/October 1993. CODEN ICTACV. ISSN 0098-9886 (print), 1097-007X (electronic).

Loparo:1993:LER

[1850] Kenneth A. Loparo and Xiangbo Feng. Lyapunov exponent and rotation number of two-dimensional linear stochastic systems with telegraphic noise. *SIAM Journal on Applied Mathematics*, 53(1):283–300, February 1993. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic).

Makino:1993:SPR

[1851] Jun Makino. On the structure of parallelized random number sources. *Computer Physics Communications*, 78(1–2):105–112, December 1993. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465593901464`.

Marsaglia:1993:LHR

[1852] George Marsaglia and Arif Zaman. Letter: How random is random enough? *Science News (Washington, DC)*, 143(11):163, March 13, 1993. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic). URL `http://www.jstor.org/stable/10.2307/3977245`. Cautionary comment on [1771].

Marsaglia:1993:MTR

[1853] George Marsaglia and Arif Zaman. Monkey tests for random number generators. *Computers and Mathematics and Applications*, 26(9):1–10, November 1993. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic).

Marsaglia:1993:RNG

[1854] George Marsaglia. Random number generation. In Ralston and Reilly, Jr. [4173], pages 1145–1148. ISBN 0-442-27679-6. LCCN QA76.15 .E48 1993.

Marsaglia:1993:TCR

[1855] George Marsaglia. Technical correspondence: Remarks on choosing and implementing random number generators. *Communications of the ACM*, 36(7):105–108, July 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Mascagni:1993:RDP

[1856] M. Mascagni, S. A. Cuccaro, D. V. Pryor, and M. L. Robinson. Recent developments in parallel pseudorandom number generation. In Sincovec et al. [4174], pages 524–529. ISBN 0-89871-315-3. LCCN QA76.58 .S55 1993 v.1-2. Two volumes.

Matias:1993:DGD

[1857] Yossi Matias, Jeffrey Scott Vitter, and Wen-Chun Ni. Dynamic generation of discrete random variates. In ACM, editor, *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms: Austin, Texax January 25–27, 1993*, pages 361–370. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89871-313-7. LCCN QA76.9.A43 A34 1993.

Maurer:1993:SGT

[1858] Ueli M. Maurer. A simplified and generalized treatment of Luby–Rackoff pseudorandom permutation generators. *Lecture Notes in Computer Science*, 658:239–??, 1993. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0658/06580239.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0658/06580239.pdf`.

Mitchell:1993:NRN

[1859] Douglas W. Mitchell. A nonlinear random number generator with known, long cycle length. *Cryptologia*, 17(1):55–62, January 1993. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639214~db=all~order=page`. random number generator; cryptographic keystreams; division algorithm; seed values; long cycle length; keystream generation.

Monagan:1993:GPD

[1860] M. B. Monagan. Gauss: a parameterized domain of computation system with support for signature functions. In Miola [4171], pages 81–94. ISBN 3-540-57235-X. LCCN QA76.9.S88I576 1993.

Morris:1993:NLM

[1861] Alfred H. Morris, Jr. NSWC library of mathematics subroutines. Report NSWCDD/TR-92/425, Naval Surface Warfare Center, Dahlgren, VA 22448-5000, USA; Silver Spring, MD 20903-5000, USA, January 1993. 464 pp. URL `https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA261511.xhtml`. See also earlier edition [1560].

N:1993:BRB

[1862] H. N. Book review: *Random Number Generators and Simulation*, by István Deák. *Mathematics of Computation*, 60(201):442, January 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2153189`. See [1502].

Nelson:1993:CVM

[1863] Barry L. Nelson and J. C. Hsu. Control-variate models of Common Random Numbers for multiple comparisons with the best. *Management Science*, 39(8):989–1001, August 1993. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Nelson:1993:RMC

[1864] Barry L. Nelson. Robust multiple comparisons under common random numbers. *ACM Transactions on Modeling and Computer Simulation*, 3 (3):225–243, July 1993. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Niederreiter:1993:FFP

[1865] Harald Niederreiter. Finite fields, pseudorandom numbers, and quasirandom points. In Mullen and Shiue [4172], pages 375–394. ISBN 0-8247-8805-2. LCCN QA247.3 .F56 1993. URL `http://www.loc.gov/catdir/enhancements/fy0745/92023503-d.html`. Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing held at the University of Nevada, Las Vegas, August 7–10, 1991.

Niederreiter:1993:FPS

[1866] Harald Niederreiter. Factorization of polynomials and some linear-algebra problems over finite fields. *Linear Algebra and its Applications*,

192:301–328, October 1993. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). Computational linear algebra in algebraic and related problems (Essen, 1992).

Niederreiter:1993:LRP

[1867] H. Niederreiter and C. P. Schnorr. Local randomness in polynomial random number and random function generators. *SIAM Journal on Computing*, 22(4):684–694, August 1993. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Niederreiter:1993:PNQ

[1868] Harald Niederreiter. Pseudorandom numbers and quasirandom points. *Zeitschrift für Angewandte Mathematik und Mechanik*, 73(7–8):T648–T652, ???? 1993. CODEN ZAMMAX. ISSN 0044-2267 (print), 1521-4001 (electronic).

NIST:1993:FPS

[1869] National Institute of Standards and Technology. *FIPS PUB 181: Standard for Automated Password Generator (APG)*. National Institute for Standards and Technology, Gaithersburg, MD, USA, October 5, 1993. LCCN ???? URL `http://www.itl.nist.gov/fipspubs/fip181.htm`.

Park:1993:ATR

[1870] Stephen K. Park, Keith W. Miller, and Paul K. Stockmeyer. Another test for randomness: Response. *Communications of the ACM*, 36(7): 108–110, July 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [1392, 1500, 1855, 1880]. The authors report that they would now recommend the MCG $x_{n+1} = 48\,271 x_n \bmod (2^{31} - 1)$ over their original $x_{n+1} = 16\,807 x_n \bmod (2^{31} - 1)$.

Pollard:1993:FCI

[1871] J. M. Pollard. Factoring with cubic integers. In *The Development of the Number Field Sieve* [4170], pages 4–10. ISBN 0-387-57013-6 (New York), 3-540-57013-6 (Berlin). LCCN QA3 .L35 v.1554.

Rajasekaran:1993:FAG

[1872] Sanguthevar Rajasekaran and Keith W. Ross. Fast algorithms for generating discrete random variates with changing distributions. *ACM Transactions on Modeling and Computer Simulation*, 3(1):1–19, January 1993. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Saarinen:1993:RNT

[1873] J. Saarinen, K. Kankaala, T. Ala-Nissila, and I. Vattulainen. On random numbers — test methods and results. Technical Report HU-TFT-93-42, Institute for Theoretical Physics, University of Helsinki, Helsinki, Finland, August 1993.

Schrift:1993:UTN

[1874] A. W. Schrift and A. Shamir. Universal tests for nonuniform distributions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(3):119–133, Summer 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Selke:1993:CFM

[1875] W. Selke, A. L. Talapov, and L. N. Shchur. Cluster-flipping Monte Carlo algorithm and correlations in "good" random number generators. *JETP Letters*, 58(??):665–668, ???? 1993. CODEN JTPLA2. ISSN 0021-3640 (print), 1090-6487 (electronic).

Sharp:1993:PRN

[1876] W. E. Sharp and Carter Bays. A portable random number generator for single-precision floating-point arithmetic. *Computers and Geosciences*, 19(4):593–??, April 1993. CODEN CGEODT, CGOSDN. ISSN 0098-3004 (print), 1873-7803 (electronic).

Sherif:1993:DTN

[1877] Yosef S. Sherif and Roger G. Dear. The development and testing of a new composite random number generator. *Computers and Mathematics and Applications*, 25(1):3–16, January 1993. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/089812219390207C`. See remarks and improvements [2113].

Sloan:1993:BRB

[1878] Ian H. Sloan. Book review: *Random Number Generation and Quasi-Monte Carlo Methods* (H. Niederreiter). *SIAM Review*, 35(4):680–681, December 1993. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Sobol:1993:RQS

[1879] I. M. Sobol' and B. V. Shukman. Random and quasirandom sequences: numerical estimates of uniformity of distribution. *Mathematical and Computer Modelling*, 18(8):39–45, October 1993. CODEN MCMOEG.

ISSN 0895-7177 (print), 1872-9479 (electronic). URL `http://www.sciencedirect.com/science/article/pii/089571779390160Z`.

Sullivan:1993:ATR

[1880] Stephen J. Sullivan. Another test for randomness. *Communications of the ACM*, 36(7):108, July 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). Sullivan reports a new test of generator uniformity and reports serious failure in the 'minimal-standard generator' proposed in [1392]. See response in [1870].

Swain:1993:AA

[1881] Tom Swain. Algorithm alley. *Dr. Dobb's Journal of Software Tools*, 18 (13):119–??, December 1993. CODEN DDJOEB. ISSN 1044-789X.

Tezuka:1993:CFP

[1882] Shu Tezuka and Masanori Fushimi. Calculation of Fibonacci polynomials for GFSR sequences with low discrepancies. *Mathematics of Computation*, 60(202):763–770, April 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153114.pdf`.

Tezuka:1993:LSA

[1883] Shu Tezuka, Pierre L'Ecuyer, and Raymond Couture. On the lattice structure of the add-with-carry and subtract-with-borrow random number generators. *ACM Transactions on Modeling and Computer Simulation*, 3(4):315–331, October 1993. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). See remark in [2046, page 248], and [1644] for the original work analyzed in this paper.

Toral:1993:GGD

[1884] Raúl Toral and Amitabha Chakrabarti. Generation of Gaussian distributed random numbers by using a numerical inversion method. *Computer Physics Communications*, 74(3):327–334, March 1993. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465593900166`.

Vattulainen:1993:IIP

[1885] I. Vattulainen, K. Kankaala, J. Saarinen, and T. Ala-Nissila. Influence of implementation on the properties of pseudorandom number generators with a carry bit. *arxiv.org*, ??(??):??, June 8, 1993. URL `http://arxiv.org/abs/hep-lat/9306008`.

Wang:1993:URP

[1886] Da Kai Wang and Aaldert Compagner. On the use of reducible polynomials as random number generators. *Mathematics of Computation*, 60(201):363–374, January 1993. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Weber:1993:AIG

[1887] K. Weber. The accelerated integer GCD algorithm. Technical Report ICM-9307-55, Institute for Computational Mathematics, Kent State University, Kent, OH, USA, July 1993.

Willemain:1993:MGA

[1888] R. Thomas Willemain and A. Philip Desautels. A method to generate autocorrelated uniform random numbers. *Journal of Statistical Computation and Simulation*, 45(1–2):23–31, February 1993. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659308811469`.

Winkler:1993:SRP

[1889] Reinhard Winkler. Some remarks on pseudorandom sequences. *Mathematica Slovaca*, 43(4):493–512, ???? 1993. CODEN MASLDM. ISSN 0139-9918 (print), 1337-2211 (electronic).

Yang:1993:NBS

[1890] Yi Xian Yang. New binary sequences with perfect staircase profile of linear complexity. *Information Processing Letters*, 46(1):27–29, April 29, 1993. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Zechner:1993:EBV

[1891] H. Zechner and E. Stadlober. Erzeugung von beta-verteilten Zufallszahlen mittels Patchwork-Verwerfung. (German) [Generating beta variates via patchwork rejection]. *Computing: Archiv für Informatik und Numerik*, 50(1):1–18, March 1993. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Zurbenko:1993:WCR

[1892] I. G. Zurbenko. On weakly correlated random numbers generator. *Journal of Statistical Computation and Simulation*, 47(1–2):79–88, June 1993. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659308811512`.

Aiello:1994:PPP

[1893] William Aiello, S. Raj Rajagopalan, and Ramarathnam Venkatesan. Practical and provable pseudorandom generators. In ACM-SIAM-SDA'94 [4176], pages 1–8. ISBN 0-89871-329-3. LCCN QA76.6 .A278 1994.

Allison:1994:UHA

[1894] Lloyd Allison. Using Hirschberg's algorithm to generate random alignments of strings. *Information Processing Letters*, 51(5):251–255, September 12, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Angus:1994:PIT

[1895] John E. Angus. The probability integral transform and related results. *SIAM Review*, 36(4):652–654, December 1994. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://epubs.siam.org/26453.htm`.

Annan:1994:RAA

[1896] J. D. Annan. A randomised approximation algorithm for counting the number of forests in dense graphs. *Combinatorics, Probability and Computing*, 3(3):273–283, September 1994. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Anonymous:1994:IPR

[1897] Anonymous. Implementation of a portable and reproducible parallel and pseudorandom number generator. In IEEE [4179], pages 311–319. ISBN 0-8186-6605-6 (paper), 0-8186-6606-4 (microfiche), 0-8186-6607-2 (case). ISSN 1063-9535. LCCN QA76.5 .S894 1994. URL `http://sc94.ameslab.gov/AP/contents.html`. IEEE catalog number 94CH34819.

Bailey:1994:PGR

[1898] Ralph W. Bailey. Polar generation of random variates with the t-distribution. *Mathematics of Computation*, 62(206):779–781, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Barcucci:1994:RGD

[1899] E. Barcucci, R. Pinzani, and R. Sprugnoli. The random generation of directed animals. *Theoretical Computer Science*, 127(2):333–350, May 23, 1994. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1994&volume=127&issue=2&aid=1476`.

Boucher:1994:GPA

[1900] M. Boucher. La génération pseudo-aléatoire cryptographiquement sécuritaire et ses considérations pratiques. (French) [Cryptographically-secure random-number generation and its practical considerations]. Masters thesis, Département d'I.R.O., Université de Montréal, Montréal, QC, Canada, 1994.

Bratley:1994:APG

[1901] Paul Bratley, Bennett L. Fox, and Harald Niederreiter. Algorithm 738: Programs to generate Niederreiter's low-discrepancy sequences. *ACM Transactions on Mathematical Software*, 20(4):494–495, December 1994. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1994-20-4/p494-bratley/`.

Brent:1994:PGF

[1902] Richard P. Brent. On the periods of generalized Fibonacci recurrences. *Mathematics of Computation*, 63(207):389–401, July 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

Cain:1994:MGF

[1903] Michael Cain. The moment-generating function of the minimum of bivariate normal random variables. *The American Statistician*, 48(2):124–125, May 1994. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Calude:1994:RIN

[1904] C. Calude and H. Juergensen. Randomness as an invariant for number representations. *Lecture Notes in Computer Science*, 812:44–66, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Calvert:1994:EDL

[1905] Ken Calvert. Eliminating disjunctions of leads-to properties (temporal logic). *Information Processing Letters*, 49(4):189–194, February 25, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chang:1994:SGM

[1906] Pao long Chang, Shiuh nan Hwang, and Chiang Kao. Some good multipliers for random number generator for 16-bit microcomputers. *Computers and Operations Research*, 21(2):199–204, February

1994. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0305054894900523`. See comments and improvements [2224].

Chen:1994:IPL

[1907] Wen Chin Chen and Wen Chun Ni. Internal path length of the binary representation of heap-ordered trees. *Information Processing Letters*, 51 (3):129–132, August 10, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Cheng:1994:ECA

[1908] Pen Cheng and Shigeru Masuyama. On the equivalence in complexity among three computation problems on maximum number of edge-disjoint *s*-*t* paths in a probabilistic graph. *Information Processing Letters*, 51(4): 195–199, August 24, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Chiang:1994:DSD

[1909] Kao Chiang. Decomposition with simulated division for efficiently generating random numbers. *Computers and Operations Research*, 21 (10):1089–1093, December 1994. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0305054894900396`.

Chiang:1994:SET

[1910] Kao Chiang and J. Y. Wong. Several extensively tested random number generators. *Computers and Operations Research*, 21(9):1035–1039, November 1994. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0305054894900744`.

Coddington:1994:ARN

[1911] Paul D. Coddington. Analysis of random number generators using Monte Carlo simulation. *International Journal of Modern Physics C [Physics and Computers]*, 5(3):547–560, June 1994. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic).

Cooperman:1994:RBC

[1912] Gene Cooperman and Larry Finkelstein. A random base change algorithm for permutation groups. *Journal of Symbolic Computation*, 17(6): 513–528, June 1994. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Coppersmith:1994:SG

[1913] Don Coppersmith, Hugo Krawczyk, and Yishay Mansour. The shrinking generator. *Lecture Notes in Computer Science*, 773:22–39, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0773/07730022.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0773/07730022.pdf`.

Corcoran:1994:MVC

[1914] William J. Corcoran. A multiloop Vigenère cipher with exceptionally long component series. *Cryptologia*, 18(4):356–371, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639272~db=all~order=page`. multiloop Vigenére cipher; exceptionally long component series; computer generation; polyalphabetic cryptographic system; character set; linear congruential generating function; component series; cryptanalysis; multiloop system; computationally secure; personal computers; Spectra Publishing; Power Basic; BASIC.

Couture:1994:LSC

[1915] Raymond Couture and Pierre L'Ecuyer. On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. *Mathematics of Computation*, 62(206):799–808, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153540.pdf`.

Cuccaro:1994:TTQ

[1916] Steven A. Cuccaro, Michael Mascagni, and Daniel V. Pryor. Techniques for testing the quality of parallel pseudorandom number generators. Technical report SRC-TR-94-128, Supercomputing Research Center: IDA, Lanham, MD, USA, October 4, 1994. 6 pp.

Davis:1994:CRA

[1917] Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic randomness from air turbulence in disk drives. In Desmedt [4178], pages 114–120. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/bibs/0839/08390114.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0839/08390114.pdf`.

DeArmon:1994:RLO

[1918] James S. DeArmon. Randomness of low-order bits in random number generators. *Simulation*, 62(6):373–377, July 1994. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/62/6/373.abstract`.

Deng:1994:DIR

[1919] L.-Y. Deng, K. H. Chan, and Y. Yuan. Design and implementation of random number generators for multiprocessor systems. *International Journal of Modelling and Simulation*, 14(4):185–191, ???? 1994. CODEN IMSIEK. ISSN 0228-6203 (print), 1925-7082 (electronic). URL `http://www.actapress.com/Content_of_Journal.aspx?JournalID=118`.

Devroye:1994:NHS

[1920] Luc Devroye and Paul Kruszewski. A note on the Horton–Strahler number for random trees. *Information Processing Letters*, 52(3):155–159, November 11, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Eastlake:1994:RRR

[1921] D. Eastlake, 3rd, S. Crocker, and J. Schiller. RFC 1750: Randomness recommendations for security, December 1994. URL `ftp://ftp.internic.net/rfc/rfc1750.txt`; `https://www.math.utah.edu/pub/rfc/rfc1750.txt`. Status: INFORMATIONAL. Obsoleted by RFC4086.

Eichenauer-Herrmann:1994:BES

[1922] J. Eichenauer-Herrmann and H. Niederreiter. Bounds for exponential sums and their applications to pseudorandom numbers. *Acta Arithmetica*, 67(3):269–281, ???? 1994. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic). URL `http://matwbn.icm.edu.pl/ksiazki/aa/aa67/aa6736.pdf`.

Eichenauer-Herrmann:1994:CNC

[1923] Jürgen Eichenauer-Herrmann. Compound nonlinear congruential pseudorandom numbers. *Monatshefte für Mathematik*, 117(3–4):213–222, September 1994. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/n82h7044q514l33x/`.

Eichenauer-Herrmann:1994:DIP

[1924] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Digital inversive pseudorandom numbers. *ACM Transactions on Modeling and Computer*

Simulation, 4(4):339–349, October 1994. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Eichenauer-Herrmann:1994:DQC

[1925] Jürgen Eichenauer-Herrmann. On the discrepancy of quadratic congruential pseudorandom numbers with power of two modulus. *Journal of Computational and Applied Mathematics*, 53(3):371–376, August 30, 1994. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042794900647`.

Eichenauer-Herrmann:1994:EIC

[1926] Jürgen Eichenauer-Herrmann and Katja Ickstadt. Explicit inversive congruential pseudorandom numbers with power of two modulus. *Mathematics of Computation*, 62(206):787–797, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2153539`.

Eichenauer-Herrmann:1994:GIC

[1927] Jürgen Eichenauer-Herrmann. On generalized inversive congruential pseudorandom numbers. *Mathematics of Computation*, 63(207):293–299, July 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/2153575`.

Eichenauer-Herrmann:1994:ILB

[1928] Jürgen Eichenauer-Herrmann. Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Mathematics of Computation*, 62(206):783–786, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153538.pdf`.

Eichenauer-Herrmann:1994:SIN

[1929] Jürgen Eichenauer-Herrmann and Harald Niederreiter. On the statistical independence of nonlinear congruential pseudorandom numbers. *ACM Transactions on Modeling and Computer Simulation*, 4(1):89–95, January 1994. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Endl:1994:CRG

[1930] R. Endl and M. Sommer. Classification of ray-generators in uniform subdivisions and octrees for ray tracing. *Computer Graphics Forum*, 13(1):3–19, March 1994. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Entacher:1994:CNP

[1931] K. Entacher. Classical and new pseudorandom number generators in the run test. In M. Vajteršic and P. Zinterhof, editors, *Proceedings of the International Workshop Parallel Numerics '94, Smolenice, September 19–21*. Slovak Academy of Sciences, Institute for Informatics, ????, Slovakia, 1994.

Gaines:1994:RGS

[1932] J. G. Gaines and T. J. Lyons. Random generation of stochastic area integrals. *SIAM Journal on Applied Mathematics*, 54(4):1132–1146, August 1994. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/23570`.

Gemmell:1994:TBE

[1933] Peter Gemmell and Mor Harchol. Tight bounds on expected time to add correctly and add mostly correctly. *Information Processing Letters*, 49 (2):77–83, January 28, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Gray:1994:QGB

[1934] Jim Gray, Prakash Sundaresan, Susanne Englert, Ken Baclawski, and Peter J. Weinberger. Quickly generating billion-record synthetic databases. In Snodgrass and Winslett [4180], pages 243–252. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994. URL `http://www.acm.org/pubs/citations/proceedings/mod/191839/p243-gray/`.

Gupta:1994:RSD

[1935] Rajiv Gupta, Scott A. Smolka, and Shaji Bhaskar. On randomization in sequential and distributed algorithms. *ACM Computing Surveys*, 26(1): 7–86, March 1994. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0360-0300/174667.html`.

Hamilton:1994:PNG

[1936] Kenneth G. Hamilton. Pseudorandom number generators for Salford FTN77. *Computer Physics Communications*, 81(1–2):237–247, June 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465594901228`.

Hartel:1994:CRN

[1937] F. Härtel. On combined random number generators. In ????, editor, *International Workshop on Mathematical Methods and Tools in Computer Simulation*, pages 7–8. V. I. Smirnov Scientific Research Institute of Mathematics and Mechanics, ????, 1994.

Hellekalek:1994:GDEa

[1938] Peter Hellekalek. General discrepancy estimates: the Walsh function system. *Acta Arithmetica*, 67(3):209–218, 1994. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic). URL `http://matwbn.icm.edu.pl/ksiazki/aa/aa67/aa6732.pdf`.

Hellekalek:1994:GDEb

[1939] P. Hellekalek. General discrepancy estimates II: The Haar function system. *Acta Arithmetica*, 67(4):313–322, 1994. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic). URL `http://matwbn.icm.edu.pl/ksiazki/aa/aa67/aa6742.pdf`.

Hennecke:1994:RER

[1940] Michael Hennecke. RANEXP: experimental random number generator package. *Computer Physics Communications*, 79(2):261–267, April 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465594900728`.

Hildebrand:1994:RWS

[1941] Martin Hildebrand. Random walks supported on random points of Z/nZ. *Probability theory and related fields*, 100(2):191–203, ???? 1994. CODEN PTRFEU. ISSN 0178-8051 (print), 1432-2064 (electronic). URL `http://link.springer.com/article/10.1007/BF01199265`.

Hill:1994:CMR

[1942] R. R. Hill and C. H. Reilly. Composition for multivariate random variables. In Tew et al. [4181], pages 332–339. ISBN 0-7803-2109-X (casebound), 0-7803-2108-1 (paperback), 0-7803-2110-3 (microfiche). LCCN QA76.9.C65 W56 1994. IEEE catalog number 94CH35705.

Holian:1994:PNG

[1943] Brad Lee Holian, Ora E. Percus, Tony T. Warnock, and Paula A. Whitlock. Pseudorandom number generator for massively parallel molecular-dynamics simulations. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 50(2):1607–1615, August

1994. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.50.1607`.

Hoogland:1994:GPR

[1944] Jiri Hoogland and Ronald Kleiss. Generation of pseudo-random variates with fixed sum and product. *Computer Physics Communications*, 79(2):179–189, April 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465594900663`.

Hormann:1994:NQR

[1945] Wolfgang Hörmann. A note on the quality of random variates generated by the ratio of uniforms method. *ACM Transactions on Modeling and Computer Simulation*, 4(1):96–106, January 1994. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hormann:1994:TRM

[1946] Wolfgang Hörmann and Gerhard Derflinger. The transformed rejection method for generating random variables, an alternative to the ratio-of-uniforms method. *Communications in Statistics: Simulation and Computation*, 23(3):847–860, ???? 1994. CODEN CSSCDB. ISSN 0361-0918.

Hormann:1994:UGD

[1947] W. Hörmann. A universal generator for discrete log-concave distributions. *Computing: Archiv für Informatik und Numerik*, 52(1):89–96, March 1994. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic).

Huber:1994:PLG

[1948] K. Huber. On the period length of generalized inversive pseudorandom number generators. *Applicable algebra in engineering, communication and computing*, 5(??):255–260, ???? 1994. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

James:1994:RFI

[1949] F. James. RANLUX: a Fortran implementation of the high-quality pseudorandom number generator of Lüscher. *Computer Physics Communications*, 79(1):111–114, February 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559490233X`. See erratum [2182].

Jimbo:1994:RBB

[1950] Shuji Jimbo and Akira Maruoka. On the relationship between ϵ-biased random variables and ϵ-dependent random variables. *Information Processing Letters*, 51(1):17–23, July 12, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Jimbo:1994:RBD

[1951] Shuji Jimbo and Akira Maruoka. On the relationship between the diameter and the size of a boundary of a directed graph. *Information Processing Letters*, 50(5):277–282, June 10, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Johnson:1994:CUD

[1952] Norman Lloyd Johnson, Samuel Kotz, and N. Balakrishnan. *Continuous univariate distributions*. Wiley series in probability and mathematical statistics. Wiley, New York, NY, USA, second edition, 1994. ISBN 0-471-58495-9 (vol. 1), 0-471-58494-0 (vol. 2). xix + 756 (vol. 1), xix + 719 (vol. 2) pp. LCCN QA273.6 .J6 1994. URL `http://www.loc.gov/catdir/toc/onix03/93045348.html`.

Kaigh:1994:SRS

[1953] W. D. Kaigh and E. F. Schuster. SRS runs and spacings tests to assess randomness. *American Statistical Association Proceedings of the Statistical Computing Section*, ??(??):272–277, ???? 1994. ISBN 1-883276-06-3. ISSN 1543-3218.

Kanatani:1994:SAG

[1954] Kenichi Kanatani. Statistical analysis of geometric computation. *Computer Vision, Graphics, and Image Processing. Image Understanding*, 59 (3):286–306, May 1994. CODEN CIUNEJ. ISSN 1049-9660 (print), 1557-7635 (electronic). URL `http://www.idealibrary.com/links/artid/ciun.1994.1020/production`; `http://www.idealibrary.com/links/artid/ciun.1994.1020/production/pdf`; `http://www.idealibrary.com/links/artid/cviu.1994.1024/production`; `http://www.idealibrary.com/links/artid/cviu.1994.1024/production/pdf`.

Kari:1994:GNS

[1955] H. H. Kari, J. Salinas, and F. Lombardi. Generating non-standard random distributions for discrete event simulation systems. *Simulation Practice and Theory*, 1(4):173–193, March 15, 1994. CODEN SPTHEH. ISSN 0928-4869 (print), 1879-1433 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0928486994900051`.

Karian:1994:RNG

[1956] Zaven A. Karian and Rohit Goyal. Random number generation and testing. *Maple Technical Newsletter*, 1(1):32–37, Spring 1994. CODEN ???? ISSN 1061-5733. URL `http://www.can.nl/Systems_and_Packages/Per_Purpose/General/Maple/mtn/mtnv1n1.html`. This article describes the Maple-language random-number generator, a multiplicative congruential generator (xnew = (A x + C) mod P) with $A = 427,419,669,081$, $C = 0$, $P = 10^{12} - 11$, and initial seed 1. It was used up to Maple Version 9 (2003). Later versions of Maple instead use the Mersenne Twister.

Karloff:1994:CWI

[1957] Howard Karloff and Yishay Mansour. On construction of k-wise independent random variables. In ACM [4177], pages 564–573. ISBN 0-89791-663-8. LCCN QA76 .A15 1994. URL `http://www.acm.org/pubs/articles/proceedings/stoc/195058/p564-karloff/p564-karloff.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/195058/p564-karloff/`. ACM order number 508930.

Kenney:1994:HTI

[1958] C. S. Kenney and A. J. Lamb. A hyperbolic tangent identity and the geometry of Padé sign function iterations. *Numerical Algorithms*, 7(2–4): 111–128, July 1994. CODEN NUALEG. ISSN 1017-1398 (print), 1572-9265 (electronic).

Kreyszig:1994:MCM

[1959] E. Kreyszig and E. J. Normington. *Maple Computer Manual for Seventh Edition Advanced Engineering Mathematics: Erwin Kreyszig*. Wiley, New York, NY, USA, 1994. ISBN 0-471-31126-X. xii + 506 pp. LCCN QA401 K74 1993. There is a companion *Instructor's Maple Manual*, but I have not yet found an exact citation for it.

Lavastre:1994:SAS

[1960] Hélène Lavastre. On the stochastic acceleration of sequences of random variables. *Applied Numerical Mathematics: Transactions of IMACS*, 15(1):77–98, August 1, 1994. CODEN ANMAEL. ISSN 0168-9274 (print), 1873-5460 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/apnum/cas_sub/browse/browse.cgi?year=1994&volume=15&issue=1&aid=502`.

Leader:1994:LOI

[1961] I. Leader and A. J. Radcliffe. Littlewood–Offord inequalities for random variables. *SIAM Journal on Discrete Mathematics*, 7(1):90–101,

February 1994. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

LEcuyer:1994:CRW

[1962] P. L'Ecuyer and G. Perron. On the convergence rates of WA and FDC derivative estimators. *Operations Research*, 42(??):643–656, ???? 1994. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).

LEcuyer:1994:SOSa

[1963] P. L'Ecuyer, N. Giroux, and P. W. Glynn. Stochastic optimization by simulation: Numerical experiments with the M/M/1 queue in steady-state. *Management Science*, 40(??):1245–1261, ???? 1994. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

LEcuyer:1994:SOSb

[1964] P. L'Ecuyer and P. W. Glynn. Stochastic optimization by simulation: Convergence proofs for the GI/G/1 queue in steady-state. *Management Science*, 40(??):1562–1578, ???? 1994. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

LEcuyer:1994:URN

[1965] Pierre L'Ecuyer. Uniform random number generation. *Annals of Operations Research*, 53(1):77–120, 1994. CODEN AOREEV. ISSN 0254-5330 (print), 1572-9338 (electronic).

Leeb:1994:PST

[1966] H. Leeb. pLab — a system for testing random numbers. In M. Vajteršic and P. Zinterhof, editors, *Proceedings of the International Workshop Parallel Numerics '94, Smolenice, September 19–21*, pages 89–99. Slovak Academy of Sciences, Institute for Informatics, ????, Slovakia, 1994. URL `ftp://random.mat.sbg.ac.at/pub/data/leebSmol.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/leebSmol.txt`.

Li:1994:RSA

[1967] Kim-Hung Li. Reservoir sampling algorithms of time complexity $O(n(1 + \log(N/n)))$. *ACM Transactions on Mathematical Software*, 20(4):481–493, December 1994. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/198429.198435`; `http://www.acm.org/pubs/citations/journals/toms/1994-20-4/p481-li/`.

Lidl:1994:IFF

[1968] Rudolph Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, UK, second edition, 1994. ISBN 0-521-46094-8 (hardcover), 1-139-17276-X (e-book). xi + 461 pp. LCCN QA247.3 .L54 1994.

Luscher:1994:PHQ

[1969] Martin Lüscher. A portable high-quality random number generator for lattice field theory simulations. *Computer Physics Communications*, 79(1):100–110, February 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465594902321`.

Ma:1994:IMC

[1970] Chang ming Ma. Implementation of a Monte Carlo code on a parallel computer system. *Parallel Computing*, 20(7):991–1005, July 12, 1994. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1994&volume=20&issue=7&aid=883`.

MacLaren:1994:CPN

[1971] N. MacLaren. Cryptographic pseudorandom numbers in simulation. *Lecture Notes in Computer Science*, 809:185–??, 1994. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Makino:1994:LFR

[1972] Jun Makino. Lagged-Fibonacci random number generators on parallel computers. *Parallel Computing*, 20(9):1357–1367, September 12, 1994. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1994&volume=20&issue=9&aid=893`.

Marsaglia:1994:MAR

[1973] George Marsaglia. The mother of all random generators. Web document, October 1994. URL `ftp://ftp.taygeta.com/pub/c/mother.c`.

Marsaglia:1994:REI

[1974] George Marsaglia, Arif Zaman, and John C. W. Marsaglia. Rapid evaluation of the inverse of the normal distribution function. *Statistics & Probability Letters*, 19(4):259–266, March 15, 1994. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic).

Marsaglia:1994:SPV

[1975] George Marsaglia and Arif Zaman. Some portable very-long-period random number generators. *Computers in Physics*, 8(1):117–121, January/February 1994. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic).

Mascagni:1994:FHQ

[1976] Michael Mascagni. A fast, high quality, and reproducible parallel lagged-Fibonacci pseudorandom number generator. Technical report SRC-TR-94-115, Supercomputing Research Center: IDA, Lanham, MD, USA, March 15, 1994. 18 pp.

Mascagni:1994:PPN

[1977] Michael Mascagni. Parallel pseudorandom number generation using additive lagged-Fibonacci recursions. Technical report SRC-TR-94-133, Supercomputing Research Center: IDA, Lanham, MD, USA, December 1, 1994. 15 pp.

Matsui:1994:LCM

[1978] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 386–397. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. URL `https://link.springer.com/chapter/10.1007/3-540-48285-7_33`.

Matsumoto:1994:TGG

[1979] Makoto Matsumoto and Yoshiharu Kurita. Twisted GFSR generators II. *ACM Transactions on Modeling and Computer Simulation*, 4(3):254–266, July 1994. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

McGrath:1994:SAB

[1980] Gary McGrath. Signal analysis via the bootstrap. *Dr. Dobb's Journal of Software Tools*, 19(2):48, 50, 52, 54–57, 81–82, February 1994. CODEN DDJOEB. ISSN 1044-789X.

Niederreiter:1994:NCP

[1981] Harald Niederreiter. On a new class of pseudorandom numbers for simulation methods. *Journal of Computational and Applied Mathematics*, 56 (1–2):159–167, December 20, 1994. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042794903859`.

Niederreiter:1994:PVG

[1982] Harald Niederreiter. Pseudorandom vector generation by the inversive method. *ACM Transactions on Modeling and Computer Simulation*, 4 (2):191–212, April 1994. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Odlyzko:1994:PKC

[1983] Andrew M. Odlyzko. Public key cryptography. *AT&T Technical Journal*, 73(5):17–23, September/October 1994. CODEN ATJOEM. ISSN 2376-676X (print), 8756-2324 (electronic). URL `http://www.research.att.com/~amo/doc/arch/public.key.crypto.pdf`; `http://www.research.att.com/~amo/doc/arch/public.key.crypto.ps`; `http://www.research.att.com/~amo/doc/arch/public.key.crypto.tex`.

Ohta:1994:INP

[1984] Shigemi Ohta, Eiichi Goto, Weng Fai Wong, and Nobuaki Yoshida. Improvement and new proposal on fast evaluation of elementary functions. (Japanese). *Transactions of the Information Processing Society of Japan*, 35(5):926–933, May 1994. CODEN JSGRD5. ISSN 0387-5806.

Pedrotti:1994:ALU

[1985] A. Pedrotti. Analysis of a list-update strategy. *Information Processing Letters*, 52(3):115–121, November 11, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Petersen:1994:LFS

[1986] W. P. Petersen. Lagged Fibonacci series random number generators for the NEC SX-3. *International Journal of High Speed Computing (IJHSC)*, 6(3):387–??, 1994. CODEN IHSCEZ. ISSN 0129-0533.

Petriu:1994:AMV

[1987] Dorina C. Petriu. Approximate mean value analysis of client-server systems with multi-class requests. *ACM SIGMETRICS Performance Evaluation Review*, 22(1):77–86, May 1994. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Piccioni:1994:IMC

[1988] Mauro Piccioni and Sergio Scarlatti. An iterative Monte Carlo scheme for generating Lie group-valued random variables. *Advances in Applied Probability*, 26(3):616–628, September 1994. CODEN AAPBBD. ISSN

0001-8678 (print), 1475-6064 (electronic). URL `http://www.jstor.org/stable/1427811`.

Plumb:1994:TRN

[1989] Colin Plumb. Truly random numbers. *Dr. Dobb's Journal of Software Tools*, 19(13):113–??, November 1994. CODEN DDJOEB. ISSN 1044-789X.

Pryor:1994:IPR

[1990] D. V. Pryor, S. A. Cuccaro, M. Mascagni, and M. L. Robinson. Implementation of a portable and reproducible parallel pseudorandom number generator. In IEEE [4179], pages 311–319. ISBN 0-8186-6605-6 (paper), 0-8186-6606-4 (microfiche), 0-8186-6607-2 (case). ISSN 1063-9535. LCCN QA76.5 .S894 1994. URL `http://sc94.ameslab.gov/AP/contents.html`. IEEE catalog number 94CH34819.

Pryor:1994:IUP

[1991] Daniel V. Pryor. Implementation and usage of a portable and reproducible parallel pseudorandom number generator. Technical report SRC-TR-94-116, Supercomputing Research Center: IDA, Lanham, MD, USA, March 15, 1994. 16 pp.

Rajsbaum:1994:PSP

[1992] Sergio Rajsbaum and Moshe Sidi. On the performance of synchronized programs in distributed networks with random processing times and transmission delays. *IEEE Transactions on Parallel and Distributed Systems*, 5(9):939–950, September 1994. CODEN ITDSEO. ISSN 1045-9219 (print), 1558-2183 (electronic).

Ramirez:1994:EUI

[1993] Octavio A. Ramirez, Charles B. Moss, and William G. Boggess. Estimation and use of the inverse hyperbolic sine transformation to model non-normal correlated random variables. *Journal of Applied Statistics*, 21(4):289–304, ???? 1994. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic).

Rarity:1994:QRN

[1994] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12): 2435–2444, December 1994. CODEN JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/09500349414552281`.

Riesel:1994:PNC

[1995] Hans Riesel. *Prime numbers and computer methods for factorization*, volume 126 of *Progress in mathematics*. Birkhäuser Boston Inc., Cambridge, MA, USA, second edition, 1994. ISBN 0-8176-3743-5. xvi + 464 pp. LCCN QA246 .R54 1994. URL `http://www.loc.gov/catdir/enhancements/fy0907/94027688-d.html`; `http://www.loc.gov/catdir/enhancements/fy0907/94027688-t.html`.

Ritter:1994:EPR

[1996] Terry Ritter. Estimating population from repetitions in accumulated random samples. *Cryptologia*, 18(2):155–190, April 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL `http://www.informaworld.com/smpp/content~content=a748639261~db=all~order=page`.

Rivest:1994:DBI

[1997] Ronald L. Rivest and Robert E. Schapire. Diversity-based inference of finite automata. *Journal of the ACM*, 41(3):555–589, May 1994. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0004-5411/176589.html`.

Schneier:1994:AAd

[1998] Bruce Schneier. Algorithm alley. *Dr. Dobb's Journal of Software Tools*, 19(13):113–??, November 1994. CODEN DDJOEB. ISSN 1044-789X.

Shallit:1994:ALS

[1999] Jeffrey Shallit and Jonathan Sorenson. Analysis of a left-shift binary GCD algorithm. *Journal of Symbolic Computation*, 17(6):473–486, June 1994. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic).

Shukhman:1994:GQR

[2000] B. Shukhman. Generation of quasi-random (LP_τ) vectors for parallel computation. *Computer Physics Communications*, 78(3):279–286, January 1994. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559490006X`.

Sitharam:1994:PGL

[2001] Meera Sitharam. Pseudorandom generators and learning algorithms for AC. In ACM [4177], pages 478–486. ISBN 0-89791-663-8. LCCN QA76

.A15 1994. URL `http://www.acm.org/pubs/articles/proceedings/stoc/195058/p478-sitharam/p478-sitharam.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/195058/p478-sitharam/`. ACM order number 508930.

Sorenson:1994:TFG

[2002] J. Sorenson. Two fast GCD algorithms. *Journal of Algorithms*, 16(1): 110–144, January 1994. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic).

Spanier:1994:QRM

[2003] Jerome Spanier and Earl H. Maize. Quasi-random methods for estimating integrals using relatively small samples. *SIAM Review*, 36(1):18–44, March 1994. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://epubs.siam.org/22673.htm`.

Strauch:1994:D

[2004] Oto Strauch. L^2 discrepancy. *Mathematica Slovaca*, 44(5):601–632, ???? 1994. CODEN MASLDM. ISSN 0139-9918 (print), 1337-2211 (electronic).

Swan:1994:AAa

[2005] Tom R. Swan. Algorithm alley. *Dr. Dobb's Journal of Software Tools*, 19(1):111–??, January 1994. CODEN DDJOEB. ISSN 1044-789X.

Szwarcfiter:1994:EKD

[2006] Jayme L. Szwarcfiter and Guy Chaty. Enumerating the kernels of a directed graph with no odd circuits. *Information Processing Letters*, 51 (3):149–153, August 10, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Takashima:1994:STT

[2007] K. Takashima. Sojourn time test for maximum-length linearly recurring sequences with characteristic primitive trinomials. *Journal of Japanese Society of Computational Statistics*, 7(??):77–87, ?? 1994. CODEN ???? ISSN 0915-2350 (print), 1881-1337 (electronic).

Tezuka:1994:DDC

[2008] Shu Tezuka. The k-dimensional distribution of combined GFSR sequences. *Mathematics of Computation*, 62(206):809–817, April 1994. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153541.pdf`.

Tezuka:1994:MDC

[2009] Shu Tezuka and Masanori Fushimi. A method of designing cellular automata as pseudorandom number generators for built-in self-test for VLSI. *Contemporary Mathematics (American Mathematical Society)*, 168(??):363–367, ???? 1994. ISSN 0271-4132 (print), 1098-3627 (electronic).

Tezuka:1994:UVL

[2010] Shu Tezuka. A unified view of long-period random number generators. *Journal of the Operations Research Society of Japan*, 37(3):211–227, ???? 1994. CODEN JORJA5. ISSN 0453-4514 (print), 1878-6871 (electronic).

Tierney:1994:MCE

[2011] Luke Tierney. Markov chains for exploring posterior distributions. *Annals of Statistics*, 22(4):1701–1728, December 1994. CODEN ASTSC7. ISSN 0090-5364 (print), 2168-8966 (electronic). URL `http://projecteuclid.org/euclid.aos/1176325750`; `http://www.jstor.org/stable/2242477`.

vanderMeer:1994:RBG

[2012] Hans van der Meer. Random bit generator in TEX. *TUGboat (Journal of the TEX Users Group)*, 15(1):57–58, March 1994. CODEN ???? ISSN 0896-3207.

Vattulainen:1994:NTR

[2013] Ilpo Vattulainen. New tests of random numbers for simulations in physical systems. *arxiv.org*, pages x + 88 + 2, 1994. ISBN 951-45-6879-6. ISSN 0786-2547. URL `http://arxiv.org/abs/cond-mat/9411062`; `https://helka.linneanet.fi/cgi-bin/Pwebrecon.cgi?BBID=750921&LANGUAGE=English`. Also issued as report HU-TFT-IR-94-4, Research Institute for Theoretical Physics, University of Helsinki, Helsinki, Finland.

Vattulainen:1994:PTR

[2014] I. Vattulainen, T. Ala-Nissila, and K. Kankaala. Physical tests for random numbers in simulations. *Physical Review Letters*, 73(19):2513–2516, November 7, 1994. CODEN PRLTAO. ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145. URL `http://link.aps.org/doi/10.1103/PhysRevLett.73.2513`.

Weingartner:1994:NCP

[2015] A. Weingartner. Nonlinear congruential pseudorandom number generators. Master's thesis, University of Salzburg, Salzburg, Austria, 1994.

URL `ftp://random.mat.sbg.ac.at/pub/data/weingaThesis.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/weingaThesis.txt`.

Wolfram:1994:CAC

[2016] Stephen Wolfram. *Cellular automata and complexity: collected papers*. Addison-Wesley, Reading, MA, USA, 1994. ISBN 0-201-62716-7, 0-201-62664-0 (paperback). 596 pp. LCCN QA267.5.C45 W65 1994. URL `http://www.loc.gov/catdir/enhancements/fy0831/93040786-b.html`; `http://www.loc.gov/catdir/enhancements/fy0831/93040786-d.html`.

Zhang:1994:PEE

[2017] Hui Zhang and Edward W. Knightly. Providing end-to-end statistical performance guarantees with bounding interval dependent stochastic models. *ACM SIGMETRICS Performance Evaluation Review*, 22(1): 211–220, May 1994. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Zijp:1994:UTC

[2018] J. R. Zijp and J. J. Bosch. Use of tabulated cumulative density functions to generate pseudorandom numbers obeying specific distributions for Monte Carlo simulations. *Applied Optics*, 33(3):533–534, January 20, 1994. CODEN APOPAI. ISSN 0003-6935.

Ahrens:1995:OTM

[2019] J. H. Ahrens. A one-table method for sampling from continuous and discrete distributions. *Computing: Archiv für Informatik und Numerik*, 54 (2):127–146, June 1995. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=245&id_volume=18&id_journal=8`.

Al-Hussaini:1995:UPT

[2020] A. N. Al-Hussaini. A unified proof of two theorems in statistics. *SIAM Review*, 37(4):596–597, December 1995. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://epubs.siam.org/27305.htm`.

Anguita:1995:CDP

[2021] D. Anguita, S. Rovetta, and R. Zunino. Compact digital pseudorandom number generator. *Electronics Letters*, 31(12):956–958, June 8, 1995. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=391003`.

Antipov:1995:COP

[2022] M. V. Antipov. Congruence operator of the pseudo-random numbers generator and a modification of Euclidean decomposition. *Monte Carlo Methods and Applications*, 1(3):203–219, ???? 1995. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1995.1.issue-3/mcma.1995.1.3.203/mcma.1995.1.3.203.xml`.

Barnes:1995:APE

[2023] John Barnes. The Ada 95 predefined environment. *Ada User Journal*, 16 (4):215–219, December 1995. CODEN AUJOET. ISSN 0268-652X. URL `http://www.adauk.org.uk/pubs/jbpredef.htm`.

Baum:1995:CCP

[2024] U. Baum and S. Blackburn. Clock-controlled pseudorandom generators on finite groups. *Lecture Notes in Computer Science*, 1008:6–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bellare:1995:XMN

[2025] Mihir Bellare, Roch Guérin, and Phillip Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. *Lecture Notes in Computer Science*, 963:15–35, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630015.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630015.pdf`.

Bowman:1995:EPR

[2026] Richard L. Bowman. Evaluating pseudo-random number generators. *Computers and Graphics*, 19(2):315–324, March–April 1995. CODEN COGRD2. ISSN 0097-8493 (print), 1873-7684 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/cag/cas_sub/browse/browse.cgi?year=1995&volume=19&issue=2&aid=9400158`.

Carrasco:1995:RRT

[2027] Juan A. Carrasco and Angel Calderón. Regenerative randomization: theory and application examples. *ACM SIGMETRICS Performance Evaluation Review*, 23(1):241–252, May 1995. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Chen:1995:IDP

[2028] Jian Chen and Paula Whitlock. Implementation of a distributed pseudorandom number generator. In Niederreiter and Shiue [4187], pages 168–185. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Childs:1995:CIH

[2029] Lindsay N. Childs. *A Concrete Introduction to Higher Algebra*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 1995. ISBN 0-387-94484-2 (hardcover), 1-4419-8702-9 (e-book). xv + 522 pp. LCCN QA155 .C53 1995.

Chou:1995:LTI

[2030] Wun-Seng Chou and Harald Niederreiter. On the lattice test for inversive congruential pseudorandom numbers. In Niederreiter and Shiue [4187], pages 186–197. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Chou:1995:PLI

[2031] Wun-Seng Chou. The period lengths of inversive congruential recursions. *Acta Arithmetica*, 73(4):325–341, 1995. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Chow:1995:NRP

[2032] Chee-Seng Chow and Amir Herzberg. Network randomization protocol: a proactive pseudo-random generator. In USENIX [4188], pages 55–64 (or 55–63??). ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL `http://www.usenix.org/publications/library/proceedings/security95/chow.html`.

Compagner:1995:OCR

[2033] A. Compagner. Operational conditions for random-number generation. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 52(5):5634–5645, November 1995. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://pre.aps.org/abstract/PRE/v52/i5/p5634_1`.

Couture:1995:LRC

[2034] Raymond Couture and Pierre L'Ecuyer. Linear recurrences with carry as random number generators. In Alexopoulos et al. [4183], pages 263–267. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56

1995. URL http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=3475. IEEE Catalog No. 95CB35865.

Cusick:1995:PPN

[2035] T. W. Cusick. Properties of the x^2 mod N pseudorandom number generator. *IEEE Transactions on Information Theory*, 41(4):1155–1159, ???? 1995. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Damien:1995:ARV

[2036] Paul Damien, Purushottam W. Laud, and Adrian F. M. Smith. Approximate random variate generation from infinitely divisible distributions with applications to Bayesian inference. *Journal of the Royal Statistical Society. Series B (Methodological)*, 57(3):547–563, ???? 1995. CODEN JSTBAJ. ISSN 0035-9246. URL http://www.jstor.org/stable/2346156.

Dan:1995:CDA

[2037] Asit Dan, Philip S. Yu, and Jen Yao Chung. Characterization of database access pattern for analytic prediction of buffer hit probability. *VLDB Journal: Very Large Data Bases*, 4(1): 127–154, January 1995. CODEN VLDBFR. ISSN 1066-8888 (print), 0949-877X (electronic). URL http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/c/Chung:Jen=Yao.html; http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/d/Dan:Asit.html; http://ftp.informatik.rwth-aachen.de/dblp/db/indices/a-tree/y/Yu:Philip_S=.html. Electronic edition.

Dellaportas:1995:RVT

[2038] Petros Dellaportas. Random variate transformations in the Gibbs sampler: issues of efficiency and convergence. *Statistics and Computing*, 5 (2):133–140, June 1995. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL http://link.springer.com/article/10.1007/BF00143944.

DeMatteis:1995:CCP

[2039] A. De Matteis and S. Pagnutti. Controlling correlations in parallel Monte Carlo. *Parallel Computing*, 21(1):73–84, January 10, 1995. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1995&volume=21&issue=1&aid=939.

Dudewicz:1995:EBR

[2040] E. J. Dudewicz, E. C. van der Meulen, M. G. SriRam, and N. K. W. Teoh. Entropy-based random number evaluation. *American Journal of*

Mathematical and Management Sciences, 15(1–2):115–153, ???? 1995. CODEN AMMSDX. ISSN 0196-6324.

Dwyer:1995:QPR

[2041] Jerry Dwyer. Quick and portable random number generators. *C/C++ Users Journal*, 13(6):33–??, June 1995. CODEN CCUJEX. ISSN 1075-2838.

Edgington:1995:RT

[2042] Eugene S. Edgington. *Randomization tests*, volume 147 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, third edition, 1995. ISBN 0-8247-9669-1. xxii + 409 pp. LCCN QA277 .E32 1995. URL `http://www.loc.gov/catdir/enhancements/fy0647/95021003-d.html`.

Eichenauer-Herrmann:1995:DBN

[2043] Jürgen Eichenauer-Herrmann. Discrepancy bounds for nonoverlapping pairs of quadratic congruential pseudorandom numbers. *Archiv der Mathematik*, 65(4):362–368, ???? 1995. CODEN ACVMAL. ISSN 0003-889X (print), 1420-8938 (electronic).

Eichenauer-Herrmann:1995:IUB

[2044] Jürgen Eichenauer-Herrmann and Harald Niederreiter. An improved upper bound for the discrepancy of quadratic congruential pseudorandom numbers. *Acta Arithmetica*, LXIX(2):193–198, ???? 1995. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Eichenauer-Herrmann:1995:NPE

[2045] Jürgen Eichenauer-Herrmann. Nonoverlapping pairs of explicit inversive congruential pseudorandom numbers. *Monatshefte für Mathematik*, 119 (1–2):49–61, March 1995. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Eichenauer-Herrmann:1995:PNG

[2046] Jürgen Eichenauer-Herrmann. Pseudorandom number generation by nonlinear methods. *International Statistical Review = Revue Internationale de Statistique*, 63(2):247–255, August 1995. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL `http://www.jstor.org/stable/1403620`.

Eichenauer-Herrmann:1995:QCP

[2047] Jürgen Eichenauer-Herrmann. Quadratic congruential pseudorandom numbers: distribution of triples. *Journal of Computational and Applied*

Mathematics, 62(2):239–253, September 20, 1995. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042794001056`.

Eichenauer-Herrmann:1995:RCM

[2048] J. Eichenauer-Herrmann and F. Emmerich. A review of compound methods for pseudorandom number generation. In P. Hellekalek, G. Larcher, and P. Zinterhof, editors, *Proceedings of the 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, November 18, 1994*, volume ACPC/TR 95-4 of *Technical Report Series*, pages 5–14. ACPC – Austrian Center for Parallel Computation, University of Vienna, Vienna, Austria, 1995.

Eichenauer-Herrmann:1995:UAA

[2049] J. Eichenauer-Herrmann. A unified approach to the analysis of compound pseudorandom numbers. *Finite Fields and their Applications*, 1(1):102–114, January 1995. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579785710076`.

Entacher:1995:IPN

[2050] K. Entacher and H. Leeb. Inversive pseudorandom number generators: empirical results. In De Pietro et al. [4184], page ?? ISBN ???? LCCN ???? URL `ftp://random.mat.sbg.ac.at/pub/data/leebSor.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/leebSor.txt`.

Entacher:1995:PSS

[2051] K. Entacher and P. Hellekalek. Parallel stochastic simulation: Inversive pseudorandom number generators. In De Pietro et al. [4184], pages 1–14. ISBN ???? LCCN ????

Feige:1995:RGP

[2052] Uriel Feige. Randomized graph products, chromatic numbers, and Lovasz j-function. In ACM [4182], pages 635–640. ISBN 0-89791-718-9. LCCN QA 76.6 A13 1995. URL `http://www.acm.org/pubs/articles/proceedings/stoc/225058/p635-feige/p635-feige.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/225058/p635-feige/`. ACM order number 508950.

Fleischer:1995:TTP

[2053] Karlheinz Fleischer. Two tests of pseudo random number generators for independence and uniform distribution. *Journal of Statistical Computation and Simulation*, 52(4):311–322, July 1995. CODEN JSCSAJ. ISSN

0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949659508811682.

Gardy:1995:DAS

[2054] Danièle Gardy and Guy Louchard. Dynamic analysis of some relational databases parameters. *Theoretical Computer Science*, 144 (1–2):125–159, June 26, 1995. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1995&volume=144&issue=1-2&aid=1939.

Gilks:1995:ARM

[2055] W. R. Gilks, N. G. Best, and K. K. C. Tan. Adaptive rejection Metropolis sampling within Gibbs sampling. *Applied Statistics*, 44(4):455–472, 1995. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). See corrigendum [2273].

Gutbrod:1995:FRN

[2056] F. Gutbrod. A fast random number generator for the Intel Paragon supercomputer. *Computer Physics Communications*, 87(3):291–306, June 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/001046559500005Z.

Hallgren:1995:LCG

[2057] Sean Hallgren. Linear congruential generators over elliptic curves. Technical Report CS-94-143, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, 1995. 12 pp.

Hamilton:1995:EBU

[2058] Kenneth G. Hamilton. Erratum: *A universal GFSR random number generator for personal computers* [Comput. Phys. Commun. **85** (1995) 127–152]. *Computer Physics Communications*, 86(1–2):208, April 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/001046559500024A. See [2059].

Hamilton:1995:UGR

[2059] Kenneth G. Hamilton. A universal GFSR random number generator for personal computers. *Computer Physics Communications*, 85(1):127–152, January 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/001046559400114H. See erratum [2058].

Han:1995:PGF

[2060] Y. Han and L. A. Hemaspaandra. Pseudorandom generators and the frequency of simplicity. *Lecture Notes in Computer Science*, 900:50–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hellekalek:1995:CBP

[2061] P. Hellekalek. Correlations between pseudorandom numbers: theory and numerical practice. In P. Hellekalek, G. Larcher, and P. Zinterhof, editors, *Proceedings of the 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, November 18, 1994*, volume ACPC/TR 95-4 of *Technical Report Series*, pages 43–73. ACPC – Austrian Center for Parallel Computation, University of Vienna, Vienna, Austria, 1995.

Hellekalek:1995:GDE

[2062] P. Hellekalek. General discrepancy estimates III: the Erdős–Turán–Koksma inequality for the Haar function system. *Monatshefte für Mathematik*, 120(1):25–45, ???? 1995. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Hellekalek:1995:IPN

[2063] P. Hellekalek. Inversive pseudorandom number generators: concepts, results, and links. In Alexopoulos et al. [4183], pages 255–262. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56 1995. URL `http://random.mat.sbg.ac.at`. IEEE Catalog No. 95CB35865.

Hennecke:1995:FIR

[2064] M. Hennecke. A Fortran 90 interface to random number generation. *Computer Physics Communications*, 90(1):117–120, September 1, 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/001046559500065N`.

Hermanns:1995:FCI

[2065] Holger Hermanns, Michael Rettelbach, and Thorsten Weiss. Formal characterisation of immediate actions in SPA with nondeterministic branching. *The Computer Journal*, 38(7):530–541, ???? 1995. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://www3.oup.co.uk/computer_journal/Volume_38/Issue_07/Vol38_07.body.html#AbstractHermanns`.

Herring:1995:TCR

[2066] Charles Herring and Julian I. Palmore. Technical correspondence: Random number generators are chaotic. *Communications of the ACM*, 38(1):121–122, January 1995. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/204895.html`.

Hormann:1995:RTS

[2067] Wolfgang Hörmann. A rejection technique for sampling from T-concave distributions. *ACM Transactions on Mathematical Software*, 21(2):182–193, June 1995. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/203082.203089`; `http://www.acm.org/pubs/citations/journals/toms/1995-21-2/p182-hormann/`.

Kaliski:1995:MIA

[2068] Burton S. Kaliski, Jr. The Montgomery inverse and its applications. *IEEE Transactions on Computers*, 44(8):1064–1065, August 1995. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=403725`. See improvements [2559, 2886].

Kessler:1995:GOC

[2069] Christoph W. Kessler and Thomas Rauber. Generating optimal contiguous evaluations for expression DAGs. *Computer Languages*, 21(2):113–127, July 1995. CODEN COLADA. ISSN 0096-0551 (print), 1873-6742 (electronic).

Koc:1995:RCS

[2070] Cemal Koç. Recurring-with-carry sequences. *Journal of Applied Probability*, 32(4):966–971, December 1995. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL `http://www.jstor.org/stable/3215210`.

Kubota:1995:DRE

[2071] K. Kubota. On distribution of rounding errors generated in additions and subtractions of floating-point numbers. *Transactions of the Japan Society for Industrial and Applied Mathematics*, 5(1):37–46, ???? 1995. CODEN ???? ISSN 0917-2246.

Kurita:1995:DWD

[2072] Yoshiharu Kurita and Makoto Matsumoto. Deviation of the weight distribution of sequences generated by generalized feedback shift registers.

Sūrikaisekikenkyūsho Kōkyūroku, 932:82–102, 1995. CODEN ???? ISSN ???? Various problems in stochastic numerical analysis, II (Japanese) (Kyoto, 1995).

Lee:1995:CSS

[2073] E.-Y Lee, K. J. Kim, and U. J. Choi. A construction of the simplest super pseudorandom permutation generator. *Computers and Mathematics and Applications*, 29(8):19–25, April 1995. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/089812219500026U`.

Leeb:1995:DT

[2074] H. Leeb. On the digit test. In P. Hellekalek, G. Larcher, and P. Zinterhof, editors, *Proceedings of the 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, November 18, 1994*, volume ACPC/TR 95-4 of *Technical Report Series*, pages 109–121. ACPC – Austrian Center for Parallel Computation, University of Vienna, Austria, Vienna, Austria, 1995. URL `ftp://random.mat.sbg.ac.at/pub/data/dtest.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/dtest.txt`.

Leeb:1995:RNC

[2075] Hannes Leeb. Random numbers for computer simulation. Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultät, University of Salzburg, Salzburg, Austria, January 1995. 137 pp. URL `http://www.inf.utfsm.cl/~hallende/download/Simul-2-2002/leebThesis.pdf`.

Lev:1995:TVD

[2076] V. F. Lev. On two versions of L^2-discrepancy and geometrical interpretation of diaphony. *Acta mathematica Academiae Scientiarum Hungaricae*, 69(4):281–300, ???? 1995. CODEN ACMTAV. ISSN 0001-5954, 0236-5294, 1588-2632.

Mahlooji:1995:GAR

[2077] Hashem Mahlooji. Generating antithetic random variates in simulation of a replacement process by rejection method. *Simulation*, 65(2):94–100, August 1995. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/65/2/94.abstract`.

Makino:1995:PFS

[2078] Jun Makino and Osamu Miyamura. Parallelized feedback shift register generators of pseudorandom numbers. *Parallel Computing*, 21 (6):1015–1028, June 12, 1995. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1995&volume=21&issue=6&aid=987`.

Marsaglia:1995:MRN

[2079] George Marsaglia. The Marsaglia random number CDROM including the Diehard Battery of Tests of randomness. Web site at the Department of Statistics, Florida State University, Tallahassee, FL, USA., 1995. URL `http://stat.fsu.edu/pub/diehard/`.

Marsaglia:1995:RVI

[2080] G. Marsaglia. Random variables with independent integer and fractional parts. *Statistica Neerlandica. Journal of the Netherlands Society for Statistics and Operations Research*, 49(2):133–137, July 1995. CODEN ???? ISSN 0039-0402 (print), 1467-9574 (electronic).

Mascagni:1995:FHQ

[2081] Michael Mascagni, Steven A. Cuccaro, Daniel V. Pryor, and M. L. Robinson. A fast, high quality, and reproducible parallel lagged-Fibonacci pseudorandom number generator. *Journal of Computational Physics*, 119(2):211–219, July 1995. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999185711308`.

Mascagni:1995:PPNa

[2082] Michael Mascagni, M. L. Robinson, Daniel V. Pryor, and Steven A. Cuccaro. Parallel pseudorandom number generation using additive lagged-Fibonacci recursions. Report ????, Supercomputing Research Center, IDA, ????, ???? 1995. 15 pp. URL `http://www.cs.fsu.edu/~mascagni/papers/RIJP1995_1.pdf`.

Mascagni:1995:PPNb

[2083] Michael Mascagni, M. L. Robinson, Daniel V. Pryor, and Steven A. Cuccaro. Parallel pseudorandom number generation using additive lagged-Fibonacci recursions. In Niederreiter and Shiue [4187], pages 263–277. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Matus:1995:CIAa

[2084] F. Matúš and M. Studený. Conditional independences among four random variables. I. *Combinatorics, Probability and Computing*, 4(3):269–278, September 1995. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Matus:1995:CIAb

[2085] F. Matúš. Conditional independences among four random variables. II. *Combinatorics, Probability and Computing*, 4(4):407–417, December 1995. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic).

Micali:1995:SMG

[2086] Silvio Micali and Ray Sidney. A simple method for generating and sharing pseudo-random functions, with applications to Clipper-like key escrow systems. *Lecture Notes in Computer Science*, 963:185–??, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/0963/09630185.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/0963/09630185.pdf`.

Miller:1995:RAC

[2087] John W. Miller. Random access from compressed datasets with perfect value hashing. *IEEE International Symposium on Information Theory*, page 454, 1995. CODEN PISTFZ. ISSN 0271-4655 (print), 2157-8125 (electronic). IEEE catalog number 95CB35738.

Moler:1995:CCR

[2088] Cleve B. Moler. Cleve's corner: Random thoughts: 10^{435} years is a very long time. Technical note, The MathWorks, Inc., 3 Apple Hill Drive, Natick, MA 01760-2098, USA, Fall 1995. 2 pp. URL `http://www.mathworks.com/company/newsletter/pdf/Cleve.pdf`.

Montanari:1995:CRG

[2089] Gian Carlo Montanari, Andrea Cavallini, Laura Tommasini, Mario Cacciari, and Alfredo Contin. Comparison of random generators for Monte Carlo estimates of Weibull parameters. *Metron*, 53(1–2):55–77, ???? 1995. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Morokoff:1995:QMC

[2090] William J. Morokoff and Russel E. Caflisch. Quasi-Monte Carlo integration. *Journal of Computational Physics*, 122(2):218–230, December 1995. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999185712090`.

Mullen:1995:TNS

[2091] Gary L. Mullen, Arijit Mahalanabis, and Harald Niederreiter. Tables of (t, m, s)-net and (t, s)-sequence parameters. In Niederreiter and Shiue [4187], pages 58–86. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Nelson:1995:UCR

[2092] B. L. Nelson and F. J. Matejcik. Using Common Random Numbers for indifference-zone selection and multiple comparisons in simulation. *Management Science*, 41(??):1935–1945, ???? 1995. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Niederreiter:1995:MRM

[2093] Harald Niederreiter. The multiple-recursive matrix method for pseudorandom number generation. *Finite Fields and their Applications*, 1(1): 3–30, January 1995. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic).

Niederreiter:1995:NDU

[2094] Harald Niederreiter. New developments in uniform pseudorandom number and vector generation. In Niederreiter and Shiue [4187], pages 87–120. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Niederreiter:1995:PVG

[2095] Harald Niederreiter. Pseudorandom vector generation by the multiple-recursive matrix method. *Mathematics of Computation*, 64(209):279–294, January 1995. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153334.pdf`.

Ong:1995:CBG

[2096] S. H. Ong. Computation of bivariate gamma and inverted beta distribution functions. *Journal of Statistical Computation and Simulation*, 51 (2-4):153–163, 1995. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Owen:1995:RPN

[2097] A. B. Owen. Randomly permuted (t, m, s)-nets and (t, s)-sequences. In Niederreiter and Shiue [4187], pages 299–317. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

Palubeckis:1995:HBB

[2098] G. Palubeckis. A heuristic-based branch and bound algorithm for unconstrained quadratic zero-one programming. *Computing: Archiv für Informatik und Numerik*, 54(4):283–301, December 1995. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=255&id_volume=20&id_journal=8`.

Pattanaik:1995:AER

[2099] S. N. Pattanaik and S. P. Mudur. Adjoint equations and random walks for illumination computation. *ACM Transactions on Graphics*, 14(1):77–102, January 1995. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0730-0301/200985.html`.

Penrice:1995:AEP

[2100] Stephen G. Penrice. Applying elementary probability theory to the NBA draft lottery. *SIAM Review*, 37(4):598–602, December 1995. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic). URL `http://epubs.siam.org/27302.htm`.

Percus:1995:TAM

[2101] Ora E. Percus and Paula A. Whitlock. Theory and application of Marsaglia's monkey test for pseudorandom number generators. *ACM Transactions on Modeling and Computer Simulation*, 5(2):87–100, April 1995. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). See [1853].

Phatak:1995:LMP

[2102] S. C. Phatak and S. Suresh Rao. Logistic map: a possible random-number generator. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 51(4):3670–3678, April 1995. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.51.3670`.

Pickover:1995:GET

[2103] Clifford A. Pickover. Generating extraterrestrial terrain. *IEEE Computer Graphics and Applications*, 15(2):18–21, March 1995. CODEN ICGADZ. ISSN 0272-1716 (print), 1558-1756 (electronic).

Pickover:1995:RNG

[2104] C. A. Pickover. Random number generators: pretty good ones are easy to find. *Visual Computer*, 11:369–377, 1995. CODEN VICOE5. ISSN 0178-2789 (print), 1432-2315 (electronic).

Powell:1995:LEP

[2105] Patrick Powell and Justin Mason. LPRng — an enhanced printer spooler system. In USENIX [4189], pages 13–24. ISBN 1-880446-73-1. LCCN QA 76.76 O63 S97 1995. URL `http://www.usenix.org/publications/library/proceedings/lisa95/papowell.html`.

Ramon:1995:PKV

[2106] J. Ramon and P. Pena. Parallelization of KENO-Va Monte Carlo code. *Computer Physics Communications*, 88(1):76–82, July 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic).

Regan:1995:PGM

[2107] K. W. Regan, D. Sivakumar, and Jin-Yi Cai. Pseudorandom generators, measure theory, and natural proofs. In IEEE [4185], pages 26–35. CODEN ASFPDV. ISBN 0-7803-3121-4 (casebound), 0-8186-7183-1 (softbound), 0-8186-7184-X (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1995. IEEE catalog number 95CB35834.

Roos:1995:CWK

[2108] Andrew Roos. A class of weak keys in the RC4 stream cipher. Technical report, Vironix Software Laboratories, ????, September 22, 1995. 1–8 pp. URL `http://isn.dnsalias.org/Luminy/WeakKeys-report.pdf`; `https://marcel.wanda.ch/Archive/WeakKeys`.

Ross:1995:TCP

[2109] D. E. Ross. Technical correspondence: Pseudo-random number generators for a calculator. *Communications of the ACM*, 38(1):122–124, January 1995. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/toc/Abstracts/0001-0782/204896.html`.

Sakamoto:1995:CMC

[2110] Munetaka Sakamoto and Susumu Morito. Combination of multiplicative congruential random-number generators with safe prime modulus. In Alexopoulos et al. [4183], pages 309–315. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56 1995. URL `http://doi.acm.org/10.1145/224401.224623`. IEEE Catalog No. 95CB35865.

Savory:1995:UMA

[2111] Paul A. Savory. Using Mathematica to aid simulation analysis. In Alexopoulos et al. [4183], pages 1324–1328. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56 1995. URL `http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=3475`. IEEE Catalog No. 95CB35865.

Schmid:1995:EMC

[2112] F. Schmid and N. B. Wilding. Errors in Monte Carlo simulations using shift register random number generators. *International Journal of Modern Physics C [Physics and Computers]*, 6(6):781–787, December 1995. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic).

Sezgin:1995:SRN

[2113] F. Sezgin. Some remarks on a new composite random number generator. *Computers and Mathematics and Applications*, 30(11):125–130, December 1995. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/089812219500169Y`. See [1877].

Sherif:1995:UWF

[2114] Yosef S. Sherif and Roger G. Dear. Using Walsh functions to test a new composite Sherif–Dear (CSD) random number generator. *Simulation*, 65 (5):338–342, November 1995. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic).

Sobol:1995:IQS

[2115] Ilya M. Sobol' and Boris V. Shukhman. Integration with quasirandom sequences: numerical experience. *International Journal of Modern Physics C [Physics and Computers]*, 6(2):263–275, April 1995. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic).

Sorenson:1995:ALE

[2116] Jonathan Sorenson. An analysis of Lehmer's Euclidean GCD algorithm. In Levelt [4186], pages 254–258. ISBN 0-89791-699-9. LCCN QA 76.95 I59 1995. URL `http://www.acm.org:80/pubs/citations/proceedings/issac/220346/p254-sorenson/`. ACM order number 505950.

Storn:1995:CO

[2117] Rainer Storn. Constrained optimization. *Dr. Dobb's Journal of Software Tools*, 20(5):119–123, May 1995. CODEN DDJOEB. ISSN 1044-789X.

Struckmeier:1995:FGL

[2118] J. Struckmeier. Fast generation of low-discrepancy sequences. *Journal of Computational and Applied Mathematics*, 61(1):29–41, July 20, 1995. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0377042794000545`.

Sugita:1995:PRN

[2119] Hiroshi Sugita. Pseudo-random number generator by means of irrational rotation. *Monte Carlo Methods and Applications*, 1(1):35–57, ???? 1995. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1995.1.issue-1/mcma.1995.1.1.35/mcma.1995.1.1.35.xml`.

Takashima:1995:STT

[2120] K. Takashima. Sojourn time test for m-sequences with characteristic pentanomials. *Journal of Japanese Society of Computational Statistics*, 8(??):37–46, ???? 1995. ISSN 0915-2350 (print), 1881-1337 (electronic).

Tezuka:1995:URN

[2121] Shu Tezuka. *Uniform random numbers: theory and practice*. The Kluwer international series in engineering and computer science. Discrete event dynamic systems. Kluwer Academic Publishers, Norwell, MA, USA, and Dordrecht, The Netherlands, 1995. ISBN 0-7923-9572-7. xii + 209 pp. LCCN QA298 .T49 1995. URL `http://www.loc.gov/catdir/enhancements/fy0813/95010562-d.html`; `http://www.loc.gov/catdir/enhancements/fy0813/95010562-t.html`.

Varhol:1995:ANS

[2122] Peter D. Varhol. An architecture for network simulation. *Dr. Dobb's Journal of Software Tools*, 20(7):70, 72, 74, 76, 78, July 1995. CODEN DDJOEB. ISSN 1044-789X.

Vattulainen:1995:CSS

[2123] I. Vattulainen, K. Kankaala, J. Saarinen, and T. Ala-Nissila. A comparative study of some pseudorandom number generators. *Computer Physics Communications*, 86(3):209–226, May 1, 1995. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465595000158`.

Vattulainen:1995:MIF

[2124] I. Vattulainen and T. Ala-Nissila. Mission impossible: Find a random pseudorandom number generator. *Computers in Physics*, 9(5):500–504, September 1995. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL `http://link.aip.org/link/?CIP/9/500/1`.

Vattulainen:1995:PMT

[2125] I. Vattulainen, T. Ala-Nissila, and K. Kankaala. Physical models as tests of randomness. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 52(3):3205–3214, September 1995. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.52.3205`.

Wagner:1995:MRW

[2126] D. Wagner. My RC4 weak keys. Post in sci.crypt, message–id 447o1l$cbj@cnn.princeton.EDU, 1995.

Walker:1995:GRV

[2127] Stephen Walker. Generating random variates from D-distributions via substitution sampling. *Statistics and Computing*, 5(4):311–315, December 1995. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00162504`.

Wegenkittl:1995:ETPa

[2128] S. Wegenkittl. Empirical testing of pseudorandom number generators. Master's thesis, University of Salzburg, 1995. URL `ftp://random.mat.sbg.ac.at//pub/publications/ste/masters_thesis/dipl.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/steThesis.txt`; `http://random.mat.sbg.ac.at/~ste/dipl/`.

Wegenkittl:1995:ETPb

[2129] S. Wegenkittl. On empirical testing of pseudorandom number generators. In De Pietro et al. [4184], page ?? ISBN ???? LCCN ???? URL `ftp://random.mat.sbg.ac.at/pub/data/steSor.ps`; `http://random.mat.sbg.ac.at/ftp/pub/data/steSor.txt`.

Wegenkittl:1995:THS

[2130] Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inversive congruential pseudorandom numbers? *Journal of Computational and Applied Mathematics*, 62(2):117–125, September 20, 1995. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042798000776`.

Wheeler:1995:TTE

[2131] David J. Wheeler and Roger M. Needham. TEA, a tiny encryption algorithm. *Lecture Notes in Computer Science*, 1008:363–366, 1995. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/p16916lx735m2562/`. See also extensions XTEA [2303] and XXTEA [2414].

Wong:1995:EHS

[2132] W. F. Wong, Yoshio Oyanagi, and Eiichi Goto. Evaluation of the Hitachi S-3800 supercomputer using six benchmarks. *The International Journal of Supercomputer Applications and High Performance Computing*, 9(1): 58–70, Spring 1995. CODEN IJSAE9. ISSN 0890-2720.

Zhu:1995:MEC

[2133] Yaochen Zhu. A method for exact calculation of the discrepancy of low-dimensional finite points sets. II. *Acta Mathematica Sinica (New Series)*, 11(4):422–434, 1995. ISSN 1000-9574. A Chinese summary appears in Acta Math. Sinica **3**9 (1996), no. 5, 720.

Aluru:1996:PAL

[2134] S. Aluru. Parallel additive lagged Fibonacci random number generators. In ACM [4190], pages 102–108. ISBN 0-89791-803-7. LCCN QA76.5 I61 1996. ACM order number 415961.

Anderson:1996:GPR

[2135] Jon E. Anderson and Thomas A. Louis. Generating pseudo-random variables from mixture models by exemplary sampling. *Journal of Statistical Computation and Simulation*, 54(1-3):45–53, 1996. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Anonymous:1996:BRPe

[2136] Anonymous. Book review: *Pseudorandomness and cryptographic applications*: By Michael Luby. Princeton University Press, Princeton, NJ. (1996). 234 pages. $24.95, £20. *Computers and Mathematics and Applications*, 31(11):139, June 1996. CODEN CMAPDK. ISSN 0898-1221

(print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122196873482`.

Antipov:1996:IRN

[2137] M. V. Antipov and G. A. Mihailov. On the improvement in random number generators by using a modulo 1 sum. *Russian Journal of Numerical Analysis and Mathematical Modelling*, 11(2):93–111, January 1996. CODEN RJNMEH. ISSN 0927-6467 (print), 1569-3988 (electronic).

Antipov:1996:SNM

[2138] M. V. Antipov. Sequences of numbers for Monte Carlo methods. *Monte Carlo Methods and Applications*, 2(3):219–235, ???? 1996. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1996.2.issue-3/mcma.1996.2.3.219/mcma.1996.2.3.219.xml`.

Armoni:1996:DSP

[2139] R. Armoni, M. Saks, A. Wigderson, and Shiyu Zhou. Discrepancy sets and pseudorandom generators for combinatorial rectangles. In IEEE [4194], pages 412–421. CODEN ASFPDV. ISBN 0-7803-3762-X (casebound), 0-8186-7594-2 (softbound), 0-8186-7596-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1996. IEEE catalog number 96CH35973. IEEE Computer Society Press order number PR07594.

Baldwin:1996:PIB

[2140] Robert W. Baldwin. Proper initialization for the BSAFE random number generator. *RSA Laboratories' Bulletin*, 3:1–2, January 25, 1996. CODEN ???? ISSN ???? URL `ftp://ftp.rsasecurity.com/pub/pdfs/bull-3.pdf`.

Banks:1996:DES

[2141] Jerry Banks, John S. Carson II, and Barry L. Nelson. *Discrete-Event System Simulation*. Prentice-Hall international series in industrial and systems engineering. Prentice-Hall, Upper Saddle River, NJ, USA, second edition, 1996. ISBN 0-13-217449-9. xii + 548 pp. LCCN T57.62 .B35 1996.

Barcucci:1996:DPP

[2142] Elena Barcucci, Alberto Del Lungo, and Renzo Pinzani. "Deco" polyominoes, permutations and random generation. *Theoretical Computer Science*, 159(1):29–42, May 28, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1996&volume=159&issue=1&aid=2140`.

Barron:1996:RTR

[2143] Nick Barron. *RSAEuro Technical Reference*. Compulink, ????, third edition, November 1996. v + 75 pp. URL `http://www.rsaeuro.com/products/RSAEuro/rsadown.shtml`; `mailto:nikb@cix.compulink.co.uk`.

Barry:1996:RTU

[2144] Timothy M. Barry. Recommendations on the testing and use of pseudorandom number generators used in Monte Carlo analysis for risk assessment. *Risk Analysis*, 16(1):93–105, February 1996. CODEN RIANDF. ISSN 1539-6924.

Beaver:1996:CPC

[2145] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In ACM [4191], pages 479–488. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. URL `http://www.acm.org/pubs/articles/proceedings/stoc/237814/p479-beaver/p479-beaver.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/237814/p479-beaver/`. ACM order number 508960. Also known as Federated Computing Research Conference (FCRS '96).

Bellare:1996:PFR

[2146] M. Bellare, R. Canetti, and H. Krawczyk. Pseudorandom functions revisited: the cascade construction and its concrete security. In IEEE [4194], pages 514–523. CODEN ASFPDV. ISBN 0-7803-3762-X (casebound), 0-8186-7594-2 (softbound), 0-8186-7596-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1996. IEEE catalog number 96CH35973. IEEE Computer Society Press order number PR07594.

Berdnikov:1996:NMP

[2147] A. S. Berdnikov, S. B. Trutia, and A. Compagner. Notebook: a MathLink program for high-quality random numbers. *Mathematica Journal*, 6(3):65–69, Summer 1996. CODEN ???? ISSN 1047-5974 (print), 1097-1610 (electronic). URL `http://www.mathematica-journal.com/issue/v6i3/article/berdnikov/contents/63berdnikov.nb`; `http://www.mathematica-journal.com/issue/v6i3/article/berdnikov/contents/63berdnikov.pdf`; `http://www.mathematica-journal.com/issue/v6i3/article/berdnikov/index.html`.

Bernhofen:1996:RBR

[2148] L. T. Bernhofen, E. J. Dudewicz, and E. C. van der Meulen. Ranking the best random number generators via entropy-uniformity theory. *American*

Journal of Mathematical and Management Sciences, 16(1–2):49–88, ???? 1996. CODEN AMMSDX. ISSN 0196-6324.

Beyer:1996:CLS

[2149] W. A. Beyer and W. W. Wood. Corrigenda: "The lattice structure of multiplicative congruential pseudo-random vectors" [Math. Comp. **25** (1971), 345–363, MR **46** #8373] by W. A. Beyerm, R. B. Roof, and Dorothy Williamson. *Mathematics of Computation*, 65(213):445–446, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2153872.pdf`. See [544].

Bland:1996:SRN

[2150] I. M. Bland and G. M. Megson. Systolic random number generation for genetic algorithms. *Electronics Letters*, 32(12):1069–1070, June 6, 1996. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=502856`.

Boppana:1996:BCP

[2151] Ravi B. Boppana and Babu O. Narayanan. The biased coin problem. *SIAM Journal on Discrete Mathematics*, 9(1):29–36, February 1996. CODEN SJDMEC. ISSN 0895-4801 (print), 1095-7146 (electronic).

Bromley:1996:QNG

[2152] B. C. Bromley. Quasirandom number generators for parallel Monte Carlo algorithms. *Journal of Parallel and Distributed Computing*, 38(1):101–104, October 10, 1996. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0132/production; http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0132/production/pdf; http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0133/production; http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0133/production/pdf`.

Brunner:1996:PCO

[2153] D. Brunner and A. Uhl. Parallel computation of optimal parameters for pseudo random number generation. *Lecture Notes in Computer Science*, 1127:78–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bryc:1996:BRB

[2154] Wlodzimierz Bryc. Book review: *Limit Theorems of Probability Theory: Sequences of Independent Random Variables* (Valentin V. Petrov).

SIAM Review, 38(3):527, ???? 1996. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Burthe:1996:FIS

[2155] Ronald Joseph Burthe, Jr. Further investigations with the strong probable prime test. *Mathematics of Computation*, 65(213):373–381, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00695-3&u=/mcom/1996-65-213/`.

Chandwani:1996:FAP

[2156] M. Chandwani and N. S. Chaudhari. Formulation and analysis of parallel context-free recognition and parsing on a PRAM model. *Parallel Computing*, 22(6):845–868, September 20, 1996. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1996&volume=22&issue=6&aid=1067`.

Coddington:1996:TRN

[2157] P. D. Coddington. Tests of random number generators using Ising model simulations. *International Journal of Modern Physics C [Physics and Computers]*, 3(3):295–303, June 1996. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/07/0703/S0129183196000235.html`.

Couture:1996:OLL

[2158] Raymond Couture and Pierre L'Ecuyer. Orbits and lattices for linear random number generators with composite moduli. *Mathematics of Computation*, 65(213):189–201, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00673-4&u=/mcom/1996-65-213/`; `http://www.jstor.org/stable/2153839`.

Devroye:1996:RVG

[2159] Luc Devroye. Random variate generation in one line of code. In Charnes et al. [4192], pages 265–272. ISBN 0-7803-3383-7. LCCN QA76.9.C65 W56 1996. URL `http://cgm.cs.mcgill.ca/~luc/wsc96.pdf`; `http://cgm.cs.mcgill.ca/~luc/wsc96.ps`. IEEE catalog number 96CB35957.

Dietzfelbinger:1996:UHW

[2160] Martin Dietzfelbinger. Universal hashing and k-wise independent random variables via integer arithmetic without primes. *Lecture Notes in*

Computer Science, 1046:567–580, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dodge:1996:NRN

[2161] Yadolah Dodge. A natural random number generator. *International Statistical Review = Revue Internationale de Statistique*, 64(3):329–344, December 1996. CODEN ISTRDP. ISSN 0306-7734 (print), 1751-5823 (electronic). URL `http://www.jstor.org/stable/1403789`.

Dorfman:1996:PSR

[2162] Jeffrey H. Dorfman. Pseudorandom sampling has a real effect on test size. *The American Statistician*, 50(2):151–??, ???? 1996. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/pdfplus/2684427.pdf`.

Dwyer:1996:TRNa

[2163] Jerry Dwyer and K. B. Williams. Testing random number generators. *C/C++ Users Journal*, 14(6):39–??, June 1996. CODEN CCUJEX. ISSN 1075-2838.

Dwyer:1996:TRNb

[2164] Jerry Dwyer and K. B. Williams. Testing random number generators, part 2. *C/C++ Users Journal*, 14(8):57–??, August 1996. CODEN CCUJEX. ISSN 1075-2838.

Eichenauer-Herrmann:1996:ABC

[2165] Jürgen Eichenauer-Herrmann and Gerhard Larcher. Average behaviour of compound nonlinear congruential pseudorandom numbers. *Finite Fields and their Applications*, 2(1):111–123, January 1996. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579796900088`.

Eichenauer-Herrmann:1996:CIC

[2166] Jürgen Eichenauer-Herrmann and Frank Emmerich. Compound inversive congruential pseudorandom numbers: an average-case analysis. *Mathematics of Computation*, 65(213):215–225, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00675-8&u=/mcom/1996-65-213/`; `http://www.jstor.org/stable/2153841`.

Eichenauer-Herrmann:1996:EPI

[2167] Jürgen Eichenauer-Herrmann. Equidistribution properties of inversive congruential pseudorandom numbers with power of two modulus.

Metrika. International Journal for Theoretical and Applied Statistics., 44(3):199–205, 1996. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic).

Eichenauer-Herrmann:1996:MEI

[2168] Jürgen Eichenauer-Herrmann. Modified explicit inversive congruential pseudorandom numbers with power of 2 modulus. *Statistics and Computing*, 6(1):31–36, March 1996. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/BF00161571`.

Emmerich:1996:PVG

[2169] Frank Emmerich. Pseudorandom vector generation by the compound inversive method. *Mathematics of Computation*, 65(214):749–760, April 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00706-5&u=/mcom/1996-65-214/`; `http://www.jstor.org/stable/2153611`.

Entacher:1996:RSP

[2170] Karl Entacher and Stefan Wegenkittl. On the relevance of splitting properties and the compound method in parallel applications of pseudorandom number generators. In Trobec et al. [4195], pages 64–74. ISBN 86-80023-25-6. LCCN ????

Fernandez:1996:FAR

[2171] J. F. Fernández and J. Rivero. Fast algorithm for random numbers with exponential and normal distributions. *Computers in Physics*, 10 (1):83–88, January 1996. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). See [2438] for a proof of the algorithm proposed here for exponential random numbers.

Fischer:1996:EPR

[2172] Jean-Bernard Fischer and Jacques Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. *Lecture Notes in Computer Science*, 1070:245–255, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1070/10700245.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1070/10700245.pdf`. EUROCRYPT96 proceedings.

Fishman:1996:MCC

[2173] George S. Fishman. *Monte Carlo: concepts, algorithms, and applications*. Springer series in operations research. Springer-Verlag, Berlin,

Germany / Heidelberg, Germany / London, UK / etc., 1996. ISBN 0-387-94527-X. xxv + 698 pp. LCCN QA298 .F57 1996.

Goldberg:1996:RNB

[2174] Ian Goldberg and David Wagner. Randomness and the Netscape browser. *Dr. Dobb's Journal of Software Tools*, 21(1):66, 68–70, January 1996. CODEN DDJOEB. ISSN 1044-789X.

Gunther:1996:ZLE

[2175] R. Günther, L. Levitin, B. Schapiro, and P. Wagner. Zipf's law and the effect of ranking on probability distributions. *International Journal of Theoretical Physics*, 35(2):395–417, 1996. CODEN IJTPBM. ISSN 0020-7748 (print), 1572-9575 (electronic).

Gutbrod:1996:PRR

[2176] F. Gutbrod. On the periods of the `ranshi` random number generator. *International Journal of Modern Physics C [Physics and Computers]*, 7 (6):909–922, December 1996. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/07/0706/S0129183196000764.html`.

Han:1996:PGF

[2177] Yenjo Han and Lane A. Hemaspaandra. Pseudorandom generators and the frequency of simplicity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(4):251–261, Fall 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/9n4p251.html`; `http://link.springer.de/link/service/journals/00145/bibs/9n4p251.pdf`; `http://link.springer.de/link/service/journals/00145/bibs/9n4p251.tex`; `http://link.springer.de/link/service/journals/00145/tocs/00904.html`.

Heinrich:1996:EAC

[2178] S. Heinrich. Efficient algorithms for computing the L_2 discrepancy. *Mathematics of Computation*, 65(216):1621–1633, October 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00756-9&u=/mcom/1996-65-216/`.

Hofmeister:1996:ISG

[2179] Thomas Hofmeister and Hanno Lefmann. Independent sets in graphs with triangles. *Information Processing Letters*, 58(5):207–210, June 10, 1996. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Hormann:1996:RIG

[2180] W. Hörmann and G. Derflinger. Rejection-inversion to generate variates from monotone discrete distributions. *ACM Transactions on Modeling and Computer Simulation*, 6(3):169–184, July 1996. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Horstmann:1996:CCL

[2181] C. S. Horstmann. C++ class libraries for numerical programming. *C++ Report*, 8(1):61–64, 66, January 1996. CODEN CRPTE7. ISSN 1040-6042.

James:1996:ERF

[2182] F. James. Erratum: RANLUX: A Fortran implementation of the high-quality pseudorandom number generator of Lüscher [Comput. Phys. Commun. **79** (1994) 111–114]. *Computer Physics Communications*, 97(3):357, September 1996. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0010465596000653`. See [1949].

Johnson:1996:RES

[2183] Brad C. Johnson. Radix-b extensions to some common empirical tests for pseudorandom number generators. *ACM Transactions on Modeling and Computer Simulation*, 6(4):261–273, October 1996. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Jones:1996:TRV

[2184] M. C. Jones and A. D. Lunn. Transformations and random variate generation: Generalised ratio-of-uniforms methods. *Journal of Statistical Computation and Simulation*, 55(1–2):49–55, ???? 1996. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Kamgar-Parsi:1996:DMW

[2185] Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh. Distribution and moments of the weighted sum of uniforms random variables, with applications in reducing Monte Carlo simulations. *Journal of Statistical Computation and Simulation*, 52(4):399–414, ???? 1996. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659508811688`.

Kao:1996:EAP

[2186] Chiang Kao and J. Y. Wong. An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus

smaller than 2^{15}. *Journal of Statistical Computation and Simulation*, 54(1–3):29–35, ???? 1996. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659608811717`.

Kato:1996:NCP

[2187] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. On a nonlinear congruential pseudorandom number generator. *Mathematics of Computation*, 65(213):227–233, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00694-1&u=/mcom/1996-65-213/`; `http://www.jstor.org/stable/2153842`. See [2188] for a treatment of the discrepancy of the inversive congruential generator, [2287] for an analysis of lattice structure of inverse congruential generators.

Kato:1996:STN

[2188] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. The serial test for a nonlinear pseudorandom number generator. *Mathematics of Computation*, 65(214):761–769, April 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00712-0&u=/mcom/1996-65-214/`; `http://www.jstor.org/stable/2153612`. See [2187] for the original work, and [2287] for a treatment of the lattice structure of the inversive congruential generator.

Kemp:1996:CFP

[2189] C. David Kemp. The construction of fast portable multiplicative congruential random number generators. *Communications of the ACM*, 39(12es):163–166, 1996. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://www.acm.org/pubs/articles/journals/cacm/1996-39-12es/a163-kemp/a163-kemp.pdf`; `http://www.acm.org/pubs/citations/journals/cacm/1996-39-12es/a163-kemp/`.

Koc:1996:ACM

[2190] Çetin Kaya Koç, Tolga Acar, and Burton S. Kaliski, Jr. Analyzing and comparing Montgomery multiplication algorithms — assessing five algorithms that speed up modular exponentiation, the most popular method of encrypting and signing digital data. *IEEE Micro*, 16(3):26–33, May/June 1996. CODEN IEMIDZ. ISSN 0272-1732 (print), 1937-4143 (electronic).

LEcuyer:1996:CMR

[2191] Pierre L'Ecuyer. Combined multiple recursive random number generators. *Operations Research*, 44(5):816–822, October 1996. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `Student:1908:PEM`.

LEcuyer:1996:CSA

[2192] Pierre L'Ecuyer. Commentary — simulation of algorithms for performance analysis. *INFORMS Journal on Computing*, 8(1):16–20, Winter 1996. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

LEcuyer:1996:LUG

[2193] P. L'Ecuyer and R. Couture. LatMRG user's guide: a toolkit for theoretical testing of simple and combined linear congruential and multiple recursive generators. Technical report, Université de, Montréal, QC, Canada, 1996.

LEcuyer:1996:MEC

[2194] Pierre L'Ecuyer. Maximally equidistributed combined Tausworthe generators. *Mathematics of Computation*, 65(213):203–213, January 1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-96-00696-5&u=/mcom/1996-65-213/`.

LEcuyer:1996:RNG

[2195] Pierre L'Ecuyer. Random number generators. In Saul Irving Gass and Carl M. Harris, editors, *Encyclopedia of Operations Research and Management Science*, pages 571–578. Kluwer Academic Publishers, Norwell, MA, USA, and Dordrecht, The Netherlands, 1996. ISBN 0-7923-9590-5. LCCN T57.6 .E53 1996.

LEcuyer:1996:TPR

[2196] P. L'Ecuyer and J.-F. Cordeau. Tests sur les points rapprochés pour les générateurs de valeurs aléatoires. (French) [Tests on nearby points for random-number generators]. In *Compte-Rendus de ASU'96: Les XXVIII-ièmes Journées de Statistique*, pages 479–482. ????, Département de Mathématiques, Université Laval, QC, Canada, 1996.

Lu:1996:PPG

[2197] Tan-Chun Lu, Yu-Song Hou, and Rong-Jaye Chen. A parallel Poisson generator using parallel prefix. *Computers and Mathematics and Applications*, 31(3):33–42, February 1996. CODEN CMAPDK. ISSN 0898-1221

(print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/0898122195002049`.

Luby:1996:PCA

[2198] Michael George Luby. *Pseudorandomness and cryptographic applications*. Princeton computer science notes. Princeton University Press, Princeton, NJ, USA, 1996. ISBN 0-691-02546-0. xvi + 234 pp. LCCN QA298 .L83 1996.

Luo:1996:TDS

[2199] Ping Luo. The two-dimensional structure of the sequence of random numbers generated by multiplicative congruential generators. *Journal on Numerical Methods and Computer Applications*, 17(1):48–56, 1996. CODEN ???? ISSN 1000-3266.

Marini:1996:CHR

[2200] Marc Marini. A class hierarchy for random number generation. *C/C++ Users Journal*, 14(10):51–??, October 1996. CODEN CCUJEX. ISSN 1075-2838.

Marsaglia:1996:DBT

[2201] George Marsaglia. DIEHARD: a battery of tests of randomness. Technical report ????, Florida State University, Tallahassee, FL, USA, 1996. URL `http://euler.bd.psu.edu/~naras/diehard/snapshots.html`; `http://stat.fsu.edu/~geo/`; `http://www.stat.fsu.edu/pub/diehard/`.

Masuda:1996:PPR

[2202] N. Masuda and F. Zimmerman. PRNGlib: a parallel random number generator library. Technical Report TR-96-08, Swiss Center for Scientific Computing, Lugano, Switzerland, 1996. 48 pp.

Matsumoto:1996:SDR

[2203] Makoto Matsumoto and Yoshiharu Kurita. Strong deviations from randomness in m-sequences based on trinomials. *ACM Transactions on Modeling and Computer Simulation*, 6(2):99–106, April 1996. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Matthews:1996:SRN

[2204] Tim Matthews. Suggestions for random number generation in software. *RSA Laboratories' Bulletin*, 1:1–4, January 22, 1996. CODEN ???? ISSN ???? URL `ftp://ftp.rsasecurity.com/pub/pdfs/bull-1.pdf`.

Mikhailov:1996:ENU

[2205] G. A. Mikhailov and M. V. Antipov. Estimations of non-uniformity for distributions of the congruent sums of random values. *Doklady Akademii Nauk SSSR*, 347(1):23–26, ???? 1996. CODEN DANKAS. ISSN 0002-3264.

Mikhailov:1996:RSR

[2206] V. G. Mikhaĭlov. Repetition of states of a random-number generator under multiple access. *Theory of Probability and its Applications*, 40 (4):679–689, ???? 1996. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). Original Russian article in *Teor. Veroyatnost. i Primenen.*, **40**(4), (1995), pp. 786–797.

Mikov:1996:LSA

[2207] Alexander I. Mikov. Large-scale addition of machine real numbers: Accuracy estimates. *Theoretical Computer Science*, 162(1):151–170, August 05, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1996&volume=162&issue=1&aid=2194`.

Mulmuley:1996:RGA

[2208] Ketan Mulmuley. Randomized geometric algorithms and pseudorandom generators. *Algorithmica*, 16(4–5):450–463, 1996. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Nemnyugin:1996:SRW

[2209] S. Nemnyugin and A. Larionov. Set of random walk tests for pseudorandom generators. In Peter Borcherds, Marian Bubak, and Andrzej Maksymowicz, editors, *Proceedings of the 8th Joint EPS-APS International Conference on Physics Computing: PC '96: September 17–21, 1996, Kraków, Poland*, pages 269–272. Academic Computer Centre CYFRONET, Kraków, Poland, 1996. ISBN 83-902363-3-8. LCCN QC20 .I45 1996.

Niederreiter:1996:IBM

[2210] Harald Niederreiter. Improved bounds in the multiple-recursive matrix method for pseudorandom number and vector generation. *Finite Fields and their Applications*, 2(3):225–240, July 1996. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579796900155`.

Niederreiter:1996:LDS

[2211] H. Niederreiter and C. Xing. Low-discrepancy sequences and global function fields with many rational places. *Finite Fields and their Applications*, 2(3):241–273, ???? 1996. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic).

Niederreiter:1996:QPG

[2212] H. Niederreiter and C. Xing. Quasirandom points and global function fields. In Cohen and Niederreiter [4193], pages 269–296. ISBN 0-521-56736-X (paperback). LCCN QA247.3 .F535 1996.

Nisan:1996:ERH

[2213] N. Nisan. Extracting randomness: How and why, a survey. In Steve Homer and Jin-Yi Cai, editors, *Proceedings of the 11th Annual IEEE Conference on Computational Complexity, 24–27 May 1996*, pages 44–58. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7386-9, 0-8186-7387-7 (casebound), 0-8186-7388-5 (microfiche). LCCN QA267 S927 1996.

Ogawa:1996:RRP

[2214] Shigeyoshi Ogawa. On a robustness of the random particle method. *Monte Carlo Methods and Applications*, 2(3):175–189, ???? 1996. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1996.2.issue-3/mcma.1996.2.3.175/mcma.1996.2.3.175.xml`; `https://www.math.utah.edu/pub/tex/bib/prng.bib`. See erratum [2305].

Paplinski:1996:HIL

[2215] A. P. Paplinski and N. Bhattacharjee. Hardware implementation of the Lehmer random number generator. *IEE Proceedings. Computers and Digital Techniques*, 143(1):93–95, 1996. CODEN ICDTEA. ISSN 1350-2387 (print), 1359-7027 (electronic). URL `http://link.aip.org/link/?ICE/143/93/1`.

Petrov:1996:LTP

[2216] Valentin V. Petrov and Wlodzimierz Bryc. Limit theorems of probability theory: Sequences of independent random variables. *SIAM Review*, 38 (3):527–??, September 1996. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).

Radovic:1996:QMC

[2217] Igor Radović, Ilya M. Sobol, and Robert F. Tichy. Quasi-Monte Carlo methods for numerical integration: Comparison of different low discrep-

ancy sequences. *Monte Carlo Methods and Applications*, 2(1):1–14, January 1996. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1996.2.issue-1/mcma.1996.2.1.1/mcma.1996.2.1.1.xml`.

Rubin:1996:OTP

[2218] Frank Rubin. One-time pad cryptography. *Cryptologia*, 20(4):359–364, 1996. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Sanchis:1996:PAC

[2219] Laura A. Sanchis and Matthew B. Squire. Parallel algorithms for counting and randomly generating integer partitions. *Journal of Parallel and Distributed Computing*, 34(1):29–35, April 10, 1996. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0043/production; http://www.idealibrary.com/links/doi/10.1006/jpdc.1996.0043/production/pdf`.

Sarkar:1996:CAM

[2220] T. K. Sarkar. A composition-alias method for generating gamma variates with shape parameter greater than 1. *ACM Transactions on Mathematical Software*, 22(4):484–492, December 1996. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1996-22-4/p484-sarkar/`.

Schervish:1996:VWT

[2221] Mark J. Schervish. P values: What they are and what they are not. *The American Statistician*, 50(3):203–206, August 1996. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2684655`.

Schneier:1996:ACP

[2222] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, New York, NY, USA, second edition, 1996. ISBN 0-471-12845-7 (cloth), 0-471-11709-9 (paper). xxiii + 758 pp. LCCN QA76.9.A25 S35 1996.

Sethumadhavan:1996:NPE

[2223] M. Sethumadhavan. On nonoverlapping pairs of explicit inversive congruential pseudorandom numbers. *Bull. Pure Appl. Sci. Sect. E Math. Stat.*, 15(2):157–164, 1996. CODEN ???? ISSN 0970-6577.

Sezgin:1996:RNG

[2224] Fatin Sezgin. A random number generator for 16-bit microcomputers. *Computers and Operations Research*, 23(2):193–198, February 1996. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/0305054895000068`.

Sezgin:1996:SIR

[2225] F. Sezgin. Some improvements for a random number generator with single-precision floating-point arithmetic. *Computers and Geosciences*, 22(4):453–455, May 1996. CODEN CGEODT, CGOSDN. ISSN 0098-3004 (print), 1873-7803 (electronic).

Sipper:1996:CEP

[2226] M. Sipper and M. Tomassini. Co-evolving parallel random number generators. *Lecture Notes in Computer Science*, 1141:950–??, 1996. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Sipper:1996:GPR

[2227] Moshe Sipper and Marco Tomassini. Generating parallel random number generators by cellular programming. *International Journal of Modern Physics C [Physics and Computers]*, 7(2):181–190, April 1996. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic).

Takashima:1996:HWT

[2228] Keizo Takashima. On Hamming weight test and sojourn time test of m-sequences. *Monte Carlo Methods and Applications*, 2(4):331–340, ???? 1996. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1996.2.issue-4/mcma.1996.2.4.331/mcma.1996.2.4.331.xml`.

Takashima:1996:LVT

[2229] K. Takashima. Last visit time tests for pseudo-random numbers. *Journal of Japanese Society of Computational Statistics*, 9(1):1–14, ???? 1996. ISSN 0915-2350 (print), 1881-1337 (electronic).

Takashima:1996:STT

[2230] K. Takashima and S. Ueda. Sojourn time test of m-sequences by Fushimi's fast generation methods. In Shinzo Watanabe, M. Fukushima, Yu. V. Prohorov, and A. N. Shiryaev, editors, *Probability Theory and*

Mathematical Statistics: proceedings of the Seventh Japan–Russia symposium: Tokyo, 26–30 July 1995, pages 471–477. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1996. ISBN 981-02-2426-5. LCCN QA276.A1 P962 1995.

Ugrin-Sparac:1996:NAG

[2231] Dimitrije Ugrin-Šparac. A natural algorithm for generation of pseudorandom numbers and its applications. *Monte Carlo Methods and Applications*, 2(3):191–217, ???? 1996. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1996.2.issue-3/mcma.1996.2.3.191/mcma.1996.2.3.191.xml`.

Ugrin-Sparac:1996:PET

[2232] G. Ugrin-Šparac and D. Ugrin-Šparac. On a possible error of type II in statistical evaluation of pseudo-random number generators. *Computing: Archiv für Informatik und Numerik*, 56(2):105–116, June 1996. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=289&id_volume=26&id_journal=8`.

Wallace:1996:FPG

[2233] C. S. Wallace. Fast pseudorandom generators for normal and exponential variates. *ACM Transactions on Mathematical Software*, 22(1):119–127, March 1996. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1996-22-1/p119-wallace/`. See comments [3159].

Wang:1996:LIL

[2234] Yongge Wang. The law of the iterated logarithm for p-random sequences. In Steve Homer and Jin-Yi Cai, editors, *Proceedings of the 11th Annual IEEE Conference on Computational Complexity, 24–27 May 1996*, pages 180–189. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. ISBN 0-8186-7386-9, 0-8186-7387-7 (casebound), 0-8186-7388-5 (microfiche). LCCN QA267 S927 1996.

Wegenkittl:1996:RSP

[2235] S. Wegenkittl and K. Entacher. On the relevance of splitting properties and the compound method in parallel applications of pseudorandom number generators. In Trobec et al. [4195], page ?? ISBN 86-80023-25-6. LCCN ???? URL `ftp://random.mat.sbg.ac.at/pub/publications/ste/PACT_slovenia/art.ps.gz`.

Alon:1997:SSD

[2236] Noga Alon, Shai Ben-David, Nicolò Cesa-Bianchi, and David Haussler. Scale-sensitive dimensions, uniform convergence, and learnability. *Journal of the ACM*, 44(4):615–631, July 1997. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org:80/pubs/citations/journals/jacm/1997-44-4/p615-alon/`.

Aluru:1997:LFR

[2237] Srinivas Aluru. Lagged Fibonacci random number generators for distributed memory parallel computers. *Journal of Parallel and Distributed Computing*, 45(1):1–12, August 25, 1997. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL `http://www.idealibrary.com/links/doi/10.1006/jpdc.1997.1363/production; http://www.idealibrary.com/links/doi/10.1006/jpdc.1997.1363/production/pdf; http://www.idealibrary.com/links/doi/10.1006/jpdc.1997.1363/production/ref`.

Annexstein:1997:GBS

[2238] F. S. Annexstein. Generating de Bruijn sequences: an efficient implementation. *IEEE Transactions on Computers*, 46(2):198–200, February 1997. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=565596`.

Arvind:1997:RBM

[2239] V. Arvind and J. Köbler. On resource-bounded measure and pseudorandomness. *Lecture Notes in Computer Science*, 1346:235–??, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1346/13460235.htm; http://link.springer-ny.com/link/service/series/0558/papers/1346/13460235.pdf`.

Athanasiu:1997:SGP

[2240] G. G. Athanasiu, E. G. Floratos, and G. K. Savvidy. K-system generator of pseudorandom numbers on Galois field. *International Journal of Modern Physics C [Physics and Computers]*, 8(3):555–565, June 1997. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/08/0803/S0129183197000448.html`.

Baker:1997:NPU

[2241] Frank B. Baker. A note on the proper use of the *Numerical Recipes* `RAN1` random number generator. *Computational Statistics & Data Anal-*

ysis, 25(2):237–239, July 31, 1997. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947397896491`. See also [2324].

Balakrishnan:1997:ASW

[2242] Hari Balakrishnan, Mark Stemm, Srinivasan Seshan, and Randy H. Katz. Analyzing stability in wide-area network performance. *ACM SIGMETRICS Performance Evaluation Review*, 25(1):2–12, June 1997. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Bellare:1997:PRN

[2243] Mihir Bellare, Shafi Goldwasser, and Daniele Micciancio. "Pseudo-Random" number generation within cryptographic algorithms: The DSS case. *Lecture Notes in Computer Science*, 1294:277–291, 1997. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1294/12940277.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1294/12940277.pdf`.

Berblinger:1997:MCI

[2244] M. Berblinger, Ch. Schlier, and T. Weiss. Monte Carlo integration with quasi-random numbers: experience with discontinuous integrands. *Computer Physics Communications*, 99(2–3):151–162, January 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465596001312`.

Berg:1997:CNF

[2245] Peer Berg, Bob Runyan, Henry Zongaro, Steve Lionel, Stu Anderson, Alan Miller, Albert Fasso, Phillip Helbig, and Loren Meissner. Captured on the Net: Fortran random number generators, intrinsic and otherwise. *ACM Fortran Forum*, 16(3):3–4, December 1997. CODEN ???? ISSN 1061-7264 (print), 1931-1311 (electronic).

Binder:1997:AMC

[2246] K. Binder. Applications of Monte Carlo methods in statistical physics. *Reports on Progress in Physics*, 60(5):487–559, May 1997. CODEN RPPHAG. ISSN 0034-4885 (print), 1361-6633 (electronic). URL `http://iopscience.iop.org/0034-4885/60/5`; `http://stacks.iop.org/0034-4885/60/i=5/a=001`.

Binder:1997:MCS

[2247] K. (Kurt) Binder and Dieter W. Heermann. *Monte Carlo simulation in statistical physics: an introduction*, volume 80 of *Springer series in*

solid-state sciences. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 1997. ISBN 3-540-63265-4 (softcover). ISSN 0171-1873. x + 150 pp. LCCN QC174.85.M64 B56 1997.

Cario:1997:MGR

[2248] M. C. Cario and B. L. Nelson. Modeling and generating random vectors with arbitrary marginal distributions and correlation matrix. Technical report, Department of Industrial Engineering and Management Sciences, Northwestern University, Evanston, IL, USA, 1997.

Coddington:1997:RNG

[2249] P. Coddington. Random number generators for parallel computers. Technical Report 13, Northeast Parallel Architecture Center, Syracuse University, Syracuse, NY, 13244-4100, USA, April 28, 1997. 26 pp. URL `http://surface.syr.edu/npac/13`. Version 1.1.

Compagner:1997:RER

[2250] A. Compagner, A. S. Berdnikov, S. B. Turtia, and A. Larionov. Rounding errors in random number generators. *Computer Physics Communications*, 106(3):207–218, November 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465597000702`.

Couture:1997:DPM

[2251] Raymond Couture and Pierre L'Ecuyer. Distribution properties of multiply-with-carry random number generators. *Mathematics of Computation*, 66(218):591–607, April 1997. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-97-00827-2&u=/mcom/1997-66-218/`; `http://www.jstor.org/stable/2153884`.

Dai:1997:RCD

[2252] Liyi Dai. Rate of convergence for derivative estimation of discrete-time Markov chains via finite-difference approximation with Common Random Numbers. *SIAM Journal on Applied Mathematics*, 57(3):731–751, June 1997. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/27173`.

Dai:1997:RRW

[2253] Jack J. Dai and Martin V. Hildebrand. Random random walks on the integers mod$n$. *Statistics & Probability Letters*, 35(4):371–379,

November 1, 1997. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167715297000357.

Deng:1997:SJC

[2254] Lih-Yuan Deng, Dennis K. J. Lin, Jiannong Wang, and Yilian Yuan. Statistical justification of combination generators. *Statistica Sinica*, 7(4):993–1003, October 1997. CODEN STSNEO. ISSN 1017-0405 (print), 1996-8507 (electronic). URL http://www3.stat.sinica.edu.tw/statistica/j7n4/j7n412/j7n412.htm.

Denk:1997:AME

[2255] G. Denk and S. Schäffler. Adams methods for the efficient solution of stochastic differential equations with additive noise. *Computing: Archiv für Informatik und Numerik*, 59(2):153–161, June 1997. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=1539&id_volume=120&id_journal=8.

Devroye:1997:RVG

[2256] Luc Devroye. Random variate generation for multivariate unimodal densities. *ACM Transactions on Modeling and Computer Simulation*, 7(4):447–477, October 1997. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Dyadkin:1997:FEL

[2257] Iosif G. Dyadkin and Kenneth G. Hamilton. A family of enhanced Lehmer random number generators, with hyperplane suppression, and direct support for certain physical applications. *Computer Physics Communications*, 107(1–3):258–280, December 22, 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.cpc.cs.qub.ac.uk/cpc/; http://www.cpc.cs.qub.ac.uk/cpc/cgi-bin/list_summary.pl?CatNumber=ADGW; http://www.sciencedirect.com/science/article/pii/S001046559700101X.

Dyadkin:1997:SBM

[2258] Iosif G. Dyadkin and Kenneth G. Hamilton. A study of 64-bit multipliers for Lehmer pseudorandom number generators. *Computer Physics Communications*, 103(2–3):103–130, July 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465597000520.

Eichenauer-Herrmann:1997:ADH

[2259] Jürgen Eichenauer-Herrmann, Frank Emmerich, and Gerhard Larcher. Average discrepancy, hyperplanes, and compound pseudorandom numbers. *Finite Fields and their Applications*, 3(3):203–218, July 1997. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1071579797901805.

Eichenauer-Herrmann:1997:AEP

[2260] Jürgen Eichenauer-Herrmann and Gerhard Larcher. Average equidistribution properties of compound nonlinear congruential pseudorandom numbers. *Mathematics of Computation*, 66(217):363–372, January 1997. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-97-00802-8&u=/mcom/1997-66-217/; http://www.jstor.org/stable/pdfplus/2153659.pdf.

Eichenauer-Herrmann:1997:CCC

[2261] J. Eichenauer-Herrmann and E. Herrmann. Compound cubic congruential pseudo-random numbers. *Computing: Archiv für Informatik und Numerik*, 59(1):85–90, March 1997. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=1451&id_volume=112&id_journal=8.

Eichenauer-Herrmann:1997:ICP

[2262] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Inversive congruential pseudorandom numbers: Distribution of triples. *Mathematics of Computation*, 66(220):1629–1644, October 1997. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-97-00867-3&u=/mcom/1997-66-220/; http://www.jstor.org/stable/pdfplus/2153689.pdf.

Eichenauer-Herrmann:1997:PSN

[2263] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Parallel streams of nonlinear congruential pseudorandom numbers. *Finite Fields and their Applications*, 3(3):219–233, July 1997. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1071579797901830.

Eichenauer-Herrmann:1997:QCP

[2264] Jürgen Eichenauer-Herrmann. Quadratic congruential pseudorandom numbers: Distribution of lagged pairs. *Journal of Computational and Applied Mathematics*, 79(1):75–85, March 3, 1997. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042796001586`.

Emmerich:1997:EPQ

[2265] Frank Emmerich. Equidistribution properties of quadratic congruential pseudorandom numbers. *Journal of Computational and Applied Mathematics*, 79(2):207–214, March 17, 1997. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042796001574`.

Entacher:1997:ASP

[2266] K. Entacher, A. Uhl, and S. Wegenkittl. Analyzing streams of pseudorandom numbers for parallel Monte Carlo integration. In Wyrzykowski et al. [4200], pages 59–71. ISBN 83-7098-365-0. LCCN ????

Entacher:1997:CSP

[2267] Karl Entacher. A collection of selected pseudorandom number generators with linear structure. Report 97-1, ACPC – Austrian Center for Parallel Computation, University of Vienna, Vienna, Austria, August 21, 1997. 25 pp. URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.53.3686`; `http://random.mat.sbg.ac.at/ftp/pub/data/genacpc.txt`.

Entacher:1997:PPL

[2268] K. Entacher and S. Wegenkittl. The pLab picturebook: Load tests and ultimate load tests, Part II: Subsequences. Report 2, University of Salzburg, Salzburg, Austria, 1997. URL `ftp://random.mat.sbg.ac.at/pub/data/pLabReport1.ps`.

Entacher:1997:PPP

[2269] K. Entacher. The pLab picturebook Part III: Bad subsequences of LCGs — the results. Report 6, University of Salzburg, Salzburg, Austria, 1997. URL `ftp://random.mat.sbg.ac.at/pub/data/pLabReport6.ps`.

Fishman:1997:MCC

[2270] George S. Fishman. *Monte Carlo: concepts, algorithms, and applications*. Springer series in operations research. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK /

etc., corrected second printing edition, 1997. ISBN 0-387-94527-X. xxv + 698 pp. LCCN QA298 .F57 1997. URL http://www.loc.gov/catdir/enhancements/fy0815/97168075-d.html; http://www.loc.gov/catdir/enhancements/fy0815/97168075-t.html.

Foster:1997:DOT

[2271] Caxton C. Foster. Drawbacks of the one-time pad. *Cryptologia*, 21(4): 350–352, 1997. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Gell-Mann:1997:ETZ

[2272] Murray Gell-Mann. RANDomness. In *The quark and the jaguar: adventures in the simple and the complex* [4197], chapter 4, pages 43–50. ISBN 0-7167-2725-0 (paperback). LCCN QC774.G45 A3 1994. URL http://www.gbv.de/dms/bowker/toc/9780716725817.pdf; http://www.zentralblattmath.org/zmath/en/search/?an=0833.00011.

Gilks:1997:CAR

[2273] W. R. Gilks, R. M. Neal, N. G. Best, and K. K. C. Tan. Corrigendum: Adaptive rejection Metropolis sampling. *Applied Statistics*, 46(4):541–??, 1997. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL http://www.blackwellpublishers.co.uk/asp/journal.asp?ref=0035-9254&src=ard&aid=091&iid=4&vid=46. See [2055].

Grabner:1997:MSR

[2274] Peter J. Grabner and Helmut Prodinger. Maximum statistics of N random variables distributed by the negative binomial distribution. *Combinatorics, Probability and Computing*, 6(2):179–183, June 1997. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=6&issueId=02.

Hamilton:1997:AR

[2275] Kenneth G. Hamilton and F. James. Acceleration of RANLUX. *Computer Physics Communications*, 101(3):241–248, May 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465597000027.

Hamilton:1997:ARP

[2276] Kenneth G. Hamilton. Assembler RANLUX for PCs. *Computer Physics Communications*, 101(3):249–253, May 1, 1997. CODEN CPHCBZ.

ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465597000179.

Hellekalek:1997:CAP

[2277] P. Hellekalek. On correlation analysis of pseudorandom numbers. In H. Niederreiter, P. Hellekalek, G. Larcher, and P. Zinterhof, editors, *Proceedings of the Second International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Salzburg, July 9–12, 1996*, Lecture Notes in Statistics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1997.

Hellekalek:1997:GRN

[2278] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [4199], page ?? ISBN 3-901608-11-7. LCCN ????

Hellekalek:1997:NPNa

[2279] P. Hellekalek. A note on pseudorandom number generators. *EUROSIM Simulations News Europe*, 20(??):8–10, ???? 1997. CODEN ???? ISSN ????

Hellekalek:1997:NPNb

[2280] Peter Hellekalek. A note on pseudorandom number generators. *Simulation Practice and Theory*, 5(6):p6–p8, August 15, 1997. CODEN SPTHEH. ISSN 0928-4869 (print), 1879-1433 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0928486997842279.

Herendi:1997:FGR

[2281] T. Herendi, T. Siegl, and R. F. Tichy. Fast Gaussian random number generation using linear transformations. *Computing: Archiv für Informatik und Numerik*, 59(2):163–181, June 1997. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=1557&id_volume=120&id_journal=8.

Heuer:1997:CCS

[2282] Andreas Heuer, Burkhard Dünweg, and Alan M. Ferrenberg. Considerations on correlations in shift-register pseudorandom number generators and their removal. *Computer Physics Communications*, 103(1):1–9, June 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S001046559700026X.

Imperiale:1997:PUG

[2283] Cosimo Imperiale. Programmable uniform-Gaussian, quasi-white noise generator and data acquisition-processing system for electrophysiology. *Measurement: Journal of the International Measurement Confederation*, 20(3):149–163, March 1997. ISSN 0263-2241 (print), 1873-412X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0263224197000237`.

James:1997:MSS

[2284] F. James, J. Hoogland, and R. Kleiss. Multidimensional sampling for simulation and integration: measures, discrepancies, and quasi-random numbers. *Computer Physics Communications*, 99(2–3):180–220, January 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465596001087`.

Kao:1997:SSG

[2285] Chiang Kao and H. C. Tang. Systematic searches for good multiple recursive random number generators. *Computers and Operations Research*, 24(10):899–905, October 1997. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0305054897000178`.

Kao:1997:UBS

[2286] Chiang Kao and Huey-Chin Tang. Upper bounds in spectral test for multiple recursive random number generators with missing terms. *Computers and Mathematics and Applications*, 33(4):119–125, February 1997. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122197000126`.

Kato:1997:LSP

[2287] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. On the lattice structure of pseudo-random numbers generated by the modified inversive congruential generator with modulus 2^α. *Japan Journal of Industrial and Applied Mathematics*, 14(1):33–38, 1997. CODEN JAPJI7. ISSN 0916-7005 (print), 1868-937x (electronic). See [2187] for the original work, and [2188] for a treatment of the discrepancy of the inversive congruential generator.

Kotz:1997:MVD

[2288] Samuel Kotz, Kai-Tai Fang, and Jia-Juan Liang. On multivariate vertical density representation and its application to random number generation.

Statistics: a Journal of Theoretical and Applied Statistics, 30(2):163–180, 1997. CODEN MOSSD5. ISSN 0233-1888 (print), 1029-4910 (electronic).

Kreckel:1997:PAM

[2289] Richard Kreckel. Parallelization of adaptive MC integrators. *Computer Physics Communications*, 106(3):258–266, November 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465597000994`.

LEcuyer:1997:BLS

[2290] Pierre L'Ecuyer. Bad lattice structures for vectors of non-successive values produced by some linear recurrences. *INFORMS Journal on Computing*, 9(1):57–60, Winter 1997. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

LEcuyer:1997:EBT

[2291] Pierre L'Ecuyer, A. Compagner, and J.-F. Cordeau. Entropy-based tests for random-number generators. Technical report, Université de Montréal, Montréal, PQ, Canada, 1997. URL `http://www.iro.umontreal.ca/%7Elecuyer/myftp/papers/myftp/papers/entrop.ps`.

LEcuyer:1997:ILS

[2292] Pierre L'Ecuyer and Raymond Couture. An implementation of the lattice and spectral tests for multiple recursive linear random number generators. *INFORMS Journal on Computing*, 9(2):206–217, Spring 1997. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

LEcuyer:1997:RNG

[2293] Pierre L'Ecuyer and Terry H. Andres. A random number generator based on the combination of four LCGs. *Mathematics and Computers in Simulation*, 44(1):99–107, May 1997. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475497000529`.

LEcuyer:1997:TBS

[2294] Pierre L'Ecuyer. Tests based on sum-functions of spacings for uniform random numbers. *Journal of Statistical Computation and Simulation*, 59(3):251–269, ???? 1997. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659708811859`.

LEcuyer:1997:URN

[2295] Pierre L'Ecuyer. Uniform random number generators: a review. In Andradóttir [4196], pages 127–134. ISBN 0-7803-4278-X. LCCN QA76.5 W78 1997.

Leeb:1997:ILC

[2296] Hannes Leeb and Stefan Wegenkittl. Inversive and linear congruential pseudorandom number generators in empirical tests. *ACM Transactions on Modeling and Computer Simulation*, 7(2):272–286, April 1997. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Li:1997:IKC

[2297] Ming Li and P. M. B. (Paul Michael Béla) Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*. Graduate texts in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 1997. ISBN 0-387-94868-6 (hardcover). xx + 637 pp. LCCN QA267.7. URL `http://catdir.loc.gov/catdir/enhancements/fy0815/96042357d.html`; `http://www.zentralblattmath.org/zmath/en/search/?an=0866.68051`.

Lidl:1997:FF

[2298] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of mathematics and its applications*. Cambridge University Press, Cambridge, UK, second edition, 1997. ISBN 0-521-39231-4 (hardcover). xiv + 755 pp. LCCN QA247.3 .L53 1997. URL `http://www.loc.gov/catdir/description/cam027/96031467.html`; `http://www.loc.gov/catdir/toc/cam029/96031467.html`.

Marsaglia:1997:RNG

[2299] George Marsaglia. A random number generator for C. Posted to the `sci.math.num-analysis` news group, September 29, 1997. URL `http://mathforum.org/kb/thread.jspa?messageID=1607565`. From the posting: "Keep the following six lines of code somewhere in your files. #define znew ((z=36969*(z&65535)+(z¿¿16))¡¡16) #define wnew ((w=18000*(w&65535)+(w¿¿16))&65535) #define IUNI (znew+wnew) #define UNI (znew+wnew)*4.656613e-10 static unsigned long z=362436069, w=521288629; void setseed(unsigned long i1,unsigned long i2)z=i1; w=i2; Whenever you need random integers or random reals in your C program, just insert those six lines at (near?) the beginning of the program. In every expression where you want a random real in $[0, 1)$ use UNI, or use IUNI for a random 32-bit integer. No need to mess with ranf() or ranf(lastI), etc, with their requisite overheads. Choices for replacing the two multipliers 36969 and 18000 are given below. Thus you

can tailor your own in-line multiply-with-carry random number generator.”.

Menezes:1997:HAC

[2300] A. J. (Alfred J.) Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997. ISBN 0-8493-8523-7. xxviii + 780 pp. LCCN QA76.9.A25 M463 1997.

Naor:1997:NTC

[2301] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In IEEE [4198], pages 458–467. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

Naveau:1997:CBC

[2302] Philippe Naveau. Comparison between the Chernoff and factorial moment bounds for discrete random variables. *The American Statistician*, 51(1):40–41, February 1997. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.amstat.org/publications/tas/abstracts/naveau.html`.

Needham:1997:TE

[2303] Roger M. Needham and David J. Wheeler. TEA extensions. Report, Cambridge University, Cambridge, UK, October 1997. URL `http://www.movable-type.co.uk/scripts/xtea.pdf`. See also original TEA [2131] and extension XXTEA [2414].

Novak:1997:DRS

[2304] S. Yu. Novak. On the distribution of the ratio of sums of random variables. *Theory of Probability and its Applications*, 41(3):479–503, ???? 1997. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/97525`. Original Russian article in *Teor. Veroyatnost. i Primenen.*, **41**(3), (1996), pp. 533–560.

Ogawa:1997:EAR

[2305] Shigeyoshi Ogawa. Erratum to the article: “On a robustness of the random particle method” [Monte Carlo Methods Appl. **2** (1996), no. 3, 175–189; MR1414863 (97j:65008)]. *Monte Carlo Methods and Applications*, 3

(1):83–??, ???? 1997. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://www.degruyter.com/view/j/mcma.1997.3.issue-1/mcma.1997.3.1.83/mcma.1997.3.1.83.xml. See [2214].

Pages:1997:SLD

[2306] Gilles Pagès and Yi-Jun Xiao. Sequences with low discrepancy and pseudo-random numbers: theoretical results and numerical tests. *Journal of Statistical Computation and Simulation*, 56(2):163–188, January 1997. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949659708811786.

Panconesi:1997:RDE

[2307] Alessandro Panconesi and Aravind Srinivasan. Randomized distributed edge coloring via an extension of the Chernoff–Hoeffding bounds. *SIAM Journal on Computing*, 26(2):350–368, April 1997. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/25076.

Pincus:1997:APR

[2308] Steve Pincus and Rudolf E. Kalman. Not all (possibly) "random" sequences are created equal. *Proceedings of the National Academy of Sciences of the United States of America*, 94:3513–3518, April 1997. CODEN PNASA6. ISSN 0027-8424 (print), 1091-6490 (electronic). URL http://www.pnas.org/cgi/content/full/94/8/3513?terms=pincus%20kalman; http://www.pnas.org/cgi/reprint/94/8/3513.pdf.

Schaber:1997:DIC

[2309] K. Schaber. Digital inversive congruential generators. Master's thesis, Institut für Mathematik, Universität Salzburg, Salzburg, Austria, 1997.

Shchur:1997:CMC

[2310] Lev N. Shchur and Henk W. J. Blöte. Cluster Monte Carlo: Scaling of systematic errors in the two-dimensional Ising model. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 55(5):R4905–R4908, May 1997. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.55.R4905.

Shchur:1997:SDR

[2311] L. N. Shchur, J. R. Heringa, and H. W. J. Blöte. Simulation of a directed random-walk model: the effect of pseudo-random-number correlations. *Physica A, Statistical Mechanics and its Applications*, 241 (3–4):579–592, July 15, 1997. CODEN PHYADX. ISSN 0378-4371 (print), 1873-2119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S037843719700126X`.

Slone:1997:EBR

[2312] Dale M. Slone and Garry H. Rodrigue. Efficient biased random bit generation for parallel lattice gas simulations. *Parallel Computing*, 22 (12):1597–1620, February 21, 1997. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/parco/cas_sub/browse/browse.cgi?year=1997&volume=22&issue=12&aid=1111`; `http://www.sciencedirect.com/science/article/pii/S0167819196000609`.

Song:1997:GDR

[2313] Peter Xue-Kun Song. Generating dependent random numbers with given correlations and margins from exponential dispersion models. *Journal of Statistical Computation and Simulation*, 56(4):317–335, ???? 1997. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949659708811797`.

Strauss:1997:NNS

[2314] Martin Strauss. Normal numbers and sources for BPP. *Theoretical Computer Science*, 178(1–2):155–169, May 30, 1997. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/tcs/cas_sub/browse/browse.cgi?year=1997&volume=178&issue=1-2&aid=2302`.

Struckmeier:1997:GRV

[2315] J. Struckmeier. Generation of random variates using asymptotic expansions. *Computing: Archiv für Informatik und Numerik*, 59(4):331–347, December 1997. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springer.at/springer.py?Page=10&Key=362&cat=300607/tocs/springer.py?Page=47&Key=340&cat=3&id_abstract=2503&id_volume=212&id_journal=8`.

Takashima:1997:RWTa

[2316] K. Takashima. Random walk tests of additive number generators. In S. Ogawa and K. Sabelfeld, editors, *Proceedings of the Workshop on*

Turbulent Diffusion and Related Problems in Stochastic Numerics, pages 55–65. Inst. Stat. Math., ????, 1997. ISBN ???? LCCN ????

Takashima:1997:RWTb

[2317] Keizo Takashima. Random walk tests of reciprocal m-sequences. *Monte Carlo Methods and Applications*, 3(2):155–166, ???? 1997. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1997.3.issue-2/mcma.1997.3.2.155/mcma.1997.3.2.155.xml`.

vanHameren:1997:GLD

[2318] André van Hameren, Ronald Kleiss, and Jiri Hoogland. Gaussian limits for discrepancies I. asymptotic results. *Computer Physics Communications*, 107(1–3):1–20, December 1997. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465597001057`.

Woodward:1997:ECD

[2319] J. Arthur Woodward and Christina G. S. Palmer. On the exact convolution of discrete random variables. *Applied Mathematics and Computation*, 83(1):69–77, April 1, 1997. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.elsevier.com/cgi-bin/cas/tree/store/amc/cas_sub/browse/browse.cgi?year=1997&volume=83&issue=1&aid=9600047`.

Wu:1997:MCR

[2320] Pei-Chi Wu. Multiplicative, congruential random-number generators with multiplier $\pm 2^{k_1} \pm 2^{k_2}$ and modulus $2^p - 1$. *ACM Transactions on Mathematical Software*, 23(2):255–265, June 1997. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1997-23-2/p255-wu/`.

Zubkov:1997:PTD

[2321] A. M. Zubkov. Peculiarities of two-dimensional distributions of a sequence generated by a linear congruential generator. In *Proceedings in discrete mathematics, Vol. 1 (Russian)*, volume 1 of *Tr. Diskretn. Mat.*, pages 113–120. Nauchn. Izd. TVP, Moscow, Russia, 1997.

Aiello:1998:DPP

[2322] William Aiello, S. Raj Rajagopalan, and Ramarathnam Venkatesan. Design of practical and provably good random number generators. *Journal of Algorithms*, 29(2):358–389, November 1998. CODEN JOALDV. ISSN 0196-6774 (print), 1090-2678 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S019667749890952X`.

Andreev:1998:NGD

[2323] Alexander E. Andreev, Andrea E. F. Clementi, and José D. P. Rolim. A new general derandomization method. *Journal of the ACM*, 45(1):179–213, January 1998. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `http://www.acm.org:80/pubs/citations/journals/jacm/1998-45-1/p179-andreev/`.

Antoch:1998:RPN

[2324] Jaromír Antoch, Jean-Marc Deshouillérs, and Gusti Putu Purnaba. Revisiting the pseudorandom number generator `ran1` from the *Numerical Recipes*. *Computational Statistics & Data Analysis*, 27(4):487–495, June 1998. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://dl.acm.org/citation.cfm?id=292570.292582; http://www.sciencedirect.com/science/article/B6V8V-3TC6SXY-8/2/594e7cff0a7497ab7b7670408b57955f`. See [2241].

Bach:1998:EPM

[2325] Eric Bach. Efficient prediction of Marsaglia–Zaman random number generators. *IEEE Transactions on Information Theory*, 44(3):1253–1257, 1998. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Baldwin:1998:PAB

[2326] Robert W. Baldwin. Preliminary analysis of the BSAFE 3.x pseudorandom number generators. *RSA Laboratories' Bulletin*, 8:1–11, September 3, 1998. CODEN ???? ISSN ???? URL `ftp://ftp.rsasecurity.com/pub/pdfs/bull-3.pdf`.

Baldwin:1998:PPR

[2327] Robert W. Baldwin and James W. Gray, III. PCKS #14: Pseudorandom number generation. World-Wide Web slide presentation., October 1998. URL `ftp://ftp.rsasecurity.com/pub/pkcs/98workshop/pkcs14_proposal3.ppt; ftp://ftp.rsasecurity.com/pub/pkcs/99workshop/workshop.zip`.

Ballesteros:1998:TRN

[2328] H. G. Ballesteros and V. Martín-Mayor. Test for random number generators: Schwinger–Dyson equations for the Ising model. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 58(5):6787–6791, November 1998. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.58.6787`.

Barni:1998:CPD

[2329] Mauro Barni, Franco Bartolini, Vito Cappellini, and Alessandro Piva. Copyright protection of digital images by embedded unperceivable marks. *Image and Vision Computing*, 16(12–13):897–906, August 1998. CODEN IVCODK. ISSN 0262-8856 (print), 1872-8138 (electronic).

Bennett:1998:R

[2330] Deborah J. Bennett. *Randomness*. Harvard University Press, Cambridge, MA, USA, 1998. ISBN 0-674-10745-4. 238 pp. LCCN QA273.15 .B46 1998.

Berleant:1998:BRA

[2331] D. Berleant and C. Goodman-Strauss. Bounding the results of arithmetic operations on random variables of unknown dependency using intervals. *Reliable Computing = Nadezhnye vychisleniia*, 4(??): 147–165, 1998. CODEN RCOMF8. ISSN 1385-3139 (print), 1573-1340 (electronic). URL `http://ee.iastate.edu/~djb/Research/Pdfs/unknownDependency.ps`.

Birman:1998:ACH

[2332] Mark Birman. Accelerating cryptography in hardware: Public key, random number generation, symmetric key. In IEEE [4204], page ?? ISBN ???? LCCN ????

Bramley:1998:TNRa

[2333] Randall Bramley. Technology news & reviews: Geographic information systems; Scalable Parallel Random Number Generators — SPRNG; portable power for laptops. *IEEE Computational Science & Engineering*, 5(1):13–15, January/March 1998. CODEN ISCEE4. ISSN 1070-9924 (print), 1558-190X (electronic). URL `http://dlib.computer.org/cs/books/cs1998/pdf/c1013.pdf`.

Brent:1998:RNG

[2334] R. P. Brent. Random number generation and simulation on vector and parallel computers. *Lecture Notes in Computer Science*, 1470:1–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cattell:1998:EST

[2335] Kevin Cattell and Jon C. Muzio. An explicit similarity transform between cellular automata and LFSR matrices. *Finite Fields and their Applications*, 4(3):239–251, July 1998. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S107157979890212X`.

Cheng:1998:RVG

[2336] Russell C. H. Cheng. Random variate generation. In Banks [4201], pages 138–172. ISBN 0-471-13403-1 (hardcover). LCCN T57.62 .H37 1998. URL `http://www.loc.gov/catdir/bios/wiley044/97051533.html`; `http://www.loc.gov/catdir/description/wiley037/97051533.html`; `http://www.loc.gov/catdir/toc/onix01/97051533.html`.

Coddington:1998:RNG

[2337] Paul D. Coddington and Sung-Hoon Ko. Random number generator for parallel computers. In Greg Egan, Richard Brent, and Dennis Gannon, editors, *ICS '98: Conference proceedings of the 1998 International Conference on Supercomputing: Melbourne, Australia, July 13–17, 1998*, pages 282–288. ACM Press, New York, NY 10036, USA, 1998. ISBN 0-89791-998-X. LCCN QA76.5 .I58 1998.

Couture:1998:GEI

[2338] Raymond Couture and Pierre L'Ecuyer. Guest editors' introduction: special issue on uniform random number generation. *ACM Transactions on Modeling and Computer Simulation*, 8(1):1–2, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

DSouza:1998:SBD

[2339] Raissa M. D'Souza, Yaneer Bar-Yam, and Mehran Kardar. Sensitivity of ballistic deposition to pseudorandom number generators. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 57(5):5044–5052, May 1998. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.57.5044`.

Eichenauer-Herrmann:1998:IUB

[2340] J. Eichenauer-Herrmann. Improved upper bounds for the discrepancy of pairs of inversive congruential pseudorandom numbers with power of two modulus. *Acta Math. Hungar.*, 79(4):295–303, 1998. CODEN AMAHE9. ISSN 0236-5294.

Eichenauer-Herrmann:1998:LBD

[2341] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Lower bounds for the discrepancy of triples of inversive congruential pseudorandom numbers with power of two modulus. *Monatshefte für Mathematik*, 125(3): 211–217, September 1998. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Eichenauer-Herrmann:1998:SQI

[2342] Jürgen Eichenauer-Herrmann, Eva Herrmann, and Stefan Wegenkittl. A survey of quadratic and inversive congruential pseudorandom numbers. In Niederreiter et al. [4207], pages 66–97. ISBN 0-387-98335-X (softcover). LCCN Q183.9 .M67 1998. URL `http://www.loc.gov/catdir/enhancements/fy0815/97034133-d.html`; `http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html`.

Ellison:1998:CRN

[2343] C. Ellison. Cryptographic random numbers. Technical report, ????, ????, 1998. Draft P1363 Appendix E.

Emmerich:1998:EPC

[2344] Frank Emmerich. Equidistribution properties of compound inversive pseudorandom vectors. *Finite Fields and their Applications*, 4(1):16–28, January 1998. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579797901945`.

Emmerich:1998:SIP

[2345] Frank Emmerich. Statistical independence properties of inversive pseudorandom vectors over parts of the period. *ACM Transactions on Modeling and Computer Simulation*, 8(2):140–152, April 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Entacher:1998:BSW

[2346] Karl Entacher. Bad subsequences of well-known linear congruential pseudorandom number generators. *ACM Transactions on Modeling and Computer Simulation*, 8(1):61–70, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Entacher:1998:LCG

[2347] K. Entacher, A. Uhl, and S. Wegenkittl. Linear congruential generators for parallel Monte Carlo: the leap-frog case. *Monte Carlo Methods and Applications*, 4(1):1–15, January 1998. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic).

Entacher:1998:LIP

[2348] K. Entacher, A. Uhl, and S. Wegenkittl. Linear and inversive pseudorandom numbers for parallel and distributed simulation. In Richard M. Fujimoto and David Bruce, editors, *Twelfth Workshop on Parallel and Distributed Simulation. PADS'98, May 26th–29th, 1998, Banff, Alberta,*

Canada, pages 90–97. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-8186-8457-7, 0-8186-8459-3. LCCN QA76.9.C65 W674 1998. URL `ftp://random.mat.sbg.ac.at/pub/publications/ste/pads98/pads_rev.ps.gz`. IEEE catalog number 98TB100233.

Evans:1998:RVG

[2349] M. Evans and T. Swartz. Random variable generation using concavity properties of transformed densities. *Journal of Computational and Graphical Statistics*, 7(4):514–528, December 1998. CODEN ???? ISSN 1061-8600 (print), 1537-2715 (electronic). URL `http://www.amstat.org/publications/jcgs/abstracts98/evans.html`.

Fuster-Sabater:1998:LPS

[2350] A. Fuster-Sabater and L. J. Garcia-Villalba. Likelihood that a pseudorandom sequence generator has optimal properties. *Electronics Letters*, 34(7):646–647, April 2, 1998. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=673772`.

Gammel:1998:HRR

[2351] B. M. Gammel. Hurst's rescaled range statistical analysis for pseudorandom number generators used in physical simulations. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 58(2):2586–2597, August 1998. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.58.2586`.

Garcia:1998:GCE

[2352] Alejandro L. Garcia and Berni J. Alder. Generation of the Chapman–Enskog distribution. *Journal of Computational Physics*, 140(1):66–70, February 10, 1998. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999198958892`.

Gentle:1998:RNG

[2353] James E. Gentle. *Random Number Generation and Monte Carlo Methods*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 0-387-98522-0. xiv + 247 pp. LCCN QA298.G46 1998. URL `http://www.science.gmu.edu/~jgentle/rngbk/index1.htm`.

Gutmann:1998:SGP

[2354] Peter Gutmann. Software generation of practically strong random numbers. In USENIX [4208], page ?? ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL http://usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf; http://www.cs.auckland.ac.nz/~pgut001/; http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix98.pdf; http://www.usenix.org/publications/library/proceedings/sec98/gutmann.html.

Hamilton:1998:AEP

[2355] K. G. Hamilton. Algorithm 780: Exponential pseudorandom distribution. *ACM Transactions on Mathematical Software*, 24(1):102–106, March 1998. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://doi.acm.org/10.1145/285861.285866; http://www.acm.org/pubs/citations/journals/toms/1998-24-1/p102-hamilton/.

Hellekalek:1998:ARQ

[2356] P. Hellekalek. On the assessment of random and quasi-random point sets. In Hellekalek and Larcher [4203], pages 49–108. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html.

Hellekalek:1998:CAP

[2357] P. Hellekalek. On correlation analysis of pseudorandom numbers. In Hellekalek and Larcher [4203], pages 251–265. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html.

Hellekalek:1998:DTP

[2358] Peter Hellekalek. Don't trust parallel Monte Carlo! In ????, editor, *Twelfth Workshop on Parallel and Distributed Simulation. PADS'98, May 26th–29th, 1998, Banff, Alberta, Canada*, pages 82–89. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998.

Hellekalek:1998:GRN

[2359] P. Hellekalek. Good random number generators are (not so) easy to find. *Mathematics and Computers in Simulation*, 46(5–6):485–505, June 1998.

CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL http://random.mat.sbg.ac.at/results/peter/A19final.pdf.

Hellekalek:1998:WST

[2360] Peter Hellekalek and Harald Niederreiter. The weighted spectral test: diaphony. *ACM Transactions on Modeling and Computer Simulation*, 8 (1):43–60, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hickernell:1998:LRH

[2361] Fred J. Hickernell. Lattice rules: How well do they measure up? In Hellekalek and Larcher [4203], pages 109–177. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html.

Hoffman:1998:RNG

[2362] Eric J. Hoffman. Random number generator. US Patent 5,706,218, January 6, 1998. URL https://www.google.com/patents/US5706218. US patent application number 08/648,553, filed 15 May 1996 by Intel Corporation.

Jakobsson:1998:PSP

[2363] Markus Jakobsson, Elizabeth Shriver, Bruce K. Hillyer, and Ari Juels. A practical secure physical random bit generator. In ACM, editor, *Proceedings of the Fifth ACM Conference on Computer and Communications Security, November 3–5, 1998, San Francisco, California*, pages 103–111. ACM Press, New York, NY 10036, USA, 1998. ISBN 1-58113-007-4. LCCN QA76.9.A25 A33 1998. URL http://www.bell-labs.com/user/shriver/random.html.

Kao:1998:RNG

[2364] Chiang Kao and J. Y. Wong. Random number generators with long period and sound statistical properties. *Computers and Mathematics and Applications*, 36(3):113–121, August 1998. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122198001333.

Kao:1998:SET

[2365] Chiang Kao and Hui-Chin Tang. Several extensively tested multiple recursive random number generators. *Computers and Mathematics and Applications*, 36(6):129–136, September 1998. CODEN CMAPDK.

ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122198001667.

Kelsey:1998:CAP

[2366] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. *Lecture Notes in Computer Science*, 1372:168–188, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1372/13720168.htm; http://link.springer-ny.com/link/service/series/0558/papers/1372/13720168.pdf; http://www.counterpane.com/pseudorandom_number.html; http://www.schneier.com/paper-prngs.html.

Knudsen:1998:JHH

[2367] Jonathan Knudsen. JavaTalk: Horseshoes, hand grenades and random numbers. *SunServer*, 12(1):16–17, January 1998. CODEN ???? ISSN 1091-4986.

Knuth:1998:SA

[2368] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, third edition, 1998. ISBN 0-201-89684-2. xiii + 762 pp. LCCN QA76.6 .K64 1997. US$52.75.

Kolmogorov:1998:TRN

[2369] A. N. Kolmogorov. On tables of random numbers. *Theoretical Computer Science*, 207(2):387–395, November 06, 1998. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.elsevier.com/cas/tree/store/tcs/sub/1998/207/2/2906.pdf.

Larcher:1998:DPS

[2370] Gerhard Larcher. Digital point sets: Analysis and application. In Hellekalek and Larcher [4203], pages 178–222. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html. See [**?**].

LEcuyer:1998:DPS

[2371] P. L'Ecuyer and P. Hellekalek. Design principles and statistical tests of random number generators. In Hellekalek and Larcher [4203], pages 223–265. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html.

LEcuyer:1998:GPI

[2372] Pierre L'Ecuyer. Good parameters and implementations for combined multiple recursive random number generators. Report, Université de Montréal, Montréal, PQ, Canada, 1998. URL `http://www.iro.umontreal.ca/blecuyer/papers.html`. Published in [2456].

LEcuyer:1998:RNGa

[2373] Pierre L'Ecuyer. Random number generation. In Banks [4201], chapter 4, pages 93–137. ISBN 0-471-13403-1 (hardcover). LCCN T57.62 .H37 1998. URL `http://www.loc.gov/catdir/bios/wiley044/97051533.html`; `http://www.loc.gov/catdir/description/wiley037/97051533.html`; `http://www.loc.gov/catdir/toc/onix01/97051533.html`.

LEcuyer:1998:RNGb

[2374] Pierre L'Ecuyer and Peter Hellekalek. Random number generators: selection criteria and testing. In Hellekalek and Larcher [4203], pages 223–265. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL `http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html`; `http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html`.

LEcuyer:1998:RNGc

[2375] Pierre L'Ecuyer. Random number generators and empirical tests. In Niederreiter et al. [4207], pages 124–138. ISBN 0-387-98335-X (softcover). LCCN Q183.9 .M67 1998. URL `http://www.loc.gov/catdir/enhancements/fy0815/97034133-d.html`; `http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html`.

LEcuyer:1998:URNa

[2376] Pierre L'Ecuyer. Uniform random number generation. In Kent et al. [4205], pages 323–339. ISBN 0-8247-2292-2 (hardcover). LCCN QA76.15 .E5 v.39.

LEcuyer:1998:URNb

[2377] P. L'Ecuyer. Uniform random number generators. In Medeiros et al. [4206], pages 97–104. ISBN 0-7803-5133-9 (softbound), 0-7803-5102-9 (casebound), 0-7803-5103-7 (microfiche). LCCN QA76.9.C65 W562 1998. IEEE catalog number 98CH36274.

Lu:1998:IPG

[2378] Chi-Jen Lu. Improved pseudorandom generators for combinatorial rectangles. *Lecture Notes in Computer Science*, 1443:223–??,

1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1443/14430223.htm; http://link.springer-ny.com/link/service/series/0558/papers/1443/14430223.pdf.

Lurie:1998:AMS

[2379] Philip M. Lurie and Matthew S. Goldberg. An approximate method for sampling correlated random variables from partially-specified distributions. *Management Science*, 44(2):203–218, February 1998. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Malov:1998:RVG

[2380] Sergey V. Malov. Random variables generated by ranks in dependent schemes. *Metrika. International Journal for Theoretical and Applied Statistics.*, 48(1):61–67, September 1998. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic). URL http://link.springer.com/article/10.1007/PL00003972.

Marsaglia:1998:MPMa

[2381] George Marsaglia and Wai Wan Tsang. The Monty Python method for generating gamma variables. *Journal of Statistical Software*, 3 (3):1–8, 1998. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/v03/i03; http://www.jstatsoft.org/v03/i03/GERMGAM.PDF; http://www.jstatsoft.org/v03/i03/GERMGAM.PS; http://www.jstatsoft.org/v03/i03/updates.

Marsaglia:1998:MPMb

[2382] George Marsaglia and Wai Wan Tsang. The Monty Python method for generating random variables. *ACM Transactions on Mathematical Software*, 24(3):341–350, September 1998. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL http://www.acm.org:80/pubs/citations/journals/toms/1998-24-3/p341-marsaglia/.

Mascagni:1998:PLC

[2383] Michael Mascagni. Parallel linear congruential generators with prime moduli. *Parallel Computing*, 24(5–6):923–936, June 1, 1998. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL http://www.elsevier.com/cas/tree/store/parco/sub/1998/24/5-6/1287.pdf; http://www.sciencedirect.com/science/article/pii/S0167819198000106.

Matsumoto:1998:DCP

[2384] M. Matsumoto and T. Nishimura. Dynamic creation of pseudorandom number generators. In Niederreiter et al. [4207], pages 56–69. ISBN 0-387-98335-X (softcover). LCCN Q183.9 .M67 1998. URL `http://www.loc.gov/catdir/enhancements/fy0815/97034133-d.html`; `http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html`.

Matsumoto:1998:MTD

[2385] Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation*, 8(1): 3–30, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `http://www.math.keio.ac.jp/~matsumoto/emt.html`.

Matsumoto:1998:SCA

[2386] Makoto Matsumoto. Simple cellular automata as pseudorandom m-sequence generators for built-in self-test. *ACM Transactions on Modeling and Computer Simulation*, 8(1):31–42, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Mende:1998:MSP

[2387] R. G. Mende, L. C. Noll, and S. Sisodiya. Method for seeding a pseudorandom number generator with a cryptographic hash of a digitization of a chaotic system. US Patent No. 5,732,138A., March 24, 1998. URL `https://www.google.com/patents/US5732138`. Patent filed 29 January 1996.

Miller:1998:BPG

[2388] Jeff Miller. Bivar: a program for generating correlated random numbers. *Behavior Research Methods, Instruments, and Computers*, 30(4): 720–723, December 1998. CODEN BRMCEW. ISSN 0743-3808 (print), 1532-5970 (electronic). URL `http://www.springerlink.com/content/m765v63np2420764/`.

Morohosi:1998:DAR

[2389] H. Morohosi and M. Fushimi. Designing asymptotically random GFSR sequences. Report METR 98-11, Department of Mathematical Engineering and Information Physics, The University of Tokyo, Tokyo, Japan, 1998.

Niederreiter:1998:AGA

[2390] H. Niederreiter and C. Xing. The algebraic-geometry approach to low-discrepancy sequences. In Niederreiter et al. [4207], pages 139–160. ISBN

0-387-98335-X (softcover). LCCN Q183.9 .M67 1998. URL http://www.loc.gov/catdir/enhancements/fy0815/97034133-d.html; http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html.

Niederreiter:1998:NSA

[2391] H. Niederreiter and C. Xing. Nets, (t, s)-sequences, and algebraic geometry. In Hellekalek and Larcher [4203], pages 267–302. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html; http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html.

Owen:1998:LSS

[2392] Art B. Owen. Latin supercube sampling for very high-dimensional simulations. *ACM Transactions on Modeling and Computer Simulation*, 8 (1):71–102, January 1998. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Park:1998:AGC

[2393] Chul Gyu Park and Dong Wan Shin. An algorithm for generating correlated random variables in a class of infinitely divisible distributions. *Journal of Statistical Computation and Simulation*, 61(1–2):127–139, ???? 1998. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949659808811905.

Patel:1998:EDL

[2394] Sarvar Patel and Ganapathy S. Sundaram. An efficient discrete log pseudo random generator. *Lecture Notes in Computer Science*, 1462:304–317, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1462/14620304.htm; http://link.springer-ny.com/link/service/series/0558/papers/1462/14620304.pdf; http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/073818.html.

Peterson:1998:JRM

[2395] Ivars Peterson. *The Jungles of Randomness: a Mathematical Safari*. Wiley, New York, NY, USA, 1998. ISBN 0-471-16449-6. viii + 239 pp. LCCN QA273.15.P48 1997. US$24.95.

Petrie:1998:NBR

[2396] C. S. Petrie and J. A. Connelly. A noise-based random bit generator IC for applications in cryptography. In IEEE, editor, *ISCAS '98: proceedings of the 1998 IEEE International Symposium on Circuits and Systems:*

May 31–June 3, 1998, Monterey Conference Center, Monterey, CA, volume 2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-7803-4455-3 (paperback), 0-7803-4456-1 (hardcover). LCCN TK7801.I22 1998.

Resende:1998:URN

[2397] F. J. Resende and B. V. Costa. Using random number generators in Monte Carlo simulations. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 58(4):5183–5184, October 1998. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.58.5183`.

Rey:1998:GRN

[2398] W. J. J. Rey. On generating random numbers, with help of $y = [(a + x)\sin(bx)] \bmod 1$. In B. Grigelionis, J. Kubilius, V. Paulauskas, H. Pragarauskas, R. Rudzkis, and V. Statulevičius, editors, *Probability theory and mathematical statistics: proceedings of the Seventh Vilnius Conference (1998), Vilnius, Lithuania, 12–18 August, 1998 [in conjunction with the 22nd European Meeting of Statisticians]*, pages 390–?? TEV, Vilnius, Lithuania, 1998. ISBN 90-6764-313-0. LCCN QA273.A1 V53 1998.

Schatte:1998:BLV

[2399] P. Schatte. On Benford's law to variable base. *Statistics & Probability Letters*, 37(4):391–397, March 30, 1998. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167715297001429`.

Schmid:1998:SNN

[2400] W. C. Schmid. Shift-nets: a new class of binary digital (t, m, s)-nets. In Hellekalek and Larcher [4203], pages 369–381. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL `http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html`; `http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html`.

Schneier:1998:YSP

[2401] Bruce Schneier. Yarrow: a secure pseudorandom number generator. World-Wide Web site., 1998. URL `http://www.schneier.com/yarrow.html`. Yarrow is no longer being supported.

Shchur:1998:RGR

[2402] Lev N. Shchur and Paolo Butera. The RANLUX generator: Resonances in a random walk test. *International Journal of*

Modern Physics C [Physics and Computers], 9(4):607–624, June 1998. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://arxiv.org/abs/hep-lat/9805017`; `http://www.worldscinet.com/ijmpc/09/0904/S0129183198000509.html`.

Soto:1998:STR

[2403] Juan Soto. Statistical testing of RNGs. World-Wide Web slide presentation., June 1998. URL `http://csrc.nist.gov/rng/Copy-of-sts.ppt`. Presented at Computer Security Division Meeting, Gaithersburg, MD.

Sugita:1998:LTS

[2404] Hiroshi Sugita and Satoshi Takanobu. Limit theorem for symmetric statistics with respect to Weyl transformation: Disappearance of dependency. *Journal of Mathematics of Kyoto University*, 38(4):653–671, ???? 1998. CODEN JMKYAZ. ISSN 0023-608X.

Takashima:1998:RWT

[2405] K. Takashima. Random walk tests of pseudo-random number generations by cellular automata. In ????, editor, *Proceedings of Third St. Petersburg Workshop on Simulations*, pages 302–305. Saint Petersburg University Press, Saint Petersburg, Russia, 1998. ISBN ???? LCCN ????

Tanaka:1998:OLA

[2406] H. Tanaka, T. Ohishi, and T. Kaneko. An optimised linear attack on pseudorandom generators using a non linear combiner. *Lecture Notes in Computer Science*, 1396:43–??, 1998. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tezuka:1998:FAM

[2407] Shu Tezuka. Financial applications of Monte Carlo and quasi-Monte Carlo methods. In Hellekalek and Larcher [4203], pages 303–329. ISBN 0-387-98554-9. LCCN QA298 .P82 1998. URL `http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html`; `http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html`.

Thomlinson:1998:NBP

[2408] Matthew W. Thomlinson, Daniel R. Simon, and Bennet Yee. Non-biased pseudo random number generator. United States Patent 5,778,069., July 7, 1998. URL `http:www.google.com/patents/US5778069`.

Trotter:1998:RTS

[2409] William T. Trotter and Peter Winkler. Ramsey theory and sequences of random variables. *Combinatorics, Probability and Computing*, 7(2):

221–238, June 1998. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL `http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=7&issueId=02`.

Vallee:1998:CAB

[2410] Brigitte Vallée. The complete analysis of the binary Euclidean algorithm. *Lecture Notes in Computer Science*, 1423:77–94, 1998. CODEN LNCSD9. ISBN 3-540-64657-4. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.csie.nuk.edu.tw/~cychen/gcd/The%20complete%20analysis%20of%20the%20binary%20Euclidean%20Algorithm.pdf`; `http://www.springer.com/computer/theoretical+computer+science/book/978-3-540-64657-0`.

Vallee:1998:DBE

[2411] Brigitte Vallée. Dynamics of the binary Euclidean algorithm: functional analysis and operators. *Algorithmica*, 22(?):660–685, ???? 1998. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `http://www.info.unicaen.fr/~brigitte/Publications/bin-gcd.ps`.

vanHameren:1998:GLD

[2412] André van Hameren, Ronald Kleiss, and Jiri Hoogland. Gaussian limits for discrepancies. *Nuclear Physics B, Proceedings Supplements*, 63(1–3):988–990, April 1998. CODEN NPBSE7. ISSN 0920-5632 (print), 1873-3832 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S092056329700964X`.

Wegenkittl:1998:THS

[2413] Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inversive congruential pseudorandom numbers? *Journal of Computational and Applied Mathematics*, 95(1–2):117–125, August 28, 1998. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic).

Wheeler:1998:CX

[2414] David J. Wheeler and Roger M. Needham. Correction to XTEA. Report, Cambridge University, Cambridge, UK, October 1998. URL `http://www.movable-type.co.uk/scripts/xxtea.pdf`. See also original TEA [2131] and first extension XTEA [2303].

Williams:1998:ELP

[2415] Hugh C. Williams. *Édouard Lucas and primality testing*, volume 22 of *Canadian Mathematical Society series of monographs and advanced*

texts. Wiley, New York, NY, USA, 1998. ISBN 0-471-14852-0 (hardcover). xviii + 525 pp. LCCN QA246 .W43 1998. URL http://www.loc.gov/catdir/description/wiley033/97044760.html; http://www.loc.gov/catdir/toc/onix04/97044760.html.

Williamson:1998:CNR

[2416] Patrica Pepple Williamson. C.449. A note on the random generation of Dirichlet variates. *Journal of Statistical Computation and Simulation*, 60(2):168–173, March 1998. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949659808811882.

Wolf:1998:RWP

[2417] Marek Wolf. Random walk on the prime numbers. *Physica A, Statistical Mechanics and its Applications*, 250(1–4):335–344, February 15, 1998. CODEN PHYADX. ISSN 0378-4371 (print), 1873-2119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0378437197006614.

Woodcock:1998:ACR

[2418] Christopher F. Woodcock and Nigel P. Smart. p-adic chaos and random number generation. *Experimental Mathematics*, 7(4):333–342, ???? 1998. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL http://projecteuclid.org/euclid.em/1047674151.

Ziff:1998:FTS

[2419] Robert M. Ziff. Four-tap shift-register-sequence random-number generators. *Computers in Physics*, 12(4):385–392, July/August 1998. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic). URL http://arxiv.org/abs/cond-mat/9710104.

Aiello:1999:HSP

[2420] William Aiello, S. Rajagopalan, and Ramarathnam Venkatesan. High-speed pseudorandom number generation with small memory. *Lecture Notes in Computer Science*, 1636:290–304, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1636/16360290.htm; http://link.springer-ny.com/link/service/series/0558/papers/1636/16360290.pdf.

Beltrami:1999:WRCa

[2421] Edward Beltrami. *What Is Random?: Chance and Order in Mathematics and Life*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany /

London, UK / etc., 1999. ISBN 1-4612-7156-8. LCCN QA273.A1-274.9; QA274-274.9.

Berdnikov:1999:CLV

[2422] A. S. Berdnikov, S. B. Turtia, and A. Compagner. The combination of LP_τ vectors and shift register RNGs as a way to generate independent random sequences for parallel computations. *Computer Physics Communications*, 121–122:612, September/October 1999. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465506700194`.

Berleant:1999:IBA

[2423] Daniel Berleant. Interval based, automatically verified arithmetic on random variables. Technical report, Dept. of Electrical and Computer Engineering, 2215 Coover Hall, Iowa State University, Ames, IA, USA, 1999. URL `http://engr.uark.edu/~djb/me/vita/vita.html`; `http://engr.uark.edu/~djb/Research/Pdfs/Overview/index.html`.

Brent:1999:FAB

[2424] Richard P. Brent. Further analysis of the binary Euclidean algorithm. Technical Report TR-7-99, Programming Research Group, Oxford University, Oxford, UK, November 4, 1999. URL `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.122.7959&rep=rep1&type=pdf`. See also earlier work [759].

Brunner:1999:OML

[2425] D. Brunner and A. Uhl. Optimal multipliers for linear congruential pseudo random number generators with prime moduli: Parallel computation and properties. *BIT Numerical Mathematics*, 39(2):193–209, June 1999. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=39&issue=2&spage=193`.

Chang:1999:EIH

[2426] T. Chang, B. Park, and Y. H. Kim. An efficient implementation of the D-homomorphism for generation of de Bruijn sequences. *IEEE Transactions on Information Theory*, 45(4):1280–1283, ???? 1999. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Chen:1999:SSM

[2427] E. J. Chen, P. L'Ecuyer, and W. D. Kelton. Seed and stream management for multiple recursive random number generators. Technical Report

????, Department of Quantitative Analysis and Operations Management, University of Cincinnati, Cincinnati, OH, USA, 1999.

Chu:1999:DTF

[2428] Pong P. Chu and Robert E. Jones. Design techniques of FPGA-based random number generator (extended abstract). In ????, editor, *MAPLD 99 Proceedings: Military and Aerospace Applications of Programmable Devices and Technologies Conference, September 28-30, 1999, Kossiakoff Conference Center, The Johns Hopkins University, Applied Physics Laboratory 11100 Johns Hopkins Road, Laurel, Maryland 20723-6099*, pages 1–2. ????, Greenbelt, MD, USA, 1999. URL `http://web.archive.org/web/20080720093740/http://klabs.org/richcontent/MAPLDCon99/Abstracts/chu.pdf`.

Coddington:1999:IIR

[2429] P. D. Coddington, J. A. Mathew, and K. A. Hawick. Interfaces and implementations of random number generators for Java Grande applications. *Lecture Notes in Computer Science*, 1593:873–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

deRaadt:1999:COO

[2430] Theo de Raadt, Niklas Hallqvist, Artur Grabowski, Angelos D. Keromytis, and Niels Provos. Cryptography in OpenBSD: An overview. In USENIX [4215], page ?? ISBN 1-880446-33-2. LCCN QA76.8.U65 U84 1999. URL `http://static.usenix.org/publications/library/proceedings/usenix99/full_papers/deraadt/deraadt_html/`; `http://www.openbsd.org/papers/crypt-paper.ps`.

Durrant:1999:RND

[2431] S. Durrant. Random numbers in data security systems. Report, Intel Corporation, ????, 1999. URL `http://www.intel.com/design/security/rng/WP_Durrant.htm`.

Eichelsbacher:1999:CPA

[2432] Peter Eichelsbacher and Małgorzata Roos. Compound Poisson approximation for dissociated random variables via Stein's method. *Combinatorics, Probability and Computing*, 8(4):335–346, July 1999. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL `http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=8&issueId=04`. Random graphs and combinatorial structures (Oberwolfach, 1997).

Entacher:1999:CSR

[2433] Karl Entacher. On the CRAY-system random number generator. *Simulation*, 72(3):163–169, March 1999. CODEN SIMUA2. ISSN 0037-5497 (print), 1741-3133 (electronic). URL `http://sim.sagepub.com/content/72/3/163.abstract`.

Entacher:1999:PRN

[2434] Karl Entacher, Andreas Uhl, and Stefan Wegenkittl. Parallel random number generation: Long-range correlations among multiple processors. *Lecture Notes in Computer Science*, 1557:107–116, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1557/15570107.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/1557/15570107.pdf`.

Entacher:1999:PSL

[2435] Karl Entacher. Parallel streams of linear random numbers in the spectral test. *ACM Transactions on Modeling and Computer Simulation*, 9(1): 31–44, January 1999. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Entacher:1999:QMC

[2436] Karl Entacher, Peter Hellekalek, and Pierre L'Ecuyer. Quasi-Monte Carlo node sets from linear congruential generators. In Niederreiter and Spanier [4214], pages 188–198. ISBN 3-540-66176-X (softcover). LCCN Q183.9 .M672 1999. URL `http://www.loc.gov/catdir/enhancements/fy0815/99047502-d.html`.

Falk:1999:SAG

[2437] Michael Falk. A simple approach to the generation of uniformly distributed random variables with prescribed correlations. *Communications in Statistics: Simulation and Computation*, 28(3):785–791, 1999. CODEN CSSCDB. ISSN 0361-0918.

Fernandez:1999:AER

[2438] Julio F. Fernández. Algorithm for exponential random numbers. *Computer Physics Communications*, 121–122:78–82, September/October 1999. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465599002854`.

Fernandez:1999:ANRa

[2439] Julio F. Fernández and Carlos Criado. Algorithm for normal random numbers. *arxiv.org*, page 5, January 20, 1999. URL `http://arxiv.org/abs/cond-mat/9901202v1`.

Fernandez:1999:ANRb

[2440] Julio F. Fernández and Carlos Criado. Algorithm for normal random numbers. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 60(3):3361–3365, September 1999. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.60.3361`. See comment [2646] and reply [2593].

Gartner:1999:PCP

[2441] Bernd Gärtner. Pitfalls in computing with pseudorandom determinants. Report, Institut für Theoretische Informatik, ETH Zürich, ETH Zentrum, CH8092 Zürich, Switzerland, 1999. URL `http://www.inf.ethz.ch/personal/gaertner/texts/own_work/random_matrices.pdf`.

Gartner:1999:RCZ

[2442] Bernd Gärtner. Ein Reinfall mit Computer-Zufallszahlen. (German) [A failure with computer random numbers]. *Mitteilungen der Deutschen Mathematiker-Vereinigung*, 2(??):55–60, ???? 1999. CODEN ???? ISSN 0947-4471. URL `http://www.inf.ethz.ch/personal/gaertner/texts/own_work/dmv.ps.gz`.

Goldreich:1999:IDB

[2443] O. Goldreich and A. Wigderson. Improved derandomization of BPP using a hitting set generator. *Lecture Notes in Computer Science*, 1671: 131–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goldreich:1999:MCP

[2444] Oded Goldreich. *Modern cryptography, probabilistic proofs, and pseudorandomness*, volume 17 of *Algorithms and combinatorics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-64766-X. ISSN 0937-5511. xv + 182 pp. LCCN QA76.9.A25 G64 1999.

Goldreich:1999:P

[2445] Oded Goldreich. Pseudorandomness. *Notices of the American Mathematical Society*, 46(10):1209–1216, November 1999. CODEN AMNOAN. ISSN 0002-9920 (print), 1088-9477 (electronic).

Gonzalez:1999:RNG

[2446] Jorge A. González and Ramiro Pino. A random number generator based on unpredictable chaotic functions. *Computer Physics Communications*, 120(2–3):109–114, August 1999. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465599002337`.

Griffin:1999:DNR

[2447] Frances Griffin, Harald Niederreiter, and Igor Shparlinski. On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In Fossorier et al. [4211], pages 87–93. ISBN 3-540-66723-7. LCCN QA268 .A35 1999. URL `http://www.loc.gov/catdir/enhancements/fy0812/99054502-d.html`.

Haastad:1999:PGO

[2448] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, August 1999. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/24470`.

Intel:1999:IRN

[2449] Intel Platform Security Division. The Intel random number generator. Intel technical brief, Intel Corporation, ????, 1999. URL `ftp://download.intel.com/design/security/rng/techbrief.pdf`.

Jun:1999:IRN

[2450] Benjamin Jun and Paul Kocher. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Research, Inc., Menlo Park, CA, USA, April 22, 1999. URL `ftp://download.intel.com/design/security/rng/CRIwp.pdf`; `http://www.cryptography.com/intelRNG.pdf`.

Kleinman:1999:SBO

[2451] Nathan L. Kleinman, James C. Spall, and Daniel Q. Naiman. Simulation-based optimization with stochastic approximation using Common Random Numbers. *Management Science*, 45(??):1570–1578, ???? 1999. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Koldobsky:1999:PDD

[2452] Alexander Koldobsky. Positive definite distributions and subspaces of L_p with applications to stable processes. *Canadian mathematical bulletin*

= *Bulletin canadien de mathématiques*, 42(3):344–353, September 1999. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Koshiba:1999:UPN

[2453] Takeshi Koshiba. Unpredictability of pseudorandom number generators on public key cryptosystems with random inputs. *Sūrikaisekikenkyūsho Kōkyūroku*, 1093:162–167, 1999. CODEN ???? ISSN ???? Models of computation and algorithms (Japanese) (Kyoto, 1999).

Larcher:1999:ADS

[2454] Gerhard Larcher, Reinhard Wolf, and Jürgen Eichenauer-Herrmann. On the average discrepancy of successive tuples of pseudo-random numbers over parts of the period. *Monatshefte für Mathematik*, 127(2):141–154, February 1999. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

LEcuyer:1999:BLC

[2455] Pierre L'Ecuyer and Richard Simard. Beware of linear congruential generators with multipliers of the form $a = \pm 2^q \pm 2^r$. *ACM Transactions on Mathematical Software*, 25(3):367–374, September 1999. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://www.acm.org/pubs/citations/journals/toms/1999-25-3/p367-l_ecuyer/`; `http://www.acm.org/pubs/citations/journals/toms/1999-25-3/p367-l_ecuyer/p367-l_ecuyer.pdf`.

LEcuyer:1999:GPI

[2456] Pierre L'Ecuyer. Good parameters and implementations for combined multiple recursive random number generators. *Operations Research*, 47(1):159–164, January/February 1999. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://pubsonline.informs.org/doi/abs/10.1287/opre.47.1.159`; `http://www.jstor.org/stable/222902`.

LEcuyer:1999:SRU

[2457] P. L'Ecuyer. Some recommendable uniform random number generators. In Helena Szczerbicka, editor, *Modelling and simulation: a tool for the next millennium: 13th European Simulation Multiconference 1999, ESM'99: June 1–4, 1999, Warsaw, Poland*, volume 1, pages 185–190. Society for Computer Simulation, San Diego, CA, USA, 1999. ISBN 1-56555-171-0 (vol. 1), 1-56555-172-9 (vol. 2). LCCN ????

LEcuyer:1999:TLC

[2458] Pierre L'Ecuyer. Tables of linear congruential generators of different sizes and good lattice structure. *Mathematics of Computation*, 68(225): 249–260, 1999. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2585108.pdf`.

LEcuyer:1999:TME

[2459] Pierre L'Ecuyer. Tables of maximally equidistributed combined LFSR generators. *Mathematics of Computation*, 68(225):261–269, January 1999. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/jourcgi/jour-pbprocess?fn=110&arg1=S0025-5718-99-01039-X&u=/mcom/1999-68-225/`.

Marsaglia:1999:RNC

[2460] George Marsaglia. Random numbers for C: The END? Message-ID `36A5FC62.17C9CC33@stat.fsu.edu`. Posting to the `sci.crypt.random-numbers`, `sci.math`, and `sci.stat.math` news groups., January 20, 1999. URL `http://groups.google.com/group/sci.crypt/browse_thread/thread/ca8682a4658a124d/`.

Mascagni:1999:SMP

[2461] M. Mascagni. Some methods of parallel pseudorandom number generation. In Heath et al. [4212], pages 277–288. ISBN 0-387-98680-4. LCCN QA76.58 .A543 1999. URL `http://www.loc.gov/catdir/enhancements/fy0817/98033425-t.html`.

Matus:1999:CIA

[2462] F. Matúš. Conditional independences among four random variables. III. Final conclusion. *Combinatorics, Probability and Computing*, 8(3):269–276, May 1999. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL `http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=8&issueId=03`.

McCullough:1999:ARS

[2463] B. D. McCullough. Assessing the reliability of statistical software: Part II. *The American Statistician*, 53(2):149–??, 1999. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.amstat.org/publications/tas/mccull.pdf`.

McCullough:1999:ASP

[2464] B. D. McCullough and B. Wilson. On the accuracy of statistical procedures in Microsoft Excel 97. *Computational Statistics & Data Anal-*

ysis, 31(1):27–37, July 28, 1999. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947399000043`.

McCullough:1999:NRE

[2465] B. D. McCullough and H. D. Vinod. The numerical reliability of econometric software. *Journal of Economic Literature*, 37(2):633–665, June 1999. CODEN JECLB3. ISSN 0022-0515 (print), 1547-1101 (electronic). URL `http://www.jstor.org/stable/2565215`; `https://www.aeaweb.org/articles?id=10.1257/jel.37.2.633`.

MRaihi:1999:CAR

[2466] D. M'Raihi, D. Naccache, D. Pointcheval, and S. Vaudenay. Computational alternatives to random number generators. *Lecture Notes in Computer Science*, 1556:72–??, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Muller:1999:CRV

[2467] Norbert Th. Müller. Computability on random variables. *Theoretical Computer Science*, 219(1–2):287–299, May 28, 1999. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/cas/tree/store/tcs/sub/1999/219/1-2/3100.pdf`.

Naor:1999:STA

[2468] Moni Naor and Omer Reingold. Synthesizers and their application to the parallel construction of pseudo-random functions. *Journal of Computer and System Sciences*, 58(2):336–375, April 1999. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S002200009891618X`.

Niederreiter:1999:DLS

[2469] Harald Niederreiter and Igor E. Shparlinski. On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. *Finite Fields and their Applications*, 5(3):246–253, July 1999. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579799902575`.

Peterson:1999:FRU

[2470] Ivars Peterson. Fibonacci at random: Uncovering a new mathematical constant. *Science News (Washington, DC)*, 155(24):376–377, June 12, 1999. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic). URL `http://www.jstor.org/stable/4011459`.

Peyravian:1999:GUB

[2471] Mohammad Peyravian, Stephen M. Matyas, Allen Roginsky, and Nev Zunic. Generating user-based cryptographic keys and random numbers. *Computers & Security*, 18(7):619–626, ???? 1999. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404899820409`.

Robert:1999:MCS

[2472] Christian P. Robert and George Casella. *Monte Carlo statistical methods*. Springer texts in statistics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 0-387-98707-X. xxi + 507 pp. LCCN QA276 .R575 1999.

Rouzankin:1999:CAR

[2473] P. S. Rouzankin and A. V. Voytishek. On the cost of algorithms for random selection. *Monte Carlo Methods and Applications*, 5(1):39–54, ???? 1999. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1999.5.issue-1/mcma.1999.5.1.39/mcma.1999.5.1.39.xml`.

Sackrowitz:1999:VRV

[2474] Harold Sackrowitz and Ester Samuel-Cahn. P values as random variables—expected P values. *The American Statistician*, 53(4):326–331, November 1999. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2686051`.

Schindler:1999:AFC

[2475] W. Schindler. AIS 20: Functionality classes and evaluation methodology for deterministic random number generators. Report, Bundesamt fur Sicherheit in der Informationstechnik (BSI), ????, December 1999. Version 2.0.

Schmid:1999:EQP

[2476] W. Ch. Schmid. The exact quality parameter of nets derived from Sobol' and Niederreiter sequences. In Iliev et al. [4213], pages 287–295. ISBN 981-02-3827-4. LCCN QA297 .R37 1999.

Shchur:1999:QRN

[2477] Lev N. Shchur. On the quality of random number generators with taps. *Computer Physics Communications*, 121–122:83–85, September/October 1999. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465599002866`.

Siu:1999:PNG

[2478] Chi Sang Obadiah Siu. Pseudorandom number generator by cellular automata and its application to cryptography. M.Phil., Chinese University of Hong Kong, Hong Kong, 1999. 68 pp.

Sobol:1999:DRR

[2479] I. M. Sobol, B. V. Shukhman, and A. Guinzbourg. On the distribution of random ranges. *Monte Carlo Methods and Applications*, 5(2):113–134, ???? 1999. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.1999.5.issue-2/mcma.1999.5.2.113/mcma.1999.5.2.113.xml`.

Sobol:1999:PRN

[2480] I. M. Sobol' and Yu. L. Levitan. A pseudo-random number generator for personal computers. *Computers and Mathematics and Applications*, 37(4–5):33–40, February/March 1999. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). Translation of the Russian original, *O datchike psevdosluchainykh chisel dlya personalnykh kompyuterov*, Matematicheskoe Modelirovanie, **2** (8) (1990), pp. 119–126, with the authors reversed.

Soto:1999:EST

[2481] Juan Soto. Empirical statistical testing of RNGs. World-Wide Web slide presentation., January 1999. URL `http://csrc.nist.gov/rng/Copy-of-rsa.ppt`. Presented at the 1999 RSA Data Security Conference, San Jose, CA.

Soto:1999:RTA

[2482] Juan Soto and Lawrence Bassham. Randomness testing of the Advanced Encryption Standard candidate algorithms. NIST internal report 6390, National Institute for Standards and Technology, Gaithersburg, MD, USA, 1999. 14 pp. URL `http://csrc.nist.gov/rng/AES-REPORT2.doc`. September.

Soto:1999:STRa

[2483] Juan Soto. Statistical testing of random number generators. In Anonymous [4210], pages 12–?? LCCN ???? URL `http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf`; `http://csrc.nist.gov/rng/AES-REPORT2.doc`.

Soto:1999:STRb

[2484] Juan Soto. Statistical testing of RNGs. World-Wide Web slide presentation., April 1999. URL `http://csrc.nist.gov/rng/ANSIX9F1.ppt`.

Presented at the ANSI X9F1 Meeting, Institute for Defense Analyses, Alexandria, VA.

Soto:1999:STRc

[2485] Juan Soto. Statistical testing of random number generators. World-Wide Web slide presentation., October 1999. URL `http://csrc.nist.gov/rng/nissc3.ppt`. Presented at The 22nd National Information Systems Security Conference, Crystal City, VA.

Stauffer:1999:IMT

[2486] Dietrich Stauffer. Ising model as test for simple random number generators. *International Journal of Modern Physics C [Physics and Computers]*, 10(5):807–808, July 1999. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/10/1005/S0129183199000619.html`.

Sudan:1999:PGX

[2487] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR Lemma (extended abstract). In ACM [4209], pages 537–546. ISBN 1-58113-067-8. LCCN QA75.5 .A14 1999. URL `http://www.acm.org/pubs/articles/proceedings/stoc/301250/p537-sudan/p537-sudan.pdf`; `http://www.acm.org/pubs/citations/proceedings/stoc/301250/p537-sudan/`. ACM order number 508990.

Tomassini:1999:GHQ

[2488] Marco Tomassini, Moshe Sipper, Mosé Zolla, and Mathieu Perrenoud. Generating high-quality random numbers in parallel by cellular automata. *Future Generation Computer Systems*, 16(2–3):291–305, December 1999. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.elsevier.com/gej-ng/10/19/19/41/25/35/abstract.html`.

Tretiakov:1999:EMC

[2489] K. V. Tretiakov and K. W. Wojciechowski. Efficient Monte Carlo simulations using a shuffled nested Weyl sequence random number generator. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 60(6):7626–7628, December 1999. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.60.7626`.

Trevisan:1999:CEU

[2490] Luca Trevisan. Construction of extractors using pseudo-random generators (extended abstract). In ACM [4209], pages 141–148. ISBN 1-58113-

067-8. LCCN QA75.5 .A14 1999. URL http://www.acm.org/pubs/articles/proceedings/stoc/301250/p141-trevisan/p141-trevisan.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/301250/p141-trevisan/. ACM order number 508990.

Vattulainen:1999:FTR

[2491] I. Vattulainen. Framework for testing random numbers in parallel calculations. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 59:7200–7204, June 1999. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.59.7200.

Watanabe:1999:SGR

[2492] Yuji Watanabe and Hideki Imai. Shared generation of random number with timestamp: How to cope with the leakage of the CA's secret. *Lecture Notes in Computer Science*, 1560:290–305, 1999. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1560/15600290.htm; http://link.springer-ny.com/link/service/series/0558/papers/1560/15600290.pdf.

Wegenkittl:1999:GRC

[2493] Stefan Wegenkittl and Makoto Matsumoto. Getting rid of correlations among pseudorandom numbers: discarding versus tempering. *ACM Transactions on Modeling and Computer Simulation*, 9(3):282–294, July 1999. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Wegenkittl:1999:GTP

[2494] Stefan Wegenkittl. Gambling tests for pseudorandom number generators. Report, Institut für Mathematik, Universität Salzburg, Salzburg, Austria, August 27, 1999.

Jenkins:19xx:IFC

[2495] Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, Accumulate, Add, and Count) is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.

Alekhnovich:2000:PGP

[2496] M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. In IEEE [4219], pages 43–53. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society Order Number PR00850.

Anonymous:2000:RNG

[2497] Anonymous. Random number generation and testing. Web site., December 2000. URL `http://csrc.nist.gov/rng/`.

Balazs:2000:ONC

[2498] Nandor L. Balazs, John C. Browne, James D. Louck, and Daniel S. Strottman. Obituary: Nicholas Constantine Metropolis. *Physics Today*, 53(10):100, October 2000. CODEN PHTOAD. ISSN 0031-9228 (print), 1945-0699 (electronic). URL `http://www.aip.org/pt/vol-53/iss-10/p100.html`.

Beichl:2000:MA

[2499] Isabel Beichl and Francis Sullivan. The Metropolis algorithm. *Computing in Science and Engineering*, 2(1):65–69, January/February 2000. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic). URL `http://dlib.computer.org/cs/books/cs2000/pdf/c1065.pdf`; `http://www.computer.org/cse/cs1999/c1065abs.htm`.

Borkowf:2000:BRB

[2500] Craig B. Borkowf. Book review: *Random Number Generation and Monte Carlo Methods* by James E. Gentle. *Technometrics*, 42(4):431–432, November 2000. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/1270960`.

Brent:2000:TYA

[2501] Richard P. Brent. Twenty years' analysis of the binary Euclidean algorithm. In Davies et al. [4217], pages 41–52. ISBN 0-333-92230-1. LCCN QA75.5 .O8 2000. URL `http://www.cs.ox.ac.uk/people/richard.brent/pd/rpb183pr.pdf`.

Chen:2000:RRI

[2502] Zhi-Zhong Chen and Ming-Yang Kao. Reducing randomness via irrational numbers. *SIAM Journal on Computing*, 29(4):1247–1256, August 2000. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/34160`.

Couture:2000:LCR

[2503] Raymond Couture and Pierre L'Ecuyer. Lattice computations for random numbers. *Mathematics of Computation*, 69(230):757–765, April 2000. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-99-01112-6; http://www.ams.org/mcom/2000-69-230/S0025-5718-99-01112-6/S0025-5718-99-01112-6.dvi; http://www.ams.org/mcom/2000-69-230/S0025-5718-99-01112-6/S0025-5718-99-01112-6.pdf; http://www.ams.org/mcom/2000-69-230/S0025-5718-99-01112-6/S0025-5718-99-01112-6.ps; http://www.ams.org/mcom/2000-69-230/S0025-5718-99-01112-6/S0025-5718-99-01112-6.tex.

Danger:2000:EFI

[2504] J. L. Danger, A. Ghazel, E. Boutillon, and H. Laamari. Efficient FPGA implementation of Gaussian noise generator for communication channel emulation. In *7th IEEE International Conference on Electronics, Circuits & Systems, December 17–20, 2000, Jounieh, Lebanon*, pages 366–369. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2000. ISBN 0-7803-6542-9. LCCN TK7801 .I226 2000. URL http://ieeexplore.ieee.org/document/911557/. IEEE catalog number 00EX445.

Deng:2000:RNG

[2505] Lih-Yuan Deng and Dennis K. J. Lin. Random number generation for the new century. *The American Statistician*, 54(2):145–150, May 2000. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL http://www.amstat.org/publications/tas/Deng.htm.

Devroye:2000:PSQ

[2506] Luc Devroye, James Fill, and Ralph Neininger. Perfect simulation from the Quicksort limit distribution. *Electronic Communications in Probability*, 5:12:95–12:99, 2000. CODEN ???? ISSN 1083-589X. URL http://ecp.ejpecp.org/article/view/1024.

Dewen:2000:NMG

[2507] H. Dewen. A novel method for generating pseudorandom integer strings and pseudorandom sequences. *Science in China. Series E, Technological sciences*, 43(4):413–420, 2000. CODEN SCETFO. ISSN 1006-9321 (print), 1862-281X (electronic).

Dyadkin:2000:SBM

[2508] Iosif G. Dyadkin and Kenneth G. Hamilton. A study of 128-bit multipliers for congruential pseudorandom number generators. *Computer Physics*

Communications, 125(1–3):239–258, March 2000. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://cpc.cs.qub.ac.uk/summaries/ADLK; http://www.elsevier.com/gej-ng/10/15/40/55/25/42/abstract.html; http://www.sciencedirect.com/science/article/pii/S0010465599004671.

Evans:2000:AIM

[2509] Michael (Michael John) Evans and T. Swartz. *Approximating integrals via Monte Carlo and deterministic methods*, volume 20 of *Oxford statistical science series*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2000. ISBN 0-19-850278-8. ix + 288 pp. LCCN QA311 .E92 2000. URL http://www.loc.gov/catdir/enhancements/fy0604/99052843-d.html; http://www.loc.gov/catdir/enhancements/fy0604/99052843-t.html.

Fukuyama:2000:PFA

[2510] Katusi Fukuyama and Tetsuo Tomokuni. On pseudorandom functions and asymptotic distributions. *Monte Carlo Methods and Applications*, 6 (3):167–174, ???? 2000. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://www.degruyter.com/view/j/mcma.2000.6.issue-3/mcma.2000.6.3.167/mcma.2000.6.3.167.xml.

Gennaro:2000:IPR

[2511] Rosario Gennaro. An improved pseudo-random generator based on discrete log. *Lecture Notes in Computer Science*, 1880:469–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1880/18800469.htm; http://link.springer-ny.com/link/service/series/0558/papers/1880/18800469.pdf.

Gentleman:2000:LSS

[2512] Robert Gentleman and Ross Ihaka. Lexical scope and statistical computing. *Journal of Computational and Graphical Statistics*, 9(3):491–508, September 2000. CODEN ???? ISSN 1061-8600 (print), 1537-2715 (electronic). URL http://www.amstat.org/publications/jcgs/abstracts00/Ihaka.htm; http://www.tandfonline.com/doi/abs/10.1080/10618600.2000.10474895.

Goldreich:2000:ITP

[2513] Oded Goldreich. Invited talk: Pseudorandomness. *Lecture Notes in Computer Science*, 1853:687–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1853/18530687.htm; http://link.

springer-ny.com/link/service/series/0558/papers/1853/18530687.pdf.

Gutierrez:2000:MDI

[2514] Jaime Gutierrez, Harald Niederreiter, and Igor E. Shparlinski. On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period. *Monatshefte für Mathematik*, 129(1): 31–36, January 2000. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Hickernell:2000:ELS

[2515] Fred J. Hickernell, Hee Sun Hong, Pierre L'Écuyer, and Christiane Lemieux. Extensible lattice sequences for quasi-Monte Carlo quadrature. *SIAM Journal on Scientific Computing*, 22(3):1117–1138 (electronic), 2000. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic).

Hormann:2000:AAG

[2516] Wolfgang Hörmann. Algorithm 802: an automatic generator for bivariate log-concave distributions. *ACM Transactions on Mathematical Software*, 26(1):201–219, March 2000. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL http://doi.acm.org/10.1145/347837.347908; http://www.acm.org/pubs/citations/journals/toms/2000-26-1/p201-hormann/; http://www.acm.org/pubs/citations/journals/toms/2000-26-1/p201-hormann/p201-hormann.pdf.

Hormann:2000:ARV

[2517] Wolfgang Hörmann and Josef Leydold. Automatic random variate generation for simulation input. In Joines et al. [4220], pages 675–683. ISBN 0-7803-6579-8 (softcover), 0-7803-6580-1 (casebound), 0-7803-6581-X (microfiche). LCCN QA76.9.C65 W568 2000. IEEE Catalog Number 00CH37165.

IEEE:2000:IPH

[2518] IEEE. The IEEE P1363 home page: Standard specifications for public-key cryptography. World-Wide Web site., 2000. URL http://grouper.ieee.org/groups/1363/index.html.

Impagliazzo:2000:EPR

[2519] Russell Impagliazzo, Ronen Shaltiel, and Avi Wigderson. Extractors and pseudo-random generators with optimal seed length. In ACM [4216], pages 1–10. ISBN 1-58113-184-4. LCCN QA76.6 .A13

2000. URL http://www.acm.org/pubs/articles/proceedings/stoc/335305/p1-impagliazzo/p1-impagliazzo.pdf; http://www.acm.org/pubs/citations/proceedings/stoc/335305/p1-impagliazzo/. ACM order number 508000.

Indyk:2000:SDP

[2520] P. Indyk. Stable distributions, pseudorandom generators, embeddings and data stream computation. In IEEE [4219], pages 189–197. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society Order Number PR00850.

Iwata:2000:PAF

[2521] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In NIST [4221], page 9. ISBN ???? LCCN ???? URL http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf; http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf.

Jennewein:2000:FCQ

[2522] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000. CODEN RSINAK. ISSN 1089-7623, 0034-6748. URL http://link.aip.org/link/?RSI/71/1675/1.

Johansson:2000:FCA

[2523] Thomas Johansson and Fredrik Jönsson. Fast correlation attacks through reconstruction of linear polynomials. In Mihir Bellare, editor, *Advances in Cryptology — CRYPTO 2000: 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000. Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 300–315. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. URL https://link.springer.com/content/pdf/10.1007/3-540-44598-6_19.

Juels:2000:HTL

[2524] A. Juels, M. Jakobsson, E. Shriver, and B. K. Hillyer. How to turn loaded dice into fair coins. *IEEE Transactions on Information Theory*,

46(3):911–921, ???? 2000. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Kabal:2000:GGP

[2525] Peter Kabal. Generating Gaussian pseudo-random deviates. Report, Department of Electrical and Computer Engineering, McGill University, Montréal, QC, Canada, 2000. URL `http://www-mmsp.ece.mcgill.ca/documents/reports/2000/kabalr2000c.pdf`.

Kelsey:2000:YND

[2526] John Kelsey, Bruce Schneier, and Niels Ferguson. Yarrow-160: Notes on the design and analysis of the Yarrow cryptographic pseudorandom number generator. In Heys and Adams [4218], pages 13–33. ISBN 3-540-67185-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1758. URL `http://www.counterpane.com/yarrow-notes.html`; `http://www.schneier.com/paper-yarrow.html`.

Knuth:2000:SPA

[2527] Donald E. Knuth. *Selected Papers on Analysis of Algorithms*, volume 102 of *CSLI Lecture Notes*. CSLI Publications, Stanford, CA, USA, 2000. ISBN 1-57586-212-3 (paperback), 1-57586-211-5 (hardcover). xvi + 621 pp. LCCN QA9.58 .K65 2000.

Law:2000:SMA

[2528] Averill M. Law and W. David Kelton. *Simulation modeling and analysis*. McGraw-Hill series in industrial engineering and management science. McGraw-Hill, New York, NY, USA, third edition, 2000. ISBN 0-07-059292-6. xxi + 760 pp. LCCN QA76.9.C65 L38 2000. URL `http://www.loc.gov/catdir/bios/mh041/99052146.html`; `http://www.loc.gov/catdir/description/mh023/99052146.html`; `http://www.loc.gov/catdir/toc/mh023/99052146.html`.

LEcuyer:2000:CPS

[2529] Pierre L'Écuyer, Jean-François Cordeau, and Richard Simard. Close-point spatial tests and their application to random number generators. *Operations Research*, 48(2):308–317, March/April 2000. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://www.jstor.org/stable/223147`.

LEcuyer:2000:FCM

[2530] Pierre L'Ecuyer and R. Touzin. Fast combined multiple recursive generators with multipliers of the form $a = \pm 2^q \pm 2^r$. In Joines et al. [4220],

pages 683–689. ISBN 0-7803-6579-8 (softcover), 0-7803-6580-1 (casebound), 0-7803-6581-X (microfiche). LCCN QA76.9.C65 W568 2000. IEEE Catalog Number 00CH37165.

LEcuyer:2000:NCL

[2531] P. L'Ecuyer and F. Panneton. A new class of linear feedback shift register generators. In Joines et al. [4220], pages 690–696. ISBN 0-7803-6579-8 (softcover), 0-7803-6580-1 (casebound), 0-7803-6581-X (microfiche). LCCN QA76.9.C65 W568 2000. IEEE Catalog Number 00CH37165.

LEcuyer:2000:VRL

[2532] Pierre L'Ecuyer and Christiane Lemieux. Variance reduction via lattice rules. *Management Science*, 46(9):1214–1235, ???? 2000. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Lemieux:2000:CMC

[2533] Christiane Lemieux and Pierre L'Ecuyer. A comparison of Monte Carlo, lattice rules and other low-discrepancy point sets. In *Monte Carlo and quasi-Monte Carlo methods 1998 (Claremont, CA)*, pages 326–340. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000.

Lepley:2000:HST

[2534] J. J. Lepley, J. G. Ellison, and A. S. Siddiqui. High-speed true random bit sequence generator. *Electronics Letters*, 36(17):1480–1481, August 17, 2000. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=865050`.

Leydold:2000:ASR

[2535] Josef Leydold. Automatic sampling with the ratio-of-uniforms method. *ACM Transactions on Mathematical Software*, 26(1):78–98, March 2000. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/347837.347863`; `http://www.acm.org/pubs/citations/journals/toms/2000-26-1/p78-leydold/`; `http://www.acm.org/pubs/citations/journals/toms/2000-26-1/p78-leydold/p78-leydold.pdf`.

Mansharamani:2000:RTG

[2536] Rajesh Mansharamani, Prasad Kallepalli, Harsha Veerabhadraiah, and Benny Mathew. RVGEN: a tool for generation of random variates. *Software — Concepts and Tools*, 19(4):161–167, October 2000. CODEN

SCOTE5. ISSN 0945-8115 (print), 1432-2188 (electronic). URL `https://link.springer.com/article/10.1007/s003789900002`.

Marsaglia:2000:ADS

[2537] J. C. Marsaglia and G. Marsaglia. The Anderson–Darling–Savage goddess-of-fit test. Unpublished. See [102, 175]., 2000.

Marsaglia:2000:MRN

[2538] George Marsaglia. The monster, a random number generator with period over 10^{2857} times as long as the previously touted longest-period one. Technical report ????, Florida State University, Tallahassee, FL, USA, ???? 2000.

Marsaglia:2000:SMG

[2539] George Marsaglia and Wai Wan Tsang. A simple method for generating gamma variables. *ACM Transactions on Mathematical Software*, 26(3): 363–372, September 2000. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Marsaglia:2000:ZMG

[2540] George Marsaglia and Wai Wan Tsang. The ziggurat method for generating random variables. *Journal of Statistical Software*, 5(8): 1–7, 2000. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v05/i08`; `http://www.jstatsoft.org/v05/i08/rnorrexp.c`; `http://www.jstatsoft.org/v05/i08/updates`; `http://www.jstatsoft.org/v05/i08/ziggurat.pdf`. See [2954, 3056].

Mascagni:2000:ASS

[2541] Michael Mascagni and Ashok Srinivasan. Algorithm 806: SPRNG: a scalable library for pseudorandom number generation. *ACM Transactions on Mathematical Software*, 26(3):436–461, September 2000. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/358407.358427`. See correction [2542].

Mascagni:2000:CAS

[2542] Michael Mascagni and Ashok Srinivasan. Corrigendum: Algorithm 806: SPRNG: a scalable library for pseudorandom number generation. *ACM Transactions on Mathematical Software*, 26(4):618–619, December 2000. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/365723.365738`. See [2541].

Mauduit:2000:FPBa

[2543] Christian Mauduit and András Sárközy. On finite pseudorandom binary sequences, V. On $(n\alpha)$ and $(n^2\alpha)$ sequences. *Monatshefte für Mathematik*, 129(3):197–216, March 2000. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/4r6x9bxdvhfgc4vk/`. See improved result in [2741].

Mauduit:2000:FPBb

[2544] Christian Mauduit and András Sárközy. On finite pseudorandom binary sequences, VI, (on $(n^k\alpha)$ sequences). *Monatshefte für Mathematik*, 130(4):281–298, September 2000. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/1d1x140wbj6qygqf/`.

Miles:2000:L

[2545] Wyman Eric Miles. LPRng. *Sys Admin: The Journal for UNIX Systems Administrators*, 9(6):8, 10, 12, 14, 16, 18, 22, June 2000. CODEN SYADE7. ISSN 1061-2688. URL `http://www.samag.com/`.

Moriai:2000:PTL

[2546] Shiho Moriai and Serge Vaudenay. On the pseudorandomness of top-level schemes of block ciphers. *Lecture Notes in Computer Science*, 1976:289–??, 2000. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/1976/19760289.htm; http://link.springer-ny.com/link/service/series/0558/papers/1976/19760289.pdf`.

Niederreiter:2000:DPN

[2547] H. Niederreiter and I. E. Shparlinski. On the distribution of pseudorandom numbers and vectors generated by inversive methods. *Applicable algebra in engineering, communication and computing*, 10(??):189–202, ???? 2000. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

Niederreiter:2000:ESD

[2548] Harald Niederreiter and Igor E. Shparlinski. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. *Acta Arithmetica*, 92(1):89–98, 2000. CODEN AARIA9. ISSN 0065-1036 (print), 1730-6264 (electronic).

Niederreiter:2000:IES

[2549] H. Niederreiter and A. Winterhof. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. *Finite Fields and their Applications*, 93(??):387–399, ???? 2000. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic).

Nishimura:2000:TBM

[2550] Takuji Nishimura. Tables of 64-bit Mersenne twisters. *ACM Transactions on Modeling and Computer Simulation*, 10(4):348–357, October 2000. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

NIST:2000:RNG

[2551] NIST. Random number generation and testing. World-Wide Web site., 2000. URL `http://csrc.nist.gov/rng/`.

Panneton:2000:GNA

[2552] François Panneton. Générateurs de nombres aléatoires utilisant des récurrences linéaires modulo 2. (French) [random-number generators using linear recurrences modulo 2]. Thèse (M.Sc.), Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2000. xiii + 179 pp. Mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de Maître ès sciences (M.Sc.) en informatique option recherche opérationnelle.

Petrie:2000:NBI

[2553] C. Petrie and J. Connelly. A noise-based IC random number generator for applications in cryptography. *IEEE Journal of Solid-State Circuits*, 47(5):615–621, ???? 2000. CODEN IJSCBC. ISSN 0018-9200 (print), 1558-173X (electronic).

Proykova:2000:HIR

[2554] Ana Proykova. How to improve a random number generator. *Computer Physics Communications*, 124(2–3):125–131, February 2000. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465599004348`.

RSA:2000:PKC

[2555] RSA. Public-key cryptography standards. World-Wide Web site., 2000. URL `http://www.rsasecurity.com/rsalabs/pkcs/`.

Saitoh:2000:DPR

[2556] Naoko Saitoh and Hiroaki Yoshida. q-deformed Poisson random variables on q-Fock space. *Journal of Mathematical Physics*, 41(8):5767–5772, August 2000. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Sasaki:2000:SCB

[2557] T. Sasaki, H. Togo, J. Tanida, and Y. Ichioka. Stream cipher based on pseudorandom number generation with optical affine transformation. *Applied Optics*, 39(14):2340–2346, May 10, 2000. CODEN APOPAI. ISSN 0003-6935.

Saucier:2000:CGS

[2558] Richard Saucier. Computer generation of statistical distributions. Report ARL-TR-2168, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, USA, March 2000. x + 105 pp. URL `http://ftp.arl.mil/random/random.pdf`.

Savas:2000:MMI

[2559] E. Savas and Ç. K. Koç. The Montgomery modular inverse—revisited. *IEEE Transactions on Computers*, 49(7):763–766, July 2000. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=863048`.

Schwab:2000:MSC

[2560] Matthias Schwab, Martin Karrenbach, and Jon Claerbout. Making scientific computations reproducible. *Computing in Science and Engineering*, 2(6):61–67, November/December 2000. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic). URL `http://dlib.computer.org/cs/books/cs2000/pdf/c6061.pdf`.

Soto:2000:RTA

[2561] Juan Soto and Lawrence Bassham. Randomness testing of the Advanced Encryption Standard finalist candidates. NIST internal report 6483, National Institute for Standards and Technology, Gaithersburg, MD, USA, April 2000. URL `http://csrc.nist.gov/rng/aes-report-final.doc`.

Stefanescu:2000:GUR

[2562] Stefan V. Stefanescu. Generating uniform random points inside a cone. *Monte Carlo Methods and Applications*, 6(2):115–130, ???? 2000. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2000.6.issue-2/mcma.2000.6.2.115/mcma.2000.6.2.115.xml`.

Stefanov:2000:OQR

[2563] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47 (4):595–598, ???? 2000. CODEN JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic).

Sugita:2000:RWS

[2564] Hiroshi Sugita and Satoshi Takanobu. Random Weyl sampling for robust numerical integration of complicated functions. *Monte Carlo Methods and Applications*, 6(1):27–48, January 2000. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2000.6.issue-1/mcma.2000.6.1.27/mcma.2000.6.1.27.xml`.

Takashima:2000:HPR

[2565] K. Takashima. Hybrid pseudo-random number generation. *Monte Carlo Methods and Applications*, 6(1):49–59, ???? 2000. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2000.6.issue-1/mcma.2000.6.1.49/mcma.2000.6.1.49.xml`.

Tomassini:2000:GHQ

[2566] M. Tomassini, M. Sipper, and M. Perrenoud. On the generation of high-quality random numbers by two-dimensional cellular automata. *IEEE Transactions on Computers*, 49(10):1146–1151, October 2000. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=888056`.

Viswanath:2000:RFS

[2567] Divakar Viswanath. Random Fibonacci sequences and the number 1.13198824 . . . . *Mathematics of Computation*, 69(231):1131–1155, July 2000. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journal-getitem?pii=S0025-5718-99-01145-X`; `http://www.ams.org/mcom/2000-69-231/S0025-5718-99-01145-X/S0025-5718-99-01145-X.dvi`; `http://www.ams.org/mcom/2000-69-231/S0025-5718-99-01145-X/S0025-5718-99-01145-X.pdf`; `http://www.ams.org/mcom/2000-69-231/S0025-5718-99-01145-X/S0025-5718-99-01145-X.ps`; `http://www.ams.org/mcom/2000-69-231/S0025-5718-99-01145-X/S0025-5718-99-01145-X.tex`.

Wikramaratna:2000:PRN

[2568] Roy S. Wikramaratna. Pseudo-random number generation for parallel processing — a splitting approach. *SIAM News*, 33(9):??, ???? 2000. CODEN ???? ISSN 0036-1437.

Yaguchi:2000:RHR

[2569] Hirotake Yaguchi. Randomness of Horner's rule and a new method of generating random numbers. *Monte Carlo Methods and Applications*, 6 (1):61–76, ???? 2000. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2000.6.issue-1/mcma.2000.6.1.61/mcma.2000.6.1.61.xml`.

Zhukov:2000:ANA

[2570] Yu. V. Zhukov. On the accuracy of normal approximation for the densities of sums of independent identically distributed random variables. *Theory of Probability and its Applications*, 44(4):785–793, December 2000. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/97794`.

Ackermann:2001:PRN

[2571] J. Ackermann, U. Tangen, B. Bödekker, J. Breyer, E. Stoll, and J. S. McCaskill. Parallel random number generator for inexpensive configurable hardware cells. *Computer Physics Communications*, 140(3): 293–302, November 1, 2001. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465501002429`.

Agrawal:2001:CDF

[2572] Mani K. Agrawal and Salah E. Elmaghraby. On computing the distribution function of the sum of independent random variables. *Computers and Operations Research*, 28(5):473–483, April 2001. CODEN CMORAP. ISSN 0305-0548 (print), 1873-765X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0305054899001331`.

Agrawal:2001:HSP

[2573] Manindra Agrawal. Hard sets and pseudo-random generators for constant depth circuits. *Lecture Notes in Computer Science*, 2245:58–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2245/22450058.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2245/22450058.pdf`.

Alexander:2001:AMC

[2574] S. A. Alexander and R. L. Coldwell. Atomic and molecular calculations using quasirandom numbers. *Journal of Computational Physics*, 172 (2):908–916, September 20, 2001. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999101968652`.

AlOsh:2001:SAG

[2575] M. A. Al Osh and S. J. Lee. A simple approach for generating correlated binary variates. *Journal of Statistical Computation and Simulation*, 70 (3):231–255, ???? 2001. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949650108812119`.

Arvind:2001:PRB

[2576] V. Arvind and Johannes Köbler. On pseudorandomness and resource-bounded measure. *Theoretical Computer Science*, 255(1–2):205–221, March 28, 2001. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.nl../31/abstract.html; http://www.elsevier.nl/gej-ng/10/41/16/197/21/31/article.pdf`.

Bailey:2001:RCF

[2577] David H. Bailey and Richard E. Crandall. On the random character of fundamental constant expansions. *Experimental Mathematics*, 10(2): 175–190, ???? 2001. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL `http://projecteuclid.org/euclid.em/999188630`.

Banks:2001:DES

[2578] Jerry Banks, John S. Carson, Barry L. Nelson, and David M. Nicol. *Discrete-Event System Simulation*. Prentice-Hall international series in industrial and systems engineering. Prentice-Hall, Upper Saddle River, NJ, USA, third edition, 2001. ISBN 0-13-088702-1. xiv + 594 pp. LCCN T57.62. B35 2000.

Barker:2001:SPE

[2579] Lawrence Barker, Henry Rolka, Deborah Rolka, and Cedric Brown. Statistical practice — equivalence testing for binomial random variables: Which test to use? *The American Statistician*, 55(4):279–287, 2001. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Battaglia:2001:GAP

[2580] Francesco Battaglia. Genetic algorithms, pseudo-random numbers generators, and Markov chain Monte Carlo methods. *Metron*, 59(1–2):131–

155, ???? 2001. CODEN MRONAM. ISSN 0026-1424 (print), 2281-695X (electronic).

Batu:2001:TRV

[2581] T. Batu, E. Fischer, L. Fortnow, R. Kumar, R. Rubinfeld, and P. White. Testing random variables for independence and identity. In IEEE [4223], pages 442–451. CODEN ASFPDV. ISBN 0-7695-1390-5, 0-7695-1391-3 (case), 0-7695-1392-1 (microfiche). ISSN 0272-5428. LCCN TK7885 .I61 2001. IEEE Computer Society order number PR01390.

Chamayou:2001:PRN

[2582] J.-F. Chamayou. Pseudo random numbers for the Landau and Vavilov distributions. *Computational Statistics*, 16(1):131–152, March 2001. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `http://link.springer.com/article/10.1007/s001800100055`.

Chen:2001:ING

[2583] Huifen Chen. Initialization for NORTA: Generation of random vectors with specified marginals and correlations. *INFORMS Journal on Computing*, 13(4):312–331, Fall 2001. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Chick:2001:NPS

[2584] Stephen E. Chick and Koichiro Inoue. New procedures to select the best simulated system using Common Random Numbers. *Management Science*, 47(8):1133–1149, August 2001. CODEN MSCIAM. ISSN 0025-1909 (print), 1526-5501 (electronic).

Chowdhury:2001:ESI

[2585] Sandeepan Chowdhury and Subhamoy Maitra. Efficient software implementation of linear feedback shift registers. *Lecture Notes in Computer Science*, 2247:297–307, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470297.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2247/22470297.pdf`.

Coffman:2001:TPS

[2586] E. G. Coffman, Jr. and Predrag Jelenković. Threshold policies for single-resource reservation systems. *ACM SIGMETRICS Performance Evaluation Review*, 28(4):9–10, March 2001. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Crandall:2001:PNC

[2587] Richard Crandall and Carl Pomerance. *Prime Numbers: a Computational Perspective*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. ISBN 0-387-94777-9. xv + 545 pp. LCCN QA246 .C74 2001.

Cryan:2001:PGN

[2588] Mary Cryan and Peter Bro Miltersen. On pseudorandom generators in NC. *Lecture Notes in Computer Science*, 2136:272–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2136/21360272.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2136/21360272.pdf`.

Entacher:2001:EOR

[2589] Karl Entacher, Thomas Schell, and Andreas Uhl. Evolutionary optimization of random number generators. In Schuëller and Spanos [4226], pages 19–26. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Entacher:2001:ORN

[2590] Karl Entacher, Thomas Schell, and Andreas Uhl. Optimization of random number generators: efficient search for high-quality LCGs. *Probabilistic Engineering Mechanics*, 16(4):289–293, October 2001. CODEN PEMEEX. ISSN 0266-8920 (print), 1878-4275 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0266892001000212`.

Entacher:2001:PQ

[2591] K. Entacher and Th. Schell. From 'pseudo' to 'quasi'. In Schuëller and Spanos [4226], pages 27–34. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Faure:2001:VS

[2592] Henri Faure. Variations on $(0, s)$-sequences. *Journal of Complexity*, 17(4):741–753, December 2001. CODEN JOCOEH. ISSN 0885-064X (print), 1090-2708 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0885064X01905904`.

Fernandez:2001:RCA

[2593] Julio F. Fernández and Carlos Criado. Reply to "Comment on 'Algorithm for normal random numbers'". *Physical Review E (Statistical physics,*

plasmas, fluids, and related interdisciplinary topics), 63:058702, April 2001. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.63.058702`. See [2440, 2646].

Fischer:2001:CLT

[2594] Hans Fischer. The Central Limit Theorem from Laplace to Cauchy: Changes in stochastic objectives and in analytical methods. Report, Katholische Universität Eichstätt, D-85071 Eichstätt, Germany, October 2001. ii + 34 pp. URL `http://mathsrv.ku-eichstaett.de/MGF/homes/didmath/seite/1850.pdf`. The URL contains a concise English version of the first 2 chapters of this book on the history of the central limit theorem, however with a partially new interpretation of the Cauchy–Bienaymé-controversy.

Fischer:2001:TRN

[2595] V. Fischer and M. Drutarovsky. True random number generator embedded in reconfigurable hardware. In Koç and Paar [4224], pages 415–430. CODEN LNCSD9. ISBN 3-540-41455-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C454 2000. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1965.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1965`.

Fluhrer:2001:SAA

[2596] Scott R. Fluhrer and David A. McGrew. Statistical analysis of the alleged RC4 keystream generator. In Gerhard Goos, Juris Hartmanis, Jan Leeuwen, and Bruce Schneier, editors, *Fast Software Encryption: 7th International Workshop, FSE 2000, New York, NY, USA, April 10–12, 2000. Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 19–30. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `https://link.springer.com/content/pdf/10.1007/3-540-44706-7_2.pdf`.

Folegati:2001:CLR

[2597] Katia Folegati and Roberto Segala. Coin lemmas with random variables. *Lecture Notes in Computer Science*, 2165:71–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2165/21650071.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2165/21650071.pdf`.

Gerosa:2001:FIB

[2598] A. Gerosa, R. Bernardini, and S. Pietri. A fully integrated 8-bit, 20MHz, truly random numbers generator, based on a chaotic system. In IEEE, editor, *SSMSD 2001 Southwest Symposium on Mixed-Signal Design, 25–27 February, 2001, Austin, Texas, USA*, pages 87–92. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. ISBN 0-7803-6742-1. LCCN TK7874.75 .S65 2001.

Golic:2001:CAS

[2599] Jovan Dj. Golić. Correlation analysis of the shrinking generator. In Joe Kilian, editor, *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 440–457. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. URL `https://iacr.org/archive/crypto2001/21390439.pdf`.

Gonsalves:2001:PAS

[2600] Richard J. Gonsalves. Pivot algorithm for self-avoiding walks on a square lattice. Fortran program, 2001. URL `http://www.physics.buffalo.edu/gonsalves/phy411-506_spring01/Files/Chapter12/saw.f`. The program contains code (near the end) for the portable `rannyu()` generator. It is a linear congruential generator with multiplier $A = 31,167,285 = 0x1db9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.

Guimond:2001:CRN

[2601] Louis-Sébastian Guimond, Jiří Patera, and Jan Patera. Combining random number generators using cut and project sequences. *Czechoslovak Journal of Physics*, 51(4):305–311, April 2001. CODEN CZYPAO. ISSN 0011-4626 (print), 1572-9486 (electronic). URL `http://link.springer.com/article/10.1023/A%3A1017533304855`.

Gutierrez:2001:IMP

[2602] J. Gutierrez and D. Gomez-Perez. Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. *Lecture Notes in Computer Science*, 2227:192–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2227/22270192.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2227/22270192.pdf`.

Gutmann:2001:RNG

[2603] Peter Gutmann. Random number generation. In *????*, chapter 6, pages 155–193. ????, ????, October 2001. ISBN ???? LCCN ???? URL `http://www.cypherpunks.to/~peter/06_random.pdf`.

Haastad:2001:PCA

[2604] Johan Håstad and Mats Näslund. Practical construction and analysis of pseudo-randomness primitives. *Lecture Notes in Computer Science*, 2248: 442–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2248/22480442.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2248/22480442.pdf`.

Hernandez:2001:DTR

[2605] Julio César Hernández, José María Sierra, Arturo Ribagorda, Benjamín Ramos, and J. C. Mex-Perera. Distinguishing TEA from a random permutation: Reduced round versions of TEA do not have the SAC or do not generate random numbers. *Lecture Notes in Computer Science*, 2260:374–377, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://163.117.174.60/downloads/Publicaciones/2001/HernandezSRRM01.pdf`; `http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600374.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2260/22600374.pdf`.

Hernandez:2001:FNO

[2606] J. C. Hernandez, A. Ribagorda, P. Isasi, and J. M. Sierra. Finding near optimal parameters for linear congruential pseudorandom number generators by means of evolutionary computation. In Spector et al. [4228], pages 1292–1298. ISBN 1-55860-774-9. LCCN QA76.623 .G46 2001. URL `http://www.cs.bham.ac.uk/~wbl/biblio/gecco2001/d24.pdf`.

Hernandez:2001:GAC

[2607] J. C. Hernández, A. Ribagorda, P. Isasi, and J. M. Sierra. Genetic algorithms can be used to obtain good linear congruential generators. *Cryptologia*, 25(3):213–229, 2001. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Howgrave-Graham:2001:PRN

[2608] N. Howgrave-Graham, J. Dyer, and R. Gennaro. Pseudo-random number generation on the IBM 4758 Secure Crypto Coprocessor. *Lecture Notes in Computer Science*, 2162:93–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

URL http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620093.htm; http://link.springer-ny.com/link/service/series/0558/papers/2162/21620093.pdf.

Iwata:2001:PAF

[2609] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of the AES finalists — RC6 and Serpent. *Lecture Notes in Computer Science*, 1978: 231–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/1978/19780231.htm; http://link.springer-ny.com/link/service/series/0558/papers/1978/19780231.pdf.

Johnson:2001:CCO

[2610] George Johnson. Connoisseurs of chaos offer a valuable product: Randomness. *New York Times*, ??(??):??, June 12, 2001. CODEN NYTIAO. ISSN 0362-4331 (print), 1542-667X, 1553-8095. URL http://www.fourmilab.ch/hotbits; http://www.nytimes.com; http://www.random.org/. Section F; Column 3; Science Desk; Pg. 1.

Kang:2001:PMT

[2611] Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. *Lecture Notes in Computer Science*, 2119:60–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2119/21190060.htm; http://link.springer-ny.com/link/service/series/0558/papers/2119/21190060.pdf.

Killmann:2001:AFC

[2612] W. Killmann and W. Schindler. AIS 31: Functionality classes and evaluation methodology for true (physical) random number generators. Report, Bundesamt fur Sicherheit in der Informationstechnik (BSI), Postfach 20 03 63, 53133 Bonn, Germany, September 9, 2001. Version 3.1.

Krause:2001:MHC

[2613] Matthias Krause and Stefan Lucks. On the minimal hardware complexity of pseudorandom function generators (extended abstract). *Lecture Notes in Computer Science*, 2010:419–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2010/20100419.htm; http://link.springer-ny.com/link/service/series/0558/papers/2010/20100419.pdf.

Kuang:2001:CSA

[2614] Lei Kuang and Armand M. Makowski. Convex stability and asymptotic convex ordering for non-stationary arrival processes. *ACM SIGMETRICS Performance Evaluation Review*, 28(4):22–23, March 2001. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

LEcuyer:2001:CQR

[2615] Pierre L'Ecuyer and Christiane Lemieux. On the choice of quasi-random point sets with a lattice structure. In Schuëller and Spanos [4226], pages 11–17. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

LEcuyer:2001:PBS

[2616] Pierre L'Ecuyer and Richard Simard. On the performance of birthday spacings tests with certain families of random number generators. *Mathematics and Computers in Simulation*, 55(1–3):131–137, February 15, 2001. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475400002536`.

LEcuyer:2001:RN

[2617] P. L'Ecuyer. Random numbers. In Smelser and Baltes [4227], pages 12734–12738. ISBN 0-08-043076-7 (set). LCCN H41 .I58 2001. URL `http://www.sciencedirect.com/science/article/pii/B0080430767004939`.

LEcuyer:2001:RNG

[2618] Pierre L'Ecuyer. Random number generators. In Gass and Harris [4222], pages 695–702. ISBN 0-7923-7827-X. LCCN T57.6. E53 2000. URL `http://www.loc.gov/catdir/enhancements/fy1004/00025363-d.htm`.

LEcuyer:2001:SUR

[2619] Pierre L'Ecuyer. Software for uniform random number generation: Distinguishing the good and the bad. In Peters et al. [4225], pages 95–105. ISBN 0-7803-7307-3 (paperback), 0-7803-7308-1 (microfiche), 0-7803-7309-X. LCCN QA76.5 .W56 2001. IEEE catalog number 01CH37304.

LEcuyer:2001:TSL

[2620] Pierre L'Ecuyer and Richard Simard. *TestU01: a Software Library in ANSI C for Empirical Testing of Random Number Generators, Software*

User's Guide. Département d'Informatique et Recherche opérationnelle, Université de Montréal, Montréal, Québec, Canada, 2001. URL `http://www.iro.umontreal.ca/~simardr/TestU01.zip`.

Lee:2001:PBG

[2621] Eonkyung Lee, Sang Jin Lee, and Sang Geun Hahn. Pseudorandomness from braid groups. *Lecture Notes in Computer Science*, 2139:486–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2139/21390486.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2139/21390486.pdf`.

Lemieux:2001:SCL

[2622] Christiane Lemieux and Pierre L'Ecuyer. On selection criteria for lattice rules and other quasi-Monte Carlo point sets. *Mathematics and Computers in Simulation*, 55(1–3):139–148, February 15, 2001. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475400002548`. The Second IMACS Seminar on Monte Carlo Methods (Varna, 1999).

Lenczewski:2001:FRV

[2623] Romuald Lenczewski. Filtered random variables, bialgebras, and convolutions. *Journal of Mathematical Physics*, 42(12):5876–5903, December 2001. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.

Levin:2001:SIC

[2624] Mordechay B. Levin. On the statistical independence of compound pseudorandom numbers over part of the period. *ACM Transactions on Modeling and Computer Simulation*, 11(3):294–311, July 2001. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Leydold:2001:SUG

[2625] Josef Leydold. A simple universal generator for continuous and discrete univariate T-concave distributions. *ACM Transactions on Mathematical Software*, 27(1):66–82, March 2001. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Leydold:2001:UAA

[2626] Josef Leydold and Wolfgang Hörmann. Universal algorithms as an alternative for generating non-uniform continuous random variates. In

Schuëller and Spanos [4226], pages 177–183. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. URL http://epub.wu.ac.at/844/1/document.pdf; http://epub.wu.ac.at/id/eprint/844. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Li:2001:SPD

[2627] Shujun Li, Qi Li, Wenmin Li, Xuanqin Mou, and Yuanlong Cai. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. *Lecture Notes in Computer Science*, 2260:205–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2260/22600205.htm; http://link.springer-ny.com/link/service/series/0558/papers/2260/22600205.pdf.

Liang:2001:NET

[2628] Yufeng Liang and P. A. Whitlock. A new empirical test for parallel pseudo-random number generators. *Mathematics and Computers in Simulation*, 55(1–3):149 158, February 15, 2001. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL http://www.sciencedirect.com/science/article/pii/S037847540000255X.

Liang:2001:TMU

[2629] Jia-Juan Liang, Kai-Tai Fang, Fred J. Hickernell, and Runze Li. Testing multivariate uniformity and its applications. *Mathematics of Computation*, 70(233):337–355, January 2001. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-00-01203-5; http://www.ams.org/mcom/2001-70-233/S0025-5718-00-01203-5/S0025-5718-00-01203-5.dvi; http://www.ams.org/mcom/2001-70-233/S0025-5718-00-01203-5/S0025-5718-00-01203-5.pdf; http://www.ams.org/mcom/2001-70-233/S0025-5718-00-01203-5/S0025-5718-00-01203-5.ps; http://www.ams.org/mcom/2001-70-233/S0025-5718-00-01203-5/S0025-5718-00-01203-5.tex.

Litvak:2001:SPE

[2630] Nelly Litvak. Some peculiarities of exponential random variables. *Journal of Applied Probability*, 38(3):787–792, September 2001. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL http://www.jstor.org/stable/3216132.

Mantin:2001:PAB

[2631] Itsik Mantin and Adi Shamir. A practical attack on broadcast RC4. In ????, editor, *FSE '01: Revised Papers from the 8th International Workshop on Fast Software Encryption*, volume ???? of *Lecture Notes in Computer Science*, pages 152–164. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001.

Mascagni:2001:PIC

[2632] M. Mascagni and S. Rahimi. Parallel inversive congruential generators: Software and field-programmable gate array implementations. In Schuëller and Spanos [4226], pages 35–39. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Moler:2001:CCN

[2633] Cleve B. Moler. Cleve's corner: Normal behavior: Ziggurat algorithm generates normally distributed random numbers. Technical note, The MathWorks, Inc., 3 Apple Hill Drive, Natick, MA 01760-2098, USA, Spring 2001. 1 pp. URL `http://www.mathworks.com/company/newsletter/clevescorner/spring01_cleve.shtml`.

Myers:2001:EAS

[2634] Steven Myers. Efficient amplification of the security of weak pseudorandom function generators. *Lecture Notes in Computer Science*, 2045: 358–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2045/20450358.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2045/20450358.pdf`.

Nelsen:2001:BRB

[2635] Roger Nelsen. Book review: *Probability and Random Variables: a Beginner's Guide*. *The American Statistician*, 55(1):82–83, February 2001. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.jstor.org/stable/2685536`.

Nelsen:2001:PRV

[2636] Roger Nelsen. Probability and random variables: a beginner's guide. *The American Statistician*, 55(1):82–??, February 2001. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Niederreiter:2001:DAN

[2637] H. Niederreiter. Design and analysis of nonlinear pseudorandom number generators. In Schuëller and Spanos [4226], pages 3–9. ISBN 90-5809-

188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Niederreiter:2001:DCI

[2638] Harald Niederreiter and Arne Winterhof. On the distribution of compound inversive congruential pseudorandom numbers. *Monatshefte für Mathematik*, 132(1):35–48, April 2001. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Niederreiter:2001:DIC

[2639] Harald Niederreiter and Igor E. Shparlinski. On the distribution of inversive congruential pseudorandom numbers in parts of the period. *Mathematics of Computation*, 70(236):1569–1574, October 2001. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journal-getitem?pii=S0025-5718-00-01273-4`; `http://www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-4/S0025-5718-00-01273-4.dvi`; `http://www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-4/S0025-5718-00-01273-4.pdf`; `http://www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-4/S0025-5718-00-01273-4.ps`; `http://www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-4/S0025-5718-00-01273-4.tex`; `http://www.jstor.org/stable/pdfplus/2698742.pdf`.

Niederreiter:2001:NCI

[2640] Harald Niederreiter and Arne Winterhof. On a new class of inversive pseudorandom numbers for parallelized simulation methods. *Periodica Mathematica Hungarica*, 42(1–2):77–87, 2001. CODEN PMHGAW. ISSN 0031-5303 (print), 1588-2829 (electronic).

NIST:2001:BST

[2641] NIST. *Batteries of Statistical Tests for Random Number Generators*. National Institute for Standards and Technology, Gaithersburg, MD, USA, 2001. URL `http://csrc.nist.gov/rng/rng6_3.html`. World-Wide Web site.

NIST:2001:SRC

[2642] NIST. Security requirements for cryptographic modules. Federal Information Processing Standards Publication FIPS PUB 140-2, National Institute for Standards and Technology, Gaithersburg, MD, USA, May 25, 2001.

Noll:2001:HGL

[2643] Landon Curt Noll, Simon Cooper, and Mel Pleasant. How good is LavaRnd? Web site, 2001. URL http://www.lavarnd.org/what/nist-test.html.

Peebles:2001:PRV

[2644] Peyton Z. Peebles. *Probability, random variables, and random signal principles*. McGraw-Hill series in electrical and computer engineering. McGraw-Hill, New York, NY, USA, fourth edition, 2001. ISBN 0-07-366007-8. xviii + 462 pp. LCCN TA340 .P43 2001. URL ftp://uiarchive.cso.uiuc.edu/pub/etext/gutenberg/; http://www.loc.gov/catdir/description/mh021/00034881.html; http://www.loc.gov/catdir/toc/mh021/00034881.html.

Peterson:2001:PMM

[2645] Ivars Peterson. Pi à la mode: Mathematicians tackled the seeming randomness of pi's digits. *Science News (Washington, DC)*, 160(9):136–137, September 1, 2001. CODEN SCNEBK. ISSN 0036-8423 (print), 1943-0930 (electronic). URL http://www.jstor.org/stable/4012633.

Probert:2001:CAN

[2646] M. I. J. Probert. Comment on "Algorithm for normal random numbers". *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 63:058701, April 2001. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.63.058701. See [2440] and reply [2593].

RAND:2001:MRD

[2647] RAND Corporation. *A Million Random Digits With 100,000 Normal Deviates*. RAND Corporation, Santa Monica, CA, USA, 2001. ISBN 0-8330-3047-7. xxv + 400 + 200 pp. LCCN QA276.25 .M55 2001. URL http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/digits.txt.zip; http://www.rand.org/pubs/monograph_reports/MR1418.html. See also [148].

Raqab:2001:ELS

[2648] Mohammad M. Raqab and M. Ahsanullah. Estimation of the location and scale parameters of generalized exponential distribution based on order statistics. *Journal of Statistical Computation and Simulation*, 69 (2):109–123, 2001. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Rukhin:2001:STS

[2649] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. *A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute for Standards and Technology, Gaithersburg, MD, USA, April 2001. xi + 153 pp. URL `http://csrc.nist.gov/rng/rng2.html`; `http://csrc.nist.gov/rng/SP800-22b.pdf`; `http://csrc.nist.gov/rng/sts-1.5.tar`; `http://csrc.nist.gov/rng/sts.data.tar`; `http://csrc.nist.gov/rng/StsGui.zip`; `http://www.cs.sunysb.edu/~algorith/implement/rng/distrib/SP800-22b.pdf`; `http://www.dtic.mil/dtic/tr/fulltext/u2/a393366.pdf`. NIST Special Publication 800-22, with revisions dated May 15, 2001.

Rukhin:2001:TRS

[2650] A. L. Rukhin. Testing randomness: a suite of statistical procedures. *Theory of Probability and its Applications*, 45(1):111–132, March 2001. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/97808`.

Schindler:2001:EOT

[2651] W. Schindler. Efficient online tests for true random number generators. *Lecture Notes in Computer Science*, 2162:103–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2162/21620103.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2162/21620103.pdf`.

Shackleford:2001:FIN

[2652] Barry Shackleford, Motoo Tanaka, Richard J. Carter, and Greg Snider. FPGA implementation of neighborhood-of-four cellular automata random number generators. Technical report ??, HP Labs, ????, 2001.

Shaltiel:2001:SEA

[2653] Ronen Shaltiel and Christopher Umans. Simple extractors for all min-entropies and a new pseudo-random generator. In IEEE [4223], pages 648–657. CODEN ASFPDV. ISBN 0-7695-1390-5, 0-7695-1391-3 (case), 0-7695-1392-1 (microfiche). ISSN 0272-5428. LCCN TK7885 .I61 2001. IEEE Computer Society order number PR01390.

Shparlinski:2001:LCN

[2654] Igor E. Shparlinski and Joseph H. Silverman. On the linear complexity of the Naor–Reingold pseudo-random function from elliptic curves.

Designs, Codes, and Cryptography, 24(3):279–289, December 2001. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.wkap.nl/oasis.htm/356536`.

Shujun:2001:PRB

[2655] L. Shujun, M. Xuanqin, and C. Yuanlong. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. *Lecture Notes in Computer Science*, 2247:316–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2247/22470316.htm; http://link.springer-ny.com/link/service/series/0558/papers/2247/22470316.pdf`.

Soubusta:2001:QRN

[2656] Jan Soubusta, Ondrej Haderka, and Martin Hendrych. Quantum random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 4356(1):54–60, 2001. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/4356/54/1`. 12th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics.

Stojanovski:2001:CBRa

[2657] T. Stojanovski and L. Kocarev. Chaos-based random number generators-part I: analysis [cryptography]. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Application*, 48(3):281–288, March 2001. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Stojanovski:2001:CBRb

[2658] T. Stojanovski, J. Pil, and L. Kocarev. Chaos-based random number generators. Part II: practical realization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Application*, 48(3):382–385, March 2001. CODEN ITCAEX. ISSN 1057-7122 (print), 1558-1268 (electronic).

Sudan:2001:PGX

[2659] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *Journal of Computer and System Sciences*, 62(2):236–266, March 2001. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000000917306`.

Swartz:2001:NTR

[2660] Ray Swartz. A new twist on random number generators. *;login: the USENIX Association newsletter*, 26(1):46–48, February 2001. CODEN

LOGNEM. ISSN 1044-6397 (print), 2169-9364 (electronic). URL `http://www.usenix.org/publications/login/2001-02/pdfs/swartz.pdf`.

Talim:2001:CRW

[2661] J. Talim, Z. Liu, Ph. Nain, and E. G. Coffman, Jr. Controlling the robots of Web search engines. *ACM SIGMETRICS Performance Evaluation Review*, 29(1):236–244, June 2001. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Tan:2001:PPR

[2662] Chih Jeng Kenneth Tan. On parallel pseudo-random number generation. *Lecture Notes in Computer Science*, 2073:589–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2073/20730589.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2073/20730589.pdf`.

Tang:2001:SAS

[2663] Hui-Chin Tang. A statistical analysis of the screening measure of multiple recursive random number generators of orders one and two. *Journal of Statistical Computation and Simulation*, 71(4):345–356, ???? 2001. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949650108812153`.

Touzin:2001:GRM

[2664] Renée Touzin. Des générateurs récursifs multiples combinés rapides avec des coefficients de la forme $\pm 2^{p_1} \pm 2^{p_2}$. (French) [Fast combined multiple recursive generators of the form $\pm 2^{p_1} \pm 2^{p_2}$]. Thèse (M.Sc.), Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2001. xiii + 128 pp. Mémoire présenté à la faculté des études supérieures en vue de l'obtention du grade de Maître ès sciences (M.Sc.) en informatique option recherche opérationnelle.

Trevisan:2001:EPG

[2665] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, July 2001. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Tu:2001:NFG

[2666] Shu-Ju Tu. *A new formalism for geometric probability and its applications to physics*. Ph.D. thesis, Purdue University, West Lafayette, IN, 2001. 179 pp.

Vadhan:2001:OP

[2667] Salil P. Vadhan. Order in pseudorandomness. *Lecture Notes in Computer Science*, 2129:10–??, 2001. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2129/21290010.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2129/21290010.pdf`.

Vanura:2001:ARC

[2668] T. Vanura. Algorithm for randomize [sic] choice from random digits. In Schuëller and Spanos [4226], pages 41–45. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Watkins:2001:ERN

[2669] R. K. Watkins, J. C. Isaacs, and S. Y. Foo. Evolvable random number generators: a schemata-based approach. In Spector et al. [4228], pages 469–473. ISBN 1-55860-774-9. LCCN QA76.623 .G46 2001.

Wegenkittl:2001:GTP

[2670] Stefan Wegenkittl. Gambling tests for pseudorandom number generators. *Mathematics and Computers in Simulation*, 55(1–3):281–288, February 15, 2001. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475400002718`.

Wu:2001:RNG

[2671] Pei-Chi Wu. Random number generation with primitive pentanomials. *ACM Transactions on Modeling and Computer Simulation*, 11(4):346–351, October 2001. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Agarwal:2002:FPN

[2672] R. C. Agarwal, R. F. Enenkel, F. G. Gustavson, A. Kothari, and M. Zubair. Fast pseudorandom-number generators with modulus 2^k or 2^{k-1} using fused multiply–add. *IBM Journal of Research and Development*, 46(1):97–116, January 2002. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic). URL `http://www.research.ibm.com/journal/rd/461/agarwal.html`; `http://www.research.ibm.com/journal/rd/461/agarwal.pdf`.

Anonymous:2002:AWG

[2673] Anonymous. *Additive white Gaussian noise (AWGN) core*. Xilinx, Inc., San Jose, CA, USA, October 30, 2002. 5 pp. URL `https://www.xilinx.com/support/documentation/ip_documentation/awgn.pdf`.

Anonymous:2002:EEG

[2674] Anonymous. EGD (Entropy Gathering Daemon). Web site., April 1, 2002. URL `http://everything2.com/title/EGD`.

Bailey:2002:RGN

[2675] David H. Bailey and Richard E. Crandall. Random generators and normal numbers. *Experimental Mathematics*, 11(4):527–546, ???? 2002. CODEN ???? ISSN 1058-6458 (print), 1944-950X (electronic). URL `http://projecteuclid.org/euclid.em/1057864662`.

Binder:2002:MCS

[2676] K. (Kurt) Binder and Dieter W. Heermann. *Monte Carlo simulation in statistical physics: an introduction*, volume 80 of *Springer series in solid-state sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fourth edition, 2002. ISBN 3-540-43221-3. ISSN 0171-1873. xii + 180 pp. LCCN QC174.85.M64 B56 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2003537870-d.html`; `http://www.loc.gov/catdir/enhancements/fy0817/2003537870-t.html`.

Brattka:2002:RNI

[2677] Vasco Brattka. Random numbers and an incomplete immune recursive set. *Lecture Notes in Computer Science*, 2380:950–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2380/23800950.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2380/23800950.pdf`.

Brent:2002:SUN

[2678] Richard P. Brent. Some uniform and normal random number generators, `ranut` version 1.03 (January 2002) and `xorgens` version 2.01 (August 2004). Web site, January 2002. URL `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/random.html`.

Brillhart:2002:FHP

[2679] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$

up to high powers, volume 22 of *Contemporary mathematics*. American Mathematical Society, Providence, RI, USA, third edition, 2002. ISBN ???? ISSN 0271-4132 (print), 1098-3627 (electronic). ???? pp. LCCN QA161.F3 F33 2002.

Cameron:2002:HDM

[2680] Craig W. Cameron, Steven H. Low, and David X. Wei. High-density model for server allocation and placement. *ACM SIGMETRICS Performance Evaluation Review*, 30(1):152–159, June 2002. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Choe:2002:FRT

[2681] Geon Ho Choe and Dong Han Kim. The first return time test of pseudorandom numbers. *Journal of Computational and Applied Mathematics*, 143(2):263–274, June 15, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042701005106`.

Churchhouse:2002:CCJ

[2682] Robert F. Churchhouse. *Codes and Ciphers: Julius Caesar, the Enigma, and the Internet*. Cambridge University Press, Cambridge, UK, 2002. ISBN 0-521-81054-X (hardcover), 0-521-00890-5 (paperback). x + 240 pp. LCCN Z103 .C48 2002. US$55.00 (hardcover), US$20.00 (paperback).

Delfs:2002:ICP

[2683] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*. Information Security and Cryptography. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-642-87126-7 (e-book), 3-642-87128-3. ISSN 1619-7100 (print), 2197-845X (electronic). xiv + 310 pp. LCCN QA76.9.A25. URL `http://www.springerlink.com/content/978-3-642-87126-9`.

DeMatteis:2002:PP

[2684] A. De Matteis and S. Pagnutti. Pseudorandom permutation. *Journal of Computational and Applied Mathematics*, 142(2):367–375, May 15, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042701004253`.

Deng:2002:DSI

[2685] L.-Y. Deng and H. Xu. Design, search, and implementation of high-dimensional, efficient, long-cycle, and portable uniform random variate

generator. Preprint 327, Department of Statistics, University of California at Los Angeles, Los Angeles, CA, USA, 2002.

Desai:2002:POT

[2686] Anand Desai, Alejandro Hevia, and Yiqun Lisa Yin. A practice-oriented treatment of pseudorandom number generators. *Lecture Notes in Computer Science*, 2332:368–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320368.htm; http://link.springer-ny.com/link/service/series/0558/papers/2332/23320368.pdf.

Dultz:2002:ORN

[2687] W. Dultz and E. Hildebrandt. Optical random-number generator based on single-photon statistics at the optical beam splitter. US Patent No. 6,393,448., May 17, 2002. URL https://www.google.com/patents/US6393448. Patent filed 17 September 1997.

Emmerich:2002:AES

[2688] Frank Emmerich. Average equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the period. *Mathematics of Computation*, 71(238):781–791, April 2002. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-01-01328-X; http://www.ams.org/mcom/2002-71-238/S0025-5718-01-01328-X/S0025-5718-01-01328-X.dvi; http://www.ams.org/mcom/2002-71-238/S0025-5718-01-01328-X/S0025-5718-01-01328-X.pdf; http://www.ams.org/mcom/2002-71-238/S0025-5718-01-01328-X/S0025-5718-01-01328-X.ps; http://www.ams.org/mcom/2002-71-238/S0025-5718-01-01328-X/S0025-5718-01-01328-X.tex; http://www.jstor.org/stable/pdfplus/2698847.pdf.

Entacher:2002:ELA

[2689] Karl Entacher, Thomas Schell, and Andreas Uhl. Efficient lattice assessment for LCG and GLP parameter searches. *Mathematics of Computation*, 71(239):1231–1242, July 2002. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journal-getitem?pii=S0025-5718-01-01415-6; http://www.ams.org/mcom/2002-71-239/S0025-5718-01-01415-6/S0025-5718-01-01415-6.dvi; http://www.ams.org/mcom/2002-71-239/S0025-5718-01-01415-6/S0025-5718-01-01415-6.pdf; http://www.ams.org/mcom/2002-71-239/S0025-5718-01-01415-6/S0025-5718-01-01415-6.ps; http://www.ams.org/mcom/2002-71-239/S0025-5718-01-01415-

6/S0025-5718-01-01415-6.tex; http://www.jstor.org/stable/pdfplus/2698904.pdf.

Fahoome:2002:JRF

[2690] Gail F. Fahoome. JMASM1: RANGEN 2.0 (Fortran 90/95). *Journal of Modern Applied Statistical Methods*, 1(1):182–190, Winter 2002. CODEN ???? ISSN 1538-9472. URL http://tbf.coe.wayne.edu/jmasm/.

Faure:2002:ARS

[2691] H. Faure and S. Tezuka. Another random scrambling of digital (t, s)-sequences. In Fang et al. [4231], pages 242–256. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

Figotin:2002:ONT

[2692] A. Figotin, A. Gordon, S. Molchanov, J. Quinn, and N. Stavrakas. Occupancy numbers in testing random number generators. *SIAM Journal on Applied Mathematics*, 62(6):1980–2011, December 2002. CODEN SMJMAP. ISSN 0036-1399 (print), 1095-712X (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/36686.

Fluhrer:2002:CSP

[2693] Scott R. Fluhrer. Cryptanalysis of the SEAL 3.0 pseudorandom function family. *Lecture Notes in Computer Science*, 2355:135–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550135.htm; http://link.springer-ny.com/link/service/series/0558/papers/2355/23550135.pdf.

Friedel:2002:FGR

[2694] I. Friedel and A. Keller. Fast generation of randomized low-discrepancy point sets. In Fang et al. [4231], pages 257–273. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

Futschik:2002:EFE

[2695] Andreas Futschik. Ist der Euro fair? Ergebnis einer empirischen Untersuchung. (German) [Is the euro fair? Results of an empirical investigation]. *Austrian Journal of Statistics*, 31(1):35–40, ???? 2002. CODEN ???? ISSN 1026-597X.

Gangnon:2002:MDE

[2696] Ronald E. Gangnon and William N. King. Minimum distance estimation of the distribution functions of stochastically ordered random variables. *Applied Statistics*, 51(4):485–492, ???? 2002. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

Gennaro:2002:CPG

[2697] Rosario Gennaro and Daniele Micciancio. Cryptanalysis of a pseudorandom generator based on braid groups. *Lecture Notes in Computer Science*, 2332:1–13, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2332/23320001.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2332/23320001.pdf`.

Gilbert:2002:NRP

[2698] Henri Gilbert and Marine Minier. New results on the pseudorandomness of some blockcipher constructions. *Lecture Notes in Computer Science*, 2355:248–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550248.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2355/23550248.pdf`.

Gleeson:2002:TRN

[2699] J. T. Gleeson. Truly random number generator based on turbulent electroconvection. *Applied Physics Letters*, 81(11):1949–1951, 2002. CODEN APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842. URL `http://link.aip.org/link/?APL/81/1949/1`.

Golic:2002:SWM

[2700] Jovan Dj. Golić, Mahmoud Salmasizadeh, and Ed Dawson. Statistical weakness of multiplexed sequences. *Finite Fields and their Applications*, 8(4):420–433, October 2002. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579701903508`.

Guimond:2002:PDP

[2701] Louis-Sébastien Guimond and Jiří Patera. Proving the deterministic period breaking of linear congruential generators using two tile quasicrystals. *Mathematics of Computation*, 71(237):319–332, 2002. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.jstor.org/stable/pdfplus/2698875.pdf`.

Hernandez:2002:AGA

[2702] Julio César Hernández, Pedro Isasi, and Arturo Ribagorda. An application of genetic algorithms to the cryptanalysis of one round TEA. In M. H. Hamza, editor, *Proceedings of Applied Informatics (AI 2002), February 18–21, 2002 Innsbruck, Austria*, page ?? Acta Press, Calgary, AB, Canada, 2002. URL `http://www.actapress.com/PaperInfo.aspx?PaperID=26972`.

Hernandez:2002:GCT

[2703] Julio César Hernández, José María Sierra, Pedro Isasi, and Arturo Ribagorda. Genetic cryptoanalysis of two rounds TEA. *Lecture Notes in Computer Science*, 2331:1024–1031, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/0pa8nj982jewn9ev/`.

Hertling:2002:SNN

[2704] Peter Hertling. Simply normal numbers to different bases. *J.UCS: Journal of Universal Computer Science*, 8(2):235–242, February 28, 2002. CODEN ???? ISSN 0948-695X (print), 0948-6968 (electronic). URL `http://www.jucs.org/jucs_8_2/simply_normal_numbers_to`.

Hormann:2002:FGO

[2705] Wolfgang Hörmann and Gerhard Derflinger. Fast generation of order statistics. *ACM Transactions on Modeling and Computer Simulation*, 12(2):83–93, April 2002. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Iwata:2002:RSS

[2706] Tetsu Iwata, Tomonobu Yoshino, Tomohiro Yuasa, and Kaoru Kurosawa. Round security and super-pseudorandomness of MISTY type structure. *Lecture Notes in Computer Science*, 2355:233–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer-ny.com/link/service/series/0558/bibs/2355/23550233.htm`; `http://link.springer-ny.com/link/service/series/0558/papers/2355/23550233.pdf`.

Janke:2002:PRN

[2707] Wolfhard Janke. Pseudo random numbers: Generation and quality checks. In Johannes Grotendorst, Dominik Marx, and Alejandro Muramatsu, editors, *Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms: Winter School, 25 February–1 March 2002, Rolduc Conference Centre, Kerkrade, The Netherlands*, volume 10, pages

447–?? John von Neumann Institute for Computing, Jülich, Germany, 2002. ISBN 3-00-009058-4. LCCN Q183.9 N492 v. 11. URL `http://www2.fz-juelich.de/nic-series/volume10/janke1.pdf`.

Jeruchim:2002:FRV

[2708] Michel C. Jeruchim, Philip Balaban, and K. Sam Shanmugan. Fundamentals of random variables and random processes for simulation. In *Simulation of Communication Systems: Modeling, Methodology, and Techniques*, Information Technology: Transmission, Processing, and Storage, pages 289–370. Kluwer Academic Publishers, Norwell, MA, USA, and Dordrecht, The Netherlands, 2002. ISBN 0-306-46267-2 (print), 0-306-46971-5 (electronic). ISSN 1389-6938. LCCN TK5102.5 S5515 2000.

Jeruchim:2002:MCS

[2709] Michel C. Jeruchim, Philip Balaban, and K. Sam Shanmugan. Monte Carlo simulation and generation of random numbers. In *Simulation of Communication Systems: Modeling, Methodology, and Techniques*, Information Technology: Transmission, Processing, and Storage, pages 371–406. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 0-306-46267-2 (print), 0-306-46971-5 (electronic). ISSN 1389-6938. LCCN TK5102.5 S5515 2000.

Jones:2002:KTP

[2710] M. C. Jones. On Khintchine's theorem and its place in random variate generation. *The American Statistician*, 56(4):304–??, November 2002. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://oberon.ingentaselect.com/cgi-bin/linker?ini=asa&reqidx=/cw/asa/00031305/v56n4/s7/p304`.

Karras:2002:SPB

[2711] D. A. Karras and V. Zorkadis. Strong pseudorandom bit sequence generators using neural network techniques and their evaluation for secure communications. *Lecture Notes in Computer Science*, 2557: 615–??, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2557/25570615.htm`; `http://link.springer.de/link/service/series/0558/papers/2557/25570615.pdf`.

Kunchenko:2002:PPE

[2712] ëIíU. P. (ëIíUriĭ Petrovich) Kunchenko. *Polynomial parameter estimations of close to Gaussian random variables*. Berichte aus der Kommunikationstechnik. Shaker, Achen, Germany, 2002. ISBN 3-8322-0032-0. ISSN 0945-0823. xiv + 396 pp. LCCN QA273 .K799 2003.

Kuo:2002:CCC

[2713] F. Y. Kuo and S. Joe. Component-by-component construction of good lattice rules with a composite number of points. *Journal of Complexity*, 18(4):943–976, ???? 2002. CODEN JOCOEH. ISSN 0885-064X (print), 1090-2708 (electronic).

LEcuyer:2002:CEG

[2714] Pierre L'Ecuyer and François Panneton. Constructions of equidistributed generators based on linear recurrences modulo 2. In Fang et al. [4231], pages 318–330. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html`.

LEcuyer:2002:OOR

[2715] Pierre L'Ecuyer, Richard Simard, E. Jack Chen, and W. David Kelton. An object-oriented random-number package with many long streams and substreams. *Operations Research*, 50(6):1073–1075, December 2002. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL `http://or.pubs/informs.org/pages/collect.html`; `http://www.iro.umontreal.ca/~lecuyer`; `http://www.jstor.org/stable/3088626`.

LEcuyer:2002:RAR

[2716] Pierre L'Ecuyer and Christiane Lemieux. Recent advances in randomized quasi-Monte Carlo methods. In Dror et al. [4230], pages 419–474. ISBN 0-7923-7463-0. LCCN QA274.2 .M63 2002. URL `http://www.loc.gov/catdir/enhancements/fy0820/2001050485-d.html`; `http://www.loc.gov/catdir/enhancements/fy0820/2001050485-t.html`.

LEcuyer:2002:SST

[2717] Pierre L'Ecuyer, Richard Simard, and Stefan Wegenkittl. Sparse serial tests of uniformity for random number generators. *SIAM Journal on Scientific Computing*, 24(2):652–668, March 2002. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/34903`.

LEcuyer:2002:TSL

[2718] Pierre L'Ecuyer and Richard Simard. TestU01: a software library in ANSI C for empirical testing of random number generators: Software user's guide. Web report, Départment d'Informatique et de Recherche Opérationelle, Université de Montréal, Montréal, Québec, Canada,

2002. URL http://www.iro.umontreal.ca/~simardr/TestU01.zip; http://www.iro.umontreal.ca/~simardr/testu01/tu01.html.

Leydold:2002:ULU

[2719] J. Leydold and W. Hörmann. UNURAN — a library for universal non-uniform random number generators. Web software archive., 2002. URL http://statistik.wu-wien.ac.at/unuran.

Leydold:2002:VTD

[2720] J. Leydold, E. Janka, and W. Hörmann. Variants of transformed density rejection and correlation introduction. In Fang et al. [4231], pages 345–356. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

Luo:2002:CGB

[2721] Ping Luo. A combined generator based on linear congruential generators and its structural improvement. *Journal on Numerical Methods and Computer Applications*, 23(1):6–17, 2002. CODEN ???? ISSN 1000-3266.

Mahmoud:2002:ISR

[2722] Hosam Mahmoud and Tatsuie Tsukiji. On the internal structure of random recursive circuits. *Journal of Computational and Applied Mathematics*, 142(1):155–171, May 1, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042701004666.

Marsaglia:2002:RGB

[2723] George Marsaglia. Re: *good* 64-bit random-number generator. Posting to the sci.crypt.random-numbers news group, September 3, 2002. URL http://groups.google.ws/group/comp.sys.sun.admin/browse_thread/thread/683ff52120e5b4d/b53ccad5aa5d6017.

Marsaglia:2002:SDP

[2724] George Marsaglia and Wai Wan Tsang. Some difficult-to-pass tests of randomness. *Journal of Statistical Software*, 7(3):1–8, 2002. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/v07/i03; http://www.jstatsoft.org/v07/i03/tuftests.c; http://www.jstatsoft.org/v07/i03/tuftests.pdf; http://www.jstatsoft.org/v07/i03/updates.

Martin:2002:ARN

[2725] P. Martin. An analysis of random number generators for a hardware implementation of genetic programming using FPGAs and Handel-C. In

W. B. Langdon, E. Cantu-Paz, K. Mathias, R. Roy, D. Davis R. Poli, K. Balakrishnan, V. Honavar, G. Rudolph, J. Wegener, L. Bull, M. A. Potter, A. C. Schultz, J. F. Miller, E. Burke, and N. Jonoska, editors, *GECCO-2002: 2002 Genetic and Evolutionary Computation Conference: presentations in the evolutionary computation in industry track: New York, New York, July 11–13, 2002*, pages 837–844. Morgan Kaufmann Publishers, San Francisco, CA, USA, 2002. ISBN 1-55860-878-8. LCCN QA76.6 I6231 2002.

Martinez:2002:CSH

[2726] Wendy L. Martinez and Angel R. Martinez. *Computational Statistics Handbook with MATLAB*. Chapman and Hall/CRC, Boca Raton, FL, USA, 2002. ISBN 1-58488-229-8, 1-4200-3563-0 (e-book). xvii + 591 pp. LCCN QA276.4 .M272 2001. US$79.95, UK£53.99.

Matsumoto:2002:NTW

[2727] M. Matsumoto and T. Nishimura. A nonempirical test on the weight of pseudorandom number generators. In Fang et al. [4231], pages 381–395. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html`.

Maurer:2002:IRS

[2728] U. M. Maurer. Indistinguishability of random systems. In G. Goos, J. Hartmanis, and J. van Leeuwen, editors, *Advances in Cryptology: Eurocrypt 2002*, number 2332 in Lecture Notes in Computer Science, pages 110–132. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. LCCN QA76.9 A25 E87.

McCullough:2002:ASP

[2729] B. D. McCullough and B. Wilson. On the accuracy of statistical procedures in Microsoft Excel 2000 and XP. *Computational Statistics & Data Analysis*, 40(4):27–37, October 28, 2002. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947302000956`.

McCullough:2002:DMF

[2730] B. D. McCullough. Does Microsoft fix errors in Excel? In *2001 proceedings: papers presented at the Annual Meeting of the American Statistical Association, Joint Statistical Meetings, Atlanta, Georgia, August 5–9, 2001*, page ?? American Statistical Association, Alexandria, VA, USA, 2002. ISBN 1-931586-13-6. LCCN ???? URL `http://www.amstat.org/sections/SRMS/Proceedings/y2001/Proceed/00177.pdf`.

McCullough:2002:RNG

[2731] B. D. McCullough. Random number generators. In Abdel H. El-Shaarawi and Walter W. Piegorsch, editors, *Encyclopedia of Environmetrics*, volume 3, page ?? Wiley, New York, NY, USA, 2002. ISBN 0-470-05733-5, 0-471-89997-6. LCCN GE45.S73 E53 2002. URL http://onlinelibrary.wiley.com/doi/10.1002/9780470057339.var009/full.

Mironov:2002:RSR

[2732] Ilya Mironov. (Not so) random shuffles of RC4. In M. Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 304–319. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. URL https://link.springer.com/chapter/10.1007/3-540-45708-9_20.

Mita:2002:PBG

[2733] R. Mita, G. Palumbo, S. Pennisi, and M. Poli. Pseudorandom bit generator based on dynamic linear feedback topology. *Electronics Letters*, 38(19):1097–1098, September 12, 2002. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1038612.

Moon:2002:IDC

[2734] Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim. Impossible differential cryptanalysis of reduced round XTEA and TEA. *Lecture Notes in Computer Science*, 2365:49–61, 2002. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer-ny.com/link/service/series/0558/bibs/2365/23650049.htm; http://link.springer-ny.com/link/service/series/0558/papers/2365/23650049.pdf; http://www.iacr.org/archive/fse2002/23650050/23650050.pdf.

Murray:2002:IYP

[2735] Mark R. V. Murray. An implementation of the Yarrow PRNG for FreeBSD. In USENIX [4232], pages 47–53. ISBN 1-880446-02-2. LCCN QA76.76.O63 B736 2002. URL http://www.usenix.org/publications/library/proceedings/bsdcon02/murray.html.

Niederreiter:2002:ADI

[2736] Harald Niederreiter and Igor E. Shparlinski. On the average distribution of inversive pseudorandom numbers. *Finite Fields and their Applications*, 8(4):491–503, October 2002. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1071579702903588.

Niederreiter:2002:ICS

[2737] Harald Niederreiter and Arne Winterhof. Incomplete character sums and polynomial interpolation of the discrete logarithm. *Finite Fields and their Applications*, 8(2):184–192, April 2002. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://www.sciencedirect.com/science/article/pii/S107157970190334X.

Niederreiter:2002:RAT

[2738] Harald Niederreiter and Igor E. Shparlinski. Recent advances in the theory of nonlinear pseudorandom number generators. In Fang et al. [4231], pages 86–102. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

NIST:2002:ERN

[2739] NIST. Examples of random number generators. World-Wide Web site., 2002. URL http://csrc.nist.gov/rng/rng6_2.html.

Papoulis:2002:PRV

[2740] Athanasios Papoulis and S. Unnikrishna Pillai. *Probability, random variables, and stochastic processes*. McGraw-Hill, New York, NY, USA, fourth edition, 2002. ISBN 0-07-366011-6, 0-07-112256-7. x + 852 pp. LCCN QA273 .P2 2002. URL http://www.loc.gov/catdir/enhancements/fy1011/2001044139-d.html; http://www.loc.gov/catdir/enhancements/fy1011/2001044139-t.html; http://www.loc.gov/catdir/enhancements/fy1106/2001044139-b.html.

Philipp:2002:MTD

[2741] Walter Philipp and Robert Tichy. Metric theorems for distribution measures of pseudorandom sequences. *Monatshefte für Mathematik*, 135 (4):321–326, April 2002. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL http://www.springerlink.com/content/61r9etxplcwmmfxn/. See [2543].

Pirsic:2002:SIN

[2742] Gottlieb Pirsic. A software implementation of Niederreiter–Xing sequences. In Fang et al. [4231], pages 434–445. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

Raqab:2002:IGE

[2743] Mohammad Z. Raqab. Inferences for generalized exponential distribution based on record statistics. *Journal of Statistical Planning and Inference*, 104(2):339–350, June 1, 2002. CODEN JSPIDN. ISSN 0378-3758 (print), 1873-1171 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378375801002464`.

Rukhin:2002:DNW

[2744] A. L. Rukhin. Distribution of the number of words with a prescribed frequency and tests of randomness. *Advances in Applied Probability*, 34 (4):775–797, 2002. CODEN AAPBBD. ISSN 0001-8678 (print), 1475-6064 (electronic).

Shackleford:2002:FIN

[2745] Barry Shackleford, Motoo Tanaka, Richard J. Carter, and Greg Snider. FPGA implementation of neighborhood-of-four cellular automata random number generators. In Stephen Trimberger, Martine Schlag, et al., editors, *FPGA 2002: Proceedings of the 2002 ACM/SIGDA Tenth International Symposium on Field-Programmable Gate Arrays, Monterey, California, USA: February 24–26, 2002*, pages 106–112. ACM Press, New York, NY 10036, USA, 2002. ISBN 1-58113-452-5. LCCN TK7895.G36 I481 2002. ACM order number 480020.

Shparlinski:2002:DDH

[2746] Igor E. Shparlinski. On the distribution of the Diffie–Hellman pairs. *Finite Fields and their Applications*, 8(2):131–141, April 2002. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579700903216`.

Sugita:2002:RNI

[2747] Hiroshi Sugita. Robust numerical integration and pairwise independent random variables. *Journal of Computational and Applied Mathematics*, 139(1):1–8, February 1, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042701003946`.

Tan:2002:PPP

[2748] Chih Jeng Kenneth Tan. The PLFG parallel pseudo-random number generator. *Future Generation Computer Systems*, 18(5):693–698, April 2002. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL `http://www.elsevier.nlhttp://www.elsevier.com/gej-ng/10/19/19/60/36/36/abstract.html`.

Tang:2002:CRN

[2749] Hui-Chin Tang. Combined random number generator via the generalized Chinese remainder theorem. *Journal of Computational and Applied Mathematics*, 142(2):377–388, May 15, 2002. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042701004241`.

Tang:2002:LBS

[2750] Hui-Chin Tang and Chiang Kao. Lower bounds in spectral tests for vectors of nonsuccessive values produced by multiple recursive generator with some zero multipliers. *Computers and Mathematics and Applications*, 43(8–9):1153–1159, April/May 2002. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122102800190`.

Tang:2002:MDM

[2751] Hui-Chin Tang. Modified decomposition method for multiple recursive random number generator. *Mathematics and Computers in Simulation*, 59(5):453–458, June 15, 2002. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475401004281`.

Tezuka:2002:RGF

[2752] S. Tezuka. On randomization of generalized Faure sequences. Report RT-0494, IBM Research, Tokyo Research Laboratory, Tokyo, Japan, 2002.

Tsaban:2002:ELF

[2753] Boaz Tsaban and Uzi Vishne. Efficient linear feedback shift registers with maximal period. *Finite Fields and their Applications*, 8(2):256–267, April 2002. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579701903399`.

Umans:2002:PRG

[2754] Christopher Umans. Pseudo-random generators for all hardnesses. In ACM [4229], pages 627–634. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Wang:2002:HOL

[2755] Y. Wang and F. J. Hickernell. A historical overview of lattice point sets. In Fang et al. [4231], pages 158–167. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html`.

Wang:2002:NCT

[2756] Yongge Wang. Note: a comparison of two approaches to pseudorandomness. *Theoretical Computer Science*, 276(1–2):449–459, April 6, 2002. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.elsevier.com/gej-ng/10/41/16/247/27/49/abstract.html`.

Wu:2002:BPR

[2757] Pei-Chi Wu, Kuo-Chan Huang, and Shih-Ting Ouyang. Bit-parallel random number generation for discrete uniform distributions. *Computer Physics Communications*, 144(3):252–260, April 2002. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465502001431`.

Yaguchi:2002:CLP

[2758] Hirotake Yaguchi. Construction of a long-period nonalgebraic and nonrecursive pseudorandom number generator. *Monte Carlo Methods and Applications*, 8(2):203–213, ???? 2002. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2002.8.issue-2/mcma.2002.8.2.203/mcma.2002.8.2.203.xml`.

Yao:2002:CBR

[2759] Jian Yao, Guanrong Chen, Chaoyuan Yue, and Yong Zhao. Chaos-based random number generators and their application to multi-access secure communications. In IEEE, editor, *ICCA. Final Program and Book of Abstracts. The 2002 International Conference on Control and Automation, June 16–19, 2002, Xiamen, Fujian Province, China*, pages 152–?? IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2002. ISBN 0-7803-7412-6. LCCN TJ212.2 .I582 2002. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=8706`.

Aamodt:2003:CSP

[2760] Ken S. Aamodt. *A cryptographically secure pseudorandom number generator*. Ph.D. thesis, Purdue University, West Lafayette, IN, USA, December 2003. 147 pp. URL `http://catalog.lib.purdue.edu/Find/Record/1380784`; `http://search.proquest.com/docview/305316022?accountid=14677`.

Andem:2003:CTE

[2761] Vikram Reddy Andem. A cryptanalysis of the Tiny Encryption Algorithm. Thesis (Master of Science), Department of Computer Science, University of Alabama, Tuscaloosa, AL, USA, 2003. viii + 60 pp.

URL `http://www.csshl.net/sites/default/files/downloadable/crypto/TEA_Cryptanalysis_-_VRAndem.pdf`.

Anonymous:2003:DR

[2762] Anonymous. `/dev/random`. Web site., June 8, 2003. From the site: "Thus, in 1994 noted Linux kernel hacker Theodore Ts'o wrote a driver for Linux, which takes information about hard to predict events like keyboard and mouse use, packet and disk drive timings, and so on, and uses it to seed a cryptographically secure random number generator. A process can then open up the 'file' `/dev/random` (usually a character device), and read out random bytes. The driver keeps an estimate of how much entropy remains in the pool — if it goes below 0 then any reads will block until more entropy is added." Also this: "the actual driver is implemented in drivers/char/random.c in the Linux source tree.".

Barak:2003:TRN

[2763] Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. *Lecture Notes in Computer Science*, 2779:166–180, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Beebe:2003:PRN

[2764] Nelson H. F. Beebe. Pseudo-random numbers: [mostly] a line [of code] at a time. Lecture notes, University of Utah, Department of Mathematics, Salt Lake City, UT 84112-0090, USA, January 14, 2003. 22 pp.

Boesgaard:2003:RNH

[2765] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius. Rabbit: a new high-performance stream cipher. In Thomas Johansson, editor, *Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, February 24–26, 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 307–329. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. URL `https://link.springer.com/chapter/10.1007/978-3-540-39887-5_23#citeas`. Revised Papers 10.

Brent:2003:RNG

[2766] Richard P. Brent and Paul Zimmermann. Random number generators with period divisible by a Mersenne prime. *Lecture Notes in Computer Science*, 2667:1–10, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bucci:2003:HSO

[2767] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC. *IEEE Transactions on Computers*, 52(4):403–409, April 2003. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1190581`.

Courtois:2003:AAS

[2768] Nicolas T. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17–21, 2003, Proceedings*, volume 2003 of *Lecture Notes in Computer Science*, pages 176–194. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. URL `https://link.springer.com/chapter/10.1007/978-3-540-45146-4_11#citeas`.

Crawford:2003:FWC

[2769] Diane Crawford, Simone Santini, Ralph Castain, William F. Dowling, John Cook, Simon Dobson, Peter J. Denning, Robert Dunham, Jef Raskin, and Dennis Tsichritzis. Forum: When is a computer more like a guitar than a washing machine?; corroboration the only way to determine Web accuracy; how to teach critical thinking about Web content; create a random number service based on the Mersenne Twister; make fair uses a legal requirement in DRM systems; "The Missing Customer" redux; enthusiasm, drive, wisdom, patience not tied to age. *Communications of the ACM*, 46(7):11–13, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Deng:2003:SHD

[2770] Lih-Yuan Deng and Hongquan Xu. A system of high-dimensional, efficient, long-cycle and portable uniform random number generators. *ACM Transactions on Modeling and Computer Simulation*, 13(4):299–309, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Devroye:2003:NUR

[2771] Luc Devroye. *Non-Uniform Random Variate Generation*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 1-4613-8645-4. xxxii + 843 pp. LCCN QA273.A1-274.9; QA274-274.9.

Dichtl:2003:HPO

[2772] Markus Dichtl. How to predict the output of a hardware random number generator. *Lecture Notes in Computer Science*, 2779:181–188, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwyer:2003:PRN

[2773] Gerald P. Dwyer, Jr. and K. B. Williams. Portable random number generators. *Journal of Economic Dynamics and Control*, 27(4):645–650, February 2003. CODEN JEDCDH. ISSN 0165-1889 (print), 1879-1743 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0165188901000653`.

Engel:2003:BLE

[2774] Hans-Andreas Engel and Christoph Leuenberger. Benford's law for exponential random variables. *Statistics & Probability Letters*, 63(4):361–365, July 15, 2003. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167715203001019`.

Epstein:2003:DIT

[2775] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. *Lecture Notes in Computer Science*, 2779:152–165, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Galmes:2003:ACM

[2776] Sebastià Galmés and Ramon Puigjaner. An algorithm for computing the mean response time of a single server queue with generalized on/off traffic arrivals. *ACM SIGMETRICS Performance Evaluation Review*, 31(1):37–46, June 2003. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Gentle:2003:RNG

[2777] James E. Gentle. *Random Number Generation and Monte Carlo Methods*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2003. ISBN 0-387-00178-6. xv + 381 pp. LCCN QA298 .G46 2003. US$79.95. URL `http://www.science.gmu.edu/~jgentle/rngbk/`.

Gibbons:2003:NSI

[2778] Jean Dickinson Gibbons and Subhabrata Chakraborti. *Nonparametric Statistical Inference*, volume 168 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, fourth edition, 2003. ISBN 0-8247-4052-1. xxiv + 645 pp. LCCN QA278.8 .G498 2003. URL `http://www.e-streams.com/es0706/es0706\_3315.html`; `http://www.loc.gov/catdir/enhancements/fy0647/2004266776-d.html`.

Goldreich:2003:SME

[2779] Oded Goldreich and Vered Rosen. On the security of modular exponentiation with application to the construction of pseudorandom generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(2):71–93, March 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Gonnet:2003:RTT

[2780] G. Gonnet. Repeating time test for $U(0,1)$ random number generators. Technical report, Department of Computer Science, ETH Zürich, Zürich, Switzerland, 2003. URL `http://www.inf.ethz.ch/~gonnet/RepetitionTest`.

Goresky:2003:EMC

[2781] Mark Goresky and Andrew Klapper. Efficient multiply-with-carry random number generators with maximal period. *ACM Transactions on Modeling and Computer Simulation*, 13(4):310–321, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Grabner:2003:CGD

[2782] Peter J. Grabner, Arnold Knopfmacher, and Helmut Prodinger. Combinatorics of geometrically distributed random variables: run statistics. *Theoretical Computer Science*, 297(1–3):261–270, March 17, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Guimond:2003:SPI

[2783] Louis-Sébastien Guimond, Jan Patera, and Jiří Patera. Statistical properties and implementation of aperiodic pseudorandom number generators. *Applied Numerical Mathematics: Transactions of IMACS*, 46(3–4): 295–318, September 2003. CODEN ANMAEL. ISSN 0168-9274 (print), 1873-5460 (electronic).

Gutierrez:2003:LNC

[2784] J. Gutierrez, I. E. Shparlinski, and A. Winterhof. On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators. *IEEE Transactions on Information Theory*, 49(1):60–64, January 2003. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).

Hellekalek:2003:EEC

[2785] Peter Hellekalek and Stefan Wegenkittl. Empirical evidence concerning AES. *ACM Transactions on Modeling and Computer Simulation*, 13(4):322–333, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `http://random.mat.sbg.ac.at/ftp/pub/publications/peter/aes_sub.ps`; `http://random.mat.sbg.ac.at/~peter/slides_YACC04.pdf`.

Hernandez:2003:FED

[2786] Julio César Hernández and Pedro Isasi. Finding efficient distinguishers for cryptographic mappings, with an application to the block cipher TEA. In IEEE, editor, *The 2003 Congress on Evolutionary Computation, 2003. CEC '03*, volume 3, pages 2189–2193. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. ISBN 0-7803-7804-0. URL `http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1299943`.

Hill:2003:UPO

[2787] David R. C. Hill. URNG: a portable optimization technique for software applications requiring pseudo-random numbers. *Simulation Modelling Practice and Theory*, 1(4):643–654, December 15, 2003. CODEN SMPTCA. ISSN 1569-190X (print), 1878-1462 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1569190X03001011`.

Hitchcock:2003:HMH

[2788] David B. Hitchcock. A history of the Metropolis–Hastings algorithm. *The American Statistician*, 57(4):254–257, November 2003. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://oberon.ingentaselect.com/cgi-bin/linker?ini=asa&reqidx=/cw/asa/00031305/v57n4/s7/p254`; `http://www.jstor.org/stable/30037292`.

Hormann:2003:CRV

[2789] Wolfgang Hörmann and Josef Leydold. Continuous random variate generation by fast numerical inversion. *ACM Transactions on Modeling*

and Computer Simulation, 13(4):347–362, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `http://statistik.wu-wien.ac.at/unuran/`.

Intel:2003:IRN

[2790] Intel Corporation. The Intel random number generator. World-Wide Web document., 2003. URL `http://developer.intel.com/design/chipsets/rng/docs.htm`.

Joe:2003:RAI

[2791] Stephen Joe and Frances Y. Kuo. Remark on Algorithm 659: Implementing Sobol's quasirandom sequence generator. *ACM Transactions on Mathematical Software*, 29(1):49–57, March 2003. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://doi.acm.org/10.1145/641876.641879`.

Kocarev:2003:CPR

[2792] Ljupco Kocarev, Goce Jakimoski, and Zarko Tasev. Chaos and pseudorandomness. *Lecture Notes in Control and Information Sciences*, 292: 682–685, 2003. CODEN ???? ISSN 0170-8643 (print), 1610-7411 (electronic).

LEcuyer:2003:CGC

[2793] Pierre L'Ecuyer and Jacinthe Granger-Piché. Combined generators with components from different families. *Mathematics and Computers in Simulation*, 62(3–6):395–404, March 2003. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475402002343`. 3rd IMACS Seminar on Monte Carlo Methods—MCM 2001 (Salzburg).

Lemieux:2003:RPL

[2794] Christiane Lemieux and Pierre L'Ecuyer. Randomized polynomial lattice rules for multivariate integration and simulation. *SIAM Journal on Scientific Computing*, 24(5):1768–1789, September 2003. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic). URL `http://epubs.siam.org/sam-bin/dbq/article/39378`.

Li:2003:ULD

[2795] Xueqing Li, Wenping Wang, Ralph R. Martin, and Adrian Bowyer. Using low-discrepancy sequences and the Crofton formula to compute surface areas of geometric models. *Computer Aided Design*, 35(9):771–782, August 2003. CODEN CAIDA5. ISSN 0010-4485 (print), 1879-

2685 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010448502001008.

Lodwick:2003:EVC

[2796] Weldon A. Lodwick and K. David Jamison. Estimating and validating the cumulative distribution of a function of random variables: Toward the development of distribution arithmetic. *Reliable Computing = Nadezhnye vychisleniia*, 9(2):127–141, April 2003. CODEN RCOMF8. ISSN 1385-3139 (print), 1573-1340 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=1385-3139&volume=9&issue=2&spage=127.

Louchard:2003:ARS

[2797] Guy Louchard and Helmut Prodinger. Ascending runs of sequences of geometrically distributed random variables: a probabilistic analysis. *Theoretical Computer Science*, 304(1–3):59–86, July 28, 2003. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Maaranen:2003:UQR

[2798] Heikki Maaranen, Kaisa Miettinen, and Marko M. Mäkelä. Using quasi random sequences in genetic algorithms. In Rudnicki and Wiak [4233], pages 33–44. ISBN 1-4020-1506-2, 90-481-6375-7 (print), 94-017-2494-6 (e-book). LCCN QA76.9.M35; T57-57.97. URL http://www.springerlink.com/content/978-94-017-2494-4.

Marsaglia:2003:EKD

[2799] George Marsaglia, Wai Wan Tsang, and Jingbo Wang. Evaluating Kolmogorov's distribution. *Journal of Statistical Software*, 8(18):1–4, 2003. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/v08/i18; http://www.jstatsoft.org/v08/i18/k.pdf.

Marsaglia:2003:RNG

[2800] George Marsaglia. Random number generators. *Journal of Modern Applied Statistical Methods*, 2(1):2–13, May 2003. CODEN ???? ISSN 1538-9472. URL http://stat.fsu.edu/pub/diehard/; http://tbf.coe.wayne.edu/jmasm/; http://www.csis.hku.hk/~diehard/.

Marsaglia:2003:TOS

[2801] George Marsaglia. Technical opinion: Seeds for random number generators: Techniques for choosing seeds for social and scientific applications of random number generators. *Communications of the ACM*, 46(5):90–93, May 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Marsaglia:2003:XR

[2802] George Marsaglia. Xorshift RNGs. *Journal of Statistical Software*, 8 (14):1–6, 2003. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v08/i14`; `http://www.jstatsoft.org/v08/i14/xorshift.pdf`. See [2846] for corrections and the equivalence of xorshift generators and the well-understood linear feedback shift register generators. See also [3600, 3700, 3807] for the failure of Marsaglia's `xorwow()` generator from this paper. See [2968, 3888] for detailed analysis.

Matsumoto:2003:SDT

[2803] Makoto Matsumoto and Takuji Nishimura. Sum-discrepancy test on pseudorandom number generators. *Mathematics and Computers in Simulation*, 434(1):431–442, March 3, 2003. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475402002276`.

McNichol:2003:HTM

[2804] Tom McNichol. How two math geeks with a lava lamp and a webcam are about to unleash chaos on the Internet. *Wired*, 11(8):??, August 2003. CODEN WREDEM. ISSN 1059-1028 (print), 1078-3148 (electronic). URL `http://www.lavarnd.org`; `http://www.wired.com/wired/archive/11.08/random.html`.

Meidl:2003:LCP

[2805] Wilfried Meidl and Arne Winterhof. On the linear complexity profile of explicit nonlinear pseudorandom numbers. *Information Processing Letters*, 85(1):13–18, January 16, 2003. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Mertens:2003:EPR

[2806] Stephan Mertens and Heiko Bauke. Entropy of pseudo random number generators. Web document, ???? 2003. URL `http://arxiv.org/abs/cond-mat/0305319`.

Mether:2003:HCL

[2807] Max Mether. The history of the central limit theorem. Class notes, Systems Analysis Laboratory, Helsinki University of Technology, Helsinki, Finland, November 6, 2003. 25 pp.

Myers:2003:EAS

[2808] Steven Myers. Efficient amplification of the security of weak pseudorandom function generators. *Journal of Cryptology: the journal of the*

International Association for Cryptologic Research, 16(1):1–24, January 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Neal:2003:SS

[2809] Radford M. Neal. Slice sampling. *Annals of Statistics*, 31(3):705–767, June 2003. CODEN ASTSC7. ISSN 0090-5364 (print), 2168-8966 (electronic). URL `http://projecteuclid.org/euclid.aos/1056562461`.

Neuenschwander:2003:GRN

[2810] Daniel Neuenschwander and Hansmartin Zeuner. Generating random numbers of prescribed distribution using physical sources. *Statistics and Computing*, 13(1):5–11, February 2003. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1023/A%3A1021999708104`.

Niederreiter:2003:EGE

[2811] Harald Niederreiter. The existence of good extensible polynomial lattice rules. *Monatshefte für Mathematik*, 139(4):297–307, ???? 2003. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Nisan:2003:HVR

[2812] Noam Nisan and Avi Wigderson. Hardness vs. randomness. Report, Institute of Computer Science Hebrew University of Jerusalem, Jerusalem, Israel, November 25, 2003. 20 pp. URL `https://www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/NOAM/HARDNESS/final.pdf`.

Owen:2003:VAS

[2813] Art B. Owen. Variance with alternative scramblings of digital nets. *ACM Transactions on Modeling and Computer Simulation*, 13(4):363–378, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Papadimitrioul:2003:FSS

[2814] G. I. Papadimitrioul, B. Sadoun, and C. Papazoglou. Fundamentals of system simulation. In Mohammad S. Obaidat and Georgios I. Papadimitriou, editors, *Applied System Simulation: Methodologies and Applications*, pages 9–39. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 1-4419-9218-9. LCCN ????

PeytonJones:2003:RNa

[2815] Simon Peyton Jones. 12 rational numbers. *Journal of Functional Programming*, 13(1):149–152, January 2003. CODEN JFPRES. ISSN 0956-

7968 (print), 1469-7653 (electronic). URL `https://www.cambridge.org/core/product/AC5742F18F56DDBC1A1F9E0183B8A215`.

PeytonJones:2003:RNb

[2816] Simon Peyton Jones. 27 random numbers. *Journal of Functional Programming*, 13(1):235–240, January 2003. CODEN JFPRES. ISSN 0956-7968 (print), 1469-7653 (electronic). URL `https://www.cambridge.org/core/product/E141AFF92D015912D4A5CC313B0D6A9F`.

Pitman:2003:IDL

[2817] Jim Pitman and Marc Yor. Infinitely divisible laws associated with hyperbolic functions. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 55(??):292–330, ???? 2003. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Reid:2003:SSE

[2818] Jason Reid. *Secure Shell in the Enterprise*. Sun blueprints. Sun Microsystems Press, Palo Alto, CA, USA, 2003. ISBN 0-13-142900-0 (paperback). xxiii + 198 pp. LCCN QA76.76.O63 R448 2003. US$39.00.

Rieck:2003:CTR

[2819] James R. Rieck. A comparison of two random number generators for the Birnbaum–Saunders distribution. *Communications in Statistics: Theory and Methods*, 32(5):929–934, 2003. CODEN CSTMDC. ISSN 0361-0926 (print), 1532-415X (electronic).

Roberts:2003:ADR

[2820] Iain Roberts. AIX 5.2 `/dev/random` and `/dev/urandom` devices. Web site, April 25, 2003. URL `http://lists.gnupg.org/pipermail/gnupg-devel/2003-April/019954.html`; `http://www.counterpane.com/yarrow.html`.

Sarkar:2003:CSC

[2821] Palash Sarkar. Computing shifts in 90/150 cellular automata sequences. *Finite Fields and their Applications*, 9(2):175–186, April 2003. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579703000029`.

Schindler:2003:ECT

[2822] Werner Schindler and Wolfgang Killmann. Evaluation criteria for true (physical) random number generators used in cryptographic applications. In *Cryptographic Hardware and Embedded Systems — CHES 2002:*

4th International Workshop, Redwood Shores, CA, USA, August 13–15, 2002, Revised Papers, volume 2523 of *Lecture Notes in Computer Science*, pages 431–449. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 3-540-36400-5. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C45426 2002; QA76.9.A25.

Seznec:2003:HUL

[2823] André Seznec and Nicolas Sendrier. HAVEGE: a user-level software heuristic for generating empirically strong random numbers. *ACM Transactions on Modeling and Computer Simulation*, 13(4):334–346, October 2003. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Sobol:2003:MCR

[2824] I. M. Sobol and E. E. Myshetskaya. Modelling correlated random variables. *Monte Carlo Methods and Applications*, 9(1):67–76, January 2003. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2003.9.issue-1/156939603322587470/156939603322587470.xml`.

Soubusta:2003:ERQ

[2825] Jan Soubusta, Ondrej Haderka, Martin Hendrych, and Pavel Pavlicek. Experimental realization of quantum random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 5259(1):7–13, 2003. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/5259/7/1`. 13th Polish-Czech-Slovak Conference on Wave and Quantum Aspects of Contemporary Optics.

Srinivasan:2003:TPR

[2826] Ashok Srinivasan, Michael Mascagni, and David Ceperley. Testing parallel random number generators. *Parallel Computing*, 29(1):69–94, January 2003. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167819102001631`.

Stipcevic:2003:NDR

[2827] Mario Stipčević. Non-deterministic random bit generator based on electronics noise. *arXiv.org*, ??(??):??, September 2003. CODEN ???? ISSN ???? URL `http://arxiv.org/abs/physics/0309010v2`.

Sugita:2003:DRW

[2828] Hiroshi Sugita. Dynamic random Weyl sampling for drastic reduction of randomness in Monte Carlo integration. *Mathematics and Computers in Simulation*, 62(3–6):529–537, March 3, 2003. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475402002318`.

Tang:2003:SDA

[2829] Hui-Chin Tang. Simulated division with approximate factoring for the multiple recursive generator with both unrestricted multiplier and non-Mersenne prime modulus. *Computers and Mathematics and Applications*, 46(8–9):1173–1181, October/November 2003. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122103902094`.

Tang:2003:SPM

[2830] Hui-Chin Tang. Symmetry properties of multiple recursive random number generators in full period and spectral test. *Applied Mathematics and Computation*, 142(2–3):291–303, October 10, 2003. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Tsang:2003:TCT

[2831] W. W. Tsang, L. C. K. Hui, K. P. Chow, and C. F. Chong. Tuning the collision test for stringency. Report, The University of Hong Kong, Hong Kong, China, April 15, 2003. URL `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.137.279`; `http://www.cs.hku.hk/cisc/projects/va/tuning.pdf`.

Tsoi:2003:CFB

[2832] K. H. Tsoi, K. H. Leung, and Philip H. W. Leong. Compact FPGA-based true and pseudo random number generators. In Kenneth L. Pocek and Jeffrey M. Arnold, editors, *FCCM 2003: 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines: proceedings: 9–11 April, 2003, Napa, California*, pages 51–61. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2003. ISBN 0-7695-1979-2. ISSN 1082-3409. LCCN TK7895.G36 I35 2003.

Tu:2003:GRI

[2833] Shu-Ju Tu and Ephraim Fischbach. Geometric random inner products: a family of tests for random number generators. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 67(1):

016113, ???? 2003. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://pre.aps.org/abstract/PRE/v67/i1/e016113.

Umans:2003:PRG

[2834] Christopher Umans. Pseudo-random generators for all hardnesses. *Journal of Computer and System Sciences*, 67(2):419–440, September 2003. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0022000003000461.

Vavriv:2003:RNG

[2835] D. D. Vavriv. Random number generators on the basis of systems with chaotic behavior. *AIP Conference Proceedings*, 676(1):373, 2003. CODEN APCPCS. ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. URL http://link.aip.org/link/?APC/676/373/1.

Al-Subaihi:2004:SCM

[2836] Ali A. Al-Subaihi. Simulating correlated multivariate pseudorandom numbers. *Journal of Statistical Software*, 9(4):1–20, ???? 2004. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/counter.php?id=85&url=v09/i04/paper.pdf&ct=1.

Alekhnovich:2004:PGP

[2837] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88, February 2004. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL http://epubs.siam.org/sam-bin/dbq/article/38994.

Altman:2004:NIS

[2838] Micah Altman, Jeff Gill, and Michael McDonald. *Numerical Issues in Statistical Computing for the Social Scientist*. Wiley, New York, NY, USA, 2004. ISBN 0-471-23633-0, 0-471-47574-2 (e-book), 0-471-47576-9 (e-book). xv + 323 pp. LCCN QA276.4 .A398 2004.

Anonymous:2004:RNG

[2839] Anonymous. Random numbers generation using quantum physics. idQuantique white paper., 2004. URL http://www.idquantique.com/products/files/quantis-whitepaper.pdf.

Anonymous:2004:TRR

[2840] Anonymous. True randomness on request. Web site., May 2004. URL http://www.randomnumber.info.

Bauke:2004:PRC

[2841] Heiko Bauke and Stephan Mertens. Pseudo random coins show more heads than tails. *Journal of Statistical Physics*, 114(3–4):1149–1169, February 2004. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL http://arxiv.org/abs/cond-mat/0307138; http://link.springer.com/article/10.1023/B%3AJOSS.0000012521.67853.9a.

Beebe:2004:CJR

[2842] Nelson H. F. Beebe. Comments on the Java Random class. Web document, March 24, 2004. URL https://www.math.utah.edu/~beebe/java/random/. This document examines Java support for random numbers, comments on its deficiencies and inefficiencies, and reports the results of two test suites.

Bellare:2004:CBG

[2843] M. Bellare and P. Rogaway. Code-based game-playing proofs and the security of triple encryption. Cryptology ePrint Archive report 2004/331, 2004. URL http://eprint.iacr.org/2004/331.

Blacher:2004:SCA

[2844] R. Blacher. Solution complète au problème des nombres aléatoires. (French) [Complete solution to the problem of random numbers], 2004. URL http://www.agro-montpellier.fr/sfds/CD/textes/blacher1.pdf. Presented at Journées Statistiques de Montpellier.

Borwein:2004:MEP

[2845] Jonathan M. Borwein and David H. Bailey. *Mathematics by Experiment: Plausible Reasoning in the 21st Century*. A. K. Peters, Ltd., Wellesley, MA, USA, 2004. ISBN 1-56881-211-6. x + 288 pp. LCCN QA76.95 .B67 2003. US$45.00.

Brent:2004:NMX

[2846] Richard P. Brent. Note on Marsaglia's xorshift random number generators. *Journal of Statistical Software*, 11(5):1–5, 2004. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/counter.php?id=101&url=v11/i05/v11i05.pdf&ct=1. See [2802, 2968, 3888]. This article shows the equivalence of xorshift generators and the well-understood linear feedback shift register generators.

Brown:2004:TRV

[2847] Timothy C. Brown. Transforming a random variable to a prescribed distribution: An application to school-based assessment. *Journal of Applied Probability*, 41A:239–252, 2004. CODEN JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL http://www.jstor.org/stable/3215980.

Bucklew:2004:IRE

[2848] James Antonio Bucklew. *Introduction to Rare Event Simulation*, volume ?? of *Springer Series in Statistics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. CODEN ???? ISBN 0-387-20078-9, 1-4419-1893-0, 1-4757-4078-6 (e-book). ISSN 0172-7397. xi + 260 pp. LCCN QA273.67 .B84 2004. URL http://link.springer.com/book/10.1007/978-1-4757-4078-3.

Conflitti:2004:MDS

[2849] Alessandro Conflitti and Igor E. Shparlinski. On the multidimensional distribution of the subset sum generator of pseudorandom numbers. *Mathematics of Computation*, 73(246):1005–1011, April 2004. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/home.html; http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-5718-03-01563-1.dvi; http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-5718-03-01563-1.pdf; http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-5718-03-01563-1.ps; http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-5718-03-01563-1.tex; http://www.jstor.org/stable/pdfplus/4099816.pdf.

Demirtas:2004:PRN

[2850] Hakan Demirtas. Pseudo-random number generation in R for commonly used multivariate distributions. *Journal of Modern Applied Statistical Methods*, 3(2):485–497, November 2004. CODEN ???? ISSN 1538-9472. URL https://jmasm.com/index.php/jmasm/article/view/159.

Deng:2004:GMP

[2851] Lih-Yuan Deng. Generalized Mersenne prime number and its application to random number generation. In Niederreiter [4236], pages 167–180. ISBN 3-540-20466-0 (softcover). LCCN Q183.9 .I526 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2004041328-d.html.

Dorfer:2004:CFE

[2852] Gerhard Dorfer, Wilfried Meidl, and Arne Winterhof. Counting functions and expected values for the lattice profile at n. *Finite Fields and their Applications*, 10(4):636–652; 1 of 1, October 2004. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579704000061`.

Espejo:2004:ANR

[2853] Mariano Ruiz Espejo and Miguel Delgado Pineda. Automatic nonuniform random variate generation. *Computational Statistics*, 19(4):659–660, December 2004. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `http://link.springer.com/article/10.1007/BF02753917`.

Feige:2004:SIR

[2854] Uriel Feige. On sums of independent random variables with unbounded variance, and estimating the average degree in a graph. In ACM [4234], pages 594–603. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

Fung:2004:AIH

[2855] E. Fung, K. Leung, N. Parimi, M. Purnaprajna, and V. C. Gaudet. ASIC implementation of a high speed WGNG for communication channel emulation [white Gaussian noise generator]. In IEEE, editor, *2004 IEEE Workshop on Signal Processing Systems Design and Implementation proceedings: October 13–15, 2004, Crowne Plaza Hotel, Austin, Texas, USA*, pages 304–309. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2004. ISBN 0-7803-8504-7. LCCN TK5102.9 .I3394 2004. URL `http://ieeexplore.ieee.org/document/1363067/`.

Goubin:2004:CLF

[2856] Louis Goubin, Christian Mauduit, and András Sárközy. Construction of large families of pseudorandom binary sequences. *Journal of Number Theory*, 106(1):56–69, May 2004. CODEN JNUTA9. ISSN 0022-314X (print), 1096-1658 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022314X04000137`.

Guan:2004:PNG

[2857] Sheng-Uei Guan and Shu Zhang. Pseudorandom number generation based on controllable cellular automata. *Future Generation Computer Systems*, 20(4):627–641, May 3, 2004. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic).

Gupta:2004:DBG

[2858] Rameshwar D. Gupta and Debasis Kundu. Discriminating between gamma and generalized exponential distributions. *Journal of Statistical Computation and Simulation*, 74(2):107–121, 2004. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Gutmann:2004:CSA

[2859] Peter Gutmann. *Cryptographic Security Architecture: Design and Verification*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 0-387-95387-6. xviii + 320 pp. LCCN QA76.9.A25 G88 2002.

Haldir:2004:HCL

[2860] R. Haldir. How to crack a linear congruential generator. Report, December 22, 2004. URL `http://www.reteam.org/papers/e59.pdf`. Web document.

Hernandez:2004:STN

[2861] Julio C. Hernandez, José María Sierra, and Andre Seznec. The SAC test: a new randomness test, with some applications to PRNG analysis. *Lecture Notes in Computer Science*, 2004:960–967, 2004. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/an44921nlaa5bf0g/`.

Hong:2004:DCT

[2862] Seokhie Hong, Deukjo Hong, Youngdai Ko, Donghoon Chang, Wonil Lee, and Sangjin Lee. Differential cryptanalysis of TEA and XTEA. *Lecture Notes in Computer Science*, 2971:402–417, 2004. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/n4exvw35x7g8t6pb/`.

Hormann:2004:ANR

[2863] Wolfgang Hörmann, Josef Leydold, and Gerhard Derflinger. *Automatic Nonuniform Random Variate Generation*. Statistics and computing, 1431-8784. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 3-540-40652-2. x + 441 pp. LCCN QA273 .H777 2004. URL `http://www.loc.gov/catdir/enhancements/fy0818/2003066410-d.html`; `http://www.loc.gov/catdir/enhancements/fy0818/2003066410-t.html`.

Jeske:2004:TAM

[2864] Daniel R. Jeske and Todd Blessinger. Tunable approximations for the mean and variance of the maximum of heterogeneous geometrically dis-

tributed random variables. *The American Statistician*, 58(4):322–327, November 2004. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Kim:2004:CNS

[2865] S. J. Kim, K. Umeno, and A. Hasegawa. Corrections of the NIST Statistical Test Suite for randomness. Technical Report 2004/018, Cryptology ePrint Archive, ????, 2004.

Kim:2004:CRN

[2866] Tae Soo Kim, Joung Nam Lee, and Jong Hyouk Kim. On the combinations of random number generators and empirical tests. *Advances and Applications in Statistics*, 4(2):155–166, August 2004. CODEN ???? ISSN 0972-3617. URL `http://www.pphmj.com/abstract/428.htm`.

Knight:2004:PDU

[2867] W. Knight. Prize draw uses heat for random numbers. *New Scientist*, 15(??):54–??, August 17, 2004. CODEN NWSCAL. ISSN 0262-4079 (print), 1364-8500 (electronic). URL `http://www.newscientist.com/article/dn6289-prize-draw-uses-heat-for-random-numbers.html`; `http://www.newscientist.com/news/news.jsp?id=ns99996289`.

LEcuyer:2004:DLR

[2868] Pierre L'Ecuyer and Renée Touzin. On the Deng–Lin random number generators and related methods. *Statistics and Computing*, 14(1):5–9, January 2004. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://dl.acm.org/citation.cfm?id=961292.961302`; `http://link.springer.com/article/10.1023/B%3ASTCO.0000009417.88960.81`.

LEcuyer:2004:PIL

[2869] Pierre L'Ecuyer. Polynomial integration lattices. In Niederreiter [4236], pages 73–98. ISBN 3-540-20466-0 (softcover). LCCN Q183.9 .I526 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2004041328-d.html`.

LEcuyer:2004:RNGa

[2870] Pierre L'Ecuyer. Random number generation. In Gentle et al. [4235], chapter II.2, pages 35–70. ISBN 3-540-40464-3. LCCN QA276.4 .H36 2004. URL `http://www.loc.gov/catdir/enhancements/fy0817/2004106523-d.html`; `http://www.loc.gov/catdir/enhancements/fy0817/2004106523-t.html`.

LEcuyer:2004:RNGb

[2871] Pierre L'Ecuyer. Random number generation and Quasi-Monte Carlo. In Teugels and Sundt [4238], pages 1363–1369. ISBN 0-470-84676-3 (hardcover). LCCN HG8781 .E47 2004. URL http://www.loc.gov/catdir/description/wiley042/2004014696.html; http://www.loc.gov/catdir/toc/ecip0419/2004014696.html. Three volumes.

Lee:2004:ECB

[2872] Po-Han Lee, Yi Chen, Soo-Chang Pei, and Yih-Yuh Chen. Evidence of the correlation between positive Lyapunov exponents and good chaotic random number sequences. *Computer Physics Communications*, 160 (3):187–203, July 15, 2004. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465504001663.

Lee:2004:GNG

[2873] Dong-U Lee, Wayne Luk, John D. Villasenor, and P. Y. K. Cheung. A Gaussian noise generator for hardware-based simulations. *IEEE Transactions on Computers*, 53(12):1523–1534, December 2004. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1347079.

Lee:2004:RNG

[2874] Lap-Piu Lee and Kwok-Wo Wong. A random number generator based on elliptic curve operations. *Computers and Mathematics and Applications*, 47(2–3):217–226, January/February 2004. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0898122104900181.

Liu:2004:SLD

[2875] Kwong-Ip Liu and Fred J. Hickernell. A scalable low discrepancy point generator for parallel computing. In Jiannong Cao, Minyi Guo, Francis Lau, and Laurence T. Yang, editors, *Parallel and Distributed Processing and Applications: Second International Symposium, ISPA 2004, Hong Kong, China, December 13–15, 2004. Proceedings*, volume 3358 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 3-540-24128-0, 3-540-30566-1. LCCN QA76.58 .I88 2004. URL http://www.springerlink.com/content/bc8n7emh9rcehny8/.

Luke:2004:DMT

[2876] Sean Luke. Documentation for the Mersenne Twister in Java. Web site., October 2004. URL `http://www.cs.gmu.edu/~sean/research/mersenne`.

Maigne:2004:PMC

[2877] Lydia Maigne, David Hill, Pascal Calvat, Vincent Breton, Romain Reuillon, Delphine Lazaro, Yannick Legre, and Denise Donnarieix. Parallelization of Monte Carlo simulations and submission to a grid environment. *Parallel Processing Letters*, 14(2):177–??, June 2004. CODEN PPLTEE. ISSN 0129-6264.

Marsaglia:2004:BURa

[2878] George Marsaglia and Wai Wan Tsang. The 64-bit universal RNG. *Statistics & Probability Letters*, 66(2):183–187, 2004. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL `http://www.doornik.com/research/randomdouble.pdf`.

Marsaglia:2004:FGD

[2879] George Marsaglia, Wai Wan Tsang, and Jingbo Wang. Fast generation of discrete random variables. *Journal of Statistical Software*, 11(3):1–8, ???? 2004. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/counter.php?id=99&url=v11/i03/discrete.pdf&ct=1`.

Martin:2004:ICF

[2880] Greg Martin and Carl Pomerance. The iterated Carmichael λ-function and the number of cycles of the power generator. *arxiv.org*, ??(??):??, June 16, 2004. URL `http://arxiv.org/abs/math/0406335`.

Mascagni:2004:PLC

[2881] Michael Mascagni and Hongmei Chi. Parallel linear congruential generators with Sophie-Germain moduli. *Parallel Computing*, 30(11):1217–1231, 2004. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Mascagni:2004:PPM

[2882] Michael Mascagni and Ashok Srinivasan. Parameterizing parallel multiplicative lagged-Fibonacci generators. *Parallel Computing*, 30(7):899–916, July 2004. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic).

Mauduit:2004:CPB

[2883] Christian Mauduit, Joël Rivat, and András Sárközy. Construction of pseudorandom binary sequences using additive characters. *Monatshefte für Mathematik*, 141(3):197–208, March 2004. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/tlp6lmgh680vawkf/`.

McCullough:2004:BRB

[2884] B. D. McCullough. Book review: *Random Number Generation and Monte Carlo Methods* by James E. Gentle. *Technometrics*, 46(2):252–253, May 2004. CODEN TCMTA2. ISSN 0040-1706 (print), 1537-2723 (electronic). URL `http://www.jstor.org/stable/25470813`.

McCullough:2004:FSE

[2885] B. D. McCullough. Fixing statistical errors in spreadsheet software: the cases of Gnumeric and Excel. *Statistical Software Newsletter*, ??(??):1–10, ???? 2004. CODEN ???? ISSN 0173-5896. URL `http://www.csdassn.org/reportdetail.cfm?ID=508`; `http://www.csdassn.org/software/reports.cfm`; `http://www.csdassn.org/software_reports/gnumeric.pdf`.

McIvor:2004:IMM

[2886] C. McIvor, M. McLoone, and J. V. McCanny. Improved Montgomery modular inverse algorithm. *Electronics Letters*, 40(18):1110–1112, September 2, 2004. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1335002`.

Mertens:2004:EPR

[2887] Stephan Mertens and Heiko Bauke. Entropy of pseudo-random-number generators. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 69(5):055702, May 2004. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.69.055702`.

Nagahara:2004:MSM

[2888] Yuichi Nagahara. A method of simulating multivariate nonnormal distributions by the Pearson distribution system and estimation. *Computational Statistics & Data Analysis*, 47(1):1–29, August 1, 2004. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947303002421`.

Ossola:2004:SED

[2889] Giovanni Ossola and Alan D. Sokal. Systematic errors due to linear congruential random-number generators with the Swendsen–Wang algorithm: a warning. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 70(2):027701, August 2004. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.70.027701`.

Panneton:2004:CEP

[2890] François Panneton. *Construction d'ensembles de points basée sur des récurrences linéaires dans un corps fini de caractéristique* 2 *pour la simulation Monte Carlo et l'intégration quasi-Monte Carlo. (French) [Construction of point sets based on linear recurrences in a finite body of characteristic* 2 *for Monte Carlo simulation and quasi-Monte Carlo integration].* Thèse (Ph.D.), Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2004. xxiv + 363 pp. Thèse présentée à la Faculté des études supérieures en vue de l'obtention du grade de Philosophiae Doctor (Ph.D.) en informatique.

Panneton:2004:RNG

[2891] François Panneton and Pierre L'Ecuyer. Random number generators based on linear recurrences in F_{2^w}. In Niederreiter [4236], pages 367–378. ISBN 3-540-20466-0 (softcover). LCCN Q183.9 .I526 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2004041328-d.html`.

Peitgen:2004:CGH

[2892] Heinz-Otto Peitgen, H. (Hartmut) Jürgens, and Dietmar Saupe. The chaos game: How randomness creates deterministic shapes. In *Chaos and fractals: new frontiers of science* [4237], chapter 7, pages 277–327. ISBN 0-387-20229-3. LCCN Q172.5.C45 P45 2004. URL `http://www.loc.gov/catdir/enhancements/fy0818/2003063341-d.html`; `http://www.loc.gov/catdir/enhancements/fy0818/2003063341-t.html`.

Rasulov:2004:QSB

[2893] Abdujabor Rasulov, Aneta Karaivanova, and Michael Mascagni. Quasirandom sequences in branching random walks. *Monte Carlo Methods and Applications*, 10(3–4):551–558, December 2004. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2004.10.issue-3-4/mcma.2004.10.3-4.551/mcma.2004.10.3-4.551.xml`.

Ryabko:2004:BSN

[2894] B. Ya. Ryabko and A. I. Pestunov. "Book Stack" as a new statistical test for random numbers. *Problems of Information Transmission*, 40 (1):66–71, January 2004. CODEN PRITA9. ISSN 0032-9460 (print), 1608-3253 (electronic). URL `http://www.springerlink.com/content/rxr43187v7p21265/`.

Ryabko:2004:NTR

[2895] B. Ya. Ryabko, V. S. Stognienko, and Y. I. Shokin. A new test for randomness and its application to some cryptographic problems. *Journal of Statistical Planning and Inference*, 123(2):365–376, July 1, 2004. CODEN JSPIDN. ISSN 0378-3758 (print), 1873-1171 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378375803001496`.

Rybakov:2004:SPL

[2896] A. S. Rybakov. Spectral properties of a linear congruential generator in special cases. *Diskret. Mat.*, 16(2):54–78, 2004. CODEN ???? ISSN 0234-0860.

Rybakov:2004:SVL

[2897] A. S. Rybakov. The shortest vectors of lattices connected with a linear congruential generator. *Diskret. Mat.*, 16(4):88–109, 2004. CODEN ???? ISSN 0234-0860.

Schmuland:2004:CLT

[2898] Byron Schmuland and Wei Sun. A Central Limit Theorem and Law of the Iterated Logarithm for a random field with exponential decay of correlations. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 56(??):209–224, ???? 2004. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Sezgin:2004:MSS

[2899] F. Sezgin. A method of systematic search for optimal multipliers in congruential random number generators. *BIT Numerical Mathematics*, 44 (1):135–149, January 2004. CODEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0006-3835&volume=44&issue=1&spage=135`.

Sugita:2004:SPR

[2900] Hiroshi Sugita. Security of pseudo-random generator and Monte Carlo method. *Monte Carlo Methods and Applications*, 10(3–4):609–615, De-

cember 2004. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2004.10.issue-3-4/mcma.2004.10.3-4.609/mcma.2004.10.3-4.609.xml`.

Szczepanski:2004:BRN

[2901] J. Szczepanski, E. Wajnryb, J. M. Amigó, Maria V. Sanchez-Vives, and M. Slater. Biometric random number generators. *Computers & Security*, 23(1):77–84, February 2004. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404804000641`.

Tang:2004:SGM

[2902] Hui-Chin Tang and Chiang Kao. Searching for good multiple recursive random number generators via a genetic algorithm. *INFORMS Journal on Computing*, 16(3):284–290, Summer 2004. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Tirler:2004:EKR

[2903] Günter Tirler, Peter Dalgaard, Wolfgang Hörmann, and Josef Leydold. An error in the Kinderman–Ramage method and how to fix it. *Computational Statistics & Data Analysis*, 47(3):433–440, October 1, 2004. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947303002937`. See [779, 1543].

Tonon:2004:URS

[2904] Fulvio Tonon. On the use of random set theory to bracket the results of Monte Carlo simulations. *Reliable Computing = Nadezhnye vychisleniia*, 10(2):107–137, April 2004. CODEN RCOMF8. ISSN 1385-3139 (print), 1573-1340 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=1385-3139&volume=10&issue=2&spage=107`.

Tsang:2004:TCT

[2905] W. W. Tsang, C. F. Chong, K. P. Chow, L. C. K. Hui, and C. W. Tso. Tuning the collision test for power. In Vladimir Estivill-Castro, editor, *Proceedings of the Twenty-Seventh Australasian Computer Science Conference (ACSC2004) Dunedin, NZ, January 2004*, volume 26 of *Conferences in research and practice in information technology*, pages 23–30. Australian Computer Society, Sydney, Australia, 2004. ISBN 1-920682-05-8. LCCN QA75.5 .A88 2004.

Tuffin:2004:RQM

[2906] Bruno Tuffin. Randomization of quasi-Monte Carlo methods for error estimation: Survey and normal approximation. *Monte Carlo Methods and Applications*, 10(3–4):617–628, December 2004. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2004.10.issue-3-4/mcma.2004.10.3-4.617/mcma.2004.10.3-4.617.xml`.

Walker:2004:HGR

[2907] J. Walker. HotBits: Genuine random numbers, generated by radioactive decay. Fourmilab Switzerland Web site., April 2004. URL `http://www.fourmilab.ch/hotbits/`.

Witkovsky:2004:MAT

[2908] Viktor Witkovský. Matlab algorithm TDIST: the distribution of a linear combination of Student's T random variables. In *COMPSTAT 2004—Proceedings in Computational Statistics*, pages 1995–2002. Physica, Heidelberg, 2004.

Wu:2004:NSC

[2909] Hongjun Wu. A new stream cipher HC-256. In B. Roy and W. Meier, editors, *Proceedings of FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 226–244. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. URL `https://iacr.org/archive/fse2004/30170226/30170226.pdf`.

Yang:2004:CBF

[2910] Hsing-Tsung Yang, Jing-Reng Huang, and Tsin-Yuan Chang. A chaos-based fully digital 120 MHz pseudo random number generator. In IEEE, editor, *Proceedings. The 2004 IEEE Asia-Pacific Conference on Circuits and Systems, 6–9 December, 2004, Tayih Landis Hotel, Tainan, Taiwan*, volume 1, pages 357–360. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2004. ISBN 0-7803-8660-4. LCCN TK5101.A1 I1187 2004; TK454.2 .I195 2004. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=9700`.

Anonymous:2005:EES

[2911] Anonymous. eSTREAM — the Ecrypt Stream Cipher Project: The eSTREAM portfolio page. Web site, 2005. URL `http://www.ecrypt.eu.org/stream/`.

Arnault:2005:DPN

[2912] F. Arnault and T. P. Berger. Design and properties of a new pseudo-random generator based on a filtered FCSR automaton. *IEEE Transactions on Computers*, 54(11):1374–1383, November 2005. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1514417`.

Balakirsky:2005:GFA

[2913] Vladimir B. Balakirsky. Generating functions associated with random binary sequences consisting of runs of lengths 1 and 2. In Helleseth et al. [4242], pages 323–338. CODEN LNCSD9. ISBN 3-540-26084-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA292 .S48 2004. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3486; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b136167`.

Banks:2005:DES

[2914] Jerry Banks, John S. Carson, Barry L. Nelson, and David M. Nicol. *Discrete-Event System Simulation*. Prentice-Hall international series in industrial and systems engineering. Pearson/Prentice-Hall, Upper Saddle River, NJ, USA, fourth edition, 2005. ISBN 0-13-129342-7, 0-13-144679-7. xvi + 608 pp. LCCN T57.62 .D53 2005.

Barak:2005:MAP

[2915] B. Barak and S. Halevi. A model and architecture for pseudo-random generation with applications to `/dev/random`. In Meadows and Syverson [4243], pages 203–212. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Beliakov:2005:CLR

[2916] Gleb Beliakov. Class library `ranlip` for multivariate nonuniform random variate generation. *Computer Physics Communications*, 170(1):93–108, July 15, 2005. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465505002596`.

Beliakov:2005:UNR

[2917] Gleb Beliakov. Universal nonuniform random vector generator based on acceptance-rejection. *ACM Transactions on Modeling and Computer Simulation*, 15(3):205–232, July 2005. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Benony:2005:CPC

[2918] Vincent Bénony, François Recher, Éric Wegrzynowski, and Caroline Fontaine. Cryptanalysis of a particular case of Klimov–Shamir pseudo-random generator. In Helleseth et al. [4242], pages 149–168. CODEN LNCSD9. ISBN 3-540-26084-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA292 .S48 2004. URL http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3486; http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b136167.

Blackburn:2005:PNP

[2919] Simon R. Blackburn, Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski. Predicting nonlinear pseudorandom number generators. *Mathematics of Computation*, 74(251):1471–1494, July 2005. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/home.html; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.dvi; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.pdf; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.ps; http://www.ams.org/mcom/2005-74-251/S0025-5718-04-01698-9/S0025-5718-04-01698-9.tex; http://www.jstor.org/stable/pdfplus/4100190.pdf.

Bogdanov:2005:PGL

[2920] Andrej Bogdanov. Pseudorandom generators for low degree polynomials. In ACM [4239], pages 21–30. ISBN 1-58113-960-8. LCCN QA75.5 A22 2005.

Calvayrac:2005:RNG

[2921] Florent Calvayrac. Random number generators and the Metropolis algorithm: application to various problems in physics and mechanics as an introduction to computational physics. *European Journal of Physics*, 26(5):S31, 2005. CODEN EJPHD4. ISSN 0143-0807 (print), 1361-6404 (electronic). URL http://stacks.iop.org/0143-0807/26/i=5/a=S04.

Castro:2005:NRG

[2922] Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of XTEA. *New Generation Computing*, 23(3):233–243, 2005. CODEN NGCOE5. ISSN 0288-3635 (print), 1882-7055 (electronic). URL http://www.springerlink.com/content/e018uh040400kh87/.

Contini:2005:SAA

[2923] Scott Contini and Igor E. Shparlinski. On Stern's attack against secret truncated linear congruential generators. *Lecture Notes in Computer Science*, 3574:180–206, 2005. CODEN LNCSD9. ISBN 3-540-26547-3. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3574`. Information Security and Privacy 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4–6, 2005. Proceedings.

Crowley:2005:TDC

[2924] P. Crowley. Truncated differential cryptanalysis of five rounds of Salsa20. In ????, editor, *Workshop Record of SASC 2006: Stream Ciphers Revisited*, page ?? ????, ????, 2005. URL `https://eprint.iacr.org/2005/375`. eSTREAM Technical Report 2005/073.

Damgaard:2005:CRM

[2925] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. *Lecture Notes in Computer Science*, 3621:378–??, 2005. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Demirtas:2005:JPR

[2926] Hakan Demirtas. JMASM 16: Pseudo-random number generation in R for some univariate distributions. *Journal of Modern Applied Statistical Methods*, 4(1):300–311, May 2005. CODEN ???? ISSN 1538-9472. URL `https://jmasm.com/index.php/jmasm/article/view/190`.

Deng:2005:EPM

[2927] Lih-Yuan Deng. Efficient and portable multiple recursive generators of large order. *ACM Transactions on Modeling and Computer Simulation*, 15(1):1–13, January 2005. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Dodge:2005:RNG

[2928] Yadolah Dodge and Giuseppe Melfi. Random number generators and rare events in the continued fraction of π. *Journal of Statistical Computation and Simulation*, 75(3):189–197, 2005. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949650410001687181`.

Eastlake:2005:RRR

[2929] D. Eastlake, 3rd, J. Schiller, and S. Crocker. RFC 4086: Randomness recommendations for security, June 2005. URL `ftp://ftp.internic.net/rfc/rfc4086.txt`; `https://www.math.utah.edu/pub/rfc/rfc4086.txt`. Status: BEST CURRENT PRACTICE. Obsoletes RFC1750.

Elsner:2005:IRN

[2930] Ulrich Elsner. The influence of random number generators on graph partitioning algorithms. *Electronic Transactions on Numerical Analysis (ETNA)*, 21:125–133, 2005. CODEN ???? ISSN 1068-9613 (print), 1097-4067 (electronic). URL `http://etna.mcs.kent.edu/vol.21.2005/pp125-133.dir/pp125-133.pdf`.

Entacher:2005:BLP

[2931] K. Entacher, T. Schell, and A. Uhl. Bad lattice points. *Computing: Archiv für Informatik und Numerik*, 75(4):281–295, August 2005. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=75&issue=4&spage=281`. See erratum [2995].

Falcioni:2005:PMC

[2932] Massimo Falcioni, Luigi Palatella, Simone Pigolotti, and Angelo Vulpiani. Properties making a chaotic system a good pseudo random number generator. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 72(1):016220, July 2005. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.72.016220`.

Gennaro:2005:IPR

[2933] Rosario Gennaro. An improved pseudo-random generator based on the discrete logarithm problem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):91–110, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=91`.

Gerlovina:2005:ABL

[2934] V. Gerlovina and V. Nekrutkin. Asymptotical behavior of linear congruential generators. *Monte Carlo Methods and Applications*, 11(2):135–162, 2005. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic).

Gong:2005:TGR

[2935] Guang Gong, Kishan Chand Gupta, Martin Hell, and Yassir Nawaz. Towards a general RC4-like keystream generator. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology: First SKLOIS Conference, CISC 2005, Beijing, China, December 15–17, 2005, Proceedings*, volume 3822 of *Lecture Notes in Computer Science*, pages 162–174. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005.

Gonnet:2005:MRG

[2936] G. Gonnet, M. Gil, and W. P. Petersen. Multiple recursive generators & the repetition test. Technical Report 476, Department of Computer Science, ETH Zürich, Zürich, Switzerland, 2005.

Gonzalez:2005:SCM

[2937] C. M. González, H. A. Larrondo, and O. A. Rosso. Statistical complexity measure of pseudorandom bit generators. *Physica A, Statistical Mechanics and its Applications*, 354(??):281–300, August 15, 2005. CODEN PHYADX. ISSN 0378-4371 (print), 1873-2119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378437105001779`.

Gubernatis:2005:MRM

[2938] J. E. Gubernatis. Marshall Rosenbluth and the Metropolis algorithm. *Physics of Plasmas*, 057303:5, May 2005. CODEN PHPAEN. ISSN 1070-664X (print), 1089-7674 (electronic), 1527-2419.

Hahn:2005:CLM

[2939] T. Hahn. Cuba — a library for multidimensional numerical integration. *Computer Physics Communications*, 168(2):78–95, June 1, 2005. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465505000792`.

Hamano:2005:DSD

[2940] K. Hamano. The distribution of the spectrum for the Discrete Fourier Transform Test included in SP800-22. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E88 (1):67–73, January 2005.

Hess:2005:LCM

[2941] Florian Hess and Igor E. Shparlinski. On the linear complexity and multidimensional distribution of congruential generators over elliptic curves.

Designs, Codes, and Cryptography, 35(1):111–117, April 2005. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic).

Hill:2005:RDS

[2942] Theodore P. Hill and Klaus Schürger. Regularity of digits and significant digits of random variables. *Stochastic Processes and Their Applications*, 115(10):1723–1743, October 2005. CODEN STOPB7. ISSN 0304-4149 (print), 1879-209X (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304414905000657`.

Hong:2005:NAT

[2943] Jin Hong and Palash Sarkar. New applications of time memory data tradeoffs. In Bimal Roy, editor, *Advances in Cryptology–ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4–8, 2005, Proceedings*, volume 11, pages 353–372. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005.

Horan:2005:NRN

[2944] D. M. Horan and R. A. Guinee. A novel random number generator based on pseudonoise sequences. *IEE Conference Publications*, 2005(CP511): 431–436, 2005. CODEN ???? ISSN ???? URL `http://link.aip.org/link/abstract/IEECPS/v2005/iCP511/p431/s1`.

Kang:2005:ETP

[2945] Mihyun Kang. Efficiency test of pseudorandom number generators using random walks. *Journal of Computational and Applied Mathematics*, 174(1):165–177, February 1, 2005. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042704001864`.

Keller:2005:NRR

[2946] Sharon S. Keller. *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*. National Institute for Standards and Technology, Gaithersburg, MD, USA, January 31, 2005. 4 pp. URL `http://csrc.nist.gov/cryptval/rng/931rngext.pdf`.

Kemp:2005:PRN

[2947] C. D. Kemp. Pseudo-random number generator. In Armitage and Colton [4240], page ?? ISBN 0-470-01181-5 (e-book), 0-470-84907-X (hardcover). LCCN QH323.5 .E53 2005. URL `http://mrw.interscience.`

wiley.com/emrw/9780470011812/home/; http://onlinelibrary.wiley.com/book/10.1002/0470011815.

Konuma:2005:DEH

[2948] Shiro Konuma and Shuichi Ichikawa. Design and evaluation of hardware pseudo-random number generator MT19937. *IEICE Transactions on Information and Systems*, 88-D(12):2876–2879, ???? 2005. ISSN 0916-8532 (print), 1745-1361 (electronic). URL http://search.ieice.org/bin/summary.php?id=e88-d_12_2876.

Kung:2005:SGT

[2949] Chingjing Kung. Searching for good two-term multiple recursive random number generators using a backpropagation algorithm. *Journal of Information & Optimization Sciences*, 26(3):527–534, 2005. CODEN JIOSDC. ISSN 0252-2667.

Larrondo:2005:ISC

[2950] H. A. Larrondo, C. M. González, M. T. Martín, A. Plastino, and O. A. Rosso. Intensive statistical complexity measure of pseudorandom number generators. *Physica A, Statistical Mechanics and its Applications*, 356(1):133–138, October 1, 2005. CODEN PHYADX. ISSN 0378-4371 (print), 1873-2119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S037843710500467X.

LEcuyer:2005:FRN

[2951] Pierre L'Ecuyer and François Panneton. Fast random number generators based on linear recurrences modulo 2: overview and comparison. In Michael Kühl et al., editors, *WSC'05: Proceedings of the 2005 Winter Simulation Conference: Hilton at the Walt Disney World Resort, Orlando, Florida, USA, December 4–7, 2005*, WSC '05, pages 110–119. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7803-9519-0. LCCN QA76.9.C65 W56 2005; T57.62. URL http://dl.acm.org/citation.cfm?id=1162708.1162732. IEEE catalog number 05CH37732.

LEcuyer:2005:PSR

[2952] Pierre L'Ecuyer and Josef Leydold. rstream: Streams of random numbers for stochastic simulation. *R News: the Newsletter of the R Project*, 5(2):16–20, November 2005. CODEN ???? ISSN 1609-3631. URL http://CRAN.R-project.org/doc/Rnews/.

Lee:2005:HGN

[2953] Dong-U Lee, Wayne Luk, John D. Villasenor, Guanglie Zhang, and Philip H. W. Leong. A hardware Gaussian noise generator using the Wallace

method. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 18(8):911–920, August 2005. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/document/1512179/`.

Leong:2005:CIZ

[2954] Philip H. W. Leong, Ganglie Zhang, and Dong-U. A comment on the implementation of the ziggurat method. *Journal of Statistical Software*, 12(7):1–44, ???? 2005. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/counter.php?id=114&url=v12/i07&ct=2;` `http://www.jstatsoft.org/counter.php?id=114&url=v12/i07/v12i07.pdf&ct=1`. See [2540].

Li:2005:ADA

[2955] Qiong Li, Sheng Ping Jin, and Ding Fang Chen. Algorithm and discrepancy analysis of compound inversive congruential pseudo-random numbers. *J. Math. (Wuhan)*, 25(2):171–174, 2005. CODEN ???? ISSN 0255-7797.

Li:2005:SEP

[2956] Huajiang Li. *A System of Efficient and Portable Multiple Recursive Generators of Large Order*. Ph.D. dissertation, Department of Mathematics, University of Memphis, Memphis, TN 38152, USA, 2005. x + 100 pp.

Li:2005:ULC

[2957] Chung-Chih Li and Bo Sun. Using linear congruential generators for cryptographic purposes. In Gongzhu Hu, editor, *Computers and their applications: proceedings of the ISCA 20th international conference; New Orleans, Louisiana, USA, March 16–18, 2005*, pages 13–19. International Society for Computers and Their Applications, Cary, NC, USA, 2005. ISBN 1-880843-54-4. LCCN QA76.76.A65 I83 2005.

Liang:2005:NPR

[2958] Heng Liang, Qinghua Liu, and Fengshan Bai. A note on a pseudo-random number generator for personal computers. *Computers and Mathematics and Applications*, 49(2–3):331–333, January/February 2005. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122105000374`.

Lim:2005:EMT

[2959] Daihyun Lim, Damith C. Ranasinghe, Srinivas Devadas, Behnam Jamali, Derek Abbott, and Peter H. Cole. Exploiting metastability and thermal

noise to build a reconfigurable hardware random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 5844(1):294–309, 2005. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/5844/294/1`. Noise in Devices and Circuits III.

Louchard:2005:MRU

[2960] Guy Louchard. Monotone runs of uniformly distributed integer random variables: a probabilistic analysis. *Theoretical Computer Science*, 346 (2–3):358–387, November 28, 2005. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Marsaglia:2005:MGF

[2961] George Marsaglia. Monkeying with the goodness-of-fit test. *Journal of Statistical Software*, 14(13):1–4, September 20, 2005. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/counter.php?id=138&url=v14/i13&ct=2;` `http://www.jstatsoft.org/counter.php?id=138&url=v14/i13/v14i13.pdf&ct=1`.

Marsaglia:2005:RPO

[2962] George Marsaglia. On the randomness of pi and other decimal expansions. *InterStat: statistics on the Internet*, page 17, October 2005. CODEN ???? ISSN 1941-689X. URL `http://interstat.statjournals.net/INDEX/Oct05.html;` `http://interstat.statjournals.net/YEAR/2005/articles/0510005.pdf`.

McCullough:2005:ASP

[2963] B. D. McCullough and Berry Wilson. On the accuracy of statistical procedures in Microsoft Excel 2003. *Computational Statistics & Data Analysis*, 49(4):1244–1252, June 15, 2005. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947304002026`.

Nawaz:2005:BRL

[2964] Yassir Nawaz, Kishan Chand Gupta, and Guang Gong. A 32-bit RC4-like keystream generator. Technical report, Cryptology ePrint Archive, 2005. 175–188 (??) pp. URL `https://eprint.iacr.org/2005/175`.

Niederreiter:2005:CNS

[2965] H. Niederreiter. Constructions of (t, m, s)-nets and (t, s)-sequences. *Finite Fields and their Applications*, 11(3):578–600, August 2005. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579705000043`.

Niederreiter:2005:DSN

[2966] Harald Niederreiter and Arne Winterhof. On the distribution of some new explicit nonlinear congruential pseudorandom numbers. In Helleseth et al. [4242], pages 266–274. CODEN LNCSD9. ISBN 3-540-26084-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA292 .S48 2004. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3486`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b136167`.

Niederreiter:2005:ESD

[2967] Harald Niederreiter and Arne Winterhof. Exponential sums and the distribution of inversive congruential pseudorandom numbers with power of two modulus. *International Journal of Number Theory*, 1(3):431–438, September 2005. CODEN ???? ISSN 1793-0421 (print), 1793-7310 (electronic). URL `https://www.worldscientific.com/doi/10.1142/S1793042105000261`.

Panneton:2005:XRN

[2968] François Panneton and Pierre L'Ecuyer. On the xorshift random number generators. *ACM Transactions on Modeling and Computer Simulation*, 15(4):346–361, October 2005. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). See [2802, 2846, 3888].

Raqab:2005:BIG

[2969] Mohamed Z. Raqab and Mohamed T. Madi. Bayesian inference for the generalized exponential distribution. *Journal of Statistical Computation and Simulation*, 75(10):841–852, 2005. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Redei:2005:JNS

[2970] Miklós Rédei. *John von Neumann selected letters*, volume 27 of *History of mathematics*. American Mathematical Society, Providence, RI, USA, 2005. ISBN 0-8218-3776-1 (hardcover). ISSN 0899-2428. xxv + 301 pp. LCCN QA29.V66 A4 2005.

RFC4086

[2971] D. Eastlake, 3rd, J. Schiller, and S. Crocker. Randomness requirements for security. RFC4086, June 2005. URL `https://www.rfc-editor.org/rfc/rfc4086.txt`.

Ryabko:2005:NTA

[2972] B. Y. Ryabko, V. A. Monarev, and Y. I. Shokin. A new type of attack on block ciphers. *Problems of Information Transmission*, 41(4):385–394, ???? 2005. CODEN PRITA9. ISSN 0032-9460 (print), 1608-3253 (electronic).

Ryabko:2005:UIT

[2973] B. Ya. Ryabko and V. A. Monarev. Using information theory approach to randomness testing. *Journal of Statistical Planning and Inference*, 133(1):95–110, July 2005. CODEN JSPIDN. ISSN 0378-3758 (print), 1873-1171 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378375804001144`.

Saitoh:2005:GPR

[2974] Y. Saitoh, J. Hori, and T. Kiryu. Generation of physical random number using frequency-modulated LC oscillation circuit with shot noise. *Electron Comm. Jpn.*, 3(388):12–??, ???? 2005. URL `????`.

Schreck:2005:DDG

[2975] Erhard Schreck and Wolfgang Ertel. Disk drive generates high speed real random numbers. *Microsystem Technologies: Sensors, Actuators, Systems Integration*, 11(8–10):616–622, August 2005. CODEN MCTCEF. ISSN 0946-7076 (print), 1432-1858 (electronic). URL `http://www.springerlink.com/content/w758310x8v52640r/`.

Shaltiel:2005:SEA

[2976] Ronen Shaltiel and Christopher Umans. Simple extractors for all min-entropies and a new pseudorandom generator. *Journal of the ACM*, 52 (2):172–216, March 2005. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Sidorenko:2005:CSB

[2977] A. Sidorenko and B. Schoenmakers. Concrete security of the Blum–Blum–Shub pseudorandom generator. In Smart [4244], pages 355–375. CODEN LNCSD9. ISBN 3-540-30276-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/978-3-540-30276-6; http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3796`.

Smith:2005:AAM

[2978] J. Cole Smith and Sheldon H. Jacobson. An analysis of the alias method for discrete random-variate generation. *INFORMS Journal on Comput-*

ing, 17(3):321–327, Summer 2005. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Stoklosa:2005:CIC

[2979] Janusz Stoklosa and Jaroslaw Bubicz. Compound inversive congruential generator as a source of keys for stream ciphers. In Hamid R. Arabnia, Liwen He, and Youngsong Mun, editors, *Proceedings of the 2005 International Conference on Security and Management, SAM '05: Las Vegas, Nevada, USA, June 20-23, 2005*, pages 473–478. CSREA Press, Las Vegas, NV, USA, 2005. ISBN 1-932415-82-3. LCCN TK5105.59 .I57 2005.

Tang:2005:EER

[2980] Hui-Chin Tang. Effective and efficient restriction on producing the multipliers for the multiple recursive random number generator. *Computers and Mathematics and Applications*, 47(8–9):1309–1315, April/May 16, 2004. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122104901241`.

Tang:2005:MLC

[2981] Hui-Chin Tang. Modulus of linear congruential random number generator. *Quality & Quantity*, 39(4):413–422, August 2005. CODEN QQEJAV. ISSN 0033-5177 (print), 1573-7845 (electronic). URL `http://www.springerlink.com/content/h051r275k8615v75/`.

Tang:2005:RMR

[2982] Hui-Chin Tang. Reverse multiple recursive random number generators. *European Journal of Operational Research*, 164(2):402–405, July 16, 2005. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377221704000396`.

Terpstra:2005:SIC

[2983] Jeff T. Terpstra. Some illustrative classroom examples regarding sums of discrete random variables with finite support. *The American Statistician*, 59(3):258–265, August 2005. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Topuzoglu:2005:LCP

[2984] Alev Topuzoglu and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher

orders. *Applicable algebra in engineering, communication and computing*, 16(4):219–228, 2005. CODEN AAECEW. ISSN 0938-1279 (print), 1432-0622 (electronic).

Tu:2005:SRD

[2985] Shu-Ju Tu and Ephraim Fischbach. A study on the randomness of the digits of π. *International Journal of Modern Physics C [Physics and Computers]*, 16(2):281–294, February 2005. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/16/1602/S01291831051602.html`. The statistical analysis in this work is flawed; see [2962, 3039].

Wichmann:2005:GGP

[2986] B. A. Wichmann and I. D. Hill. Generating good pseudo-random numbers. Report, National Physical Laboratory, Teddington, UK, December 5, 2005. URL `http://resource.npl.co.uk/docs/science_technology/scientific_computing/ssfm/documents/wh_rng_version096.zip`.

Wiese:2005:IPN

[2987] Kay C. Wiese, Andrew Hendriks, Alain Deschenes, and Belgacem Ben Youssef. The impact of pseudorandom number quality on P-RnaPredict, a parallel genetic algorithm for RNA secondary structure prediction. In Beyer et al. [4241], pages 479–480. ISBN 1-59593-010-8 (paperback). LCCN QA76.623 .G44 2005. URL `http://www.cs.bham.ac.uk/~wbl/biblio/gecco2005lbp/papers/52-wiese.pdf`. ACM order number 910050.

Wiese:2005:PRP

[2988] Kay C. Wiese, Andrew Hendriks, Alain Deschenes, and Belgacem Ben Youssef. P-RnaPredict — a parallel evolutionary algorithm for RNA folding: effects of pseudorandom number quality. *IEEE Transactions on Nanobioscience*, 4(3):219–227, September 2005. ISSN 1536-1241.

Wu:2005:CBR

[2989] Hongjin Wu. Cryptanalysis of a 32-bit RC4-like stream cipher. Paper 2005/219, Cryptology ePrint Archive, ????, 2005. URL `https://eprint.iacr.org/2005/219`. See [2964].

Zhang:2005:ZBH

[2990] Guanglie Zhang, Philip H. W. Leong, Dong-U Lee, John D. Villasenor, Ray C. C. Cheung, and Wayne Luk. Ziggurat-based hardware Gaussian

random number generator. In IEEE, editor, *2005 International Conference on Field Programmable Logic and Applications(FPL): Tampere Hall, Tampere, Finland, August 24–26, 2005*, pages 275–280. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2005. ISBN 0-7803-9362-7. LCCN TK7895.G36 I33 2005. URL `http://ieeexplore.ieee.org/document/1515734/`; `http://www.ee.usyd.edu.au/people/philip.leong/UserFiles/File/papers/zig_fpl05.pdf`; `https://courses.cs.washington.edu/courses/cse591n/07wi/papers/fpl05_dul98.pdf`.

Zuquete:2005:EHQ

[2991] André Zúquete. An efficient high quality random number generator for multi-programmed systems. *Journal of Computer Security*, 13(2): 243–263, March 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic). URL `http://dl.acm.org/citation.cfm?id=1077819.1077821`.

Aistleitner:2006:NZG

[2992] Christoph Aistleitner. *Normale Zahlen. (German) [Normal Numbers]*. Diplomarbeit, Technische Universität Wien, Vienna, Austria, January 23, 2006. URL `http://www.geometrie.tuwien.ac.at/drmota/Diplomarbeit_Aistleitner.ps`.

Alon:2006:MPF

[2993] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl. Measures of pseudorandomness for finite sequences: Minimal values. *Combinatorics, Probability and Computing*, 15(1–2):1–29, January 2006. CODEN CPCOFG. ISSN 0963-5483 (print), 1469-2163 (electronic). URL `http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=15&issueId=01`.

Aly:2006:LCP

[2994] Hassan Aly and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials. *Designs, Codes, and Cryptography*, 39(2):155–162, May 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=2&spage=155`.

Anonymous:2006:E

[2995] Anonymous. Erratum. *Computing: Archiv für Informatik und Numerik*, 77(1):129, February 2006. CODEN CMPTA2. ISSN 0010-485X

(print), 1436-5057 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=77&issue=1&spage=129. See [2931].

Barak:2006:ERU

[2996] Boaz Barak, Russell Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. *SIAM Journal on Computing*, 36(4):1095–1118, ???? 2006. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Barash:2006:POE

[2997] L. Barash and L. N. Shchur. Periodic orbits of the ensemble of Sinai–Arnold cat maps and pseudorandom number generation. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 73(3):036701, March 2006. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.73.036701.

Barker:2006:RRN

[2998] Elaine Barker and John Kelsey. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. National Institute for Standards and Technology, Gaithersburg, MD, USA, 2006. viii + 123 pp. URL http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90_DRBG-June2006-final.pdf.

BenAtti:2006:BMA

[2999] Nadia Ben Atti, Gema M. Diaz-Toca, and Henri Lombardi. The Berlekamp–Massey algorithm revisited. *Applicable Algebra in Engineering, Communication, and Computing*, 17(1):75–82, April 2006. CODEN ???? ISSN 0938-1279 (print), 1432-0622 (electronic).

Berkovitz:2006:EHR

[3000] Joseph Berkovitz, Roman Frigg, and Fred Kronz. The ergodic hierarchy, randomness and Hamiltonian chaos. *Studies in History and Philosophy of Modern Physics*, 37(4):661–691, December 2006. CODEN ???? ISSN 1355-2198 (print), 1879-2502 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1355219806000700.

Brent:2006:FRR

[3001] Richard P. Brent. Fast and reliable random number generators for scientific computing. *Lecture Notes in Computer Science*, 3732:1–10, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Brent:2006:SLP

[3002] Richard Peirce Brent. Some long-period random number generators using shifts and xors. *The ANZIAM Journal*, 48(??):C188–C202 (2009), 2006. CODEN AJNOA2. ISSN 1446-1811 (print), 1446-8735 (electronic). URL http://arxiv.org/abs/1004.3115; https://journal.austms.org.au/ojs/index.php/ANZIAMJ/article/view/40; https://maths-people.anu.edu.au/~brent/pd/rpb224.pdf; https://maths-people.anu.edu.au/~brent/random.html.

Cools:2006:CEL

[3003] Ronald Cools, Frances Y. Kuo, and Dirk Nuyens. Constructing embedded lattice rules for multivariate integration. *SIAM Journal on Scientific Computing*, 28(6):2162–2188, January 2006. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic).

Creutzig:2006:BRW

[3004] Jakob Creutzig. Book review: W. Hörmann, J. Leydold, G. Derflinger: *Automatic nonuniform random variate generation. Metrika. International Journal for Theoretical and Applied Statistics.*, 64(2):247–248, October 2006. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00184-006-0087-2.

Devroye:2006:NRV

[3005] Luc Devroye. Chapter 4: Nonuniform random variate generation. In Henderson and Nelson [4245], pages 83–121. ISBN 0-444-51428-7. LCCN HG176.7 .F56 2008. URL http://www.sciencedirect.com/science/article/pii/S0927050706130042.

Dick:2006:WSD

[3006] J. Dick, H. Niederreiter, and F. Pillichshammer. Weighted star discrepancy of digital nets in prime bases. In Niederreiter and Talay [4246], pages 77–96. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html; http://www.loc.gov/catdir/toc/fy0614/2005930449.html.

Dickinson:2006:EEL

[3007] A. Dickinson. Explaining effective low-dimensionality. In Niederreiter and Talay [4246], pages 97–112. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html; http://www.loc.gov/catdir/toc/fy0614/2005930449.html.

El-Mahassni:2006:DNC

[3008] Edwin D. El-Mahassni, Igor E. Shparlinski, and Arne Winterhof. Distribution of nonlinear congruential pseudorandom numbers modulo almost squarefree integers. *Monatshefte für Mathematik*, 148(4):297–307, August 2006. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/a57353180vx75415/`.

Evans:2006:DOS

[3009] Diane L. Evans, Lawrence M. Leemis, and John H. Drew. The distribution of order statistics for discrete random variables with applications to bootstrapping. *INFORMS Journal on Computing*, 18(1):19–30, Winter 2006. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Faure:2006:SCR

[3010] H. Faure. Selection criteria for (random) generation of digital $(0, s)$-sequences. In Niederreiter and Talay [4246], pages 113–126. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Feige:2006:SIR

[3011] Uriel Feige. On sums of independent random variables with unbounded variance and estimating the average degree in a graph. *SIAM Journal on Computing*, 35(4):964–984, ???? 2006. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Finnigin:2006:CPN

[3012] Kevin M. Finnigin. Cryptanalysis of pseudorandom number generators in wireless sensor networks. Master's thesis, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA, 2006.

Galperin:2006:SSU

[3013] E. A. Galperin and I. Galperin. Small sample uniformity in random number generation. *Computers and Mathematics and Applications*, 52(1–2):95–108, July 2006. CODEN CMAPDK. ISSN 0898-1221 (print), 1873-7668 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0898122106001842`.

Gammel:2006:LFN

[3014] Berndt M. Gammel and Rainer Göttfert. Linear filtering of nonlinear shift-register sequences. In Ytrehus [4248], pages 354–370. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

Gennaro:2006:RC

[3015] Rosario Gennaro. Randomness in cryptography. *IEEE Security & Privacy*, 4(2):64–67, March/April 2006. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Gil:2006:RTP

[3016] Manuel Gil, Gaston H. Gonnet, and Wesley P. Petersen. A repetition test for pseudo-random number generators. *Monte Carlo Methods and Applications*, 12(5–6):385–393, ???? 2006. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2006.12.issue-5/156939606779329017/156939606779329017.xml`; `http://www.inf.ethz.ch/personal/gonnet/RepetitionTest.html`.

Gomez-Perez:2006:ESD

[3017] Domingo Gomez-Perez, Jaime Gutierrez, and Igor E. Shparlinski. Exponential sums with Dickson polynomials. *Finite Fields and their Applications*, 12(1):16–25, January 2006. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579704000401`.

Goodman:2006:SRN

[3018] Joseph K. Goodman and Julie R. Irwin. Special random numbers: Beyond the illusion of control. *Organizational Behavior and Human Decision Processes*, 99(2):161–174, March 2006. CODEN OBDPFO. ISSN 0749-5978 (print), 1095-9920 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0749597805001123`.

Gutterman:2006:ALR

[3019] Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the Linux random number generator. Report, The Hebrew University of Jerusalem and University of Haifa, Jerusalem and Haifa, Israel, March 6, 2006. 18 pp. URL `http://www.pinkas.net/PAPERS/gpr06.pdf`.

Hanley:2006:PFR

[3020] James A. Hanley and Dana Teltsch. The PDF of a function of a random variable. *The American Statistician*, 60(1):61–67, February 2006. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Hars:2006:MIA

[3021] Laszlo Hars. Modular inverse algorithms without multiplications for cryptographic applications. *EURASIP Journal on Embedded Systems*, 2006:1–13, 2006. CODEN ???? ISSN 1687-3955 (print), 1687-3963 (electronic). URL `http://downloads.hindawi.com/journals/es/2006/032192.pdf`. Article ID 32192.

Hartinger:2006:NUL

[3022] J. Hartinger and R. Kainhofer. Non-uniform low-discrepancy sequence generation and integration of singular integrands. In Niederreiter and Talay [4246], pages 163–179. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Hechenleitner:2006:PSG

[3023] Bernhard Hechenleitner and Karl Entacher. A parallel search for good lattice points using LLL-spectral tests. *Journal of Computational and Applied Mathematics*, 189(1–2):424–441, May 1, 2006. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042705001652`.

Hong:2006:DRN

[3024] Jinkeun Hong, Kihong Kim, and Dongcheul Son. The design of random number generator in an embedded crypto module. *Lecture Notes in Computer Science*, 4331:990–999, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/m76315733120854t/`. Proceedings of Frontiers of High Performance Computing and Networking — ISPA 2006 Workshops.

Indyk:2006:SDP

[3025] Piotr Indyk. Stable distributions, pseudorandom generators, embeddings, and data stream computation. *Journal of the ACM*, 53(3):307–323, May 2006. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Joe:2006:CGR

[3026] S. Joe. Construction of good rank-1 lattice rules based on the weighted star discrepancy. In Niederreiter and Talay [4246], pages 181–196. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Kossovsky:2006:TBU

[3027] Alex Ely Kossovsky. Towards a better understanding of the leading digits phenomena. *CoRR*, 2006. CODEN ???? ISSN ???? URL `http://arxiv.org/abs/math/0612627`.

Kuipers:2006:UDS

[3028] Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Dover Publications, Inc., New York, NY, USA, 2006. ISBN 0-486-45019-8 (paperback). xviii + 390 pp. LCCN QA292 .K84 2006. URL `http://www.loc.gov/catdir/enhancements/fy0625/2005056064-d.html`; `http://www.loc.gov/catdir/toc/fy0612/2005056064.html`.

Kundu:2006:JCW

[3029] Debasis Kundu, Anubhav Manglick, and Rameshwar D. Gupta. JMASM 22: a convenient way of generating normal random variables using generalized exponential distribution. *Journal of Modern Applied Statistical Methods*, 5(1):266–272, May 2006. CODEN ???? ISSN 1538-9472. URL `https://jmasm.com/index.php/jmasm/article/view/242`.

Kung:2006:BML

[3030] Ching-Jing Kung. 32-bit multipliers for linear congruential random number generators. *Journal of Discrete Mathematical Sciences and Cryptography*, 9(3):441–448, 2006. CODEN ???? ISSN 0972-0529.

Lamenca-Martinez:2006:LNP

[3031] Carlos Lamenca-Martinez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Lamar: a new pseudorandom number generator evolved by means of genetic programming. *Lecture Notes in Computer Science*, 4193:850–859, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/c60q42qt2m035685/`.

Law:2006:SMA

[3032] Averill M. Law. *Simulation modeling and analysis*. McGraw-Hill series in industrial engineering and management science. McGraw-Hill, New York, NY, USA, fourth edition, 2006. ISBN 0-07-298843-6 (hardcover), 0-07-125519-2 (paperback), 0-07-329441-1, 0-07-110336-8, 0-07-110051-2. xix + 768 pp. LCCN QA76.9.C65 L38 2005. URL `http://catdir.loc.gov/catdir/toc/ecip0611/2006010073.html`.

LEcuyer:2006:CUR

[3033] Pierre L'Ecuyer. Chapter 3: Uniform random number generation. In Henderson and Nelson [4245], pages 55–81. ISBN 0-444-51428-7. LCCN

HG176.7 .F56 2008. URL http://www.sciencedirect.com/science/article/pii/S0927050706130030.

LEcuyer:2006:ISB

[3034] Pierre L'Ecuyer and Richard Simard. Inverting the symmetrical beta distribution. *ACM Transactions on Mathematical Software*, 32(4):509–520, December 2006. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

LEcuyer:2006:TSL

[3035] Pierre L'Ecuyer and Richard Simard. TestU01, a software library in ANSI C for empirical testing of random number generators. Report ??, Département d Informatique et de Recherche Operationnelle, Université de Montréal, Montréal, QC, Canada, 2006. ???? pp.

Lee:2006:HGN

[3036] Dong-U Lee, John D. Villasenor, Wayne Luk, and Philip H. W. Leong. A hardware Gaussian noise generator using the Box–Muller method and its error analysis. *IEEE Transactions on Computers*, 55(6):659–671, June 2006. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1628955.

Lee:2006:IBH

[3037] Dong-U Lee, Ray C. C. Cheung, John D. Villasenor, and Wayne Luk. Inversion-based hardware Gaussian random number generator: A case study of function evaluation via hierarchical segmentation. In George A. Constantinides, editor, *2006 IEEE International Conference on Field Programmable Technology: December 13-15, 2006, Bangkok, Thailand: proceedings*, pages 33–40. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7803-9728-2. LCCN TK7895.G36 I33 2006. URL http://ieeexplore.ieee.org/document/4042413/.

Maffre:2006:WKT

[3038] Samuel Maffre. A weak key test for braid based cryptography. *Designs, Codes, and Cryptography*, 39(3):347–373, June 2006. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=39&issue=3&spage=347.

Marsaglia:2006:RCS

[3039] George Marsaglia. Refutation of claims such as "Pi is less random than we thought". *InterStat: statistics on the Internet*, January 23, 2006. CODEN ???? ISSN 1941-689X. URL `http://interstat.statjournals.net/YEAR/2006/articles/0601001.pdf`.

Matsumoto:2006:PNG

[3040] M. Matsumoto, M. Saito, H. Haramoto, and T. Nishimura. Pseudorandom number generation: Impossibility and compromise. *J.UCS: Journal of Universal Computer Science*, 12(6):672–690, ???? 2006. CODEN ???? ISSN 0948-6968. URL `http://www.jucs.org/jucs_12_6/pseudorandom_number_generation_impossibility`.

Matsumoto:2006:UPN

[3041] Makoto Matsumoto. To the users of pseudorandom number generators—from a developer of Mersenne Twister. *J. Japan Statist. Soc.*, 35(2, Japanese Issue):165–180, 2006. CODEN ???? ISSN 0389-5602.

McCullough:2006:RT

[3042] B. D. McCullough. A review of TESTU01. *Journal of Applied Econometrics*, 21(5):677–682, July/August 2006. CODEN JAECET. ISSN 0883-7252 (print), 1099-1255 (electronic). URL `http://www.jstor.org/stable/25146455`.

Miller:2006:MCL

[3043] S. J. Miller and M. J. Nigrini. The Modulo 1 Central Limit Theorem and Benford's Law for products. *International Journal of Algebra*, 3(3):119–130, July 2006. CODEN ???? ISSN 1312-8868. URL `http://adsabs.harvard.edu/abs/2006math.....7686M`; `http://arxiv.org/abs/math/0607686`.

Mueller:2006:SMG

[3044] Maik Mueller, Michael Freidrich, Klaus Kiefer, Ralf Miko, and Juergen Schneider. System and method for generating pseudo-random numbers. United States Patent 7,894,602., March 31, 2006. URL `http:www.google.com/patents/US7894602`.

Nau:2006:RN

[3045] Richard W. Nau. A random number. *SIGCSE Bulletin (ACM Special Interest Group on Computer Science Education)*, 38(3):345, September 2006. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Nuyens:2006:FAC

[3046] Dirk Nuyens and Ronald Cools. Fast algorithms for component-by-component construction of rank-1 lattice rules in shift-invariant reproducing kernel Hilbert spaces. *Mathematics of Computation*, 75(254): 903–920, April 2006. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/mcom/2006-75-254/S0025-5718-06-01785-6/home.html`; `http://www.ams.org/mcom/2006-75-254/S0025-5718-06-01785-6/S0025-5718-06-01785-6.dvi`; `http://www.ams.org/mcom/2006-75-254/S0025-5718-06-01785-6/S0025-5718-06-01785-6.pdf`; `http://www.ams.org/mcom/2006-75-254/S0025-5718-06-01785-6/S0025-5718-06-01785-6.ps`.

Nuyens:2006:FCCa

[3047] D. Nuyens and R. Cools. Fast component-by-component construction, a reprise for different kernels. In Niederreiter and Talay [4246], pages 373–387. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Nuyens:2006:FCCb

[3048] Dirk Nuyens and Ronald Cools. Fast component-by-component construction of rank-1 lattice rules with a non-prime number of points. *Journal of Complexity*, 22(1):4–28, February 2006. CODEN JOCOEH. ISSN 0885-064X (print), 1090-2708 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0885064X05000658`.

Panneton:2006:IDH

[3049] F. Panneton and P. L'Ecuyer. Infinite-dimensional highly-uniform point sets defined via linear recurrences in $\mathbf{F}_{2^w}$. In Niederreiter and Talay [4246], pages 419–429. ISBN 3-540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Panneton:2006:ILP

[3050] François Panneton, Pierre L'Ecuyer, and Makoto Matsumoto. Improved long-period generators based on linear recurrences modulo 2. *ACM Transactions on Mathematical Software*, 32(1):1–16, March 2006. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Polack:2006:CHR

[3051] Jean-Dominique Polack. Are concert halls random number generators? *Journal of the Acoustical Society of America*, 120(5):3101, ???? 2006.

CODEN JASMAN. ISSN 0001-4966. URL `http://asadl.org/jasa/resource/1/jasman/v120/i5/p3101_s4`.

Purczynski:2006:FGF

[3052] Jan Purczyński and Przemysław Włodarski. On fast generation of fractional Gaussian noise. *Computational Statistics & Data Analysis*, 50 (10):2537–2551, June 20, 2006. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947305001003`.

Rinehart:2006:PRN

[3053] Nicole J. Rinehart, John L. Bradshaw, Simon A. Moss, Avril V. Brereton, and Bruce J. Tonge. Pseudo-random number generation in children with high-functioning autism and Asperger's disorder: further evidence for a dissociation in executive functioning? *Autism : the international journal of research and practice*, 10(1):70–85, January 2006. ISSN 1362-3613.

Ripley:2006:SS

[3054] Brian D. Ripley. *Stochastic Simulation*. Wiley series in probability and statistics. Wiley-Interscience, New York, NY, USA, 2006. ISBN 0-470-00960-8. xi + 237 pp. LCCN QA76.9.C65 R57 2006.

Rose:2006:CSP

[3055] Gregory Gordon Rose, Alexander Gantman, and Lu Xiao. Cryptographically secure pseudo-random number generator. United States Patent 8,019,802., August 23, 2006. URL `http:www.google.com/patents/US8019802`.

Rubin:2006:EGE

[3056] Herman Rubin and Brad C. Johnson. Efficient generation of exponential and normal deviates. *Journal of Statistical Computation and Simulation*, 76(6):509–518, June 2006. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/10629360500108004`.

Rybakov:2006:LES

[3057] A. S. Rybakov. Letter to the editors: "Spectral properties of a linear congruential generator in special cases" (Russian) [Diskret. Mat. **16** (2004), no. 2, 54–78; MR2084569]. *Diskret. Mat.*, 18(1):158, 2006. CODEN ???? ISSN 0234-0860.

Schanze:2006:EDT

[3058] Thomas Schanze. An exact D-dimensional Tsallis random number generator for generalized simulated annealing. *Computer Physics Communi-*

cations, 175(11–12):708–712, December 1–15, 2006. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465506002980`.

Schmidt:2006:BRJ

[3059] Volker Schmidt. Book review: James E. Gentle: *Random number generation and Monte Carlo methods. Metrika. International Journal for Theoretical and Applied Statistics.*, 64(2):251–252, October 2006. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00184-006-0089-0`.

Schroeder:2006:RNG

[3060] Manfred R. Schroeder. *Random Number Generators*, chapter 27, pages 287–292. Volume 7 of *Springer Series in Information Sciences* [4247], fourth edition, 2006. ISBN 3-540-26598-8, 3-540-26596-1. ISSN 0720-678X. LCCN QA241.

Sezgin:2006:DLP

[3061] F. Sezgin. Distribution of lattice points. *Computing: Archiv für Informatik und Numerik*, 78(2):173–193, October 2006. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=78&issue=2&spage=173`.

Simka:2006:MTR

[3062] M. Simka, V. Fischer, M. Drutarovsky, and J. Fayolle. Model of a true random number generator aimed at cryptographic application. In *ISCAS 2006: 2006 IEEE International Symposium on Circuits and Systems: Circuits and systems: at crossroads of life and technology: proceedings: May 21–24: Kos International Convention Centre (KICC), Island of Kos, Greece*, pages 5619–5623. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 0-7803-9390-2. LCCN TK454 .I15 2006. URL `http://www.ieeexplore.ieee.org/xpl/RecentCon.jsp?punumber=11145`. IEEE catalog number 06CH37717C.

Skoge:2006:PHH

[3063] Monica Skoge, Aleksandar Donev, Frank H. Stillinger, and Salvatore Torquato. Packing hyperspheres in high-dimensional Euclidean spaces. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 74(4):041127, October 2006. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.74.041127`.

Steinfeld:2006:PSE

[3064] Ron Steinfeld, Josef Pieprzyk, and Huaxiong Wang. On the provable security of an efficient RSA-based pseudorandom generator. *Lecture Notes in Computer Science*, 4284:194–209, 2006. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/content/pdf/10.1007/11935230_13.pdf`.

Tang:2006:EAT

[3065] Hui-Chin Tang. An exhaustive analysis of two-term multiple recursive random number generators with efficient multipliers. *Journal of Computational and Applied Mathematics*, 192(2):411–416, August 2006. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://dl.acm.org/citation.cfm?id=1148032.1148047`.

Tang:2006:TAF

[3066] Hui-Chin Tang. Theoretical analyses of forward and backward heuristics of multiple recursive random number generators. *European Journal of Operational Research*, 174(3):1760–1768, November 1, 2006. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377221705003887`.

Thomas:2006:NUR

[3067] David B. Thomas and Wayne Luk. Non-uniform random number generation through piecewise linear approximations. In Koen Bertels, Philip Leong, and Eduardo Boemo, editors, *International Conference on Field Programmable Logic and Applications, 2006: FPL '06, 28–30 August 2006, Madrid, Spain: proceedings*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN 1-4244-0312-X. LCCN TK7895.G36 I48 2006. URL `http://ieeexplore.ieee.org/document/4100981/`.

Wang:2006:SQR

[3068] P. X. Wang, G. L. Long, and Y. S. Li. Scheme for a quantum random number generator. *Journal of Applied Physics*, 100(5):056107, 2006. CODEN JAPIAU. ISSN 0021-8979 (print), 1089-7550 (electronic), 1520-8850. URL `http://link.aip.org/link/?JAP/100/056107/1`.

Wichmann:2006:GGP

[3069] B. A. Wichmann and I. D. Hill. Generating good pseudo-random numbers. *Computational Statistics & Data Analysis*, 51(3):1614–1622, December 1, 2006. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947306001836`. This work extends a widely-used

generator [1053] developed for 16-bit arithmetic to a new four-part combination generator for 32-bit arithmetic with a period of $2^{121} \approx 10^{36}$.

Wu:2006:PUM

[3070] Pei-Chi Wu and Kuo-Chan Huang. Parallel use of multiplicative congruential random number generators. *Computer Physics Communications*, 175(1):25–29, July 2006. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465506001007`.

Xu:2006:CFG

[3071] P. Xu, Y. L. Wong, T. K. Horiuchi, and P. A. Abshire. Compact floating-gate true random number generator. *Electronics Letters*, 42 (23):1346–1347, November 9, 2006. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4027820`.

Atman:2007:ATA

[3072] Micah Atman, Jeff Gill, and Michael P. McDonald. `accuracy`: Tools for accurate and reliable statistical computing. *Journal of Statistical Software*, 21(1):1–30, July 2007. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v21/i01`.

Aumasson:2007:BR

[3073] Jean-Philippe Aumasson. On a bias of Rabbit. In ????, editor, *State of the Art of Stream Ciphers Workshop (SASC 2007), eSTREAM, ECRYPT Stream Cipher Project, Report*, volume 29, page ?? ????, ????, 2007. URL `https://www.aumasson.jp/data/papers/Aum07.pdf`; `https://www.researchgate.net/publication/252292685_On_a_bias_of_Rabbit`.

Barker:2007:RRN

[3074] Elaine B. Barker and John M. Kelsey. *Recommendation for random number generation using deterministic random bit generators (revised)*. National Institute for Standards and Technology, Gaithersburg, MD, USA, March 2007. viii + 124 pp. URL `http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf`; `https://www.nist.gov/publications/recommendation-random-number-generation-using-deterministic-random-bit-generators-2`.

Bauke:2007:RNL

[3075] Heiko Bauke and Stephan Mertens. Random numbers for large-scale distributed Monte Carlo simulations. *Physical Review E (Statistical*

physics, plasmas, fluids, and related interdisciplinary topics), 75(6(part 2)):066701, June 2007. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL `http://pre.aps.org/abstract/PRE/v75/i6/e066701`.

Becher:2007:TUA

[3076] Verónica Becher, Santiago Figueira, and Rafael Picchi. Turing's unpublished algorithm for normal numbers. *Theoretical Computer Science*, 377 (1–3):126–138, May 31, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Bhatnagar:2007:ANB

[3077] Shalabh Bhatnagar. Adaptive Newton-based multivariate smoothed functional algorithms for simulation optimization. *ACM Transactions on Modeling and Computer Simulation*, 18(1):2:1–2:35, December 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Brent:2007:SLP

[3078] Richard Pierce Brent. Some long-period random number generators using shifts and xors. *The ANZIAM Journal*, 48(??):C188–C202, ???? 2007. CODEN AJNOA2. ISSN 1446-1811 (print), 1446-8735 (electronic). URL `http://journal.austms.org.au/ojs/index.php/ANZIAMJ/article/view/40/79`. Proceedings of the Computational Techniques and Applications Conference.

Brown:2007:SAN

[3079] Daniel R. L. Brown and Kristian Gjøsteen. A security analysis of the NIST SP 800-90 elliptic curve random number generator. In Menezes [4252], pages 466–481. ISBN 3-540-74142-9 (paperback). LCCN QA76.9.A25 C79 2007. URL `http://dl.acm.org/citation.cfm?id=1777777.1777815`.

Cheung:2007:HGA

[3080] Ray C. C. Cheung, Dong-U Lee, Wayne Luk, and John D. Villasenor. Hardware generation of arbitrary random number distributions from uniform distributions via the inversion method. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 15(8):952–962, August 2007. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/document/4276772/`.

Chiu:2007:CKC

[3081] Sung Nok Chiu. Correction to Koen's critical values in testing spatial randomness. *Journal of Statistical Computation and Simulation*, 77(11):

1001–1004, November 2007. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/10629360600989147`. See [1635].

Cowles:2007:BRB

[3082] Mary Kathryn Cowles. Book review: *Automatic Nonuniform Random Variate Generation*. *Journal of the American Statistical Association*, 102 (479):1079–1080, September 2007. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic).

Delfs:2007:ICP

[3083] Hans Delfs and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*, volume 1 of *Information Security and Cryptography*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2007. ISBN 3-540-49243-7 (hardcover), 3-540-49244-5. ISSN 1619-7100 (print), 2197-845X (electronic). xvi + 367 pp. LCCN QA76.9A25 D44 2007; QA76.9.D35. URL `http://www.springerlink.com/content/gm2886`.

Doornik:2007:CHP

[3084] Jurgen A. Doornik. Conversion of high-period random numbers to floating point. *ACM Transactions on Modeling and Computer Simulation*, 17 (1):3:1–3:5, January 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Dorrendorf:2007:CRNa

[3085] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. Technical report 2007/419, Cryptology ePrint Archive, International Association for Cryptologic Research, San Jose, CA, USA, 2007. URL `http://eprint.iacr.org/2007/419`.

Dorrendorf:2007:CRNb

[3086] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. In Rebecca N. Wright, Paul F. Syverson, and David Evans, editors, *CCS '07: proceedings of the 14th ACM Conference on Computer and Communications Security: Alexandria, Virginia, USA, October 29–November 2, 2007*, pages 476–485. ACM Press, New York, NY 10036, USA, 2007. ISBN 1-59593-703-X. LCCN QA76.9.A25.

Drutarovsky:2007:RCB

[3087] M. Drutarovsky and P. Galajda. A robust chaos-based true random number generator embedded in reconfigurable switched-capacitor hardware. In IEEE, editor, *17th International Conference Radioelektronika, 24–25 April, 2007, Brno, Czech Republic*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 1-4244-0821-0 (paperback), 1-4244-0822-9 (e-book). LCCN TK6541.

Dupuis:2007:ISS

[3088] Paul Dupuis, Kevin Leder, and Hui Wang. Importance sampling for sums of random variables with regularly varying tails. *ACM Transactions on Modeling and Computer Simulation*, 17(3):14:1–14:21, July 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Echeverria:2007:FGR

[3089] Pedro Echeverria and Marisa Lopez-Vallejo. FPGA Gaussian random number generator based on quintic Hermite interpolation inversion. In IEEE, editor, *50th Midwest Symposium on Circuits and Systems, 2007: MWSCAS 2007, Montréal, QC, Canada, 5–8 August 2007*, pages 871–874. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 1-4244-1175-0, 1-4244-1176-9. LCCN TK3226 .M55 2007. URL `http://ieeexplore.ieee.org/document/4488710/`.

Edgington:2007:RT

[3090] Eugene S. Edgington and Patrick Onghena. *Randomization tests*. Statistics, textbooks and monographs. Chapman and Hall/CRC, Boca Raton, FL, USA, fourth edition, 2007. ISBN 1-58488-589-0. 345 pp. LCCN QA277 .E32 2007. URL `http://www.loc.gov/catdir/enhancements/fy0745/2006032352-d.html`; `http://www.loc.gov/catdir/toc/ecip072/2006032352.html`.

Englund:2007:FCI

[3091] Håkon Englund, Thomas Johansson, and Meltem Sönmez Turan. A framework for chosen IV statistical analysis of stream ciphers. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *Progress in Cryptology — INDOCRYPT 2007: 8th International Conference on Cryptology in India, Chennai, India, December 9–13, 2007, Proceedings*, pages 268–281. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007.

Gerlovina:2007:LBS

[3092] V. M. Gerlovina. The limit behavior of sequences generated by parallel linear congruential generators. *Vestnik St. Petersburg Univ. Math.*, 40 (4):306–309, 2007. CODEN ???? ISSN 1063-4541.

Gutierrez:2007:ISP

[3093] Jaime Gutierrez and Álvar Ibeas. Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits. *Designs, Codes, and Cryptography*, 45(2):199–212, November 2007. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=45&issue=2&spage=199`.

Haramoto:2007:EJA

[3094] H. Haramoto, M. Matsumoto, T. Nishimura, F. Panneton, and P. L'Ecuyer. Efficient jump ahead for F_2-linear random number generators. GERAD Report G-2006-62, Group for Research in Decision Analysis, Montréal, QC, Canada, May 2007. URL `http://www.gerad.ca/fichiers/cahiers/G-2006-62.pdf`. To appear in INFORMS Journal on Computing.

Hars:2007:PRS

[3095] Laszlo Hars and Gyorgy Petruska. Pseudorandom recursions: Small and fast pseudorandom number generators for embedded applications. *EURASIP Journal on Embedded Systems*, 2007:1–13, 2007. ISSN 1687-3955 (print), 1687-3963 (electronic). URL `http://jes.eurasipjournals.com/content/2007/1/098417`.

Hasan:2007:FSU

[3096] Osman Hasan and Sofiène Tahar. Formalization of the Standard Uniform random variable. *Theoretical Computer Science*, 382(1):71–83, August 28, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Hell:2007:GSC

[3097] M. Hell, T. Johansson, and W. Meier. Grain: a stream cipher for constrained environments. *International Journal of Wireless and Mobile Computing*, 2(1):86–93, May 2007. CODEN ???? ISSN 1741-1084 (print), 1741-1092 (electronic). URL `https://dl.acm.org/doi/10.1504/IJWMC.2007.013798`.

Hormann:2007:ITD

[3098] Wolfgang Hörmann, Josef Leydold, and Gerhard Derflinger. Inverse transformed density rejection for unbounded monotone densities. *ACM Transactions on Modeling and Computer Simulation*, 17(4):18:1–18:??, September 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hormann:2007:SGD

[3099] W. Hörmann. A simple generator for the t distribution. *Computing: Archiv für Informatik und Numerik*, 81(4):317–322, December 2007. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0010-485X&volume=81&issue=4&spage=317`.

Juneja:2007:AFS

[3100] S. Juneja, R. L. Karandikar, and P. Shahabuddin. Asymptotics and fast simulation for tail probabilities of maximum of sums of few random variables. *ACM Transactions on Modeling and Computer Simulation*, 17 (2):7:1–7:35, April 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Kang:2007:PFS

[3101] W. N. Kang, F. P. Kelly, N. H. Lee, and R. J. Williams. Product form stationary distributions for diffusion approximations to a flow-level model operating under a proportional fair sharing policy. *ACM SIGMETRICS Performance Evaluation Review*, 35(2):36–38, September 2007. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Kundu:2007:CWG

[3102] Debasis Kundu and Rameshwar D. Gupta. A convenient way of generating gamma random variables using generalized exponential distribution. *Computational Statistics & Data Analysis*, 51(6):2796–2802, March 1, 2007. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947306003616`.

Kung:2007:RFB

[3103] Ching-Jing Kung and Hui-Chin Tang. A revised forward and backward heuristic for two-term multiple recursive random number generators. *Applied Mathematics and Computation*, 185(1):240–246, February 1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300306008551`.

LEcuyer:2007:EPB

[3104] Pierre L'Ecuyer. Efficient and portable 32-bit random variate generators (1986). In *Proceedings of the 39th conference on Winter simulation: 40 years! The best is yet to come*, WSC '07, pages 5:1–5:3. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 1-4244-1306-0. LCCN T57.62 .C64 2007. URL `http://dl.acm.org/citation.cfm?id=1351542.1352006`.

LEcuyer:2007:LRN

[3105] Pierre L'Ecuyer and François Panneton. F_2-linear random number generators. GERAD Report 2007-21, Group for Research in Decision Analysis, Montréal, QC, Canada, February 2007. ???? pp. To appear with minor revisions in *Advancing the Frontiers of Simulation: A Festschrift in Honor of George S. Fishman*.

LEcuyer:2007:TCL

[3106] Pierre L'Ecuyer and Richard Simard. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*, 33(4):22:1–22:40, August 2007. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

LEcuyer:2007:TSL

[3107] Pierre L'Ecuyer and Richard Simard. `TestU01`, a software library in ANSI C for empirical testing of random number generators: User's guide, compact version. Report, Département d Informatique et de Recherche Operationnelle, Université de Montréal, Montréal, QC, Canada, April 23, 2007. 219 pp.

Lim:2007:MCA

[3108] Chjan Lim and Joseph Nebus. *The Monte Carlo Approach*, chapter 4, pages 51–65. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 0-387-35075-6, 0-387-49431-6 (e-book). LCCN QA911 .L466 2007.

Liu:2007:NLR

[3109] Huaning Liu. A note on local randomness in polynomial random number and random function generators. *Applied Mathematics and Computation*, 186(2):1360–1366, March 15, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Matsumoto:2007:CDI

[3110] Makoto Matsumoto, Isaku Wada, Ai Kuramoto, and Hyo Ashihara. Common defects in initialization of pseudorandom number generators.

ACM Transactions on Modeling and Computer Simulation, 17(4):15:1–15:??, September 2007. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Matsumoto:2007:FSC

[3111] Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. A fast stream cipher with huge state space and quasigroup filter for software. In Adams et al. [4250], pages 246–263. ISBN 3-540-77360-6, 3-540-77359-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S22 2007eb.

Meidl:2007:LCP

[3112] Wilfried Meidl and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions. *Finite Fields and their Applications*, 13(3):628–634, July 2007. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579705000961`.

Mislove:2007:DRV

[3113] Michael Mislove. Discrete random variables over domains. *Theoretical Computer Science*, 380(1–2):181–198, June 21, 2007. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Morgenstern:2007:URR

[3114] Thomas Morgenstern. Uniform random rational number generation. In Karl-Heinz Waldmann and Ulrike M. Stocker, editors, *Operations Research Proceedings 2006*, volume 2006 (Part XIX), pages 569–574. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-69995-3. LCCN T57.6.A1G47 2006.

Nadarajah:2007:LCL

[3115] Saralees Nadarajah and Samuel Kotz. On the linear combination of Laplace and logistic random variables. *Journal of Applied Statistics*, 34 (2):185–194, ???? 2007. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic).

Nekrutkin:2007:AAO

[3116] V. Nekrutkin and M. Samakhova. Admissible and asymptotically optimal linear congruential generators. *Monte Carlo Methods and Applications*, 13(3):227–244, 2007. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2007.13.issue-3/mcma.2007.012/mcma.2007.012.xml`.

Panditaratne:2007:TRN

[3117] Vidura Panditaratne. True random number generator goes online. World-Wide Web document, July 18, 2007. URL `http://pressesc.com/01184778212_qrbgs`; `http://qrbg.irb.hr/`; `http://random.irb.hr/`.

Pareschi:2007:SLN

[3118] F. Pareschi, R. Rovatti, and G. Setti. Second-level NIST randomness tests for improving test reliability. In IEEE, editor, *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2007), 27–30 May 2007, New Orleans, LA*, pages 1437–1440. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2007. ISBN 1-4244-0920-9 (print), 1-4244-0921-7 (electronic). LCCN TK454.2 .I22a 2007. URL `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4252919`.

Pazo-Robles:2007:MPS

[3119] María Eugenia Pazo-Robles and Amparo Fúster-Sabater. Modeling pseudorandom sequence generators using cellular automata: The alternating step generator. In Simos and Maroulis [4253], pages 969–972. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL `http://proceedings.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=APCPCS000963000002000969000001&idtype=cvips`.

Perez:2007:RJI

[3120] Carlos Javier Pérez, Hansgeorg Schwibbe, and Petra Weidner. RAGE: a Java-implemented visual random generator. *Journal of Statistical Software*, 17(10):1–10, January 2007. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v17/i10`.

Rusu:2007:PRN

[3121] Florin Rusu and Alin Dobra. Pseudo-random number generation for sketch-based estimations. *ACM Transactions on Database Systems*, 32 (2):11:1–11:??, June 2007. CODEN ATDSD3. ISSN 0362-5915 (print), 1557-4644 (electronic).

Santhanam:2007:CLB

[3122] Rahul Santhanam. Circuit lower bounds for Merlin–Arthur classes. In ACM [4249], pages 275–283. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

Sathyanarayana:2007:GPS

[3123] S. V. Sathyanarayana, M. Aswatha Kumar, and K. N. Hari Bhat. Generation of pseudorandom sequence over elliptic curve group and their properties. *Journal of Discrete Mathematical Sciences and Cryptography*, 10(6):731–747, December 2007. CODEN ???? ISSN 0972-0529. URL `http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=10&issue_id=06`.

Shakil:2007:PMR

[3124] M. Shakil and B. M. Golam Kibria. On the product of Maxwell and Rice random variables. *Journal of Modern Applied Statistical Methods*, 6(1): 212–218, May 2007. CODEN ???? ISSN 1538-9472. URL `https://jmasm.com/index.php/jmasm/article/view/294`.

Sinescu:2007:GIR

[3125] V. Sinescu and S. Joe. Good intermediate-rank lattice rules based on the weighted star discrepancy. In Ovidiu Cârjă and Ioan I. Vrabie, editors, *Applied analysis and differential equations: Iaşi, Romania, 4–9 September 2006/*, pages 329–342. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 2007. ISBN 981-270-594-5. LCCN QA299.6 .I44 2006.

Sinescu:2007:GLR

[3126] Vasile Sinescu and Stephen Joe. Good lattice rules based on the general weighted star discrepancy. *Mathematics of Computation*, 76(258): 989–1004, April 2007. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/mcom/2007-76-258/S0025-5718-06-01943-0/home.html`; `http://www.ams.org/mcom/2007-76-258/S0025-5718-06-01943-0/S0025-5718-06-01943-0.dvi`; `http://www.ams.org/mcom/2007-76-258/S0025-5718-06-01943-0/S0025-5718-06-01943-0.pdf`; `http://www.ams.org/mcom/2007-76-258/S0025-5718-06-01943-0/S0025-5718-06-01943-0.ps`.

Stipcevic:2007:QRN

[3127] M. Stipçević and B. Medved Rogina. Quantum random number generator. *Review of Scientific Instruments*, 78(045104):9, 2007. CODEN RSINAK. ISSN 1089-7623, 0034-6748. URL `http://qrbg.irb.hr/0609043v2.pdf`.

Suematsu:2007:GPR

[3128] C. Suematsu, N. Namekata, I. Shimada, and S. Inoue. Generation of physical random numbers by means of photon counting. *Electronics and*

communications in Japan. Part 3, Fundamental electronic science, 90 (2):1–8, 2007. CODEN ECJSER. ISSN 1042-0967 (print), 1520-6440 (electronic).

Sunar:2007:PST

[3129] B. Sunar, W. J. Martin, and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers*, 56(1):109–119, January 2007. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4016501`.

Tang:2007:ALC

[3130] Hui-Chin Tang. An analysis of linear congruential random number generators when multiplier restrictions exist. *European Journal of Operational Research*, 182(2):820–828, October 16, 2007. CODEN EJORDT. ISSN 0377-2217 (print), 1872-6860 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377221706009003`.

Thomas:2007:GRN

[3131] David B. Thomas, Wayne Luk, Philip H. W. Leong, and John D. Villasenor. Gaussian random number generators. *ACM Computing Surveys*, 39(4):11:1–11:38, ???? 2007. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Thomas:2007:HQU

[3132] David B. Thomas and Wayne Luk. High quality uniform random number generation using LUT optimised state-transition matrices. *Journal of VLSI Signal Processing*, 47(1):77–92, 2007. CODEN JVSPED. ISSN 0922-5773 (print), 1573-109x (electronic). From the issue entitled "Special Issue: Field Programmable Technology. Guest Editors: Gordon Brebner, Samarjit Chakraborty, and Weng-Fai Wong".

Thomas:2007:NUR

[3133] David B. Thomas and Wayne Luk. Non-uniform random number generation through piecewise linear approximations. *IET Computers & Digital Techniques*, 1(4):312–321, July 2007. ISSN 1751-8601 (print), 1751-861X (electronic). URL `http://cas.ee.ic.ac.uk/people/dt10/research/thomas-07-piecewise-linear-jrnl.pdf`; `http://ieeexplore.ieee.org/document/4271374/`.

Tsoi:2007:HPP

[3134] K. H. Tsoi, K. H. Leung, and Philip H. W. Leong. High performance physical random number generator. *IET Computers & Digital Tech-*

niques, 1(4):349–352, 2007. CODEN ???? ISSN 1751-8601 (print), 1751-861X (electronic). URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4117424;` `http://link.aip.org/link/?CDT/1/349/1`.

Turiel:2007:QRB

[3135] Thomas P. Turiel. Quantum random bit generators. *The American Statistician*, 61(3):255–259, August 2007. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Vadhan:2007:UTP

[3136] Salil P. Vadhan. The unified theory of pseudorandomness: guest column. *ACM SIGACT News*, 38(3):39–54, September 2007. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic). URL `http://doi.acm.org/10.1145/1324215.1324225`.

Viola:2007:PBC

[3137] Emanuele Viola. Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates. *SIAM Journal on Computing*, 36(5):1387–1403, ???? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Wijaya:2007:PSM

[3138] Sastra Wijaya, Syn Kiat Tan, and Sheng-Uei Guan. Permutation and sampling with maximum length CA or pseudorandom number generation. *Applied Mathematics and Computation*, 185(1):312–321, February 1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Yan:2007:EJC

[3139] Jun Yan. Enjoy the joy of copulas: With a package `copula`. *Journal of Statistical Software*, 21(4):1–21, October 2007. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v21/i04`.

Ahmad:2008:ATT

[3140] David Ahmad. Attack trends: Two years of broken crypto: Debian's dress rehearsal for a global PKI compromise. *IEEE Security & Privacy*, 6(5):70–73, September/October 2008. CODEN ???? ISSN 1540-7993 (print), 1558-4046 (electronic).

Alimohammad:2008:CAG

[3141] Amirhossein Alimohammad, Saeed Fouladi Fard, Bruce F. Cockburn, and Christian Schlegel. A compact and accurate Gaussian variate generator. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*,

16(5):517–527, May 2008. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/document/4476028/`.

Alimohammad:2008:EAH

[3142] A. Alimohammad, S. F. Fard, B. F. Cockburn, and C. Schlegel. On the efficiency and accuracy of hybrid pseudo-random number generators for FPGA-based simulations. In *2008. IPDPS 2008. IEEE International Symposium on Parallel and Distributed Processing*, pages 1–8. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4536524`.

Alioto:2008:APE

[3143] M. Alioto, L. Fondelli, and S. Rocchi. Analysis and performance evaluation of area-efficient true random bit generators on FPGAs. In *2008. ISCAS 2008. IEEE International Symposium on Circuits and Systems*, pages 1572–1575. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4541732`.

Alvarez:2008:ETR

[3144] T. Alvarez, E. Sanz, E. Sastre, and M. Bolajraf. Evalua-Test: a random test generator. In *2008. IEEM 2008. IEEE International Conference on Industrial Engineering and Engineering Management*, pages 718–723. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4737963`.

Attya:2008:ROC

[3145] A. B. Attya, Y. G. Hegazy, and M. A. Moustafa. Random operation of conventional distributed generators based on generation techniques. In *2008. CCECE 2008. Canadian Conference on Electrical and Computer Engineering*, pages 001203–001206. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4564729`.

Aumasson:2008:NFL

[3146] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. New features of Latin dances: Analysis of Salsa, ChaCha and Rumba. In Kaisa Nyberg, editor, *Fast Software Encryption: 15th International Workshop, FSE 2008, Lausanne, Switzer-*

land, February 10–13, 2008, Revised Selected Papers, pages 470–488. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. URL `https://eprint.iacr.org/2007/472.pdf`.

Babbage:2008:MSC

[3147] Steve Babbage and Matthew Dodd. The Mickey stream ciphers. In Robshaw and Billet [4259], pages 191–209. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). LCCN QA76.9.A25 N486 2008.

Bader:2008:DFP

[3148] D. A. Bader, A. Chandramowlishwaran, and V. Agarwal. On the design of fast pseudo-random number generators for the cell broadband engine and an application to risk analysis. In *2008. ICPP '08. 37th International Conference on Parallel Processing*, pages 520–527. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4625889`.

Balachandran:2008:TRN

[3149] G. K. Balachandran and R. E. Barnett. A 440-nA true random number generator for passive RFID tags. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 55(11):3723–3732, ???? 2008. CODEN ???? ISSN 1549-8328 (print), 1558-0806 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4543874`.

Banks:2008:FIP

[3150] S. Banks, P. Beadling, and A. Ferencz. FPGA implementation of pseudo random number generators for Monte Carlo methods in quantitative finance. In *2008. ReConFig '08. International Conference on Reconfigurable Computing and FPGAs*, pages 271–276. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4731806`.

Basu:2008:CCE

[3151] Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul. A complete characterization of the evolution of RC4 pseudo random generation algorithm. *Journal of Mathematical Cryptology*, 2(3):257–289, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Beirami:2008:PMD

[3152] A. Beirami, H. Nejati, and Y. Massoud. A performance metric for discrete-time chaos-based truly random number generators. In *2008. MWSCAS 2008. 51st Midwest Symposium on Circuits and Systems*, pages 133–136. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4616754`.

Bello:2008:OPR

[3153] L. Bello. `openssl` — predictable random number generator. Debian security advisory 1571-1., 2008.

Berbain:2008:SFS

[3154] Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert. Sosemanuk, a fast software-oriented stream cipher. In Robshaw and Billet [4259], pages 98–118. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). LCCN QA76.9.A25 N486 2008.

Bernstein:2008:CVS

[3155] Daniel J. Bernstein. ChaCha, a variant of Salsa20. In ????, editor, *Workshop Record of SASC 2008: The State of the Art of Stream Ciphers*, page ?? ????, ????, 2008. URL `https://cr.yp.to/chacha/chacha-20080120.pdf; https://cr.yp.to/papers.html#chcha`.

Bernstein:2008:SFS

[3156] Daniel J. Bernstein. The Salsa20 family of stream ciphers. In Robshaw and Billet [4259], pages 84–97. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). LCCN QA76.9.A25 N486 2008. URL `http://cr.yp.to/papers.html#Salsafamily`.

Blaszczyk:2008:NMT

[3157] M. Blaszczyk and R. A. Guinee. A novel modelled true random binary number generator for key stream generation in cryptographic applications. In *MILCOM 2008. IEEE Military Communications Conference, 2008*, pages 1–7. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4753211`.

Blaszczyk:2008:TRB

[3158] Marta Blaszczyk and R. A. Guinee. A true random binary sequence generator based on chaotic circuit. In *IET Irish Signals and Systems*

Conference, 2008. (ISSC 2008), pages 294–299. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4780969`.

Brent:2008:SCC

[3159] Richard P. Brent. Some comments on C. S. Wallace's random number generators. *The Computer Journal*, 51(5):579–584, February 2008. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). See [2233].

Bucci:2008:FDR

[3160] M. Bucci and R. Luzzi. Fully digital random bit generators for cryptographic applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 55(3):861–875, ???? 2008. CODEN ???? ISSN 1549-8328 (print), 1558-0806 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4432925`.

Calude:2008:QRV

[3161] Cristian S. Calude and Karl Svozil. Quantum randomness and value indefiniteness. *Advanced Science Letters*, 1(2):165–168, December 2008. CODEN ASLDAM. ISSN 1936-6612 (print), 1936-7317 (electronic). URL `http://www.ingentaconnect.com/content/asp/asl/2008/00000001/00000002/art00004`.

Cesmelioglu:2008:CSP

[3162] Ayça Çesmelioglu, Wilfried Meidl, and Alev Topuzoglu. On the cycle structure of permutation polynomials. *Finite Fields and their Applications*, 14(3):593–614, July 2008. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579707000500`.

Chen:2008:FBS

[3163] Zhixiong Chen. Finite binary sequences constructed by explicit inversive methods. *Finite Fields and their Applications*, 14(3):579–592, July 2008. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579707000494`.

Chen:2008:GFT

[3164] Chi-Chi Chen and Hui-Chin Tang. On goodness-of-fit tests for multiple recursive random number generators. *Applied Mathematics and Compu-*

tation, 200(1):70–79, June 15, 2008. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic).

Chen:2008:RKD

[3165] L. Chen. Recommendation for key derivation using pseudorandom functions. NIST Special Publication 800-108, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2008.

Chen:2008:SCS

[3166] Woei-Luen Chen, Yung-Hsiang Lin, Hrong-Sheng Gau, and Chia-Hung Yu. STATCOM controls for a self-excited induction generator feeding random loads. *IEEE Transactions on Power Delivery*, 23(4):2207–2215, ???? 2008. CODEN ITPDE5. ISSN 0885-8977 (print), 1937-4208 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4512032`.

Chindris:2008:HER

[3167] G. Chindris, A. Suciu, and M. Muresan. High-entropy random number generators using system on chip devices. In *ISSE '08. 31st International Spring Seminar on Electronics Technology, 2008*, pages 280–283. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5276652`.

Christen:2008:OPR

[3168] L. Christen, O. Yilmaz, S. Nuccio, Xiaoxia Wu, and A. E. Willner. Optical pseudo-random bit sequence generator using a dual-drive Mach–Zehnder modulator as a linear feedback shift register. In *LEOS 2008. 21st Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2008*, pages 274–275. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4688596`.

Collins:2008:TSI

[3169] Joseph C. Collins. Testing, selection, and implementation of random number generators. Technical report AD-A486 637, AD-ARL-TR-4498, Army Research Laboratory, Survivability Lethality Analysis Directorate, Aberdeen Proving Ground, MD, USA, July 2008. 82 pp. URL `http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA486637`.

Cordero:2008:DPV

[3170] Arel Cordero. DiceHash: Publicly verifiable random number generator. Web page., April 2008. URL http://www.eecs.berkeley.edu/~arel/dicehash.html.

Das:2008:ASS

[3171] Abhimanyu Das and David Kempe. Algorithms for subset selection in linear regression. In ACM [4254], pages 45–54. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

DeCanniere:2008:T

[3172] Christophe De Canniere and Bart Preneel. Trivium. In Robshaw and Billet [4259], pages 244–266. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). LCCN QA76.9.A25 N486 2008.

Deng:2008:DIE

[3173] L.-Y. Deng, H. Li, J.-J. H. Shiau, and G. H. Tsai. Design and implementation of efficient and portable multiple recursive generators with few zero coefficients. In Keller et al. [4257], pages 263–273. ISBN 3-540-74495-9 (paperback), 3-540-74496-7. LCCN Q183.9 .I526 2006. URL http://catdir.loc.gov/catdir/toc/fy0803/2007936240.htm.

Deng:2008:ICS

[3174] L. Y. Deng. Issues on computer search for large order multiple recursive generators. In Keller et al. [4257], pages 251–261. ISBN 3-540-74495-9 (paperback), 3-540-74496-7. LCCN Q183.9 .I526 2006. URL http://catdir.loc.gov/catdir/toc/fy0803/2007936240.htm.

Deng:2008:IRN

[3175] Lih-Yuan Deng, Rui Guo, Dennis K. J. Lin, and Fengshan Bai. Improving random number generators in the Monte Carlo simulations via twisting and combining. *Computer Physics Communications*, 178 (6):401–408, March 15, 2008. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S001046550700447X.

Drutarovsky:2008:CSC

[3176] M. Drutarovsky and M. Varchola. Cryptographic system on a chip based on Actel ARM7 soft-core with embedded true random number generator. In *2008. DDECS 2008. 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD

20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4538778.

Dumbgen:2008:EBA

[3177] Lutz Dümbgen and Christoph Leuenberger. Explicit bounds for the approximation error in Benford's law. *Electronic Communications in Probability*, 13:99–112, 2008. CODEN ???? ISSN 1083-589X. URL http://arxiv.org/abs/0705.4488; http://weber.math.washington.edu/~ejpecp/ECP/index.php.

Dynes:2008:HSP

[3178] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields. A high speed, postprocessing free, quantum random number generator. *Applied Physics Letters*, 93(3):031109, ???? 2008. CODEN APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4836140.

El-Mahassni:2008:DCD

[3179] Edwin D. El-Mahassni and Domingo Gomez. On the distribution of counter-dependent nonlinear congruential pseudorandom number generators in residue rings. *International Journal of Number Theory*, 4 (6):1009–1018, December 2008. ISSN 1793-0421 (print), 1793-7310 (electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042108001857.

Eryilmaz:2008:ROS

[3180] Serkan Eryilmaz and Alexei Stepanov. Runs in an ordered sequence of random variables. *Metrika. International Journal for Theoretical and Applied Statistics.*, 67(3):299–313, April 2008. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-926X (electronic). URL http://link.springer.com/article/10.1007/s00184-007-0134-7.

Esquivel:2008:PGF

[3181] M. L. Esquível. Probability generating functions for discrete real-valued random variables. *Theory of Probability and its Applications*, 52(1):40–57, ???? 2008. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Fechner:2008:TRN

[3182] B. Fechner and A. Osterloh. A true random number generator with built-in attack detection. In *2008. DepCos-RELCOMEX '08. Third International Conference on Dependability of Computer Systems*, pages 111–118. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver

Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4573047`.

Guitouni:2008:RHI

[3183] Z. Guitouni, M. Machhout, and R. Tourki. Reconfigurable hardware implementation of a random number generator based on 2-D cellular automata. In *2008. DTIS 2008. 3rd International Conference on Design and Technology of Integrated Systems in Nanoscale Era*, pages 1–5. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4540219`.

Gutierrez:2008:ESN

[3184] Jaime Gutierrez and Arne Winterhof. Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions. *Finite Fields and their Applications*, 14(2):410–416, April 2008. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579707000275`.

Haastad:2008:PCA

[3185] Johan Håstad and Mats Näslund. Practical construction and analysis of pseudo-randomness primitives. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):1–26, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=1`.

Haramoto:2008:EJA

[3186] Hiroshi Haramoto, Makoto Matsumoto, Takuji Nishimura, François Panneton, and Pierre L'Ecuyer. Efficient jump ahead for $\mathbf{F}_2$-linear random number generators. *INFORMS Journal on Computing*, 20(3):385–390, Summer 2008. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Haramoto:2008:FJA

[3187] Hiroshi Haramoto, Makoto Matsumoto, and Pierre L'Ecuyer. A fast jump ahead algorithm for linear recurrences in a polynomial space. In Golomb et al. [4255], pages 290–298. ISBN 3-540-85912-8, 3-540-85911-X. LCCN QA292 .S48 2008eb.

Holleman:2008:WCT

[3188] J. Holleman, S. Bridges, B. P. Otis, and C. Diorio. A 3 W CMOS true random number generator with adaptive floating-gate offset can-

cellation. *IEEE Journal of Solid-State Circuits*, 43(5):1324–1336, ???? 2008. CODEN IJSCBC. ISSN 0018-9200 (print), 1558-173X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4494657`.

Hou:2008:LPD

[3189] Li gang Hou, Xiao hong Peng, and Wu chen Wu. A low power dynamic pseudo random bit generator for test pattern generation. In *2008. ICSICT 2008. 9th International Conference on Solid-State and Integrated-Circuit Technology*, pages 2079–2082. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4734986`.

Howes:2008:U

[3190] L. Howes and D. B. Thomas. Efficient random number generation and application using CUDA. In Nguyen [4258], chapter 37, pages 805–830. ISBN 0-321-51526-9. LCCN T385 .G6882 2008. URL `http://www.loc.gov/catdir/toc/ecip0720/2007023985.html`.

Inaltekin:2008:ANE

[3191] Hazer Inaltekin and Stephen B. Wicker. The analysis of Nash equilibria of the one-shot random-access game for wireless networks and the behavior of selfish nodes. *IEEE/ACM Transactions on Networking*, 16(5):1094–1107, October 2008. CODEN IEANEP. ISSN 1063-6692 (print), 1558-2566 (electronic).

Jang:2008:CDH

[3192] D. Jang, J. U. Kang, A. Kruckman, J. Kudo, and S. J. Miller. Chains of distributions, hierarchical Bayesian models and Benford's Law. *ArXiv e-prints*, May 2008. CODEN ???? ISSN ???? URL `http://adsabs.harvard.edu/abs/2008arXiv0805.4226J`; `http://arxiv.org/abs/0805.4226`.

Joe:2008:CSS

[3193] Stephen Joe and Frances Y. Kuo. Constructing Sobol' sequences with better two-dimensional projections. *SIAM Journal on Scientific Computing*, 30(5):2635–2654, ???? 2008. CODEN SJOCE3. ISSN 1064-8275 (print), 1095-7197 (electronic).

Jovanovic-Dolecek:2008:UMT

[3194] Gordana Jovanovic-Dolecek and Alfonso Fernandez-Vazquez. Use of MATLAB in teaching the fundamentals of random variables. *SIGCSE*

Bulletin (ACM Special Interest Group on Computer Science Education), 40(4):46–51, December 2008. CODEN SIGSD3. ISSN 0097-8418 (print), 2331-3927 (electronic).

Kalos:2008:MCM

[3195] Malvin H. Kalos and Paula A. Whitlock. *Monte Carlo methods*. Wiley-VCH, Weinheim, Germany, second edition, 2008. ISBN 3-527-40760-X. xii + 203 pp. LCCN QA298 .K35 2008.

Kang:2008:HPP

[3196] Byung-Heon Kang, Dong-Ho Lee, and Chun-Pyo Hong. High-performance pseudorandom number generator using two-dimensional cellular automata. In Adam Osseiran et al., editors, *Proceeding, Fourth IEEE International Symposium on Electronic Design, Test and Applications: Delta '08, 23–25 January 2008, SAR, China*, pages 597–602. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN 0-7695-3110-5. LCCN TK7855.

Kato:2008:QSC

[3197] Kentaro Kato and Osamu Hirota. A quantum stream cipher by Yuen 2000 protocol with nonlinear random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7092(1): 70920H, 2008. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7092/70920H/1; http://spie.org/x648.html?product_id=794584`. Quantum Communications and Quantum Imaging VI.

Katsoprinakis:2008:QRN

[3198] G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis. Quantum random number generator based on spin noise. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 77(5):054101, May 2008. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.77.054101`.

Katti:2008:SPR

[3199] R. S. Katti and R. G. Kavasseri. Secure pseudo-random bit sequence generation using coupled linear congruential generators. In *2008. ISCAS 2008. IEEE International Symposium on Circuits and Systems*, pages 2929–2932. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4542071`.

Katz:2008:RRNa

[3200] O. Katz, D. A. Ramon, and I. A. Wagner. A robust random number generator based on a differential current-mode chaos. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 16(12):1677–1686, ???? 2008. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4668639`.

Katz:2008:RRNb

[3201] O. Katz, D. A. Ramon, and I. A. Wagner. A robust random number generator based on a differential current-mode chaos. In *IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems 2008. COMCAS 2008*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4562804`.

Kiessler:2008:BRBe

[3202] Peter C. Kiessler. Book review: *An Introduction to Random Sets; Theory of Random Sets*. *Journal of the American Statistical Association*, 103 (482):884, June 2008. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic).

Killmann:2008:DPR

[3203] Wolfgang Killmann and Werner Schindler. A design for a physical RNG with robust entropy estimators. *Lecture Notes in Computer Science*, 5154:146–163, 2008. CODEN LNCSD9. ISBN 3-540-85053-8, 3-540-85052-X. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/73wv01812724286j/`. Proceedings of Cryptographic Hardware and Embedded Systems — CHES 2008.

Kim:2008:TRG

[3204] Chihurn Kim, Geon Ho Choe, and Dong Han Kim. Tests of randomness by the gambler's ruin algorithm. *Applied Mathematics and Computation*, 199(1):195–210, May 15, 2008. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300307009873`. See critical remarks [3464].

Kolokotronis:2008:CPN

[3205] Nicholas Kolokotronis. Cryptographic properties of nonlinear pseudorandom number generators. *Designs, Codes, and Cryptography*, 46(3):

353–363, March 2008. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=46&issue=3&spage=353.

Langdon:2008:FHQ

[3206] W. B. Langdon. A fast high quality pseudo random number generator for graphics processing units. In IEEE, editor, *IEEE Congress on Evolutionary Computation, CEC 2008, Hong Kong, China, 1–6 June, 2008*, pages 459–465. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN 1-4244-1822-4 (print), 1-4244-1823-2. LCCN QA76.87. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4630838.

LEcuyer:2008:CPS

[3207] Pierre L'Ecuyer. Comparison of point sets and sequences for Quasi-Monte Carlo and for random number generation. In Golomb et al. [4255], pages 1–17. ISBN 3-540-85912-8, 3-540-85911-X. LCCN QA292 .S48 2008eb. Invited paper.

Lee:2008:HAS

[3208] JunKyu Lee, G. D. Peterson, R. J. Harrison, and R. J. Hinde. Hardware accelerated Scalable Parallel Random Number Generators for Monte Carlo methods. In *2008. MWSCAS 2008. 51st Midwest Symposium on Circuits and Systems*, pages 177–180. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4616765.

Lee:2008:PRN

[3209] Michael J. Lee. Pseudo-random-number generators and the square site percolation threshold. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 78(3):031131, September 2008. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.78.031131.

Leiva:2008:RNG

[3210] Víctor Leiva, Antonio Sanhueza, Pranab K. Sen, and Gilberto A. Paula. Random number generators for the generalized Birnbaum–Saunders distribution. *Journal of Statistical Computation and Simulation*, 78(11): 1105–1118, 2008. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/00949650701550242.

Leiva:2008:RPG

[3211] Víctor Leiva, Hugo Hernández, and Antonio Sanhueza. An R package for a general class of inverse Gaussian distributions. *Journal of Statistical Software*, 26(4):1–21, June 2008. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v26/i04`.

Leopardi:2008:TTU

[3212] P. Leopardi. Testing the tests: Using random number generators to improve empirical tests. In *Monte Carlo and Quasi-Monte Carlo Methods*, pages 501–512. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008.

Li:2008:IKC

[3213] Ming Li and P. M. B. (Paul Michael Béla) Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*. Texts in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 2008. ISBN 0-387-33998-1 (hardcover), 0-387-49820-6 (e-book). xxiii + 790 pp. LCCN QA267.7 .L5 2008. URL `http://link.springer.com/10.1007/978-0-387-49820-1`.

Li:2008:RNG

[3214] Wei Li, Kangshun Li, Wensheng Zhang, Chao Wang, and Ying Huang. A random number generator based on particle dynamical evolutionary algorithm. In *2008. ICNC '08. Fourth International Conference on Natural Computation*, volume 1, pages 161–165. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4666831`.

Li:2008:SAD

[3215] Xin Li, Y. Shoshan, A. Fish, and G. A. Jullien. A simplified approach for designing secure random number generators in HW. In *ICECS 2008. 15th IEEE International Conference on Electronics, Circuits and Systems 2008*, pages 372–375. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4674868`.

Liu:2008:CMI

[3216] Chao-Liang Liu, Gwoboa Horng, and Hsin-Yu Liu. Computing the modular inverses is as simple as computing the GCDs. *Finite Fields and their Applications*, 14(1):65–75, 2008. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic).

Liu:2008:PDH

[3217] Huaning Liu and Cundian Yang. On a problem of D. H. Lehmer and pseudorandom binary sequences. *Bull. Braz. Math. Soc. (N.S.)*, 39(3): 387–399, 2008. ISSN 1678-7544.

Lovett:2008:UPG

[3218] Shachar Lovett. Unconditional pseudorandom generators for low degree polynomials. In ACM [4254], pages 557–562. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Maitra:2008:ARP

[3219] Subhamoy Maitra and Goutam Paul. Analysis of RC4 and proposal of additional layers for better security margin. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology — INDOCRYPT 2008: 9th International Conference on Cryptology in India, Kharagpur, India, December 14–17, 2008. Proceedings*, volume 5365 of *Lecture Notes in Computer Science*, pages 27–39. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008.

Martin:2008:IPR

[3220] Clyde F. Martin and Mara D. Neusel. Invariants of pseudo-random number generators. *Communications in Information and Systems*, 8 (1):39–54, ???? 2008. CODEN ???? ISSN 1526-7555. URL `http://projecteuclid.org/euclid.cis/1233153122`.

Masaro:2008:RODb

[3221] Joe Masaro and Chi Song Wong. Robustness of optimal designs for correlated random variables. *Linear Algebra and its Applications*, 429 (7):1639–1646, October 1, 2008. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic).

Matsumoto:2008:CSC

[3222] Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita. CryptMT3 stream cipher. In Robshaw and Billet [4259], pages 7–19. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). LCCN QA76.9.A25 N486 2008.

Matsumoto:2008:MPR

[3223] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita. 1200μ m^2 physical random-number generators based on SiN MOSFET for secure smart-card application. In *ISSCC 2008. Digest*

of Technical Papers. IEEE International Solid-State Circuits Conference, 2008, pages 414–624. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4523233`.

McCullough:2008:ASP

[3224] B. D. McCullough and David A. Heiser. On the accuracy of statistical procedures in Microsoft Excel 2007. *Computational Statistics & Data Analysis*, 52(10):4570–4578, June 15, 2008. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947308001606`.

McCullough:2008:MEW

[3225] B. D. McCullough. Microsoft Excel's 'not The Wichmann–Hill' random number generators. *Computational Statistics & Data Analysis*, 52 (10):4587–4593, June 15, 2008. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S016794730800162X`.

Miller:2008:OSB

[3226] Steven J. Miller and Mark J. Nigrini. Order statistics and Benford's law. *International Journal of Mathematics and Mathematical Sciences*, 2008. CODEN ???? ISSN 0161-1712 (print), 1687-0425 (electronic). URL `http://arxiv.org/abs/math/0601344`. Article ID 382948.

Moler:2008:NCM

[3227] Cleve B. Moler. *Numerical computing with MATLAB*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, second edition, 2008. ISBN 0-89871-660-8 (hardcover), 0-89871-560-1 (paperback), 0-89871-795-7 (e-book). xi + 336 pp. LCCN QA297 .M625 2008.

Murdoch:2008:VRV

[3228] Duncan J. Murdoch, Yu-Ling Tsai, and James Adcock. *P*-values are random variables. *The American Statistician*, 62(3):242–245, August 2008. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Murphy:2008:CLW

[3229] Thomas E. Murphy and Rajarshi Roy. Chaotic lasers: The world's fastest dice. *Nature Photonics*, 2(12):714–715, December 2008. CODEN NPAHBY. ISSN 1749-4893. URL `http://www.nature.com/nphoton/journal/v2/n12/full/nphoton.2008.239.html`.

Nandakumar:2008:EET

[3230] Satyadev Nandakumar. An effective ergodic theorem and some applications. In ACM [4254], pages 39–44. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Nguyen:2008:ODD

[3231] T. D. Nguyen, L. L. Yang, S. X. Ng, and L. Hanzo. An optimal degree distribution design and a conditional random integer generator for the systematic Luby transform coded wireless internet. In *WCNC 2008. IEEE Wireless Communications and Networking Conference, 2008*, pages 243–248. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4489079`.

Niederreiter:2008:CPN

[3232] Harald Niederreiter and Joël Rivat. On the correlation of pseudorandom numbers generated by inversive methods. *Monatshefte für Mathematik*, 153(3):251–264, March 2008. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic). URL `http://www.springerlink.com/content/e823857873133320/`.

Niederreiter:2008:ESN

[3233] Harald Niederreiter and Arne Winterhof. Exponential sums for nonlinear recurring sequences. *Finite Fields and their Applications*, 14(1): 59–64, January 2008. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579706000773`.

Niuda:2008:BFL

[3234] K. Niuda. Bounds on fixed-length post-processing functions for stationary biased random number generators. In *2008. ISITA 2008. International Symposium on Information Theory and Its Applications*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4895580`.

Ozdemir:2008:RNG

[3235] K. Ozdemir, S. Kilinc, and S. Ozoguz. Random number generator design using continuous-time chaos. In *SIU 2008. IEEE 16th Signal Processing, Communication and Applications Conference, 2008*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4632650`.

Petit:2008:BCB

[3236] C. Petit, F. Standaert, O. Pereira, T. Malkin, and M. Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In ????, editor, *ASIAN ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, pages 56–65. ACM Press, New York, NY 10036, USA, 2008. ISBN ???? LCCN ????

Petit:2008:EPR

[3237] C. Petit, N. Veyrat-Charvillon, and J.-J. Quisquater. Efficiency and pseudo-randomness of a variant of Zémor–Tillich hash function. In *15th IEEE International Conference on Electronics, Circuits and Systems, 2008 (ICECS 2008)*, pages 906–909. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, August 2008.

Reuillon:2008:RDS

[3238] R. Reuillon, D. R. C. Hill, Z. El Bitar, and V. Breton. Rigorous distribution of stochastic simulations using the DistMe Toolkit. *IEEE Transactions on Nuclear Science*, 55(1 (part 3)):595–603, February 2008. CODEN IETNAE. ISSN 0018-9499 (print), 1558-1578 (electronic). URL `http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4448523`.

Rousseau:2008:RNG

[3239] Christiane Rousseau and Yvan Saint-Aubin. Random number generators. In *Mathematics and Technology* [4260], pages 1–23. ISBN 0-387-69216-9. ISSN 1867-5506. LCCN QA37.3.R6814 2008.

Rukhin:2008:TRA

[3240] Andrew L. Rukhin and Zeev Volkovich. Testing randomness via aperiodic words. *Journal of Statistical Computation and Simulation*, 78(12):1133–1144, December 2008. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/10629360600864142`.

Rumley:2008:PRN

[3241] S. Rumley and M. Becker. Pseudo random numbers generators available as Web services. In *2008. SPECTS 2008. International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, pages 91–97. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4667548`.

Saito:2008:SOF

[3242] Mutsuo Saito and Makoto Matsumoto. SIMD-oriented fast Mersenne Twister: a 128-bit pseudorandom number generator. In Keller et al. [4257], pages 607–622. ISBN 3-540-74495-9 (paperback), 3-540-74496-7. LCCN Q183.9 .I526 2006. URL `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/MTGP/`; `http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/SFMT/`.

Schlier:2008:SHS

[3243] Christoph Schlier. On scrambled Halton sequences. *Applied Numerical Mathematics: Transactions of IMACS*, 58(10):1467–1478, October 2008. CODEN ANMAEL. ISSN 0168-9274 (print), 1873-5460 (electronic).

Schneier:2008:SSR

[3244] B. Schneier. Schneier on security: Random number bug in Debian Linux. Web document, May 2008. URL `http://www.schneier.com/blog/archives/2008/05/random_number_b.html`.

Shen:2008:RRL

[3245] Yi-Dong Shen. Reasoning with recursive loops under the PLP framework. *ACM Transactions on Computational Logic*, 9(4):27:1–27:??, August 2008. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Sinescu:2008:CLR

[3246] Vasile Sinescu. Construction of lattice rules for multiple integration based on a weighted discrepancy. Master of Philosophy (MPhil), University of Waikato, Hamilton, New Zealand, April 11, 2008. v + 154 pp. URL `http://adt.waikato.ac.nz/uploads/approved/adt-uow20080411.095059/public/02whole.pdf`; `http://hdl.handle.net/10289/2542`.

Sinescu:2008:GLR

[3247] V. Sinescu and S. Joe. Good lattice rules with a composite number of points based on the product weighted star discrepancy. In Keller et al. [4257], pages 645–658. ISBN 3-540-74495-9 (paperback), 3-540-74496-7. LCCN Q183.9 .I526 2006. URL `http://catdir.loc.gov/catdir/toc/fy0803/2007936240.htm`.

Somaiya:2008:LCU

[3248] Manas Somaiya, Christopher Jermaine, and Sanjay Ranka. Learning correlations using the mixture-of-subsets model. *ACM Transactions on*

Knowledge Discovery from Data (TKDD), 1(4):3:1–3:??, January 2008. CODEN ???? ISSN 1556-4681 (print), 1556-472X (electronic).

Stosic:2008:FRN

[3249] Borko D. Stosić. Fast random number generation using 128-bit multimedia extension registers on Pentium class machines. *Communications in Statistics: Simulation and Computation*, 37(2):360–367, 2008. CODEN CSSCDB. ISSN 0361-0918.

Tan:2008:SEC

[3250] Zuowen Tan and Qi Wu. Study of exponentially cross-coupled chaotic systems for a random bit generator. In *2008. IITAW '08. International Symposium on Intelligent Information Technology Application Workshops*, pages 224–227. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4731919`.

Tan:2008:SLC

[3251] Zuowen Tan and Qi Wu. Study of linearly cross-coupled chaotic systems for a random bit generator. In *2008. CIS '08. International Conference on Computational Intelligence and Security*, volume 2, pages 267–272. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4724779`.

Tanizaki:2008:SGR

[3252] Hisashi Tanizaki. A simple gamma random number generator for arbitrary shape parameters. *Economics Bulletin [Nashville, Tennessee]*, 3 (7):1–10, ???? 2008. ISSN 1545-2921. URL `http://www.accessecon.com/pubs/EB/2008/Volume3/EB-07C10012A.pdf`; `https://ideas.repec.org/a/ebl/ecbull/eb-07c10012.html`.

Thamrin:2008:PBR

[3253] N. M. Thamrin, G. Witjaksono, A. Nuruddin, and M. S. Abdullah. A photonic-based random number generator for cryptographic application. In *Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008. SNPD '08*, pages 356–361. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4617397`.

Thomas:2008:MGR

[3254] David B. Thomas and Wayne Luk. Multivariate Gaussian random number generation targeting reconfigurable hardware. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 1(2):12:1–12:??, June 2008. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Thomas:2008:REG

[3255] David B. Thomas and Wayne Luk. Resource efficient generators for the floating-point uniform and exponential distributions. In IEEE [4256], pages 102–107. ISBN 1-4244-1897-6 (paperback), 1-4244-1898-4. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4569858`; `http://www.gbv.de/dms/tib-ub-hannover/631855815.pdf`. IEEE catalog number CFP08063-PRT.

Tokunaga:2008:TRN

[3256] C. Tokunaga, D. Blaauw, and T. Mudge. True random number generator with a metastability-based quality control. *IEEE Journal of Solid-State Circuits*, 43(1):78–85, ???? 2008. CODEN IJSCBC. ISSN 0018-9200 (print), 1558-173X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4443211`.

Toyama:2008:GPR

[3257] Junichiro Toyama and Shunji Kawamoto. Generation of pseudo-random numbers by chaos-type function and its application to cryptosystems. *Electrical Engineering in Japan*, 163(3):67–74, April 30, 2008. CODEN ???? ISSN 1520-6416.

Uchida:2008:FPR

[3258] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis. Fast physical random bit generation with chaotic semiconductor lasers. *Nature Photonics*, 2(12):728–732, November 23, 2008. CODEN NPAHBY. ISSN 1749-4893. URL `http://www.nature.com/nphoton/journal/v2/n12/full/nphoton.2008.227.html`.

Udawatta:2008:TVN

[3259] K. Udawatta, M. Ehsanian, S. Maidanov, and S. Musunuri. Test and validation of a non-deterministic system — True Random Number Generator. In *HLDVT '08. IEEE International High Level Design Validation and Test Workshop, 2008*, pages 77–84. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4695881`.

Varbanets:2008:ESS

[3260] Sergey Varbanets. Exponential sums on the sequences of inversive congruential pseudorandom numbers. *Šiauliai Math. Semin.*, 3(11):247–261, 2008. CODEN ???? ISSN 1822-511X.

Varbanets:2008:ICGa

[3261] S. Varbanets. On inversive congruential generator for pseudorandom numbers with prime power modulus. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 29(??):277–296, ???? 2008. CODEN ???? ISSN 0138-9491.

Varbanets:2008:ICGb

[3262] S. P. Varbanets. Inversive congruential generator with prime power modulus. *Vīsn. Odes. Nats. Unīv.*, 13(17, Matematika i Mekhanika):86–102, 2008. CODEN ???? ISSN ???? URL `http://www.nbuv.gov.ua/portal/Natural/Vonu_math/2008/visnik_math_2008_v17/086-102_varbanets.pdf`.

Walker:2008:EPN

[3263] John Walker. ENT: A pseudorandom number sequence test program. Web site, January 28, 2008. URL `http://www.fourmilab.ch/random/`.

Wang:2008:DCP

[3264] Xing-Yuan Wang and Xiao-Juan Wang. Design of chaotic pseudo-random bit generator and its applications in stream-cipher cryptography. *International Journal of Modern Physics C [Physics and Computers]*, 19 (5):813–820, May 2008. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/19/1905/S0129183108012479.html`.

Ware:2008:RIE

[3265] Willis H. Ware. *RAND and the information evolution: a history in essays and vignettes*. Rand Corporation, Santa Monica, CA, 2008. ISBN 0-8330-4513-X, 0-8330-4816-3, 1-282-45123-5. xxvi + 201 pp. LCCN QA76.27. URL `http://www.jstor.org/stable/10.7249/cp537rc; https://www.rand.org/content/dam/rand/pubs/corporate_pubs/2008/RAND_CP537.pdf`.

Wikramaratna:2008:ACR

[3266] Roy S. Wikramaratna. The additive congruential random number generator — a special case of a multiple recursive generator. *Journal of Computational and Applied Mathematics*, 216(2):371–387, July 1,

2008. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042707002671.

Willink:2008:UPN

[3267] Robin Willink. A unique property of the normal distribution associated with perturbing a general random variable. *The American Statistician*, 62(2):144–146, May 2008. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Wold:2008:AER

[3268] K. Wold and Chik How Tan. Analysis and enhancement of random number generator in FPGA based on oscillator rings. In *2008. ReConFig '08. International Conference on Reconfigurable Computing and FPGAs*, pages 385–390. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4731825.

Xiang:2008:NPR

[3269] Fei Xiang, Shui-Sheng Qiu, and Jie-Xin Pu. A new pseudo-random number generator with application in RSA. In *2008. ICCS 2008. 11th IEEE Singapore International Conference on Communication Systems*, pages 152–156. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4737162.

Xu:2008:SMS

[3270] Peng Xu, T. Horiuchi, and P. Abshire. Stochastic model and simulation of a random number generator circuit. In *2008. ISCAS 2008. IEEE International Symposium on Circuits and Systems*, pages 2977–2980. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4542083.

Yaguchi:2008:NNP

[3271] Hirotake Yaguchi and Izumi Kubo. A new nonrecursive pseudorandom number generator based on chaos mappings. *Monte Carlo Methods and Applications*, 14(1):85–98, May 2008. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://hdl.handle.net/10076/9251; http://www.degruyter.com/view/j/mcma.2008.14.issue-1/mcma.2008.005/mcma.2008.005.xml.

Yang:2008:LLM

[3272] Y. Yang, X. Yang, and C. Zhou. Lmcgrid: a low management cost grid computation model. *International Journal of Computers and Applications*, 30(1):56–61, 2008. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2008.11441875`.

Yang:2008:NTR

[3273] Yang Yang and Guang Zeng. A new type of random number generator for software implementation. In *2008. ISISE '08. International Symposium on Information Science and Engineering*, volume 2, pages 236–238. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4732384`.

Alhakim:2009:MSG

[3274] Abbas Alhakim and Mufutau Akinwande. A multiple stream generator based on de Bruijn digraph homomorphisms. *Journal of Statistical Computation and Simulation*, 79(11):1371–1380, ???? 2009. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949650802322129`.

Anyanwu:2009:DCS

[3275] Matthew N. Anyanwu, Lih-Yuan Deng, and Dipankar Dasgupta. Design of cryptographically strong generator by linearly generated sequences. *International Journal of Computer Science and Security (IJCSS)*, 3(3): 186–200, June 2009. CODEN ???? ISSN 1985-1553. URL `http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue3/IJCSS-78.pdf`.

Awerbuch:2009:RRN

[3276] Baruch Awerbuch and Christian Scheideler. Robust random number generation for peer-to-peer systems. *Theoretical Computer Science*, 410 (6–7):453–466, February 28, 2009. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Aycock:2009:COU

[3277] J. Aycock, J. M. G. Cardenas, and D. M. N. de Castro. Code obfuscation using pseudo-random number generators. In *2009. CSE '09. International Conference on Computational Science and Engineering*, volume 3, pages 418–423. IEEE Computer Society Press, 1109 Spring Street, Suite

300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283236.

Bastos-Filho:2009:IQR

[3278] C. J. A. Bastos-Filho, J. D. Andrade, M. R. S. Pita, and A. D. Ramos. Impact of the quality of random numbers generators on the performance of particle swarm optimization. In *IEEE International Conference on Systems, Man and Cybernetics 2009. SMC 2009.*, pages 4988–4993. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5346366.

Blacher:2009:FRN

[3279] R. Blacher. File of random number. Rapport de recherche LJK, Université de Grenoble, Grenoble, France, 2009. URL http://www-ljk.imag.fr/membres/Rene.Blacher/GEAL/node3.html.

Blacher:2009:PRN

[3280] R. Blacher. A perfect random number generator. Rapport de recherche LJK, Université de Grenoble, Grenoble, France, 2009. URL http://hal.archives-ouvertes.fr/hal-00426555/fr/.

Blaszczyk:2009:EVT

[3281] Marta Blaszczyk and Richard A. Guinee. Experimental validation of a true random binary digit generator fusion with a pseudo random number generator for cryptographic module application. In *IET Irish Signals and Systems Conference (ISSC 2009)*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5524689.

Blaszczyk:2009:HIP

[3282] M. Blaszczyk and R. A. Guinee. Hardware implementation on PCB in tandem with FPGA and experimental validation of a novel true random binary generator. In *SOCC 2009. IEEE International SOC Conference, 2009*, pages 47–50. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5398100.

Cao:2009:DSB

[3283] Fuqiang Cao and Shuguo Li. A double-scroll based true random number generator with power and throughput adjustable. In *2009. ASICON '09. IEEE 8th International Conference on ASIC*, pages 309–312. IEEE

Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5351446`.

Cecen:2009:NHN

[3284] Songul Cecen, R. Murat Demirer, and Coskun Bayrak. A new hybrid nonlinear congruential number generator based on higher functional power of logistic maps. *Chaos, Solitons & Fractals*, 42(2):847–853, October 30, 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0960077909000678`.

Chen:2009:FPM

[3285] Chi-Chi Chen and Hui-Chin Tang. Full period of a multiple recursive random number generator with generalized Mersenne prime number. *Journal of Information & Optimization Sciences*, 30(5):1059–1065, 2009. CODEN JIOSDC. ISSN 0252-2667.

Chen:2009:MTR

[3286] Wei Chen, Wenyi Che, Zhongyu Bi, Jing Wang, Na Yan, Xi Tan, Junyu Wang, Hao Min, and Jie Tan. A 1.04 μW truly random number generator for Gen2 RFID tag. In *A-SSCC 2009. IEEE Asian Solid-State Circuits Conference, 2009*, pages 117–120. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5357193`.

Chi:2009:PQN

[3287] Hongmei Chi. Parallel quasirandom number generations for heterogeneous computing environments. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 24(1):21–29, 2009. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Childs:2009:CIH

[3288] Lindsay N. Childs. *A Concrete Introduction to Higher Algebra*. Undergraduate texts in mathematics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., third edition, 2009. ISBN 0-387-74527-0, 0-387-74725-7 (e-book). xiv + 603 pp. LCCN QA155 .C53 2009.

Cline:2009:CTP

[3289] D. Cline, A. Razdan, and P. Wonka. A comparison of tabular PDF inversion methods. *Computer Graphics Forum*, 28(1):154–160, March 2009. CODEN CGFODY. ISSN 0167-7055 (print), 1467-8659 (electronic).

Colavito:2009:CLT

[3290] L. Colavito and D. Silage. Composite look-up table Gaussian pseudo-random number generator. In *2009. ReConFig '09. International Conference on Reconfigurable Computing and FPGAs*, pages 314–319. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5382071`.

Colavito:2009:EPL

[3291] L. Colavito and D. Silage. Efficient PGA LFSR implementation whitens pseudo random numbers. In *2009. ReConFig '09. International Conference on Reconfigurable Computing and FPGAs*, pages 308–313. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/document/5382070/`.

Curto:2009:CVA

[3292] José Dias Curto and José Castro Pinto. The coefficient of variation asymptotic distribution in the case of non-iid random variables. *Journal of Applied Statistics*, 36(1):21–32, January 2009. CODEN ???? ISSN 0266-4763 (print), 1360-0532 (electronic).

Czernik:2009:CRN

[3293] Pawel Czernik and Jakub Olszyna. Cryptographic random number generators for low-power distributed measurement system. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7502(1): 75022A, 2009. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7502/75022A/1`. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2009.

Danko:2009:IPR

[3294] A. Danko and W. Danko. Improving pseudo-random generators. In *2009. ICBAKE 2009. International Conference on Biometrics and Kansei Engineering*, pages 163–166. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5223218`.

DeMicco:2009:QRC

[3295] L. De Micco, H. A. Larrondo, A. Plastino, and O. A. Rosso. Quantifiers for randomness of chaotic pseudo-random number generators. *Philosophical transactions. Series A, Mathematical, physical, and engineering*

sciences, 367(1901):3281–3296, August 28, 2009. ISSN 1364-503x (print), 1471-2962 (electronic).

Deng:2009:SPM

[3296] Lih-Yuan Deng, Huajiang Li, and Jyh-Jen Horng Shiau. Scalable parallel multiple recursive generators of large order. *Parallel Computing*, 35(1):29–37, January 2009. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167819108001099`.

Devroye:2009:RVG

[3297] Luc Devroye. Random variate generation for exponentially and polynomially tilted stable distributions. *ACM Transactions on Modeling and Computer Simulation*, 19(4):18:1–18:??, October 2009. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Dodson:2009:IGT

[3298] C. T. J. Dodson. Information geometry for testing pseudorandom number generators. *arxiv.org*, ??(??):??, July 10, 2009. URL `http://arxiv.org/abs/0907.1835v1`.

Dogaru:2009:HCA

[3299] R. Dogaru. Hybrid cellular automata as pseudo-random number generators with binary synchronization property. In *ISSCS 2009. International Symposium on Signals, Circuits and Systems 2009*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5206126`.

Dorrendorf:2009:CRN

[3300] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. *ACM Transactions on Information and System Security*, 13(1):10:1–10:32, October 2009. CODEN ATISBQ. ISSN 1094-9224 (print), 1557-7406 (electronic).

Dryver:2009:CSE

[3301] Arthur Dryver. Code snippet: The enhancement of teaching materials for applied statistics courses by combining random number generation and portable document format files via LaTeX. *Journal of Statistical Software*, 31(CS-3):1–9, September 2009. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v31/c03`.

Edrees:2009:HOZ

[3302] Hassan M. Edrees, Brian Cheung, McCullen Sandora, David B. Nummey, and Deian Stefan. Hardware-optimized Ziggurat algorithm for high-speed Gaussian random number generators. In Toomas P. Plaks, editor, *Proceedings of the 2009 International Conference on Engineering of Reconfigurable Systems & Algorithms, ERSA 2009: [at the 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing], WORLDCOMP '09, July 13–16, 2009, Las Vegas, Nevada, USA*, pages 254–260. CSREA Press, ????, 2009. ISBN 1-60132-101-5. LCCN TP302.1-532 I613/2009. URL `http://sprocom.cooper.edu/sprocom2/pubs/conference/ecsns2009ersa.pdf`; `http://www.deian.net/pubs/conference/ersa2009.pdf`.

Faure:2009:GHS

[3303] Henri Faure and Christiane Lemieux. Generalized Halton sequences in 2008: a comparative study. *ACM Transactions on Modeling and Computer Simulation*, 19(4):15:1–15:??, October 2009. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Feldhofer:2009:HIS

[3304] Martin Feldhofer and Johannes Wolkerstorfer. Hardware implementation of symmetric algorithms for RFID security. In Paris Kitsos and Yan Zhang, editors, *RFID Security: Techniques, Protocols and System-on-Chip Design*, pages 373–415. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-76481-X (e-book), 0-387-76480-1 (hardcover). LCCN TK6553 .R45 2008eb. URL `http://www.springerlink.com/content/q1160h1036371331/`.

Fischer:2009:SRF

[3305] Simon Fischer, Willi Meier, and Dirk Stegemann. Some remarks on FCSRs and implications for stream ciphers. *Journal of Mathematical Cryptology*, 3(3):227–236, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Galassi:2009:GSL

[3306] Mark Galassi. *GNU scientific library: reference manual*. A GNU manual. Network Theory, Bristol, UK, third edition, 2009. ISBN 0-9546120-7-8. xvi + 573 pp. LCCN ????

Gao:2009:MPL

[3307] Zhi-Han Gao and Fang-Wei Fu. The minimal polynomial over $\mathbf{F}_q$ of linear recurring sequence over $\mathbf{F}_{q^m}$. *Finite Fields and their Applications*,

15(6):774–784, December 2009. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579709000550`.

Gauvrit:2009:SRI

[3308] N. Gauvrit and J.-P. Delahaye. Scatter and regularity imply Benford's law ... and more. *ArXiv e-prints*, October 2009. CODEN ???? ISSN ???? URL `http://adsabs.harvard.edu/abs/2009arXiv0910.1359G`; `http://arxiv.org/abs/0910.1359`.

Gelenbe:2009:ASN

[3309] Erol Gelenbe. Analysis of single and networked auctions. *ACM Transactions on Internet Technology (TOIT)*, 9(2):8:1–8:??, May 2009. CODEN ???? ISSN 1533-5399 (print), 1557-6051 (electronic).

Gentle:2009:GRN

[3310] James E. Gentle. Generation of random numbers. In *Computational Statistics*, Statistics and Computing, pages 305–331. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-98143-8 (print), 0-387-98144-6 (electronic). LCCN QA276.4 .G46 2009. URL `http://link.springer.com/chapter/10.1007/978-0-387-98144-4_7`.

Guha:2009:EEC

[3311] Sudipto Guha and Kamesh Munagala. Exceeding expectations and clustering uncertain data. In Paredaens and Su [4266], pages 269–278. ISBN 1-60558-553-X. LCCN ????

Guinee:2009:EVH

[3312] R. A. Guinee and M. Blaszczyk. Experimental validation of the hardware implementation of a novel true random binary sequence generator for keystream applications. In *MILCOM 2009. IEEE Military Communications Conference, 2009*, pages 1–7. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5379810`.

Guinee:2009:NTR

[3313] R. A. Guinee and M. Blaszczyk. A novel true random binary sequence generator based on a chaotic double scroll oscillator combination with a pseudo random generator for cryptographic applications. In *ICITST 2009. International Conference for Internet Technology and Secured Transactions, 2009*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,

USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5402536.

Guo:2009:RNG

[3314] Weisen Guo and S. B. Kraines. A random network generator with finely tunable clustering coefficient for small-world social networks. In *2009. CASON '09. International Conference on Computational Aspects of Social Networks*, pages 10–17. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5176096.

Gyorfi:2009:HPT

[3315] T. Gyorfi, O. Cret, and A. Suciu. High performance true random number generator based on FPGA block RAMs. In *2009. IPDPS 2009. IEEE International Symposium on Parallel & Distributed Processing*, pages 1–8. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5161207.

Hai-Wei:2009:HSL

[3316] Shen Hai-Wei and Li Jin-Ping. A high-speed and long-period combined pseudo-random number generator. In *2009. ISCID '09. Second International Symposium on Computational Intelligence and Design*, volume 1, pages 112–114. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5370180.

Haramoto:2009:AST

[3317] Hiroshi Haramoto. Automation of statistical tests on randomness to obtain clearer conclusion. In L'Ecuyer and Owen [4265], pages 411–421 (part 3). ISBN 3-642-04106-X, 3-642-04107-8 (e-book). LCCN Q183.9 .I526 2008.

Hartshorn:2009:BRB

[3318] Kevin Hartshorn. Book review: *The fabulous Fibonacci numbers* by Alfred Posamentier and Ingmar Lehmann. *Journal of Mathematics and the Arts*, 3(2):113–116, ???? 2009. CODEN ???? ISSN 1751-3472 (print), 1751-3480 (electronic). URL http://www.tandfonline.com/doi/abs/10.1080/17513470902897569.

Hashim:2009:RMS

[3319] F. H. Hashim, M. Othman, and M. Ismail. A random matrix spreading code generator for WCDMA rake receiver. In *2009. ISIE 2009. IEEE International Symposium on Industrial Electronics*, pages 2216–2218. IEEE

Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5213125`.

Heidergott:2009:GEC

[3320] Bernd Heidergott and Felisa J. Vázquez-Abad. Gradient estimation for a class of systems with bulk services: a problem in public transportation. *ACM Transactions on Modeling and Computer Simulation*, 19(3):13:1–13:??, June 2009. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Holcomb:2009:PSS

[3321] D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers*, 58(9):1198–1210, September 2009. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4674345`.

Hornfeck:2009:MCG

[3322] Wolfgang Hornfeck and Bernd Harbrecht. Multiplicative congruential generators, their lattice structure, its relation to lattice-sublattice transformations and applications in crystallography. *Acta crystallographica. Section A, Foundations of crystallography*, 65(6):532–542, 2009. CODEN ACACEQ. ISSN 0108-7673 (print), 1600-5724 (electronic).

Hu:2009:TRN

[3323] Yue Hu, Xiaofeng Liao, Kwok wo Wong, and Qing Zhou. A true random number generator based on mouse movement and chaotic cryptography. *Chaos, Solitons & Fractals*, 40(5):2286–2293, 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Jun:2009:HPP

[3324] Ding Jun, Li Na, Guo Yixiong, and Yang Jun. A high-performance pseudo-random number generator based on FPGA. In *2009. WNIS '09. International Conference on Wireless Networks and Information Systems*, pages 290–293. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5381941`.

Kanter:2009:OUR

[3325] do Kanter, Yaara Aviad, Igor Reidler, Elad Cohen, and Michael Rosenbluh. An optical ultrafast random bit generator. *Nature Photonics*, 4(1):58–61, December 13, 2009. CODEN NPAHBY. ISSN 1749-

4885 (print), 1749-4893 (electronic). URL http://www.nature.com/nphoton/journal/v4/n1/full/nphoton.2009.235.html.

Katti:2009:EHI

[3326] R. S. Katti and S. K. Srinivasan. Efficient hardware implementation of a new pseudo-random bit sequence generator. In *2009. ISCAS 2009. IEEE International Symposium on Circuits and Systems*, pages 1393–1396. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5118025.

Ladd:2009:FRN

[3327] Anthony J. C. Ladd. A fast random number generator for stochastic simulations. *Computer Physics Communications*, 180(11):2140–2142, November 2009. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465509001994.

Langdon:2009:FHQ

[3328] W. B. Langdon. A fast high quality pseudo random number generator for nVidia CUDA. In Franz Rothlauf, editor, *GECCO '09 Proceedings of the 11th Annual Conference Companion on Genetic and Evolutionary Computation Conference: Late Breaking Papers*, pages 2511–2513. ACM Press, New York, NY 10036, USA, 2009. ISBN 1-60558-505-X. LCCN ???? URL http://www.cs.ucl.ac.uk/staff/W.Langdon/ftp/gp-code/random-numbers/cuda_park-miller.tar.gz.

Laracy:2009:RVG

[3329] Joseph R. Laracy. Random variate generator. *Software — Practice and Experience*, 39(1):105–110, January 2009. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

LEcuyer:2009:LRN

[3330] Pierre L'Ecuyer and François Panneton. F_2-linear random number generators. In Alexopoulos et al. [4262], pages 169–193. ISBN 1-4419-0816-1 (hardcover). LCCN QA76.9.C65 A383 2009. URL http://link.springer.com/chapter/10.1007/b110059_9.

LEcuyer:2009:TV

[3331] Pierre L'Ecuyer and Richard Simard. TestU01 version 1.2.3. Web site, August 18, 2009. URL http://simul.iro.umontreal.ca/testu01/tu01.html.

Lee:2009:ERA

[3332] Jooyoung Lee and Yongjin Yeom. Efficient RFID authentication protocols based on pseudorandom sequence generators. *Designs, Codes, and Cryptography*, 51(2):195–210, May 2009. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=51&issue=2&spage=195`.

Lee:2009:HHA

[3333] JunKyu Lee, Yu Bi, Gregory D. Peterson, Robert J. Hinde, and Robert J. Harrison. HASPRNG: Hardware Accelerated Scalable Parallel Random Number Generators. *Computer Physics Communications*, 180 (12):2574–2581, December 2009. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465509002100`.

Lemieux:2009:PNG

[3334] Christiane Lemieux. Pseudorandom number generators. In *Monte Carlo and Quasi-Monte Carlo Sampling*, Springer Series in Statistics, pages 1–30. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 0-387-78164-1 (print), 0-387-78165-X (electronic). LCCN ???? URL `http://link.springer.com/chapter/10.1007/978-0-387-78165-5_3`. Chapter 3.

Leydold:2009:RRI

[3335] Josef Leydold and Wolfgang Hörman. Runuran — R interface to the UNU.RAN random variate generators, version 0.10.1. Web site, 2009. URL `http://cran.r-project.org/`.

Leydold:2009:URL

[3336] Josef Leydold and Wolfgang Hörman. UNU.RAN — a library for non-uniform universal random variate generation, version 1.4.1. Web site, 2009. URL `http://statistik.wu.ac.at/unuran/`.

Marchi:2009:PPR

[3337] A. Marchi, A. Liverani, and A. Del Giudice. Polynomial pseudo-random number generator via cyclic phase. *Mathematics and Computers in Simulation*, 79(11):3328–3338, July 2009. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475409001463`.

Markenos:2009:FIA

[3338] A. T. Markenos and S. W. Moore. The frequency injection attack on ring-oscillator-based true random number generators. In Clavier and Gaj [4264], pages 317–331. CODEN LNCSD9. ISBN 3-642-04137-X (print), 3-642-04138-8 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/content/978-3-642-04138-9.

McCullough:2009:AES

[3339] B. D. McCullough. The accuracy of econometric software. In Belsley and Kontoghiorghes [4263], chapter 2, pages 55–79. ISBN 0-470-74385-9. LCCN HB143.5 .H357 2009. URL http://catalogimages.wiley.com/images/db/jimages/9780470743850.jpg; http://www.loc.gov/catdir/enhancements/fy0913/2009025907-d.html; http://www.loc.gov/catdir/enhancements/fy0913/2009025907-t.html.

Mitchum:2009:DPR

[3340] S. T. Mitchum and R. H. Klenke. Divergent path random number generators. In *SOUTHEASTCON '09. IEEE Southeastcon, 2009*, pages 109–114. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5174059.

Mustafa:2009:DPR

[3341] H. A. U. Mustafa. Detection of pseudo random noise generator's parameters for link analysis. In *2009. ICET 2009. International Conference on Emerging Technologies*, pages 362–367. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5353143.

Nakura:2009:ROB

[3342] T. Nakura, M. Ikeda, and K. Asada. Ring oscillator based random number generator utilizing wake-up time uncertainty. In *A-SSCC 2009. IEEE Asian Solid-State Circuits Conference, 2009*, pages 121–124. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5357194.

Nandi:2009:ISA

[3343] Mridul Nandi. Improved security analysis for OMAC as a pseudorandom function. *Journal of Mathematical Cryptology*, 3(2):133–148, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Nekrutkin:2009:STS

[3344] V. Nekrutkin and R. Sabitov. Spectral test and spectral distance for multiplicative generators with moduli 2^p. *Monte Carlo Methods and Applications*, 15(1):1–10, May 2009. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2009.15.issue-1/mcma.2009.001/mcma.2009.001.xml`.

Nies:2009:CR

[3345] André. Nies. *Computability and Randomness*, volume 51 of *Oxford logic guides*. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 2009. ISBN 0-19-923076-5. xv + 433 pp. LCCN QA267.7 .N54 2009. URL `http://catdir.loc.gov/catdir/enhancements/fy0908/2008041662-b.html`; `http://catdir.loc.gov/catdir/enhancements/fy0908/2008041662-d.html`; `http://catdir.loc.gov/catdir/enhancements/fy0908/2008041662-t.html`.

Okten:2009:GNK

[3346] Giray Ökten. Generalized von Neumann–Kakutani transformation and random-start scrambled Halton sequences. *Journal of Complexity*, 25(4):318–331, August 2009. CODEN JOCOEH. ISSN 0885-064X (print), 1090-2708 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0885064X08000897`. See [905].

Orlov:2009:ORN

[3347] Michael Orlov. Optimized random number generation in an interval. *Information Processing Letters*, 109(13):722–725, June 15, 2009. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).

Paindaveine:2009:MRT

[3348] Davy Paindaveine. On multivariate runs tests for randomness. *Journal of the American Statistical Association*, 104(488):1525–1538, December 2009. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic).

Pareschi:2009:PAC

[3349] F. Pareschi, G. Scotti, L. Giancane, R. Rovatti, G. Setti, and A. Trifiletti. Power analysis of a chaos-based random number generator for cryptographic security. In *2009. ISCAS 2009. IEEE International Symposium on Circuits and Systems*, pages 2858–2861. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5118398`.

Petrov:2009:SLL

[3350] V. V. Petrov. On the strong law of large numbers for nonnegative random variables. *Theory of Probability and its Applications*, 53(2):346–349, ???? 2009. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Qiu:2009:CMW

[3351] Meikang Qiu and Edwin H.-M. Sha. Cost minimization while satisfying hard/soft timing constraints for heterogeneous embedded systems. *ACM Transactions on Design Automation of Electronic Systems*, 14(2):25:1–25:??, March 2009. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Reidler:2009:USR

[3352] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter. Ultrahigh-speed random number generation based on a chaotic semiconductor laser. *Physical Review Letters*, 103(2):024102, July 2009. CODEN PRLTAO. ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145. URL `http://link.aps.org/doi/10.1103/PhysRevLett.103.024102`.

Ridout:2009:GRN

[3353] M. S. Ridout. Generating random numbers from a distribution specified by its Laplace transform. *Statistics and Computing*, 19(4):439–450, December 2009. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/s11222-008-9103-x`.

Santoro:2009:FEF

[3354] R. Santoro, O. Sentieys, and S. Roy. On-the-fly evaluation of FPGA-based true random number generator. In *2009. ISVLSI '09. IEEE Computer Society Annual Symposium on VLSI*, pages 55–60. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5076383`.

Santoro:2009:LMR

[3355] R. Santoro, O. Sentieys, and S. Roy. On-line monitoring of random number generators for embedded security. In *2009. ISCAS 2009. IEEE International Symposium on Circuits and Systems*, pages 3050–3053. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5118446`.

Sindhikara:2009:BSS

[3356] D. J. Sindhikara, S. Kim, A. F. Voter, and A. E. Roitberg. Bad seeds sprout perilous dynamics: Stochastic thermostat induced trajectory synchronization in biomolecules. *Journal of Chemical Theory and Computation*, 5(6):1624–1631, June 9, 2009. CODEN JCTCCE. ISSN 1549-9618 (print), 1549-9626 (electronic). URL `http://pubs.acs.org/doi/abs/10.1021/ct800573m`.

Sinescu:2009:BWS

[3357] V. Sinescu and P. L'Ecuyer. On the behavior of weighted star discrepancy bounds for shifted lattice rules. In L'Ecuyer and Owen [4265], pages 603–616. ISBN 3-642-04106-X, 3-642-04107-8 (e-book). LCCN Q183.9 .I526 2008.

Srinivasan:2009:BPV

[3358] S. Srinivasan, S. Mathew, V. Erraguntla, and R. Krishnamurthy. A 4Gbps 0.57pJ/bit process-voltage-temperature variation tolerant all-digital true random number generator in 45nm CMOS. In *2009 22nd International Conference on VLSI Design*, pages 301–306. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4749691`.

Sun:2009:CPR

[3359] Fuyan Sun and Shutang Liu. Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos, Solitons & Fractals*, 41(5):2216–2219, ???? 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Svozil:2009:TCQ

[3360] Karl Svozil. Three criteria for quantum random-number generators based on beam splitters. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 79(5):054306, May 2009. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.79.054306`.

Tafazzoli:2009:PCE

[3361] Ali Tafazzoli, Stephen Roberts, Robert Klein, Reid Ness, and Robert Dittus. Probabilistic cost-effectiveness comparison of screening strategies for colorectal cancer. *ACM Transactions on Modeling and Computer Simulation*, 19(2):6:1–6:??, March 2009. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Tang:2009:FPS

[3362] Hui-Chin Tang and Chi-Chi Chen. Full period and spectral test of linear congruential generator and second-order multiple recursive generator. *Journal of Information & Optimization Sciences*, 30(4):769–777, 2009. CODEN JIOSDC. ISSN 0252-2667.

Tawfeeq:2009:RNG

[3363] S. K. Tawfeeq. A random number generator based on single-photon avalanche photodiode dark counts. *Journal of Lightwave Technology*, 27(24):5665–5667, ???? 2009. CODEN JLTEDG. ISSN 0733-8724 (print), 1558-2213 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5286273`.

Thamrin:2009:EHB

[3364] N. M. Thamrin, G. Witjaksono, A. Nuruddin, and M. S. Abdullah. An enhanced hardware-based hybrid random number generator for cryptosystem. In *2009. ICIME '09. International Conference on Information Management and Engineering*, pages 152–156. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5077017`.

Tian:2009:PTE

[3365] Tian Tian and Wen-Feng Qi. Periods of termwise exclusive ors of maximal length FCSR sequences. *Finite Fields and their Applications*, 15(2):214–235, April 2009. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579708000762`.

Tisa:2009:OCQ

[3366] Simone Tisa and Franco Zappa. One-chip quantum random number generator. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7236(1):72360J, 2009. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7236/72360J/1`. Quantum Communications Realized II.

Tong:2009:RAPa

[3367] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number generator. In *2009. CSO 2009. International Joint Conference on Computational Sciences and Optimization*, volume 1, pages 292–294. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring,

MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5193698`.

Tong:2009:RAPb

[3368] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number generator for face recognition system. In *2009. ICBBE 2009. 3rd International Conference on Bioinformatics and Biomedical Engineering*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5162237`.

Tzeng:2009:RNG

[3369] Jengnan Tzeng, I-Te Chen, and Jer-Min Tsai. Random number generator designed by the divergence of scaling functions. In *2009. IIH-MSP '09. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 1038–1041. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5337396`.

Uchida:2009:FPR

[3370] A. Uchida, T. Honjo, K. Amano, K. Hirano, H. Someya, H. Okumura, S. Yoshimori, K. Yoshimura, P. Davis, and Y. Tokura. Fast physical random bit generator based on chaotic semiconductor lasers: Application to quantum cryptography. In *Lasers and Electro-Optics 2009 and the European Quantum Electronics Conference. CLEO Europe - EQEC 2009. European Conference on*, page 1. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5192510`.

Umlauft:2009:GNS

[3371] Martina Umlauft and Peter Reichl. Getting network simulation basics right — a note on seed setting effects for the ns-2 random number generator. *Lecture Notes in Electrical Engineering*, 44:215–228, 2009. CODEN ???? ISSN 1876-1100.

vanMeel:2009:GFS

[3372] J. A. van Meel, D. Frenkel, and P. Charbonneau. Geometrical frustration: a study of four-dimensional hard spheres. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 79(3):030201, March 2009. CODEN PLEEE8. ISSN 1539-3755

(print), 1550-2376 (electronic). URL `http://link.aps.org/doi/10.1103/PhysRevE.79.030201`.

Verloop:2009:HTA

[3373] I. M. Verloop, U. Ayesta, and R. Núñez-Queija. Heavy-traffic analysis of the M/PH/1 discriminatory processor sharing queue with phase-dependent weights. *ACM SIGMETRICS Performance Evaluation Review*, 37(2):42–44, September 2009. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Volos:2009:IEP

[3374] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos. Image encryption process based on a chaotic True Random Bit Generator. In *2009 16th International Conference on Digital Signal Processing*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5201107`.

vonzurGathen:2009:SSP

[3375] Joachim von zur Gathen and Igor E. Shparlinski. Subset sum pseudorandom numbers: fast generation and distribution. *Journal of Mathematical Cryptology*, 3(2):149–163, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wang:2009:NPR

[3376] Qianxue Wang, C. Guyeux, and J. M. Bahi. A novel pseudo-random number generator based on discrete chaotic iterations. In *2009. INTERNET '09. First International Conference on Evolving Internet*, pages 71–76. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5277860`.

Wayne:2009:PAT

[3377] Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, ???? 2009. CODEN JMOPEW. ISSN 0950-0340 (print), 1362-3044 (electronic). URL `http://www.tandfonline.com/doi/abs/10.1080/09500340802553244`.

Wei:2009:BFT

[3378] W. Wei and H. Guo. Bias-free true random-number generator. *Optics Letters*, 34(12):1876–1878, ???? 2009. CODEN OPLEDP. ISSN 0146-9592.

Wei:2009:QRN

[3379] Wei Wei and Hong Guo. Quantum random number generator based on the photon number decision of weak laser pulses. In *2009. CLEO/ PACIFIC RIM '09. Conference on Lasers & Electro Optics & The Pacific Rim Conference on Lasers and Electro-Optics*, pages 1–2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5292482`.

Wold:2009:OST

[3380] K. Wold and S. Petrovic. Optimizing speed of a true random number generator in FPGA by spectral analysis. In *2009. ICCIT '09. Fourth International Conference on Computer Sciences and Convergence Information Technology*, pages 1105–1110. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5369959`.

Xiao-chen:2009:URN

[3381] Gu Xiao-chen and Zhang Min-xuan. Uniform random number generator using leap ahead LFSR architecture. In *2009. ICCCS '09. International Conference on Computer and Communications Security*, pages 150–154. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380287`.

Yamanashi:2009:SRN

[3382] Y. Yamanashi and N. Yoshikawa. Superconductive random number generator using thermal noises in SFQ circuits. *IEEE Transactions on Applied Superconductivity*, 19(3):630–633, ???? 2009. CODEN ITASE9. ISSN 1051-8223 (print), 1558-2515 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5075615`.

Youssef:2009:IEU

[3383] M. I. Youssef, M. Zahara, A. E. Emam, and M. A. Elghany. Image encryption using pseudo random number and chaotic sequence generators. In *NRSC 2009. National Radio Science Conference, 2009*, pages 1–15. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5233974`.

Yu:2009:ESC

[3384] Senhua Yu and D. Dasgupta. An empirical study of Conserved Self Pattern Recognition Algorithm: Comparing to other one-class classifiers and

evaluating with random number generators. In *2009. NaBIC 2009. World Congress on Nature & Biologically Inspired Computing*, pages 403–408. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5393571`.

Yuhua:2009:EDR

[3385] Wang Yuhua, Wang HongYong, Guan Aihong, and Zhang Huanguo. Evolutionary design of random number generator. In *2009. JCAI '09. International Joint Conference on Artificial Intelligence*, pages 256–259. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5158988`.

Zhu:2009:WFB

[3386] Hegui Zhu, Xiangde Zhang, and Lianping Yang. Weierstrass function-based uniform random number generator. In *2009. GCIS '09. WRI Global Congress on Intelligent Systems*, volume 2, pages 343–347. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2009. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5209417`.

Abbott:2010:QRN

[3387] Alistair A. Abbott, Cristian S. Calude, and Karl Svozil. A quantum random number generator certified by value indefiniteness. Research Report CDMTCS-396, Centre for Discrete Mathematics and Theoretical Computer Science, The University of Auckland, Auckland, NZ, December 2010. URL `http://www.cs.auckland.ac.nz/CDMTCS/researchreports/396cris.pdf`.

Agapie:2010:RPH

[3388] Stefan C. Agapie and Paula A. Whitlock. Random packing of hyperspheres and Marsaglia's parking lot test. *Monte Carlo Methods and Applications*, 16(3–4):197–209, December 2010. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2010.16.issue-3-4/mcma.2010.019/mcma.2010.019.xml`.

Akhshani:2010:PRN

[3389] Afshin Akhshani, Sohrab Behnia, Amir Akhavan, Siew-Choo Lim, and Zainuriah Hassan. Pseudo random number generator based on synchronized chaotic maps. *International Journal of Modern Physics C*

[Physics and Computers], 21(2):275–290, February 2010. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL `http://www.worldscinet.com/ijmpc/21/2102/S0129183110015117.html`.

Anashin:2010:NAE

[3390] Vladimir Anashin. Non-Archimedean ergodic theory and pseudorandom generators. *The Computer Journal*, 53(4):370–392, May 2010. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/cgi/content/abstract/53/4/370`; `http://comjnl.oxfordjournals.org/cgi/reprint/53/4/370`.

Anyanwu:2010:DCS

[3391] Matthew N. Anyanwu, Lih-Yuan Deng, and Dipankar Dasgupta. Design of cryptographically strong generator by linearly generated sequences. Report ??, The University of Memphis, Memphis, TN 38152, USA, January 12, 2010. URL `http://ais.cs.memphis.edu/files/papers/Mathew-security-paper.pdf`.

Banks:2010:DES

[3392] Jerry Banks, John S. Carson, Barry L. Nelson, and David M. Nicol. *Discrete-Event System Simulation*. Prentice-Hall, Upper Saddle River, NJ, USA, fifth edition, 2010. ISBN 0-13-606212-1, 0-13-815037-0 (paperback). xviii + 622 pp. LCCN T57.62 .D53 2010.

Barsegov:2010:EPR

[3393] Valeri A. Barsegov. Efficient pseudo-random number generators for biomolecular simulations on graphics processors. *Abstracts of Papers of the American Chemical Society*, 240(??):94–PHYS, August 22, 2010. CODEN ACSRAL. ISSN 0065-7727.

Bassham:2010:STS

[3394] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report SP 800-22 Rev. 1a., National Institute for Standards and Technology, Gaithersburg, MD, USA, 2010.

Bastos-Filho:2010:IRN

[3395] C. J. A. Bastos-Filho, M. A. C. Oliveira, D. N. O. Nascimento, and A. D. Ramos. Impact of the random number generator quality on particle swarm optimization algorithm running on graphic processor units. In *2010 10th International Conference on Hybrid Intelligent Systems (HIS)*,

pages 85–90. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5601073.

Bellare:2010:PFP

[3396] Mihir Bellare and David Cash. Pseudorandom functions and permutations provably secure against related-key attacks. *Lecture Notes in Computer Science*, 6223:666–684, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/r15187t06828272v/.

Berger:2010:FFF

[3397] Arno Berger and Theodore P. Hill. Fundamental flaws in Feller's classical derivation of Benford's Law. *ArXiv e-prints*, May 2010. CODEN ???? ISSN ???? URL http://adsabs.harvard.edu/abs/2010arXiv1005.2598B; http://arxiv.org/abs/1005.2598.

Binder:2010:MCS

[3398] K. (Kurt) Binder and Dieter W. Heermann. *Monte Carlo simulation in statistical physics: an introduction*. Graduate texts in physics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fifth edition, 2010. ISBN 3-642-03162-5. ISSN 1868-4513. xiv + 200 pp. LCCN QC174.85.M64 B56 2010.

Blacher:2010:PRN

[3399] R. Blacher. A perfect random number generator. II. Rapport de recherche LJK, Université de Grenoble, Grenoble, France, 2010. URL http://hal.archives-ouvertes.fr/hal-00443576/fr/.

Borovkov:2010:ILL

[3400] A. A. Borovkov. Integro-local and local theorems on normal and large deviations of the sums of nonidentically distributed random variables in the triangular array scheme. *Theory of Probability and its Applications*, 54(4):571–587, ???? 2010. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Braverman:2010:PGR

[3401] Mark Braverman, Anup Rao, Ran Raz, and Amir Yehudayoff. Pseudorandom generators for regular branching programs. In IEEE [4274], pages 40–47. ISBN 0-7695-4244-1, 1-4244-8525-8. ISSN 0272-5428. LCCN QA76 .S95 2010. URL http://opac.ieeecomputersociety.org/opac?year=2010&volume=00&catalog=4244&acronym=focs. IEEE Computer Society order number P4244.

Brody:2010:CPP

[3402] Joshua Brody and Elad Verbin. The coin problem and pseudo-randomness for branching programs. In IEEE [4274], pages 30–39. ISBN 0-7695-4244-1, 1-4244-8525-8. ISSN 0272-5428. LCCN QA76 .S95 2010. URL `http://opac.ieeecomputersociety.org/opac?year=2010&volume=00&catalog=4244&acronym=focs`. IEEE Computer Society order number P4244.

Calude:2010:EEQ

[3403] Cristian S. Calude, Michael J. Dinneen, Monica Dumitrescu, and Karl Svozil. Experimental evidence of quantum randomness incomputability. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 82 (2):022102, August 2010. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.82.022102`.

Chang:2010:PRN

[3404] Weiling Chang, Binxing Fang, Xiaochun Yun, Shupeng Wang, and Xiangzhan Yu. A pseudo-random number generator based on LZSS. In *2010 Data Compression Conference (DCC)*, page 524. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5453503`.

Chari:2010:DSC

[3405] Suresh Chari, Vincenzo V. Diluoffo, Paul A. Karger, Elaine R. Palmer, Tal Rabin, Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, Michael Steiner, and David C. Toll. Designing a side channel resistant random number generator. In Gollmann et al. [4272], pages 49–64. ISBN 3-642-12509-3 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.S62 C36 2010. URL `http://www.informatik.uni-trier.de/~ley/db/conf/cardis/cardis2010.html#ChariDKPRRRSST10`.

Chaudhuri:2010:SI

[3406] Swarat Chaudhuri and Armando Solar-Lezama. Smooth interpretation. *ACM SIGPLAN Notices*, 45(6):279–291, June 2010. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Chen:2010:RED

[3407] Shih-Liang Chen, TingTing Hwang, and Wen-Wei Lin. Randomness enhancement for a digitalized modified-logistic map based pseudo random

number generator. In *2010 International Symposium on VLSI Design Automation and Test (VLSI-DAT)*, pages 164–167. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5496716`.

Cheong:2010:ERE

[3408] Siotai Cheong and Pingyi Fan. The effect of random encoding generators on the performance of LT codes. In *2010 International Conference on Communications and Mobile Computing (CMC)*, volume 2, pages 306–310. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5471271`.

Chi:2010:GPR

[3409] Hongmei Chi and Yanzhao Cao. Generating parallel random sequences via parameterizing EICGs for heterogeneous computing environments. *Lecture Notes in Computer Science*, 6019:409–417, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://www.springerlink.com/content/kp3hj81g12216435/`. Proceedings of Computational Science and Its Applications — ICCSA 2010.

Derflinger:2010:RVG

[3410] Gerhard Derflinger, Wolfgang Hörmann, and Josef Leydold. Random variate generation by numerical inversion when only the density is known. *ACM Transactions on Modeling and Computer Simulation*, 20(4):18:1–18:??, October 2010. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

DeRoover:2010:MPR

[3411] C. De Roover and M. Steyaert. A 500 mV 650 pW random number generator in 130 nm CMOS for a UWB localization system. In *2010 Proceedings of the ESSCIRC*, pages 278–281. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5619875`.

deSchryver:2010:NHE

[3412] Christian de Schryver, Daniel Schmidt, Norbert Wehn, Elke Korn, Henning Marxen, and Ralf Korn. A new hardware efficient inversion based random number generator for non-uniform distributions. In Viktor Prasanna, editor, *International Conference on Reconfigurable Computing and FPGAs (ReConFig), 2010: 13–15 December 2010,*

Cancun, Mexico: proceedings, pages 190–195. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 0-7695-4314-6, 1-4244-9523-7. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5695304; https://ems.eit.uni-kl.de/fileadmin/ems/pdf/schsch_10.pdf`.

Doty-Humphrey:2010:PRC

[3413] C. Doty-Humphrey. Practically random: C++ library of statistical tests for RNGs. Web site., 2010. URL `https://sourceforge.net/projects/pracrand`.

Downey:2010:ARC

[3414] R. G. (Rod G.) Downey and Denis Roman Hirschfeldt. *Algorithmic Randomness and Complexity*. Theory and applications of computability. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 0-387-95567-4 (hardcover), 0-387-68441-7 (e-book). ISSN 2190-619X. xxviii + 855 pp. LCCN QA267.7 .D67 2010. URL `http://catdir.loc.gov/catdir/enhancements/fy1202/2011377427-d.html; http://catdir.loc.gov/catdir/enhancements/fy1202/2011377427-t.html`.

Duplys:2010:KRU

[3415] P. Duplys, E. Böhl, and W. Rosenstiel. Key randomization using a power analysis resistant deterministic random bit generator. In *2010 IEEE 16th International On-Line Testing Symposium (IOLTS)*, pages 229–234. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5560197`.

ElHaddad:2010:QMC

[3416] R. El Haddad, C. Lécot, P. L'Ecuyer, and N. Nassif. Quasi-Monte Carlo methods for Markov chains with continuous multi-dimensional state space. *Mathematics and Computers in Simulation*, 81(3):560–567, November 2010. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475410002648`.

Feldman:2010:BMC

[3417] Richard M. Feldman and Ciriaco Valdez-Flores. Basics of Monte Carlo simulation. In *Applied probability and stochastic processes* [4271], pages 45–72. ISBN 3-642-05155-3, 3-642-05158-8. LCCN QA274 .F45 2010. URL `http://swbplus.bsz-bw.de/bsz314370110inh.htm; http://swbplus.bsz-bw.de/bsz314370110kap.htm; http://swbplus.bsz-`

bw.de/bsz314370110vor.htm; http://www.gbv.de/dms/zbw/609423665.pdf.

Gabizon:2010:DEW

[3418] Ariel Gabizon. *Deterministic Extraction from Weak Random Sources*. Monographs in theoretical computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-14902-2, 3-642-14903-0 (e-book). 148 pp. LCCN QA564 .G33 2011.

Gabriel:2010:GUQ

[3419] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711–715, August 29, 2010. CODEN NPAHBY. ISSN 1749-4885 (print), 1749-4893 (electronic). URL http://www.nature.com/nphoton/journal/v4/n10/full/nphoton.2010.197.html.

Gong:2010:APR

[3420] Chunye Gong, Jie Liu, Lihua Chi, Qingfeng Hu, Li Deng, and Zhenghu Gong. Accelerating pseudo-random number generator for MCNP on GPU. *AIP Conference Proceedings*, 1281(1):1335–1337, 2010. CODEN APCPCS. ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. URL http://link.aip.org/link/?APC/1281/1335/1.

Gotlieb:2010:URT

[3421] Arnaud Gotlieb and Matthieu Petit. A uniform random test data generator for path testing. *The Journal of Systems and Software*, 83(12): 2618–2626, December 2010. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).

Guler:2010:DIR

[3422] U. Güler, S. Ergün, and G. Dündar. A digital IC random number generator with logic gates only. In *2010 17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, pages 239–242. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5724498.

Guler:2010:HSI

[3423] U. Güler and S. Ergün. A high speed IC random number generator based on phase noise in ring oscillators. In *Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 425–428. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver

Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5537698.

Guo:2010:TRN

[3424] Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei. Truly random number generation based on measurement of phase noise of a laser. *Physical Review E (Statistical physics, plasmas, fluids, and related interdisciplinary topics)*, 81(5):051137, May 2010. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL http://link.aps.org/doi/10.1103/PhysRevE.81.051137.

Guyeux:2010:IRN

[3425] C. Guyeux, Qianxue Wang, and J. M. Bahi. Improving random number generators by chaotic iterations application in data hiding. In *2010 International Conference on Computer Application and System Modeling (ICCASM)*, volume 13, pages V13–643–V13–647. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5622199.

Haitner:2010:EIC

[3426] Iftach Haitner, Omer Reingold, and Salil Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. In ACM [4267], pages 437–446. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Hongo:2010:RNG

[3427] Kenta Hongo, Ryo Maezono, and Kenichi Miura. Random number generators tested on quantum Monte Carlo simulations. *Journal of Computational Chemistry*, 31(11):2186–2194, August 2010. CODEN JCCHDD. ISSN 0192-8651 (print), 1096-987X (electronic).

Hotoleanu:2010:RTT

[3428] D. Hoţoleanu, O. Crettţ, A. Suciu, T. Gyorfi, and L. Vácariu. Real-time testing of true random number generators through dynamic reconfiguration. In *2010 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD)*, pages 247–250. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5615649.

Jaksic:2010:QCL

[3429] V. Jaksić, Y. Pautrat, and C.-A. Pillet. A quantum central limit theorem for sums of independent identically distributed random variables. *Journal of Mathematical Physics*, 51(1):015208, January 2010. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427. URL `http://jmp.aip.org/resource/1/jmapaq/v51/i1/p015208_s1`.

Jones:2010:GPP

[3430] David Jones. Good practice in (pseudo) random number generation for bioinformatics applications. Report, Bioinformatics Group, University College London, London, UK, May 7, 2010. 13 pp. URL `http://www0.cs.ucl.ac.uk/staff/d.jones/GoodPracticeRNG.pdf`.

Jones:2010:IMD

[3431] Willie D. Jones. Intel makes a digital coin tosser for future processors. *IEEE Spectrum*, ??(??):??, June 29, 2010. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://spectrum.ieee.org/computing/hardware/intel-makes-a-digital-coin-tosser-for-future-processors`.

Kang:2010:FIG

[3432] Minsu Kang. FPGA implementation of Gaussian-distributed pseudo-random number generator. In *2010 6th International Conference on Digital Content, Multimedia Technology and its Applications (IDC)*, pages 11–13. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5568516`.

Kawai:2010:AOA

[3433] Reiichiro Kawai. Asymptotically optimal allocation of stratified sampling with adaptive variance reduction by strata. *ACM Transactions on Modeling and Computer Simulation*, 20(2):9:1–9:??, April 2010. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Kwon:2010:QRN

[3434] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum random number generator using photon-number path entanglement. *Proceedings of the SPIE — The International Society for Optical Engineering*, 7815 (1):78150D, 2010. CODEN PSISDG. ISSN 0277-786X (print), 1996-756X (electronic). URL `http://link.aip.org/link/?PSI/7815/78150D/1`. Quantum Communications and Quantum Imaging VIII.

Lan:2010:RNG

[3435] Jingjing Lan, Wang Ling Goh, Zhi Hui Kong, and Kiat Seng Yeo. A random number generator for low power cryptographic application. In *2010 International SoC Design Conference (ISOCC)*, pages 328–331. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5682906`.

LEcuyer:2010:CPR

[3436] P. L'Ecuyer and C. Sanvido. Coupling from the past with randomized quasi-Monte Carlo. *Mathematics and Computers in Simulation*, 81(3):476–489, November 2010. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475409002912`.

LEcuyer:2010:DIE

[3437] Pierre L'Ecuyer, David Munger, and Bruno Tuffin. On the distribution of integration error by randomly-shifted lattice rules. *Electron. J. Stat.*, 4:950–993, 2010. ISSN 1935-7524.

LEcuyer:2010:PNG

[3438] Pierre L'Ecuyer. Pseudorandom number generators. In Cont [4269], page ?? ISBN 0-470-06160-X, 0-470-05756-4. LCCN HG106 .E53 2010. Four volumes.

Lirkov:2010:APR

[3439] I. Lirkov and S. Stoilova. Analysis of pseudo-random properties of nonlinear congruential generators with power of two modulus by numerical computing of the b-adic diaphony. In *Proceedings of the 2010 International Multiconference on Computer Science and Information Technology (IMCSIT)*, pages 309–315. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5679724`.

Liu:2010:TRN

[3440] Yu Liu, Wenzhuo Tang, and Hong Guo. True random number generator based on the phase noise of laser. In *2010 Conference on Lasers and Electro-Optics (CLEO) and Quantum Electronics and Laser Science Conference (QELS)*, pages 1–2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5499968`.

Lovett:2010:PGC

[3441] Shachar Lovett, Partha Mukhopadhyay, and Amir Shpilka. Pseudorandom generators for CC0[p] and the Fourier spectrum of low-degree polynomials over finite fields. In IEEE [4274], pages 695–704. ISBN 0-7695-4244-1, 1-4244-8525-8. ISSN 0272-5428. LCCN QA76 .S95 2010. URL `http://opac.ieeecomputersociety.org/opac?year=2010&volume=00&catalog=4244&acronym=focs`. IEEE Computer Society order number P4244.

Luan:2010:PRC

[3442] Lan Luan. The pseudo-random code generator design based on FPGA. In *2010 International Conference on System Science, Engineering Design and Manufacturing Informatization (ICSEM)*, volume 2, pages 282–284. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5640219`.

Luo:2010:PAE

[3443] Yiyuan Luo, Xuejia Lai, and Zheng Gong. Pseudorandomness analysis of the (extended) Lai–Massey scheme. *Information Processing Letters*, 111(2):90–96, December 31, 2010. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). See [1637].

Maaref:2010:GVR

[3444] A. Maaref and R. Annavajjala. The gamma variate and random shape parameter and some applications. *IEEE Communications Letters*, 14 (12):1146–1148, December 2010. CODEN ICLEF6. ISSN 1089-7798 (print), 1558-2558 (electronic). URL `https://ieeexplore.ieee.org/document/5620992`.

Marsaglia:2010:SKR

[3445] George Marsaglia. SUPER KISS random-number generator. Web posting, November 3, 2010. URL `http://www.velocityreviews.com/forums/t704080-re-rngs-a-super-kiss.html`.

Marton:2010:RDC

[3446] Kinga Marton, Alin Suciu, and Iosif Ignat. Randomness in digital cryptography: a survey. *Romanian Journal of Information Science and Technology*, 13(3):219–240, ???? 2010. CODEN ???? ISSN 1453-8245. URL `http:www.imt.ro/romjist/Volum13/Number13_3/pdf/KMarton.pdf`.

Meka:2010:PGP

[3447] Raghu Meka and David Zuckerman. Pseudorandom generators for polynomial threshold functions. In ACM [4267], pages 427–436. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Moghadam:2010:DRN

[3448] I. Zarei Moghadam, A. S. Rostami, and M. R. Tanhatalab. Designing a random number generator with novel parallel LFSR substructure for key stream ciphers. In *2010 International Conference on Computer Design and Applications (ICCDA)*, volume 5, pages V5–598–V5–601. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5541188.

Murguia:2010:IAP

[3449] J. S. Murguía, M. Mejía Carlos, H. C. Rosu, and G. Flores-Eraña. Improvement and analysis of a pseudo-random bit generator by means of cellular automata. *International Journal of Modern Physics C [Physics and Computers]*, 21(6):741–756, June 2010. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL http://www.worldscinet.com/ijmpc/21/2106/S0129183110015440.html.

NanoOpticsGroup:2010:HBR

[3450] Nano-Optics Group and PicoQuant GmbH. High bit rate quantum random number generator service. Humboldt University of Berlin Web site., 2010. URL http://qrng.physik.hu-berlin.de/.

Navin:2010:CSR

[3451] A. H. Navin, E. S. A. Khani, M. K. Mirnia, and S. Y. Torabi. Chi-square random variable generator: Data-oriented approach. In *2010 International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 460–465. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5702014.

Navin:2010:ETU

[3452] A. H. Navin, Z. Navadad, B. Aasadi, and M. Mirnia. Encrypted tag by using data-oriented random number generator to increase security in wireless sensor network. In *2010 International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 335–338. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver

Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5701989.

Ning:2010:GRO

[3453] Liaoyi Ning, Wenchuan Wu, and Boming Zhang. Generator random outage model for risk-based monthly maintenance scheduling. In *2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, pages 126–130. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5528986.

Orue:2010:TNP

[3454] A. B. Orue, G. Alvarez, A. Guerra, G. Pastor, M. Romera, and F. Montoya. Trident, a new pseudo random number generator based on coupled chaotic maps. *arxiv.org*, ??(??):??, August 2010. URL http://arxiv.org/abs/1008.2345.

Ostafe:2010:DGS

[3455] Alina Ostafe and Igor E. Shparlinski. On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. *Mathematics of Computation*, 79(269):501–511, January 2010. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journals/mcom/2010-79-269/S0025-5718-09-02271-6/home.html; http://www.ams.org/journals/mcom/2010-79-269/S0025-5718-09-02271-6/S0025-5718-09-02271-6.pdf.

Ostafe:2010:MPP

[3456] Alina Ostafe. Multivariate permutation polynomial systems and nonlinear pseudorandom number generators. *Finite Fields and their Applications*, 16(3):144–154, May 2010. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1071579709000823.

Ostafe:2010:PNH

[3457] Alina Ostafe and Igor E. Shparlinski. Pseudorandom numbers and hash functions from iterations of multivariate polynomials. *Cryptography and Communications*, 2(1):49–67, April 2010. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s12095-009-0016-0.

Ostafe:2010:PNM

[3458] Alina Ostafe, Elena Pelican, and Igor E. Shparlinski. On pseudorandom numbers from multivariate polynomial systems. *Finite Fields and their Applications*, 16(5):320–328, September 2010. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579710000511`.

Panneton:2010:RSR

[3459] François Panneton and Pierre L'Ecuyer. Resolution-stationary random number generators. *Mathematics and Computers in Simulation*, 80(6):1096–1103, February 2010. CODEN MCSIDR. ISSN 0378-4754 (print), 1872-7166 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0378475407002625`.

Pareschi:2010:ITH

[3460] F. Pareschi, G. Setti, and R. Rovatti. Implementation and testing of high-speed CMOS true random number generators based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 57(12): 3124–3137, ???? 2010. CODEN ???? ISSN 1549-8328 (print), 1558-0806 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5556050`.

Pashley:2010:GRN

[3461] P. J. Pashley and A. Amodeo. Generating random numbers. In Peterson et al. [4275], pages 184–189. ISBN 0-08-044894-1 (e-book), 0-08-044893-3 (set), 0-08-044895-X (vol. 1), 0-08-044896-8 (vol. 2), 0-08-044897-6 (vol. 3), 0-08-044898-4 (vol. 4), 0-08-044899-2 (vol. 5), 0-08-044900-X (vol. 6), 0-08-044901-8 (vol. 7), 0-08-044902-6 (vol. 8). LCCN LB15 .I569 2010. URL `http://www.sciencedirect.com/science/article/pii/B9780080448947013750`. Eight volumes.

Passerat-Palmbach:2010:RIG

[3462] Jonathan Passerat-Palmbach, Claude Mazel, Antoine Mahul, and David R. C. Hill. Reliable initialization of GPU-enabled parallel stochastic simulations using Mersenne Twister for graphics processors. In Gerrit K. Janssens, editor, *Modelling and Simulation 2010: the European Simulation and Modelling Conference 2010; ESM'2010; October 25–27, 2010, Hasselt, Belgium*, pages 187–195. EUROSIS-ETI, Ostend, Belgium, 2010. ISBN 90-77381-57-0. LCCN ???? URL `http://www.mathpubs.com/detail/1501.07701v1/Reliable-Initialization-of-GPU-enabled-Parallel-Stochastic-Simulations-Using-Mersenne-Twister-for-Gr`.

Peris-Lopez:2010:CSP

[3463] Pedro Peris-Lopez, Enrique San Millán, Jan C. A. van der Lubbe, and Luis A. Entrena. Cryptographically secure pseudo-random bit generator for RFID tags. In *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5678035`.

Plesser:2010:RSI

[3464] Hans Ekkehard Plesser and Anders Grønvik Jahnsen. Re-seeding invalidates tests of random number generators. *Applied Mathematics and Computation*, 217(1):339–346, September 1, 2010. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300310006259`. See [3204].

Proschan:2010:BQQ

[3465] Michael A. Proschan and Jeffrey S. Rosenthal. Beyond the quintessential quincunx. *The American Statistician*, 64(1):78–82, February 2010. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).

Qi:2010:DFR

[3466] Aixue Qi, Chunyan Han, and Guangyi Wang. Design and FPGA realization of a pseudo random sequence generator based on a switched chaos. In *2010 International Conference on Communications, Circuits and Systems (ICCCAS)*, pages 417–420. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5581965`.

Quantis:2010:RNG

[3467] Quantis. Random number generation using quantum physics. ID Quantique white paper Version 3.0, ID Quantique SA, 1227 Carouge/Geneva, Switzerland, April 2010. 8 pp. URL `http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf`.

Quantis:2010:RTR

[3468] Quantis. Randomness test report. ID Quantique white paper Version 2.0, ID Quantique SA, 1227 Carouge/Geneva, Switzerland, April

2010. 4 pp. URL http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-test.pdf.

Ristenpart:2010:WGR

[3469] Thomas Ristenpart and Scott Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In Anonymous [4268], page ?? ISBN 1-891562-29-0, 1-891562-30-4. LCCN ???? URL http://www.isoc.org/isoc/conferences/ndss/10/pdf/15.pdf; http://www.isoc.org/isoc/conferences/ndss/10/proceedings.shtml.

Roper:2010:CRNa

[3470] James Roper. Cracking random number generators — Part 1. Web blog., September 20, 2010. URL https://jazzy.id.au/2010/09/20/cracking_random_number_generators_part_1.html.

Roper:2010:CRNb

[3471] James Roper. Cracking random number generators — Part 2. Web blog., September 21, 2010. URL https://jazzy.id.au/2010/09/21/cracking_random_number_generators_part_2.html.

Roper:2010:CRNc

[3472] James Roper. Cracking random number generators — Part 3. Web blog., September 22, 2010. URL https://jazzy.id.au/2010/09/22/cracking_random_number_generators_part_3.html.

Roper:2010:CRNd

[3473] James Roper. Cracking random number generators — Part 4. Web blog., September 25, 2010. URL https://jazzy.id.au/2010/09/25/cracking_random_number_generators_part_4.html.

Rukhin:2010:SRS

[3474] A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2010. ???? pp.

Saiprasert:2010:MMM

[3475] C. Saiprasert, C.-S. Bouganis, and G. A. Constantinides. Mapping multiple multivariate Gaussian random number generators on an FPGA. In

2010 International Conference on Field Programmable Logic and Applications (FPL), pages 89–94. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5694226`.

Saiprasert:2010:OHA

[3476] Chalermpol Saiprasert, Christos-S. Bouganis, and George A. Constantinides. An optimized hardware architecture of a multivariate Gaussian random number generator. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 4(1):2:1–2:??, December 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Saito:2010:VMT

[3477] Mutsuo Saito. A variant of Mersenne Twister suitable for graphic processors. *CoRR*, 2010. CODEN ???? ISSN ???? URL `http://arxiv.org/abs/1005.4973`; `http://arxiv.org/abs/1005.4973v2`; `http://www.mendeley.com/research/variant-mersenne-twister-suitable-graphic-processors/`.

Segui:2010:AIP

[3478] Joan Melia Segui, Joaquin Garcia Alfaro, and Jordi Herrera Joancomarti. Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags. *Lecture Notes in Computer Science*, 5064:34–56, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://hal.archives-ouvertes.fr/hal-00527593/en/`.

Seznec:2010:PCM

[3479] Andre Seznec. A phase change memory as a secure main memory. *IEEE Computer Architecture Letters*, 9(1):5–8, January/June 2010. CODEN ???? ISSN 1556-6056 (print), 1556-6064 (electronic).

Shen:2010:PQR

[3480] Yong Shen, Liang Tian, and Hongxin Zou. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 81(6):063814, June 2010. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.81.063814`.

Shi:2010:MED

[3481] Hongsong Shi, Shaoquan Jiang, and Zhiguang Qin. More efficient DDH pseudorandom generators. *Designs, Codes, and Cryptography*, 55(1):

45–64, April 2010. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=55&issue=1&spage=45.

Shin:2010:AFG

[3482] Kaeyoung Shin and Raghu Pasupathy. An algorithm for fast generation of bivariate Poisson random vectors. *INFORMS Journal on Computing*, 22(1):81–92, Winter 2010. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic).

Srinivasan:2010:ADP

[3483] S. Srinivasan, S. Mathew, R. Ramanarayanan, F. Sheikh, M. Anders, H. Kaul, V. Erraguntla, R. Krishnamurthy, and G. Taylor. 2.4GHz 7mW all-digital PVT-variation tolerant true random number generator in 45nm CMOS. In IEEE [4273], pages 203–204. ISBN 1-4244-5454-9. LCCN ???? URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5560296.

Stankovski:2010:GDN

[3484] Paul Stankovski. Greedy distinguishers and nonrandomness detectors. *Lecture Notes in Computer Science*, 6498:210–226, 2010. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/h7704638w5187711/.

Suciu:2010:PIN

[3485] A. Suciu, I. Nagy, K. Marton, and I. Pinca. Parallel implementation of the NIST Statistical Test Suite. In Ioan Alfred Letia, editor, *Proceedings, 2010 IEEE 6th International Conference on Intelligent Computer Communication and Processing: Cluj-Napoca, Romania, August 26–28, 2010*, pages 363–368. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-8228-3 (print), 1-4244-8230-5 (electronic). LCCN QA76.76.E95. URL http://ieeexplore.ieee.org/servlet/opac?punumber=5598248. IEEE catalog number CFP1009D-ART.

Tang:2010:BHA

[3486] Hui-Chin Tang, K. H. Hsieh, and T. L. Chao. A backward heuristic algorithm for two-term multiple recursive random number generators. *Journal of Discrete Mathematical Sciences and Cryptography*, 13(6):593–600, December 2010. CODEN ???? ISSN 0972-0529. URL http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=13&issue_id=06.

Tang:2010:BLC

[3487] Hui-Chin Tang, Kuang-Hang Hsieh, and Hwapeng Chang. A 32-bit linear congruential random number generator with prime modulus. *Journal of Discrete Mathematical Sciences and Cryptography*, 13(5):479–486, October 2010. CODEN ???? ISSN 0972-0529. URL http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=13&issue_id=05.

Tang:2010:OMR

[3488] Hui-Chin Tang, K. H. Hsieh, and Hwapeng Chang. A 4217th-order multiple recursive random number generator with modulus $2^{31} - 69$. *Journal of Discrete Mathematical Sciences and Cryptography*, 13(4):393–398, August 2010. CODEN ???? ISSN 0972-0529. URL http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=13&issue_id=04.

Tarsa:2010:STR

[3489] I. G. Társa, G.-D. Budariu, and C. Grozea. Study on a true random number generator design for FPGA. In *2010 8th International Conference on Communications (COMM)*, pages 461–464. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5509075.

Tavas:2010:IRN

[3490] V. Tavas, A. S. Demirkol, S. Ozoguz, S. Kilinc, A. Toker, and A. Zeki. An IC random number generator based on chaos. In *2010 International Conference on Applied Electronics (AE)*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5599594.

Thomas:2010:FOU

[3491] David B. Thomas and Wayne Luk. FPGA-optimised uniform random number generators using LUTs and shift registers. In *2010 International Conference on Field Programmable Logic and Applications (FPL)*, pages 77–82. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5694224.

Tirdad:2010:HNN

[3492] K. Tirdad and A. Sadeghian. Hopfield neural networks as pseudo random number generators. In *2010 Annual Meeting of the North American*

Fuzzy Information Processing Society (NAFIPS), pages 1–6. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5548182`.

Tomasik:2010:AAG

[3493] J. Tomasik and M.-A. Weisser. aSHIIP: Autonomous generator of random Internet-like topologies with inter-domain hierarchy. In *2010 IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS)*, pages 388–390. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5581550`.

Urivskiy:2010:MMS

[3494] Alexey V. Urivskiy, Andrey L. Chmora, Alexey Bogachov, Mikhail Nekrasov, and Sergey Zakharov. Method for making seed value used in pseudo random number generator and device thereof. United States Patent 7,773,748., August 10, 2010. URL `http:www.google.com/patents/US7773748`.

Vakhania:2010:QGR

[3495] N. N. Vakhania and G. Z. Chelidze. Quaternion Gaussian random variables. *Theory of Probability and its Applications*, 54(2):363–369, ???? 2010. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/tvp/resource/1/tprbau/v54/i2/p363_s1`.

Valtchanov:2010:CRS

[3496] B. Valtchanov, V. Fischer, A. Aubert, and F. Bernard. Characterization of randomness sources in ring oscillator-based true random number generators in FPGAs. In *2010 IEEE 13th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, pages 48–53. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5491819`.

Varbanets:2010:ICG

[3497] P. Varbanets and S. Varbanets. On inversive congruential generator with a variable shift for pseudorandom numbers with prime power modulus. *Ann. Univ. Sci. Budapest. Sect. Comput.*, 32(??):151–176, ???? 2010. CODEN ???? ISSN 0138-9491.

Wikramaratna:2010:TEC

[3498] Roy S. Wikramaratna. Theoretical and empirical convergence results for additive congruential random number generators. *Journal of Computational and Applied Mathematics*, 233(9):2302–2311, March 1, 2010. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042709006931`.

Williams:2010:FPR

[3499] Caitlin R. S. Williams, Julia C. Salevan, Xiaowen Li, Rajarshi Roy, and Thomas E. Murphy. Fast physical random number generator using amplified spontaneous emission. *Optics Express*, 18(23):23584–23597, November 8, 2010. CODEN OPEXFF. ISSN 1094-4087.

Wong:2010:ARF

[3500] Knneth Koon-Ho Wong, Gary Carter, and Ed Dawson. An analysis of the RC4 family of stream ciphers against algebraic attacks. In Colin Boyd and Willy Susilo, editors, *AISC '10: Proceedings of the Eighth Australasian Conference on Information Security*, volume 105 of *Lecture Notes in Computer Science*, pages 67–74. Australian Computer Society, P.O. Box 319 Darlinghurst, NSW 2010, Australia, 2010. URL `https://dl.acm.org/doi/pdf/10.5555/1862266.1862277`.

Wu:2010:ULT

[3501] J. Wu and M. O'Neill. Ultra-lightweight true random number generators. *Electronics Letters*, 46(14):988–990, July 2010. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-911X (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5507606`.

Xiaohui:2010:DCR

[3502] Guan Xiaohui and Qian Yaguan. The design of combined random number generator. In *2010 International Conference on Multimedia Information Networking and Security (MINES)*, pages 640–643. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5671018`.

Xin:2010:IEB

[3503] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In *2010 International Conference on Computer Application and System Modeling (ICCASM)*, volume 9, pages V9–238–V9–241. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,

USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5623043.

Ying:2010:DRN

[3504] Liu Ying, Wang Shu, Yue Jing, and Liang Xiao. Design of a random number generator from fingerprint. In *2010 International Conference on Computational and Information Sciences (ICCIS)*, pages 278–280. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5709056.

Yoo:2010:IRR

[3505] Sang-Kyung Yoo, Deniz Karakoyunlu, Berk Birand, and Berk Sunar. Improving the robustness of ring oscillator TRNGs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 3(2):9:1–9:??, May 2010. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Yu:2010:NRN

[3506] Weizhong Yu and Guoqiang Bai. A novel random number generator based on continuous-time chaos. In *2010 2nd IEEE International Conference on Network Infrastructure and Digital Content*, pages 1052–1055. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5657957.

Zafar:2010:GRN

[3507] Fahad Zafar, Marc Olano, and Aaron Curtis. GPU random numbers via the Tiny Encryption Algorithm. In ????, editor, *HPG '10 Proceedings of the Conference on High Performance Graphics, Saarbrucken, Germany, June 25–27, 2010*, pages 133–141. Eurographics Association, Aire-la-Ville, Switzerland, 2010. ISBN ???? LCCN ???? URL http://www.cs.umbc.edu/~olano/papers/GPUTEA.pdf.

Zhmurov:2010:EPR

[3508] A. Zhmurov, K. Rybnikov, Y. Kholodov, and V. Barsegov. Efficient pseudo-random number generators for biomolecular simulations on graphics processors. *arxiv.org*, 2010. CODEN ???? ISSN ???? arXiv:1003.1123v1[physics.chem-ph].

Zimand:2010:SEC

[3509] Marius Zimand. Simple extractors via constructions of cryptographic pseudo-random generators. *Theoretical Computer Science*, 411(10):1236–

1250, March 4, 2010. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Abbott:2011:NNS

[3510] Alastair A. Abbott and Cristian S. Calude. Von Neumann normalisation and symptoms of randomness: An application to sequences of quantum random bits. *Lecture Notes in Computer Science*, 6714:40–51, 2011. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-21341-0_10/`.

Abbott:2011:QRN

[3511] Alastair Avery Abbott. Quantum random numbers: Certification and generation. Master of Science in Computer Science, Department of Computer Science, The University of Auckland, Auckland, NZ, 2011. viii + 73 pp.

Al-Abiachi:2011:CDN

[3512] A. M. Al-Abiachi, F. Ahmad, and K. Ruhana. A conceptual design of novel modern random key-stream generator for high immunity correlation attack. In *2011 UkSim 13th International Conference on Computer Modelling and Simulation (UKSim)*, pages 399–402. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5754253`.

Amaki:2011:JAO

[3513] T. Amaki, M. Hashimoto, and T. Onoye. Jitter amplifier for oscillator-based true random number generator. In *2011 16th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 81–82. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5722301`.

Amaki:2011:OBT

[3514] Takehiko Amaki, Masanori Hashimoto, and Takao Onoye. An oscillator-based true random number generator with jitter amplifier. In *2011 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 725–728. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5937668`.

Anonymous:2011:QRB

[3515] Anonymous. Quantum random bit generator service. Project developed by Centre for Informatics and Computing, Rud̄er Boškoviç Institute, Zagreb, Croatia, 2011. URL `http://random.irb.hr/`..

Anonymous:2011:QRG

[3516] Anonymous. Q.R.N.G. service. Project developed by PicoQuant GmbH and the Nano-Optics groups at the Department of Physics of Humboldt University, Berlin, Germany, 2011. URL `https://qrng.physik.hu-berlin.de/`.

Anthes:2011:QR

[3517] Gary Anthes. The quest for randomness. *Communications of the ACM*, 54(4):13–15, April 2011. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Araneus:2011:AA

[3518] Araneus Information Systems Oy. Araneus Alea I. Web site, 2011. URL `http://www.araneus.fi/products-alea-eng.html`. From the Web site: "The Alea I uses a reverse biased semiconductor junction to generate wide-band Gaussian white noise. This noise is amplified and digitized using an analog-to-digital converter. The raw output bits from the A/D converter are then further processed by an embedded microprocessor to combine the entropy from multiple samples into each final random bit and remove any bias caused by imperfections in the noise source and A/D converter.".

Bahi:2011:DFC

[3519] J. M. Bahi, Xiaole Fang, C. Guyeux, and Qianxue Wang. On the design of a family of CI pseudo-random number generators. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6040161`.

Bahi:2011:ECS

[3520] Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU. *arxiv.org*, ??(??):??, December 22, 2011. URL `http://arxiv.org/abs/1112.5239`.

Barash:2011:ADD

[3521] L. Yu. Barash. Applying dissipative dynamical systems to pseudorandom number generation: Equidistribution property and statistical independence of bits at distances up to logarithm of mesh size. *Europhysics Letters*, 95(1):10003–??, July 2011. CODEN EULEEJ. ISSN 0295-5075 (print), 1286-4854 (electronic). URL http://iopscience.iop.org/0295-5075/95/1/10003.

Barash:2011:RPL

[3522] L. Yu. Barash and L. N. Shchur. RNGSSELIB: Program library for random number generation, SSE2 realization. *Computer Physics Communications*, 182(7):1518–1527, July 2011. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465511001159.

Baudet:2011:SOB

[3523] Mathieu Baudet, David Lubicz, Julien Micolod, and André Tassiaux. On the security of oscillator-based random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(2):398–425, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/content/h65x0542r0214386/.

Bauke:2011:TRN

[3524] Heiko Bauke. Tina's random number generator library. Web site., 2011. URL http://numbercrunch.de/trng/.

Becker:2011:BLC

[3525] T. Becker, A. Greaves-Tunnell, S. J. Miller, R. Ronan, and F. W. Strauch. Benford's Law and continuous dependent random variables. *ArXiv e-prints*, November 2011. CODEN ???? ISSN ???? URL http://adsabs.harvard.edu/abs/2011arXiv1111.0568B; http://arxiv.org/abs/1111.0568.

Behnia:2011:NDM

[3526] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin. A novel dynamic model of pseudo random number generator. *Journal of Computational and Applied Mathematics*, 235(12):3455–3463, April 15, 2011. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0377042711000793.

Bellovin:2011:FMI

[3527] Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. *Cryptologia*, 35(3):203–222, 2011. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic).

Bernstein:2011:ESN

[3528] Daniel J. Bernstein. Extending the Salsa20 nonce. In ????, editor, *Workshop Record of Symmetric Key Encryption Workshop*, page ?? ????, ????, 2011. URL `https://cr.yp.to/snuffle/xsalsa-20110204.pdf`.

Blackburn:2011:DSS

[3529] Simon R. Blackburn, Alina Ostafe, and Igor E. Shparlinski. On the distribution of the subset sum pseudorandom number generator on elliptic curves. *arXiv.org*, ??(??):??, February 5, 2011. URL `http://arxiv.org/abs/1102.1053`.

Blanchet:2011:ERE

[3530] Jose Blanchet and Chenxin Li. Efficient rare event simulation for heavy-tailed compound sums. *ACM Transactions on Modeling and Computer Simulation*, 21(2):9:1–9:??, February 2011. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Boerstler:2011:RNG

[3531] David W. Boerstler, Eskinder Hailu, H. Peter Hofstee, and John Samuel Liberty. Random number generator. US Patent 7,890,561, February 15, 2011. URL `https://www.google.com/patents/US7890561`. US Patent Application Number 11/204,402, filed 16 August 2005, and assigned to IBM Corporation.

Bohl:2011:FAR

[3532] E. Bohl and P. Duplys. Fault attack resistant deterministic random bit generator usable for key randomization. In *2011 IEEE 17th International On-Line Testing Symposium (IOLTS)*, pages 194–195. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5993840`.

Bradley:2011:PTR

[3533] T. Bradley, J. Toit, R. Tong, M. Giles, and P. Woodhams. Parallelization techniques for random number generations. In mei Hwu [4278], chapter 16, page ?? ISBN 0-12-384988-8. LCCN T385 .G6875 2011.

Brown:2011:DRN

[3534] Robert G. Brown, Dirk Eddelbuettel, and David Bauer. Dieharder: a random number test suite. Web site., 2011. URL `http://phy.duke.edu/~rgb/General/dieharder.php`.

Bustard:2011:QRB

[3535] Philip J. Bustard, Doug Moffatt, Rune Lausten, Guorong Wu, Ian A. Walmsley, and Benjamin J. Sussman. Quantum random bit generation using stimulated Raman scattering. *Optics Express*, 19(25):25173–25180, December 5, 2011. CODEN OPEXFF. ISSN 1094-4087.

Cai:2011:ADB

[3536] Ying Cai and Tiefeng Wang. Analysis and design of binary pseudo-random sequences based on the Magma package. In *2011 International Conference on Electrical and Control Engineering (ICECE)*, pages 5759–5762. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, September 2011.

Carter:2011:TQS

[3537] Michael Carter. A toolbox for quasirandom simulation. *Mathematica Journal*, 13(??):??, ???? 2011. CODEN ???? ISSN 1047-5974 (print), 1097-1610 (electronic). URL `http://www.mathematica-journal.com/2011/12/a-toolbox-for-quasirandom-simulation/`.

Chan:2011:TRN

[3538] J. J. M. Chan, B. Sharma, Jiaqing Lv, G. Thomas, R. Thulasiram, and P. Thulasiraman. True random number generator using GPUs and histogram equalization techniques. In *2011 IEEE 13th International Conference on High Performance Computing and Communications (HPCC)*, pages 161–170. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6062989`.

Chen:2011:ARN

[3539] I-Te Chen, Jer-Min Tsai, and Jengnan Tzeng. Audio random number generator and its application. In *2011 International Conference on Machine Learning and Cybernetics (ICMLC)*, volume 4, pages 1678–1683. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6017002`.

Chevallier:2011:LSB

[3540] N. Chevallier. Law of the sum of Bernoulli random variables. *Theory of Probability and its Applications*, 55(1):27–41, ???? 2011. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL `http://epubs.siam.org/tvp/resource/1/tprbau/v55/i1/p27_s1`.

Click:2011:QRN

[3541] Timothy H. Click, Aibing Liu, and George A. Kaminski. Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems. *Journal of Computational Chemistry*, 32(3):513–524, February 2011. CODEN JCCHDD. ISSN 0192-8651 (print), 1096-987X (electronic).

Dabal:2011:CBP

[3542] P. Dabal and R. Pelka. A chaos-based pseudo-random bit generator implemented in FPGA device. In *2011 IEEE 14th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, pages 151–154. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5783069`.

David:2011:HSN

[3543] Matei David, Periklis A. Papakonstantinou, and Anastasios Sidiropoulos. How strong is Nisan's pseudo-random generator? *Information Processing Letters*, 111(16):804–808, August 30, 2011. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019011001190`. See [1765].

Demchik:2011:PRN

[3544] Vadim Demchik. Pseudo-random number generators for Monte Carlo simulations on ATI Graphics Processing Units. *Computer Physics Communications*, 182(3):692–705, March 2011. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465510004868`.

deOliveira:2011:DRP

[3545] Tiago de Oliveira and Norian Marranghello. Design of a reconfigurable pseudorandom number generator for use in intelligent systems. *Neurocomputing*, 74(10):1510–1519, May 2011. CODEN NRCGEO. ISSN 0925-2312 (print), 1872-8286 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0925231211000993`.

Desai:2011:PRN

[3546] V. V. Desai, V. B. Deshmukh, and D. H. Rao. Pseudo random number generator using Elman neural network. In *2011 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, pages 251–254. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6069312`.

Devroye:2011:DCM

[3547] Luc Devroye and Lancelot F. James. The double CFTP method. *ACM Transactions on Modeling and Computer Simulation*, 21(2):10:1–10:??, February 2011. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Duan:2011:POR

[3548] Huawei Duan and Guangxue Chen. Parametrical optimization of a random number generator for digital image halftoning. In C. B. Povloviq and C. W. Lu, editors, *Proceedings: the 3rd International Symposium on Information Engineering and Electronic Commerce, IEEC 2011: 22–24 July 2011, Huangshi, China*, pages 99–102. American Society of Mechanical Engineers, 345 E. 47th St., New York, NY 10017, USA, 2011. ISBN 0-7918-5975-4. LCCN HF5548.32 .I5837 2011.

Ergun:2011:IPS

[3549] S. Ergun. IC postprocessing stage for random number generators and an alternative design methodology. In *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 213–217. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6079505`.

Ergun:2011:RRN

[3550] Salih Ergun. Regional random number generator from a cross-coupled chaotic oscillator. In *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 1–4. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6026513`.

Ergun:2011:TRN

[3551] Salih Ergün. A truly random number generator based on a pulse-excited cross-coupled chaotic oscillator. *The Computer Journal*, 54

(10):1592–1602, October 2011. CODEN CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL `http://comjnl.oxfordjournals.org/content/54/10/1592.full.pdf+html`.

Ferrucci:2011:FBR

[3552] F. N. Ferrucci, C. A. Verrastro, G. E. Rios, and D. S. Estryk. FPGA-based random pulse generator for emulation of a neutron detector system in a nuclear reactor. In *2011 VII Southern Conference on Programmable Logic (SPL)*, pages 103–108. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5782633`.

Flenner:2011:HPA

[3553] Arjuna Flenner and Gary Hewer. A Helmholtz principle approach to parameter free change detection and coherent motion using exchangeable random variables. *SIAM Journal on Imaging Sciences*, 4(1):243–276, ???? 2011. CODEN SJISBI. ISSN 1936-4954. URL `http://epubs.siam.org/siims/resource/1/sjisbi/v4/i1/p243_s1`.

Fontaine:2011:LCG

[3554] Caroline Fontaine. Linear congruential generator. In van Tilborg and Jajodia [4282], pages Part 12, 721–721. ISBN 1-4419-5905-X (print), 1-4419-5906-8 (e-book). LCCN QA76.9.A25 E53 2011.

Gibbons:2011:NSI

[3555] Jean Dickinson Gibbons and Subhabrata Chakraborti. *Nonparametric Statistical Inference*. Statistics, textbooks and monographs. Taylor and Francis, Boca Raton, FL, USA, fifth edition, 2011. ISBN 1-4200-7761-9. xx + 630 pp. LCCN QA278.8 .G498 2011.

Gilli:2011:GRN

[3556] Manfred Gilli, Dietmar Maringer, and Enrico Schumann. Generating random numbers. In *Numerical Methods and Optimization in Finance* [4277], chapter 6, pages 119–158. ISBN 0-12-375662-6. LCCN HG106 .G55 2011. URL `http://www.sciencedirect.com/science/article/pii/B9780123756626000067`.

Godavarty:2011:UQG

[3557] Vinod Kumar Godavarty. Using quasigroups for generating pseudorandom numbers. *arxiv.org*, ??(??):??, December 5, 2011. URL `http://arxiv.org/abs/1112.1048`.

Gopalan:2011:PGC

[3558] Parikshit Gopalan, Raghu Meka, Omer Reingold, and David Zuckerman. Pseudorandom generators for combinatorial shapes. In ACM [4276], pages 253–262. ISBN ???? LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x.`.

Griffiths:2011:FFL

[3559] Martin Griffiths. Families of Fibonacci and Lucas sums via the moments of a random variable. *Fibonacci Quarterly*, 49(1):76–81, February 2011. CODEN FIBQAU. ISSN 0015-0517. URL `http://www.fq.math.ca/Abstracts/49-1/griffiths2.pdf`.

Guo:2011:PBS

[3560] Xiao Yan Guo. Pseudorandom binary sequences constructed by a generalized D. H. Lehmer problem. *J. Jilin Univ. Sci.*, 49(1):47–50, 2011. ISSN 1671-5489.

Haitner:2011:PRI

[3561] Iftach Haitner, Danny Harnik, and Omer Reingold. On the power of the randomized iterate. *SIAM Journal on Computing*, 40(6):1486–1528, ???? 2011. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). URL `http://epubs.siam.org/sicomp/resource/1/smjcat/v40/i6/p1486_s1`.

Han:2011:MTB

[3562] Shuangshuang Han, Lequan Min, and Ting Liu. Marotto's theorem-based chaotic pseudo-random number generator and performance analysis. In *2011 International Conference on Multimedia Technology (ICMT)*, pages 2500–2503. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6002469`.

Harase:2011:ELR

[3563] Shin Harase. An efficient lattice reduction method for $\mathbf{F}_2$-linear pseudorandom number generators using Mulders and Storjohann algorithm. *Journal of Computational and Applied Mathematics*, 236(2):141–149, August 15, 2011. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042711003281`.

Harase:2011:FLR

[3564] Shin Harase, Makoto Matsumoto, and Mutsuo Saito. Fast lattice reduction for $\mathbf{F_2}$-linear pseudorandom number generators. *Mathematics*

of Computation, 80(273):395–407, January 2011. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journals/mcom/2011-80-273/S0025-5718-2010-02391-9/home.html`; `http://www.ams.org/journals/mcom/2011-80-273/S0025-5718-2010-02391-9/S0025-5718-2010-02391-9.pdf`.

Heam:2011:SEU

[3565] P. C. Heam and C. Nicaud. Seed: An easy-to-use random generator of recursive data structures for testing. In *2011 IEEE Fourth International Conference on Software Testing, Verification and Validation (ICST)*, pages 60–69. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5770595`.

Hedayatpour:2011:HFB

[3566] S. Hedayatpour and S. Chuprat. Hash functions-based random number generator with image data source. In *2011 IEEE Conference on Open Systems (ICOS)*, pages 69–73. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6079248`.

Hill:2011:BMC

[3567] Jack C. Hill and Shlomo S. Sawilowsky. Bias in Monte Carlo simulations due to pseudo-random number generator initial seed selection. *Journal of Modern Applied Statistical Methods*, 10(1):??, ???? 2011. CODEN ???? ISSN 1538-9472. URL `https://jmasm.com/index.php/jmasm/article/view/521`.

Hofert:2011:SET

[3568] Marius Hofert. Sampling exponentially tilted stable distributions. *ACM Transactions on Modeling and Computer Simulation*, 22(1):3:1–3:??, December 2011. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hung:2011:DRD

[3569] Meei-Ling Hung, Cheng-Fang Huang, Jui-Sheng Lin, Jun-Juh Yan, Teh-Lu Liao, and Yuan-Tai Hsieh. Design of random digital sequence generators and its application of secure communication. In *2011 International Conference on Fluid Power and Mechatronics (FPM)*, pages 889–892. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6045887`.

Hwang:2011:SID

[3570] Dah-Yan Hwang. Some inequalities for differentiable convex mapping with application to weighted trapezoidal formula and higher moments of random variables. *Applied Mathematics and Computation*, 217(23): 9598–9605, August 1, 2011. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300311005935`.

Ishiguro:2011:LDR

[3571] Tsukasa Ishiguro, Shinsaku Kiyomoto, and Yutaka Miyake. Latin dances revisited: New analytic results of Salsa20 and ChaCha. In Sihan Qing, Willy Susilo, Guilin Wang, and Dongmei Liu, editors, *Information and Communications Security: 13th International Conference, ICICS 2011, Beijing, China, November 23–26, 2011: Proceedings*, volume 7043 of *Lecture Notes in Computer Science*, pages 255–266. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011.

Jian:2011:TBQ

[3572] Yi Jian, Min Ren, E. Wu, Guang Wu, and Heping Zeng. Two-bit quantum random number generator based on photon-number-resolving detection. *Review of Scientific Instruments*, 82(7):073109, ???? 2011. CODEN RSINAK. ISSN 1089-7623, 0034-6748. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967967`.

Kao:2011:EAT

[3573] T. C. Kao and H. C. Tang. An exhaustive analysis of two-term multiple recursive random number generators with double precision floating point restricted multipliers. *Journal of Discrete Mathematical Sciences and Cryptography*, 14(2):185–191, April 2011. CODEN ???? ISSN 0972-0529. URL `http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=14&issue_id=02`.

Kleimo:2011:RNG

[3574] Kleimo. The random name generator. Web site, 2011. URL `http://www.kleimo.com/random/name.cfm`. From the Web site: "The random name generator uses data from the US Census to randomly generate male and female names".

Koucky:2011:PGG

[3575] Michal Koucký, Prajakta Nimbhorkar, and Pavel Pudlák. Pseudorandom generators for group products: extended abstract. In ACM [4276], pages 263–272. ISBN ???? LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x`..

LEcuyer:2011:AZV

[3576] Pierre L'Ecuyer and Bruno Tuffin. Approximating zero-variance importance sampling in a reliability setting. *Annals of Operations Research*, 189:277–297, 2011. CODEN AOREEV. ISSN 0254-5330 (print), 1572-9338 (electronic).

LEcuyer:2011:NUR

[3577] Pierre L'Ecuyer. Non-uniform random variate generations. In Lovric [4281], pages 991–995. ISBN 3-642-04898-6. LCCN QA276.14 .I58 2011.

LEcuyer:2011:URN

[3578] Pierre L'Ecuyer. Uniform random number generators. In Lovric [4281], pages 1625–1630. ISBN 3-642-04898-6. LCCN QA276.14 .I58 2011.

Leydold:2011:GGI

[3579] Josef Leydold and Wolfgang Hörmannb. Generating generalized inverse Gaussian random variates by fast inversion. *Computational Statistics & Data Analysis*, 55(1):213–217, January 1, 2011. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947310002847`.

Li:2011:CBT

[3580] Xuan Li, Guoji Zhang, and Yuliang Liao. Chaos-based true random number generator using image. In *2011 International Conference on Computer Science and Service System (CSSS), 27–29 June, 2011*, pages 2145–2147. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5974933`.

Li:2011:OOH

[3581] Guang Li and Xiangzhong Xu. An object-oriented high-performance pseudorandom number generator package for analysis simulation. In *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pages 250–253. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp={\&}arnumber=6014434`.

Liu:2011:GUN

[3582] Huaning Liu. Gowers uniformity norm and pseudorandom measures of the pseudorandom binary sequences. *International Journal of Number Theory*, 7(5):1279–1302, August 2011. ISSN 1793-0421 (print), 1793-7310

(electronic). URL https://www.worldscientific.com/doi/10.1142/S1793042111004137.

Liu:2011:NPR

[3583] Weiyang Liu and Nanjian Wu. A novel parallel random number generator for wireless medical security applications. In *2011 International Conference of Electron Devices and Solid-State Circuits (EDSSC)*, pages 1–2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6117706.

Liu:2011:PRC

[3584] N. Liu. Pseudo-randomness and complexity of binary sequences generated by the chaotic system. *Communications in Nonlinear Science and Numerical Simulation*, 16(2):761–768, ???? 2011. CODEN ???? ISSN 1007-5704 (print), 1878-7274 (electronic).

Liu:2011:SBA

[3585] Yu Liu, Kaijie Wu, and Ramesh Karri. Scan-based attacks on linear feedback shift register based stream ciphers. *ACM Transactions on Design Automation of Electronic Systems*, 16(2):20:1–20:??, March 2011. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Liu:2011:TRN

[3586] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw. A true random number generator using time-dependent dielectric breakdown. In *2011 Symposium on VLSI Circuits (VLSIC)*, pages 216–217. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5986112.

Malik:2011:EHI

[3587] J. S. Malik, J. N. Malik, A. Hemani, and N. D. Gohar. An efficient hardware implementation of high quality AWGN generator using Box–Muller method. In IEEE, editor, *ISCIT 2011: 12–14 October, 2011, Hangzhou, China: The 11th International Symposium on Communications and Information Technologies (ISCIT 2011)*, pages 449–454. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 1-4577-1294-6. LCCN TK5105. URL http://ieeexplore.ieee.org/document/6090035/.

Malik:2011:GHT

[3588] Jamshaid Sarwar Malik, Jameel Nawaz Malik, Ahmed Hemani, and N. D. Gohar. Generating high tail accuracy Gaussian random numbers in hardware using central limit theorem. In IEEE, editor, *IEEE/IFIP 19th International Conference on VLSI and System-on-Chip (VLSI-SoC), 2011: 3–5 October 2011, Kowloon, Hong Kong*, pages 60–65. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 1-4577-0171-5, 1-4577-0169-3, 1-4577-0170-7. LCCN TK7874.75. URL `http://ieeexplore.ieee.org/document/6081630/`.

Marinucci:2011:RFS

[3589] Domenico Marinucci and Giovanni Peccati. *Random Fields on the Sphere: Representation, Limit Theorems and Cosmological Applications*, volume 389 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, UK, 2011. ISBN 0-521-17561-5. 341 pp. LCCN QA406 .M37 2011.

Marton:2011:PUR

[3590] K. Marton, A. Suciu, and D. Petricean. A parallel unpredictable random number generator. In *2011 10th Roedunet International Conference (RoEduNet)*, pages 1–5. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5993701`.

Merhi:2011:SPR

[3591] M. Merhi, J. C. Hernandez-Castro, and P. Peris-Lopez. Studying the pseudo random number generator of a low-cost RFID tag. In *2011 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, pages 381–385. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6068666`.

Mohamed:2011:EAG

[3592] Nader M. A. Mohamed. Efficient algorithm for generating Maxwell random variables. *Journal of Statistical Physics*, 145(6):1653–1660, December 2011. CODEN JSTPSB. ISSN 0022-4715 (print), 1572-9613 (electronic). URL `http://link.springer.com/article/10.1007/s10955-011-0364-y`.

Mukherjee:2011:RGU

[3593] Nilanjan Mukherjee, Janusz Rajski, Grzegorz Mrugalski, Artur Pogiel, and Jerzy Tyszer. Ring generator: An ultimate linear feedback shift

register. *Computer*, 44(6):64–71, June 2011. CODEN CPTRB4. ISSN 0018-9162 (print), 1558-0814 (electronic).

Paul:2011:RSC

[3594] Goutam Paul and Subhamoy Maitra. *RC4 Stream Cipher and Its Variants*. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 2011. ISBN 0-367-38216-4, 0-429-10372-7, 1-4398-3135-1 (hardcover), 1-4398-3137-8 (e-book). xxv + 285 pp. LCCN QA76.9.A25. URL `http://www.taylorfrancis.com/books/9781439831373`.

Phillips:2011:PRN

[3595] Carolyn L. Phillips, Joshua A. Anderson, and Sharon C. Glotzer. Pseudo-random number generation for Brownian Dynamics and Dissipative Particle Dynamics simulations on GPU devices. *Journal of Computational Physics*, 230(19):7191–7201, August 10, 2011. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999111003329`.

Qiu:2011:ATB

[3596] Meikang Qiu and Edwin H.-M. Sha. 2011 ACM TODAES best paper award. *ACM Transactions on Design Automation of Electronic Systems*, 16(4):36:1–36:??, October 2011. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Quantis:2011:RRW

[3597] Quantis. Redefining randomness: When random numbers cannot be left to chance. Technical report, ID Quantique SA, 1227 Carouge/Geneva, Switzerland, November 28, 2011. 4 pp. URL `http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-specs.pdf`; `http://www.idquantique.com/true-random-number-generator/quantis-resource-center.html`.

Ren:2011:QRN

[3598] Min Ren, E. Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng. Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 83(2):023820, February 2011. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.83.023820`.

Rose:2011:KBT

[3599] Greg Rose. KISS: a bit too simple. Report, Qualcomm Inc., San Diego, CA, USA, April 18, 2011. URL `http://eprint.iacr.org/2011/007.pdf`.

Salmon:2011:PRN

[3600] John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as $1, 2, 3$. In Lathrop et al. [4280], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????

Seyedzadeh:2011:IEA

[3601] Seyed Mohammad Seyedzadeh and Yasaman Hashemi. Image encryption algorithm based on Choquet Fuzzy Integral with self-adaptive pseudo-random number generator. In *2011 11th International Conference on Intelligent Systems Design and Applications (ISDA)*, pages 642–647. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6121728`.

Seyedzadeh:2011:IES

[3602] S. M. Seyedzadeh and S. Mirzakuchaki. Image encryption scheme based on Choquet fuzzy integral with pseudo-random keystream generator. In *2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, pages 101–106. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5960982`.

Shaolan:2011:EDE

[3603] Zhang Shaolan, Xing Guobo, and Yang Yixian. An efficient domain extension to construct a cryptographic hash function. In IEEE [4279], pages 424–427. ISBN 0-7695-4353-7, 1-61284-289-5. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5750113`.

Shparlinski:2011:ADP

[3604] Igor E. Shparlinski. On the average distribution of pseudorandom numbers generated by nonlinear permutations. *Mathematics of Computation*, 80(274):1053–1061, April 2011. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journals/mcom/2011-80-274/S0025-5718-2010-02408-1/home.html`; `http://www.ams.org/journals/mcom/2011-80-274/S0025-5718-2010-02408-1/S0025-5718-2010-02408-1.pdf`.

Simard:2011:CTS

[3605] Richard Simard and Pierre L'Ecuyer. Computing the two-sided Kolmogorov–Smirnov distribution. *Journal of Statistical Software*, 39 (11):1–18, March 2011. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v39/i11`.

Sinescu:2011:ECS

[3606] Vasile Sinescu and Pierre L'Ecuyer. Existence and construction of shifted lattice rules with an arbitrary number of points and bounded weighted star discrepancy for general decreasing weights. *Journal of Complexity*, 27(5):449–465, 2011. CODEN JOCOEH. ISSN 0885-064X (print), 1090-2708 (electronic).

Soucarros:2011:ITT

[3607] M. Soucarros, C. Canovas-Dumas, J. Clediere, P. Elbaz-Vincent, and D. Real. Influence of the temperature on true random number generators. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 24–27. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5954990`.

Stafford:2011:BBM

[3608] David Stafford. Better bit mixing: Improving on Murmur–Hash3's 64-bit finalizer. Blog on "Twiddling the Bits"., September 28, 2011. URL `http://zimbry.blogspot.com/2011/09/better-bit-mixing-improving-on.html`.

Stipcevic:2011:QRN

[3609] M. Stipcevic. Quantum random number generators and their use in cryptography. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 1474–1479. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967293`.

Suciu:2011:URN

[3610] A. Suciu, D. Lebu, and K. Marton. Unpredictable random number generator based on mobile sensors. In *2011 IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, pages 445–448. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6047913`.

Sugiura:2011:DGG

[3611] T. Sugiura, Y. Yamanashi, and N. Yoshikawa. Demonstration of 30 Gbit/s generation of superconductive true random number generator. *IEEE Transactions on Applied Superconductivity*, 21(3):843–846, ???? 2011. CODEN ITASE9. ISSN 1051-8223 (print), 1558-2515 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5674104`.

Symul:2011:RTD

[3612] T. Symul, S. M. Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, June 8, 2011. CODEN APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842. URL `http://apl.aip.org/resource/1/applab/v98/i23`.

Tang:2011:ESG

[3613] Hui-Chin Tang and Hwapeng Chang. An exhaustive search for good 64-bit linear congruential random number generators with restricted multiplier. *Computer Physics Communications*, 182(11):2326–2330, November 2011. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465511002360`.

Tang:2011:PES

[3614] H. C. Tang, K. H. Hsieh, and C. J. Wang. A partial exhaustive search for good two-term third-order multiple recursive random number generators. *Journal of Discrete Mathematical Sciences and Cryptography*, 14(4):341–348, August 2011. CODEN ???? ISSN 0972-0529. URL `http://www.connectjournals.com/achivestoc.php?bookmark=CJ-003072&volume=14&issue_id=04`.

Taylor:2011:DR

[3615] Greg Taylor and George Cox. Digital randomness. *IEEE Spectrum*, 48(9):32–58, September 2011. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://spectrum.ieee.org/semiconductors/processors/behind-intels-new-randomnumber-generator/`.

Veillette:2011:TCP

[3616] Mark S. Veillette and Murad S. Taqqu. A technique for computing the pdfs and cdfs of nonnegative infinitely divisible random variables. *Journal of Applied Probability*, 48(1):217–237, March 2011. CODEN

JPRBAM. ISSN 0021-9002 (print), 1475-6072 (electronic). URL `http://www.jstor.org/stable/29777456`.

Versolatto:2011:MPR

[3617] F. Versolatto and A. M. Tonello. A MIMO PLC random channel generator and capacity analysis. In *2011 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pages 66–71. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5764452`.

Wahl:2011:UQR

[3618] Michael Wahl, Matthias Leifgen, Michael Berlin, Tino Rohlicke, Hans-Jurgen Rahn, and Oliver Benson. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 98(17):171105, ???? 2011. CODEN APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5759033`.

Wang:2011:CRN

[3619] Miao Wang, Feng Guo, Hongshan Qu, and Song Li. Combined random number generators: a review. In *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, pages 443–447. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6014760`.

Wang:2011:LTA

[3620] Jiun-Chau Wang. Limit theorems for additive conditionally free convolution. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 63(1):222–240, February 2011. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Wang:2011:MPF

[3621] Li-Ping Wang. On minimal polynomials over $\mathbf{F}_{q^m}$ and over $\mathbf{F}_q$ of a finite-length sequence over $\mathbf{F}_{q^m}$. *Finite Fields and their Applications*, 17(3):294–301, May 2011. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1071579711000025`.

Wei:2011:HSB

[3622] W. Wei, G. Xie, A. Dang, and H. Guo. A high speed and bias-free optical random number generator. *IEEE Photonics Technology Letters*, PP(99):1, ???? 2011. CODEN ???? ISSN 1041-1135 (print), 1941-0174 (electronic). URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6109313`.

Wikramaratna:2011:CIM

[3623] Roy S. Wikramaratna. The centro-invertible matrix: a new type of matrix arising in pseudo-random number generation. *Linear Algebra and its Applications*, 434(1):144–151, January 1, 2011. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). See corrigendum [3708].

Wu:2011:TEH

[3624] Bo-Han Wu, Chun-Ju Yang, Chia-Cheng Tso, and Chung-Yang (Ric) Huang. Toward an extremely-high-throughput and even-distribution pattern generator for the constrained random simulation techniques. In *2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 602–607. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6105392`.

Xing-Yuan:2011:PRS

[3625] Wang Xing-Yuan, Qin Xue, and Xie Yi-Xin. Pseudo-random sequences generated by a class of one-dimensional smooth map. *Chinese Physics Letters*, 28(8):080501, 2011. CODEN CPLEEU. ISSN 0256-307X (print), 1741-3540 (electronic). URL `http://stacks.iop.org/0256-307X/28/i=8/a=080501`.

Yingni:2011:FBM

[3626] Duan Yingni and Zhang Haifeng. FPGA-based multi-bit all state pseudo-random sequences generator. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, pages 858–861. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6066489`.

Zhmurov:2011:GRN

[3627] A. Zhmurov, K. Rybnikov, Y. Kholodov, and V. Barsegov. Generation of random numbers on graphics processors: forced indentation in silico of the bacteriophage HK97. *Journal of Physical Chemistry. B. Condensed matter, materials, surfaces, interfaces & biophysical*, 115(18):5278–5288,

May 12, 2011. CODEN JPCBFK. ISSN 1089-5647 (print), 1520-6106 (electronic).

Abbott:2012:NNQ

[3628] Alastair A. Abbott and Cristian S. Calude. Von Neumann normalisation of a quantum random number generator. *Computability*, 1(1):59–83, ???? 2012. CODEN ???? ISSN 2211-3568 (print), 2211-3576 (electronic). URL http://iospress.metapress.com/content/82271271358877v0.

Abbott:2012:SKS

[3629] Alistair A. Abbott, Cristian S. Calude, J. Conder, and Karl Svozil. Strong Kochen–Specker theorem and incomputability of quantum randomness. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 86(6):062109, December 2012. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL http://pra.aps.org/abstract/PRA/v86/i6/e062109.

Abbott:2012:TFA

[3630] John Abbott. Twin-float arithmetic. *Journal of Symbolic Computation*, 47(5):536–551, May 2012. CODEN JSYCEH. ISSN 0747-7171 (print), 1095-855X (electronic). URL http://www.sciencedirect.com/science/article/pii/S0747717111001970.

Anonymous:2012:CTC

[3631] Anonymous. CUDA Toolkit 5.0 CURAND guide. Web document, 2012. URL http://docs.nvidia.com/cuda/pdf/CURAND_Library.pdf.

Applebaum:2012:PGL

[3632] Benny Applebaum. Pseudorandom generators with long stretch and low locality from random local one-way functions. In ACM [4283], pages 805–816. ISBN 1-4503-1245-4. LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Barash:2012:GSP

[3633] L. Yu. Barash. Geometric and statistical properties of pseudorandom number generators based on multiple recursive transformations. In Leszek Plaskota and Henryk Woźniakowski, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2010*, volume 23 of *Springer Proceedings in Mathematics and Statistics*, pages 265–280. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. ISSN 2194-1009. URL http://link.springer.com/chapter/10.1007/978-3-642-27440-4_12.

Barker:2012:RRN

[3634] E. B. Barker and J. M. Kelsey. Recommendation for random number generation using deterministic random bit generators. NIST Special Publication 800-90a, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2012.

Bayon:2012:CEA

[3635] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, and François Poucheret. Contactless electromagnetic active attack on ring oscillator based true random number generator. *Lecture Notes in Computer Science*, 7275:151–166, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-29912-4_12/`.

Becher:2012:TNN

[3636] Verónica Becher. Turing's normal numbers: Towards randomness. In Cooper et al. [4284], pages 35–45. ISBN 3-642-30869-4. LCCN ???? URL `http://www.springerlink.com/content/5016568053026532/`.

Beisbart:2012:WMC

[3637] Claus Beisbart and John D. Norton. Why Monte Carlo simulations are inferences and not experiments. *International Studies in the Philosophy of Science*, 26(4):403–422, 2012. CODEN ???? ISSN 0269-8595 (print), 1469-9281 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/02698595.2012.748497`.

Berger:2012:CPR

[3638] Thierry P. Berger and Marine Minier. Cryptanalysis of pseudo-random generators based on vectorial FCSRs. *Lecture Notes in Computer Science*, 7668:209–224, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-34931-7_13/`.

Bergman:2012:GRV

[3639] Jakob Bergman. Generating random variates from a bicompositional Dirichlet distribution. *Journal of Statistical Computation and Simulation*, ??(??):??, ???? 2012. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163. URL `http://www.tandfonline.com/doi/abs/10.1080/00949655.2011.558088`. In press (checked: 07 February 2012, 28 March 2012).

Bertoni:2012:KSF

[3640] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak sponge function family. Web site, October 24, 2012. URL http://keccak.noekeon.org/.

Bokhari:2012:CTS

[3641] M. U. Bokhari, Shadab Alam, and Faheem Syeed Masoodi. Cryptanalysis techniques for stream cipher: a survey. *International Journal of Computer Applications*, 60(9):6–12, December 2012. CODEN ???? ISSN 0975-8887. URL https://www.ijcaonline.org/archives/volume60/number9/9721-4187/.

Boldyreva:2012:NPG

[3642] Alexandra Boldyreva and Virendra Kumar. A new pseudorandom generator from collision-resistant hash functions. Report, School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA, February 6, 2012. URL http://eprint.iacr.org/2012/056.

Boureanu:2012:PFA

[3643] Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. On the pseudorandom function assumption in (secure) distance-bounding protocols. *Lecture Notes in Computer Science*, 7533:100–120, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-33481-8_6/.

Cesaratto:2012:PRK

[3644] Eda Cesaratto and Brigitte Vallée. Pseudorandomness of a random Kronecker sequence. *Lecture Notes in Computer Science*, 7256:157–171, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29344-3_14/.

Chang:2012:TRR

[3645] Shu jen Chang, Ray Perlner, William Burr, Meltem Sönmez Turan, John Kelsey, Souradyuti Paul, and Lawrence Bassham. Third-round report of the SHA-3 cryptographic hash algorithm competition. Interagency Report 7896, NIST, 100 Bureau Drive, Gaithersburg, MD 20899, USA, 2012. 121–?? pp. URL https://csrc.nist.gov/pubs/ir/7896/final.

Chen:2012:ECR

[3646] Xi Chen, Bruce E. Ankenman, and Barry L. Nelson. The effects of Common Random Numbers on stochastic kriging metamodels. *ACM Transac-*

tions on Modeling and Computer Simulation, 22(2):7:1–7:20, March 2012. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Chi:2012:ESN

[3647] Zhiyi Chi. On exact sampling of nonnegative infinitely divisible random variables. *Advances in Applied Probability*, 44(3):842–873, September 2012. CODEN AAPBBD. ISSN 0001-8678 (print), 1475-6064 (electronic). URL `http://www.jstor.org/stable/41714078`.

Chiu:2012:MTR

[3648] Yu-Tzu Chiu. A memristor true random-number generator. *IEEE Spectrum*, ??(??):??, July 12, 2012. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://spectrum.ieee.org/semiconductors/memory/a-memristor-true-randomnumber-generator`.

Cohen:2012:SMI

[3649] Michael P. Cohen. Sample means of independent standard Cauchy random variables are standard Cauchy: a new approach. *American Mathematical Monthly*, 119(3):240–244, March 2012. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL `http://www.jstor.org/stable/pdfplus/10.4169/amer.math.monthly.119.03.240.pdf`.

Colbeck:2012:FRC

[3650] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, ??(??):??, ???? 2012. CODEN NPAHAX. ISSN 1745-2473 (print), 1745-2481 (electronic). URL `http://www.nature.com/nphys/journal/vaop/ncurrent/full/nphys2300.html`; `http://www.sciencenews.org/view/generic/id/340530/title/Physicists_go_totally_random`.

Deng:2012:ECS

[3651] Lih-Yuan Deng, Jyh-Jen H. Shiau, and Henry Horng-Shing Lu. Efficient computer search of large-order multiple recursive pseudo-random number generators. *Journal of Computational and Applied Mathematics*, 236(13):3228–3237, July 2012. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic).

Deng:2012:LOM

[3652] Lih-Yuan Deng, Jyh-Jen Horng Shiau, and Henry Horng-Shing Lu. Large-order multiple recursive generators with modulus $2^{31} - 1$. *INFORMS Journal on Computing*, 24(4):636–647, Fall 2012. ISSN

1091-9856 (print), 1526-5528 (electronic). URL http://joc.journal.informs.org/content/24/4/636.

deSchryver:2012:HER

[3653] Christian de Schryver, Daniel Schmidt, Norbert Wehn, Elke Korn, Henning Marxen, Anton Kostiuk, and Ralf Korn. A hardware efficient random number generator for nonuniform distributions with arbitrary precision. *International Journal of Reconfigurable Computing*, 2012(??):12:1–12:11, January 2012. ISSN 1687-7209. URL https://www.hindawi.com/journals/ijrc/2012/675130/. Article ID 675130.

Du:2012:LCP

[3654] Xiaoni Du, Andrew Klapper, and Zhixiong Chen. Linear complexity of pseudorandom sequences generated by Fermat quotients and their generalizations. *Information Processing Letters*, 112(6):233–237, March 15, 2012. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S002001901100322X.

Dunn:2012:PNG

[3655] William L. Dunn and J. Kenneth Shultis. Pseudorandom number generators. In Dunn and Shultis [4285], chapter 3, pages 47–68. ISBN 0-444-51575-5 (hardcover). LCCN QA298 .D86 2012. URL http://www.sciencedirect.com/science/article/pii/B9780444515759000038.

Dyson:2012:MC

[3656] George Dyson. Monte Carlo. In *Turing's cathedral: the origins of the digital universe* [4286], chapter 10, pages 175–199. ISBN 0-375-42277-3 (hardcover). LCCN QA76.17 .D97 2012. Pages 191–192 describe the origin of the Monte Carlo method.

Dyson:2012:UD

[3657] George Dyson. Ulam's demons. In *Turing's cathedral: the origins of the digital universe* [4286], chapter 11, pages 200–224. ISBN 0-375-42277-3 (hardcover). LCCN QA76.17 .D97 2012. Pages 191–192 describe the origin of the Monte Carlo method.

Fischer:2012:CLS

[3658] Viktor Fischer. A closer look at security in random number generators design. *Lecture Notes in Computer Science*, 7275:167–182, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-29912-4_13/.

Gopalan:2012:BPG

[3659] P. Gopalan, R. Meka, O. Reingold, L. Trevisan, and S. Vadhan. Better pseudorandom generators from milder pseudorandom restrictions. In IEEE [4289], pages 120–129. ISBN 1-4673-4383-8. ISSN 0272-5428. LCCN QA76 .S95 2012. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6375289`. IEEE Computer Society order number P????.

Gutierrez:2012:HAG

[3660] R. Gutierrez, V. Torres, and J. Valls. Hardware architecture of a Gaussian noise generator based on the inversion method. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 59(8):501–505, August 2012. ISSN 1549-7747 (print), 1558-3791 (electronic). URL `http://ieeexplore.ieee.org/document/6236107/`.

Hall:2012:DRA

[3661] Timothy Hall. Dominated rejection algorithms for generating random variates. *WIREs Computational Statistics*, 4(6):561–564, November/December 2012. CODEN ???? ISSN 1939-0068 (print), 1939-5108 (electronic).

Hamburg:2012:AII

[3662] Mike Hamburg, Paul Kocher, and Mark E. Marson. Analysis of Intel's Ivy Bridge digital random number generator. Report, Cryptography Research, Inc., San Francisco, CA 94105, USA, March 12, 2012. 22 pp. URL `http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf`.

Heninger:2012:MYP

[3663] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium, August 2012*, pages 205–220. USENIX, Berkeley, CA, USA, 2012. URL `https://factorable.net/weakkeys12.conference.pdf`; `https://factorable.net/weakkeys12.extended.pdf`; `https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/heninger`.

Holenstein:2012:CPG

[3664] T. Holenstein and M. Sinha. Constructing a pseudorandom generator requires an almost linear number of calls. In IEEE [4289], pages 698–707. ISBN 1-4673-4383-8. ISSN 0272-5428. LCCN QA76

.S95 2012. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6375349`. IEEE Computer Society order number P????.

Horstmann:2012:JEC

[3665] Cay S. Horstmann. *Java for everyone: compatible with Java 5, 6, and 7*. Wiley, New York, NY, USA, second edition, 2012. ISBN 1-118-06331-7 (paperback). xxxiii + 589 pp. LCCN QA76.73.J38 H675445 2012.

Horvath:2012:ARM

[3666] Gábor Horváth and Miklós Telek. Acceptance-rejection methods for generating random variates from matrix exponential distributions and rational arrival processes (abstract only). *ACM SIGMETRICS Performance Evaluation Review*, 39(4):27, April 2012. CODEN PEREDN. ISSN 0163-5999 (print), 1557-9484 (electronic).

Horvath:2012:EGP

[3667] Gábor Horváth, Philipp Reinecke, Miklós Telek, and Katinka Wolter. Efficient generation of PH-distributed random variates. *Lecture Notes in Computer Science*, 7314:271–285, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-30782-9_19/`.

Impagliazzo:2012:PS

[3668] R. Impagliazzo, R. Meka, and D. Zuckerman. Pseudorandomness from shrinkage. In IEEE [4289], pages 111–119. ISBN 1-4673-4383-8. ISSN 0272-5428. LCCN QA76 .S95 2012. URL `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6375288`. IEEE Computer Society order number P????.

Kaczynski:2012:BNR

[3669] W. Kaczynski, L. Leemis, N. Loehr, and J. McQueston. Bivariate nonparametric random variate generation using a piecewise-linear cumulative distribution function. *Communications in Statistics: Simulation and Computation*, 41(4):469–496, 2012. CODEN CSSCDB. ISSN 0361-0918.

Kaczynski:2012:NRV

[3670] W. Kaczynski, L. Leemis, N. Loehr, and J. McQueston. Nonparametric random variate generation using a piecewise-linear cumulative distribution function. *Communications in Statistics: Simulation and Computation*, 41(4):449–468, 2012. CODEN CSSCDB. ISSN 0361-0918.

Karakostas:2012:DAC

[3671] George Karakostas, Jeff Kinne, and Dieter van Melkebeek. On derandomization and average-case complexity of monotone functions. *Theoretical Computer Science*, 434(1):35–44, May 25, 2012. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397512001582`.

Lacharme:2012:LPN

[3672] Patrick Lacharme, Andrea Röck, Vincent Strubel, and Marion Videau. The Linux pseudorandom number generator revisited. Report, ????, ????, May 24, 2012. 23 pp. URL `https://eprint.iacr.org/2012/251.pdf`.

Lam:2012:QRN

[3673] Ping Koy Lam, Thomas Symul, and Syed Assad. Quantum random number generator. Web site, April 2012. URL `http://photonics.anu.edu.au/qoptics/Research/qrng.php`; `http://www.scientificcomputing.com/news-DA-Worlds-Fastest-Random-Number-Generator-Developed-from-Sounds-of-Silence-041212.aspx`. Random numbers are generated from quantum vacuum noise. See [3612] for details.

LEcuyer:2012:RNG

[3674] P. L'Ecuyer. Random number generation. In Gentle et al. [4287], pages 35–71. ISBN 3-642-21550-5 (print), 3-642-21551-3 (e-book). LCCN QA276.4 .H36 2012. URL `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-b.html`; `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-d.html`; `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-t.html`.

Leiserson:2012:DPR

[3675] Charles E. Leiserson, Tao B. Schardl, and Jim Sukha. Deterministic parallel random-number generation for dynamic-multithreading platforms. *ACM SIGPLAN Notices*, 47(8):193–204, August 2012. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). PPOPP '12 conference proceedings.

Lenstra:2012:RWW

[3676] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, Whit is right. Report, EPFL IC LACAL, Lausanne, Switzerland, February 14, 2012. 16 pp. URL `http://eprint.iacr.org/2012/064`.

Li:2012:PER

[3677] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To. Period extension and randomness enhancement using high-throughput reseeding–mixing PRNG. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 20(2):385–389, February 2012. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `https://ieeexplore.ieee.org/document/5711011`.

Li:2012:SHF

[3678] Y. Li, P. Chow, J. Jiang, M. Zhang, and S. Wei. Software/hardware framework for generating parallel Gaussian random numbers based on the Monty Python method. In IEEE, editor, *FPT'12: 2012 International Conference on Field-Programmable Technology: December 10–12, 2012, Seoul National University, Seoul, Korea*, pages 190–197. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2012. ISBN 1-4673-2846-4 (paperback), 1-4673-2844-8, 1-4673-2845-6. LCCN TK7895.G36 I33 2012. URL `http://ieeexplore.ieee.org/document/6412133/`.

Li:2012:TST

[3679] Liang Li. Testing several types of random number generators. MS thesis, Department of Computer Science, Florida State University, Tallahassee, FL, USA, Fall 2012. vi + 91 pp. URL `http://search.proquest.com/pqdtglobal/docview/1287745850/`.

Manssen:2012:RNG

[3680] M. Manssen, M. Weigel, and A. K. Hartmann. Random number generators for massively parallel simulations on GPU. *European Physical Journal — Special Topics*, 210(??):53–71, 2012. CODEN EPJSAC. ISSN 1951-6355 (print), 1951-6401 (electronic).

Marandi:2012:AOQ

[3681] lireza Marandi, Nick C. Leindecker, Konstantin L. Vodopyanov, and Robert L. Byer. All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators. *Optics Express*, 20(17): 19322–19330, August 13, 2012. CODEN OPEXFF. ISSN 1094-4087.

Marquardt:2012:PNG

[3682] Pascal Marquardt, Pavol Svaba, and Tran van Trung. Pseudorandom number generators based on random covers for finite groups. *Designs, Codes, and Cryptography*, 64(1–2):209–220, July 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http:`

//www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=64&issue=1&spage=209.

Mascagni:2012:PRN

[3683] Michael Mascagni and Lin-Yee Hin. Parallel random number generators in Monte Carlo derivative pricing: An application-based test. *Monte Carlo Methods and Applications*, 18(2):161–??, June 2012. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://www.degruyter.com/view/j/mcma.2012.18.issue-2/mcma-2012-0005/mcma-2012-0005.xml.

Masse:2012:RNS

[3684] Bruno Massé and Dominique Schneider. Random number sequences and the first digit phenomenon. *Electronic Journal of Probability*, 17:86:1–86:17, 2012. CODEN ???? ISSN 1083-6489. URL http://ejp.ejpecp.org/article/view/1900.

Miles:2012:SPN

[3685] Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *Lecture Notes in Computer Science*, 7417:68–85, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-32009-5_5/.

Miszczak:2012:GUT

[3686] Jarosław Adam Miszczak. Generating and using truly random quantum states in Mathematica. *Computer Physics Communications*, 183(1):118–124, January 2012. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465511002748.

Molina-Gil:2012:PGS

[3687] J. Molina-Gil, P. Caballero-Gil, A. Fúster-Sabater, and C. Caballero-Gil. Pseudorandom generator to strengthen cooperation in VANETs. *Lecture Notes in Computer Science*, 6928:365–373, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/978-3-642-27579-1_47.

Nandapalan:2012:HPP

[3688] Nimalan Nandapalan, Richard P. Brent, Lawrence M. Murray, and Alistair P. Rendell. High-performance pseudorandom number generation on

graphics processing units. *Lecture Notes in Computer Science*, 7203:609–618, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31464-3_62`.

Nazzal:2012:UGA

[3689] D. Nazzal, M. Mollaghasemi, H. Hedlund, and A. Bozorgi. Using genetic algorithms and an indifference-zone ranking and selection procedure under common random numbers for simulation optimisation. *Journal of Simulation*, 6(1):56–66, 2012. ISSN 1747-7778 (print), 1747-7786 (electronic).

Neves:2012:FSN

[3690] Samuel Neves and Filipe Araujo. Fast and small nonlinear pseudorandom number generators for computer simulation. *Lecture Notes in Computer Science*, 7203:92–101, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.com/chapter/10.1007/978-3-642-31464-3_10/`.

NIST:2012:RRN

[3691] NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2012. URL `http://csrc.nist.gov/publications/PubsSPs.html#800-90A`.

Ostafe:2012:PVS

[3692] Alina Ostafe. Pseudorandom vector sequences of maximal period generated by triangular polynomial dynamical systems. *Designs, Codes, and Cryptography*, 63(1):59–72, April 2012. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0925-1022&volume=63&issue=1&spage=59`.

Pareschi:2012:STR

[3693] F. Pareschi, R. Rovatti, and G. Setti. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, 7(2):491–505, April 2012. CODEN ???? ISSN 1556-6013.

Passerat-Palmbach:2012:PRS

[3694] Jonathan Passerat-Palmbach, Claude Mazel, and David R. C. Hill. Pseudo-random streams for distributed and parallel stochastic simulations on GP-GPU. *Journal of Simulation*, 6(3):141–151, August

2012. CODEN ???? ISSN 1747-7778 (print), 1747-7786 (electronic). URL http://www.palgrave-journals.com/jos/journal/v6/n3/abs/jos20128a.html.

Pirsic:2012:BFD

[3695] Gottlieb Pirsic and Arne Winterhof. Boolean functions derived from pseudorandom binary sequences. *Lecture Notes in Computer Science*, 7280:101–109, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-30615-0_9/.

Quantis:2012:REQ

[3696] Quantis. Randomness extraction for the Quantis true random number generator. White paper, ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge/Geneva, Switzerland, 2012. 7 pp.

Rainville:2012:EOL

[3697] François-Michel D. Rainville, Christian Gagné, Olivier Teytaud, and Denis Laurendeau. Evolutionary optimization of low-discrepancy sequences. *ACM Transactions on Modeling and Computer Simulation*, 22(2):9:1–9:25, March 2012. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Reuillon:2012:PSS

[3698] Romain Reuillon, Mamadou K. Traore, Jonathan Passerat-Palmbach, and David R. C. Hill. Parallel stochastic simulations with rigorous distribution of pseudo-random numbers with DistMe: Application to life science simulations. *Concurrency and Computation: Practice and Experience*, 24(??):??, ???? 2012. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic). URL http://onlinelibrary.wiley.com/doi/10.1002/cpe.1883/abstract.

Riesel:2012:PNC

[3699] Hans Riesel. *Prime numbers and computer methods for factorization*. Modern Birkhäuser classics. Birkhäuser Boston Inc., Cambridge, MA, USA, second edition, 2012. ISBN 0-8176-8297-X. xviii + 464 pp. LCCN QA246 .R54 2012.

Saito:2012:DCS

[3700] Mutsuo Saito and Makoto Matsumoto. A deviation of CURAND: Standard pseudorandom number generator in CUDA for GPGPU. Slides presented at the Tenth International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, February

2012. URL http://www.mcqmc2012.unsw.edu.au/slides/MCQMC2012_Matsumoto.pdf.

Saito:2012:RGR

[3701] Takeshi Saito, Koichi Ishii, Isao Tatsuno, Susumu Sukagawa, and Tomotake Yanagita. Randomness and genuine random number generator with self-testing functions. In ????, editor, *Joint International Conference on Supercomputing in Nuclear Applications and Monte Carlo, Hitotsubashi Memorial Hall Tokyo, October 2010*, page ?? ????, ????, 2012. URL http://www.letech-rng.jp/SNA+MC2010-Paper.pdf.

Sen:2012:FNR

[3702] Pradeep Sen and Soheil Darabi. On filtering the noise from the random parameters in Monte Carlo rendering. *ACM Transactions on Graphics*, 31(3):18:1–18:15, May 2012. CODEN ATGRDF. ISSN 0730-0301 (print), 1557-7368 (electronic).

Shrestha:2012:DIL

[3703] Rahul Shrestha and Roy Paily. Design and implementation of a linear feedback shift register interleaver for turbo decoding. *Lecture Notes in Computer Science*, 7373:30–39, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/chapter/10.1007/978-3-642-31494-0_4/.

Troyer:2012:REQ

[3704] M. Troyer and R. Renner. A randomness extractor for the Quantis device. Technical report, ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge/Geneva, Switzerland, September 19, 2012. 7 pp. URL http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-rndextract-whitepaper.pdf.

Vadhan:2012:CPS

[3705] Salil Vadhan and Colin Jia Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In ACM [4283], pages 817–836. ISBN 1-4503-1245-4. LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Vazirani:2012:CQD

[3706] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In ACM [4283], pages 61–76. ISBN 1-4503-1245-4. LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Walsh:2012:BRB

[3707] James A. Walsh. Book review: *Randomness and Recurrence in Dynamical Systems*, by Rodney Nillsen. The Carus Mathematical Monographs Number 31, Mathematical Association of America, Washington, DC, 2010, xviii + 357 pp., ISBN 978-0-88385-043-5, $52.95. *American Mathematical Monthly*, 119(5):434–438, May 2012. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic). URL `http://www.jstor.org/stable/pdfplus/10.4169/amer.math.monthly.119.05.434.pdf`.

Wikramaratna:2012:CCI

[3708] Roy S. Wikramaratna. Corrigendum to "The centro-invertible matrix: a new type of matrix arising in pseudo-random number generation" [Linear Algebra Appl. (2011) 144–151]. *Linear Algebra and its Applications*, 437(6):1428, September 15, 2012. CODEN LAAPAW. ISSN 0024-3795 (print), 1873-1856 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0024379512003874`. See [3623].

Yalta:2012:CSR

[3709] A. Talha Yalta and Sven Schreiber. Code snippet: Random number generation in `gretl`. *Journal of Statistical Software*, 50(CS-1):??, August 2012. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v50/c01`.

Zhang:2012:RAG

[3710] Rui Zhang and Lawrence M. Leemis. Rectangles algorithm for generating normal variates. *Naval Research Logistics*, 59(1):52–57, February 2012. CODEN NRLOEP. ISSN 0894-069X (print), 1520-6750 (electronic).

Afshar:2013:ESR

[3711] Y. Afshar, F. Schmid, A. Pishevar, and S. Worley. Exploiting seeding of random number generators for efficient domain decomposition parallelization of dissipative particle dynamics. *Computer Physics Communications*, 184(4):1119–1128, April 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465512003992`.

Anonymous:2013:ERN

[3712] Anonymous. Evaluation of random number generators: Version 0.10. Report, Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, 53133 Bonn, Germany, March 1, 2013. URL `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_AIS_31_Evaluation_of_random_number_generators_e.pdf?__blob=publicationFile`.

Applebaum:2013:PGL

[3713] Benny Applebaum. Pseudorandom generators with long stretch and low locality from random local one-way functions. *SIAM Journal on Computing*, 42(5):2008–2037, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

AragonArtacho:2013:WRN

[3714] Francisco Aragón Artacho, David H. Bailey, Jonathan M. Borwein, and Peter B. Borwein. Walking on real numbers. *The Mathematical Intelligencer*, 35(1):42–60, March 2013. CODEN MAINDC. ISSN 0343-6993 (print), 1866-7414 (electronic). URL `http://gigapan.com/gigapans/106803`; `http://www.davidhbailey.com/dhbpapers/tools-walk.pdf`.

Bailey:2013:NNP

[3715] David H. Bailey and Jonathan M. Borwein. Normal numbers and pseudorandom generators. In Bailey et al. [4291], pages 1–18. ISBN 1-4614-7620-8, 1-4614-7621-6 (e-book). ISSN 2194-1009. LCCN QA241. URL `http://public.eblib.com/choice/publicfullrecord.aspx?p=1466708`; `http://swb.eblib.com/patron/FullRecord.aspx?p=1466708`; `http://www.myilibrary.com?id=547562`.

Barash:2013:GPS

[3716] L. Yu. Barash and L. N. Shchur. On the generation of parallel streams of pseudorandom numbers. *Programmnaya inzheneriya*, 1(??):24–??, ???? 2013. CODEN ???? ISSN ????

Barash:2013:PGA

[3717] L. Yu. Barash and L. N. Shchur. PRAND: GPU accelerated parallel random number generation library. *Computer Physics Communications*, ??(??):??, ???? 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). Submitted.

Barash:2013:RPL

[3718] L. Yu. Barash and L. N. Shchur. RNGSSELIB: Program library for random number generation. More generators, parallel streams of random numbers and Fortran compatibility. *Computer Physics Communications*, 184(10):2367–2369, October 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465513001422`.

Becker:2013:SDL

[3719] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL `http://people.umass.edu/gbecker/BeckerChes13.pdf`.

Beliakov:2013:EIBa

[3720] Gleb Beliakov, Michael Johnstone, Doug Creighton, and Tim Wilkin. An efficient implementation of Bailey and Borwein's algorithm for parallel random number generation on graphics processing units. *Computing: Archiv für Informatik und Numerik*, 95(4):309–326, April 2013. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://link.springer.com/article/10.1007/s00607-012-0234-8`. See also [3721].

Beliakov:2013:EIBb

[3721] G. Beliakov, D. Creighton, M. Johnstone, and T. Wilkin. Efficient implementation of Bailey and Borwein pseudo-random number generator based on normal numbers. *Computer Physics Communications*, 184(8):1999–2004, August 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465513001276`. See also [3720].

Claessen:2013:SPN

[3722] Koen Claessen and Michał H. Pałka. Splittable pseudorandom number generators using cryptographic hashing. *ACM SIGPLAN Notices*, 48 (12):47–58, December 2013. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). Haskell '14 conference proceedings.

Deng:2013:FTQ

[3723] Dong-Ling Deng and Lu-Ming Duan. Fault-tolerant quantum random-number generator certified by Majorana fermions. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 88(1):012323:1–012323:6, July 2013. CODEN PLRAAN. ISSN 1050-2947 (print), 1094-1622, 1538-4446, 1538-4519. URL `http://link.aps.org/doi/10.1103/PhysRevA.88.012323`.

Dodis:2013:SAP

[3724] Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergniaud, and Daniel Wichs. Security analysis of pseudo-random number genera-

tors with input: `/dev/random` is not robust. In Ahmad-Reza Sadeghi, editor, *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications security — CCS '13*, pages 647–658. ACM Press, New York, NY 10036, USA, 2013.

Ducklin:2013:ARN

[3725] Paul Ducklin. Android random number flaw implicated in Bitcoin thefts. Web news story., August 12, 2013. URL `http://nakedsecurity.sophos.com/2013/08/12/android-random-number-flaw-implicated-in-bitcoin-thefts/`. From the story: "It looks as though, at least on occasion, the Java-based PRNG on Android will repeat its pseudorandom sequences, thanks to a flaw in Android's so-called `SecureRandom` Java class.".

Frauchiger:2013:TRR

[3726] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv.org*, ??(??):??, November 13, 2013. URL `http://arxiv.org/abs/1311.4547`.

Gao:2013:GGA

[3727] Shuang Gao and Gregory D. Peterson. GASPRNG: GPU accelerated scalable parallel random number generator library. *Computer Physics Communications*, 184(4):1241–1249, April 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465512003979`.

Gilchrist:2013:PEP

[3728] Jeff Gilchrist. Pseudoprime enumeration with probabilistic primality tests (Fermat base 2, Baillie–PSW, Miller–Rabin, Lucas, Lucas–Selfridge). Web site, July 7, 2013. URL `https://gilchrist.greatsite.net/jeff/factoring/pseudoprimes.html`.

Gopalan:2013:PGC

[3729] Parikshit Gopalan, Raghu Meka, Omer Reingold, and David Zuckerman. Pseudorandom generators for combinatorial shapes. *SIAM Journal on Computing*, 42(3):1051–1076, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Gugala:2013:RNG

[3730] Karol Gugala, Aleksandra Świetlicka, Michał Burdajewicz, and Andrzej Rybarczyk. Random number generation system improving simulations of stochastic models of neural cells. *Computing: Archiv für Informatik*

und Numerik, 95(1s):259–275, May 2013. CODEN CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL `http://link.springer.com/content/pdf/10.1007/s00607-012-0267-z.pdf`.

Gutierrez:2013:PML

[3731] Jaime Gutierrez, Álvar Ibeas, Domingo Gómez-Pérez, and Igor E. Shparlinski. Predicting masked linear pseudorandom number generators over finite fields. *Designs, Codes, and Cryptography*, 67(3):395–402, June 2013. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `http://link.springer.com/article/10.1007/s10623-012-9615-4`.

Haitner:2013:EIC

[3732] Iftach Haitner, Omer Reingold, and Salil Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. *SIAM Journal on Computing*, 42(3):1405–1430, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Hamze:2013:SAR

[3733] Firas Hamze, Ziyu Wang, and Nando de Freitas. Self-avoiding random dynamics on integer complex systems. *ACM Transactions on Modeling and Computer Simulation*, 23(1):9:1–9:??, January 2013. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hill:2013:SIP

[3734] David R. C. Hill, Claude Mazel, Jonathan Passerat-Palmbach, and Mamadou K. Traore. Special issue papers: Distribution of random streams for simulation practitioners. *Concurrency and Computation: Practice and Experience*, 25(10):1427–1442, July 2013. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Hladky:2013:RNG

[3735] J. Hladký. Random number generators based on the aperiodic infinite words, source programs for statistical tests. Web site., 2013. URL `https://github.com/jirka-h/aprng`.

Hu:2013:PSG

[3736] HanPing Hu, LingFeng Liu, and NaiDa Ding. Pseudorandom sequence generator based on the Chen chaotic system. *Computer Physics Communications*, 184(3):765–768, March 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465512003931`.

IBM:2013:IPC

[3737] IBM. IBM PCIe Cryptographic Coprocessor. Web document, 2013. URL `http://www-03.ibm.com/security/cryptocards/pciecc/overview.shtml`.

Imai:2013:CRN

[3738] Junichi Imai. Comparison of random number generators via Fourier transform. *Monte Carlo Methods and Applications*, 19(3):237–??, September 2013. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2013.19.issue-3/mcma-2013-0012/mcma-2013-0012.xml`.

Kane:2013:PLF

[3739] Daniel M. Kane and Raghu Meka. A PRG for Lipschitz functions of polynomials with applications to sparsest cut. In ACM [4290], pages 1–10. ISBN 1-4503-2029-5.

Khoshkenar:2013:NTR

[3740] Amin Khoshkenar and Hashem Mahlooji. A new test of randomness for Lehmer generators based on the Manhattan distance between pairs of consecutive random numbers. *Communications in Statistics: Simulation and Computation*, 42(1):202–214, 2013. CODEN CSSCDB. ISSN 0361-0918.

Lang:2013:TRS

[3741] Gabriel Lang and Eric Marcon. Testing randomness of spatial point patterns with the Ripley statistic. *ESAIM: Probability and Statistics*, 17 (??):767–??, ???? 2013. CODEN ???? ISSN 1292-8100 (print), 1262-3318 (electronic).

Leonenko:2013:BRD

[3742] Nikolai Leonenko. Book review: Domenico Marinucci and Giovanni Peccati, *Random Fields on the Sphere: Representation, Limit Theorems and Cosmological Applications*, London Mathematical Society Lecture Notes Series 389. Published by the Cambridge University Press, Cambridge, 2011. Number of Pages: 341. Price £40.00, ISBN 978-0-521-17561-6. *Journal of Time Series Analysis*, 34(5):602–603, September 2013. CODEN JTSADL. ISSN 0143-9782 (print), 1467-9892 (electronic).

Liberty:2013:THR

[3743] John S. Liberty, Adrian Barrera, David W. Boerstler, Thomas B. Chadwick, Scott R. Cottier, H. Peter Hofstee, Julie A. Rosser, and Marty L. Tsai. True hardware random number generation implemented in the

32-nm SOI POWER7+ processor. *IBM Journal of Research and Development*, 57(6):4:1–4:7, November–December 2013. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

Liu:2013:ITT

[3744] Y. Liu, M. Y. Zhu, B. Luo, J. W. Zhang, and H. Guo. Implementation of 1.6 Tb s^{-1} truly random number generation based on a super-luminescent emitting diode. *Laser Physics Letters*, 10(4):045001:1–045001:5, April 2013. CODEN LPLABC. ISSN 1612-2011 (print), 1612-202X (electronic). URL `http://iopscience.iop.org/1612-202X/10/4/045001/article`; `http://stacks.iop.org/1612-202X/10/i=4/a=045001`.

Ma:2013:PQR

[3745] Xiongfeng Ma, Feihu Xu, He Xu, Xiaoqing Tan, Bing Qi, and Hoi-Kwong Lo. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 87(6):062327, June 21, 2013. CODEN PHRVAO. ISSN 0031-899X (print), 1536-6065 (electronic). URL `http://journals.aps.org/pra/abstract/10.1103/PhysRevA.87.062327`.

Malik:2013:UCB

[3746] Jamshaid Sarwar Malik, Ahmed Hemani, and N. D. Gohar. Unifying CORDIC and Box–Muller algorithms: An accurate and efficient Gaussian random number generator. In *2013 IEEE 24th International Conference on Application-Specific Systems, Architectures and Processors (ASAP 2013): Washington, DC, USA, 5–7 June 2013*, pages 277–280. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2013. ISBN 1-4799-0494-5 (paperback), 1-4799-0493-7, 1-4799-0492-9. LCCN ???? URL `http://ieeexplore.ieee.org/document/6567590/`.

Martino:2013:EEG

[3747] Luca Martino and David Luengo. Extremely efficient generation of Gamma random variables for $\alpha \geq 1$. *arXiv.org*, 2013. URL `https://arxiv.org/abs/1304.3800`.

Mascagni:2013:PPR

[3748] Michael Mascagni and Lin-Yee Hin. Parallel pseudo-random number generators: A derivative pricing perspective with the Heston stochastic volatility model. *Monte Carlo Methods and Applications*, 19(2): 77–??, July 2013. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2013.19.issue-2/mcma-2013-0006/mcma-2013-0006.xml`.

Meka:2013:PGP

[3749] Raghu Meka and David Zuckerman. Pseudorandom generators for polynomial threshold functions. *SIAM Journal on Computing*, 42(3):1275–1301, ???? 2013. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Melia-Segui:2013:JPL

[3750] Joan Melia-Segui, Joaquin Garcia-Alfaro, and Jordi Herrera-Joancomarti. J3Gen: a PRNG for low-cost passive RFID. *Sensors (Basel, Switzerland)*, 13(3):3816–3830, March 2013. ISSN 1424-8220.

Miszczak:2013:EOQ

[3751] Jaroslaw Adam Miszczak. Employing online quantum random number generators for generating truly random quantum states in Mathematica. *Computer Physics Communications*, 184(1):257–258, January 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465512002780`.

Mouha:2013:TFO

[3752] Nicky Mouha and Bart Preneel. Towards finding optimal differential characteristics for ARX: Application to Salsa20. *IACR Cryptology ePrint Archive Report*, ??(??):1–19, 2013. URL `https://eprint.iacr.org/2013/328`. Report 2013/328.

Mukherjee:2013:OEC

[3753] Pratyay Mukherjee. An overview of eSTREAM ciphers. Report ????, Centre of Excellence in Cryptology, Indian Statistical Institute, Kolkata, India, 2013. 1–214 pp. URL `https://pratyay.net/wp-content/uploads/2017/03/estream.pdf`.

Mukhopadhyay:2013:RBI

[3754] Nitis Mukhopadhyay and Mun S. Son. Ratios X/Z, Y/Z built from independent random variables (X, Y) and Z may not always be dependent. *Statistical Methodology*, 14(??):62–66, September 2013. CODEN ???? ISSN 1572-3127 (print), 1878-0954 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1572312713000178`.

Ozkaynak:2013:SPP

[3755] Fatih Özkaynak and Sirma Yavuz. Security problems for a pseudorandom sequence generator based on the Chen chaotic system. *Computer Physics Communications*, 184(9):2178–2181, September 2013. CODEN

CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465513001604.

Pae:2013:EOR

[3756] Sung il Pae. Exact output rate of Peres's algorithm for random number generation. *Information Processing Letters*, 113(5–6):160–164, March 15, 2013. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019013000033.

Sainudiin:2013:PER

[3757] Raazesh Sainudiin, Gloria Teng, Jennifer Harlow, and Dominic Lee. Posterior expectation of regularly paved random histograms. *ACM Transactions on Modeling and Computer Simulation*, 23(1):6:1–6:??, January 2013. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Saito:2013:VMT

[3758] Mutsuo Saito and Makoto Matsumoto. Variants of Mersenne Twister suitable for graphic processors. *ACM Transactions on Mathematical Software*, 39(2):12:1–12:20, February 2013. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Schretter:2013:DIM

[3759] Colas Schretter and Harald Niederreiter. A direct inversion method for non-uniform quasi-random point sequences. *Monte Carlo Methods and Applications*, 19(1):1–??, March 2013. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://www.degruyter.com/view/j/mcma.2013.19.issue-1/mcma-2012-0014/mcma-2012-0014.xml.

Sezgin:2013:FBP

[3760] Fatin Sezgin and Tevfik Metin Sezgin. Finding the best portable congruential random number generators. *Computer Physics Communications*, 184(8):1889–1897, August 2013. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465513001100.

Shi:2013:IKR

[3761] Zhenqing Shi, Bin Zhang, Dengguo Feng, and Wenling Wu. Improved key recovery attacks on reduced-round Salsa20 and ChaCha. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *Information Security and Cryptology — ICISC 2012: 15th International Conference, Seoul, Korea, November 28–30, 2012, Revised Selected Papers*, volume 7839

of *Lecture Notes in Computer Science*, pages 337–351. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2013.

Stroustrup:2013:CPL

[3762] Bjarne Stroustrup. *The C++ programming language*. Addison-Wesley, Reading, MA, USA, fourth edition, 2013. ISBN 0-321-56384-0 (paperback), 0-321-95832-2 (hardcover), 0-13-352283-0 (e-book). xiv + 1346 pp. LCCN QA76.73.C153 S77 2013.

Thomas:2013:LSF

[3763] David B. Thomas and Wayne Luk. The LUT-SR family of uniform random number generators for FPGA architectures. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 21(4):761–770, April 2013. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/document/6190771/`.

Thomas:2013:PGG

[3764] David B. Thomas. Parallel generation of Gaussian random numbers using the Table-Hadamard transform. In IEEE, editor, *Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pages 161–168. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2013. ISBN 0-7685-4969-8. LCCN TK7895.G36. URL `https://ieeexplore.ieee.org/document/6546012`.

Xi:2013:LTB

[3765] Bowei Xi, Kean Ming Tan, and Chuanhai Liu. Logarithmic transformation-based gamma random number generators. *Journal of Statistical Software*, 55(4):1–17, October 2013. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v55/i04`.

Zhu:2013:NIC

[3766] Hegui Zhu, Cheng Zhao, Xiangde Zhang, and Lianping Yang. A novel iris and chaos-based random number generator. *Computers & Security*, 36 (??):40–48, July 2013. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404813000321`.

Abdul:2014:MGK

[3767] R. F. Abdul and R. L. Mace. A method to generate kappa distributed random deviates for particle-in-cell simulations. *Computer Physics Communications*, 185(10):2383–2386, October 2014. CODEN CPHCBZ.

ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S001046551400160X.

Anawis:2014:ARR

[3768] Mark Anawis. Applications for randomness: Random numbers have been shown to be valuable in sampling, simulations, modeling, data encryption, gambling and even musical composition. *Scientific Computing*, 31 (11):28–30, November 2014. CODEN SCHRCU. ISSN 1930-5753 (print), 1930-6156 (electronic). URL http://digital.scientificcomputing.com/scientificcomputing/hpc_source_sc14_special_edition. Special issue for Supercomputing 2014 (SC14), defining the market: 30 years of high-performance computing (1984–2014).

Anonymous:2014:CEF

[3769] Anonymous. Coming down the editorial fence — not random. *Physical Review X*, 4(3):??, September 2014. CODEN PRXHAE. ISSN 2160-3308. URL http://journals.aps.org/prx/edannounce/PhysRevX.4.031056.

Anonymous:2014:RNG

[3770] Anonymous. Random number generation. NIST Web site., July 16, 2014.

Barabesi:2014:NUR

[3771] Lucio Barabesi and Luca Pratelli. A note on a universal random variate generator for integer-valued random variables. *Statistics and Computing*, 24(4):589–596, July 2014. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL http://link.springer.com/article/10.1007/s11222-013-9390-8.

Barash:2014:PGA

[3772] L. Yu. Barash and L. N. Shchur. PRAND: GPU accelerated parallel random number generation library: Using most reliable algorithms and applying parallelism of modern GPUs and CPUs. *Computer Physics Communications*, 185(4):1343–1353, April 2014. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0010465514000204.

Baron:2014:LSP

[3773] Joshua Baron, Yuval Ishai, and Rafail Ostrovsky. On linear-size pseudorandom generators and hardcore functions. *Theoretical Computer Science*, 554(??):50–63, October 16, 2014. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S030439751400437X.

Blacher:2014:PRN

[3774] René Blacher. Proved random numbers obtained from hardware devices. *Communications in Statistics: Simulation and Computation*, 43(5):1020–1035, 2014. CODEN CSSCDB. ISSN 0361-0918.

Braverman:2014:PGR

[3775] Mark Braverman, Anup Rao, Ran Raz, and Amir Yehudayoff. Pseudorandom generators for regular branching programs. *SIAM Journal on Computing*, 43(3):973–986, ???? 2014. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Brown:2014:DRN

[3776] R. G. Brown. Dieharder: A random number test suite, version 3.31.1. Duke University Physics Department Web site, 2014. URL `http://www.phy.duke.edu/~rgb/General/dieharder.php`.

Chen:2014:EES

[3777] Guangyi Chen. Are electroencephalogram (EEG) signals pseudo-random number generators? *Journal of Computational and Applied Mathematics*, 268(??):1–4, October 1, 2014. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S037704271400123X`.

Cheng:2014:GBR

[3778] Ching-Wei Cheng, Ying-Chao Hung, and Narayanaswamy Balakrishnan. Generating beta random numbers and Dirichlet random vectors in R: the package rBeta2009. *Computational Statistics & Data Analysis*, 71(??):1011–1020, March 2014. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167947313000753`.

Devroye:2014:RVG

[3779] Luc Devroye. Random variate generation for the generalized inverse Gaussian distribution. *Statistics and Computing*, 24(2):239–246, March 2014. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/s11222-012-9367-z`.

Dodis:2014:HEY

[3780] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too — optimal recovery strategies for compromised RNGs. Report, Dept. of Computer Science,

New York University; Dept. of Computer Science and Applied Mathematics, Weizmann Institute; Dept. of Computer Science, Northeastern University, New York, NY, USA; Tel Aviv, Israel; Boston, MA, USA, March 3, 2014. 27 pp. URL http://eprint.iacr.org/2014/167; https://www.schneier.com/fortuna.html.

Doty-Humphrey:2014:STP

[3781] C. Doty-Humphrey. Specific tests in PractRand. Web site., 2014. URL http://pracrand.sourceforge.net/Tests_engines.txt.

England:2014:ERG

[3782] D. G. England, P. J. Bustard, D. J. Moffatt, J. Nunn, R. Lausten, and B. J. Sussman. Efficient Raman generation in a waveguide: A route to ultrafast quantum random number generation. *Applied Physics Letters*, 104(5):051117:1–051117:4, ???? 2014. CODEN APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842. URL ????.

Fang:2014:FAP

[3783] Xiaole Fang, Qianxue Wang, Christophe Guyeux, and Jacques M. Bahi. FPGA acceleration of a pseudorandom number generator based on chaotic iterations. *Journal of Information Security and Applications (JISA)*, 19(1):78–87, February 2014. CODEN ???? ISSN 2214-2126. URL http://www.sciencedirect.com/science/article/pii/S221421261400012X.

Fukushima:2014:SDS

[3784] Akio Fukushima, Takayuki Seki, Kay Yakushiji, Hitoshi Kubota, Hiroshi Imamura, Shinji Yuasa, and Koji Ando. Spin dice: A scalable truly random number generator based on spintronics. *Applied Physics Express*, 7(8):083001:1–083001:5, August 2014. CODEN APEPC4. ISSN 1882-0778 (print), 1882-0786 (electronic). URL http://iopscience.iop.org/1882-0786/7/8/083001/article; http://stacks.iop.org/1882-0786/7/i=8/a=083001.

Gomez-Perez:2014:AEA

[3785] Domingo Gómez-Pérez, Alina Ostafe, and Igor Shparlinski. Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators. *Mathematics of Computation*, 83(287):1535–1550, 2014. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://www.ams.org/journals/mcom/2014-83-287/S0025-5718-2013-02780-9; http://www.ams.org/journals/mcom/2014-83-287/S0025-5718-2013-02780-9/S0025-5718-2013-02780-9.pdf.

Haigh:2014:ABE

[3786] T. Haigh, M. Priestley, and C. Rope. Los Alamos bets on ENIAC: Nuclear Monte Carlo simulations, 1947–1948. *IEEE Annals of the History of Computing*, 36(3):42–63, July 2014. CODEN IAHCEX. ISSN 1058-6180 (print), 1934-1547 (electronic).

Healey:2014:SPS

[3787] Christopher Healey, Sigrún Andradóttir, and Seong-Hee Kim. Selection procedures for simulations with multiple constraints under independent and correlated sampling. *ACM Transactions on Modeling and Computer Simulation*, 24(3):14:1–14:??, June 2014. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Hormann:2014:GGI

[3788] Wolfgang Hörmann and Josef Leydold. Generating generalized inverse Gaussian random variates. *Statistics and Computing*, 24(4):547–557, July 2014. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/s11222-013-9387-3`.

Hosseini:2014:GPR

[3789] Seyed Morteza Hosseini, Hossein Karimi, and Majid Vafaei Jahan. Generating pseudo-random numbers by combining two systems with complex behaviors. *Journal of Information Security and Applications (JISA)*, 19 (2):149–162, April 2014. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212614000039`.

Hu:2014:MBA

[3790] Jiaqiao Hu, Enlu Zhou, and Qi Fan. Model-based annealing random search with stochastic averaging. *ACM Transactions on Modeling and Computer Simulation*, 24(4):21:1–21:??, August 2014. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Kawai:2014:ADT

[3791] Shinji Kawai, Fukuhito Ooshita, Hirotsugu Kakugawa, and Toshimitsu Masuzawa. Analysis of distributed token circulation algorithm with faulty random number generator. *Parallel Processing Letters*, 24(1): 1450002, March 2014. CODEN PPLTEE. ISSN 0129-6264 (print), 1793-642X (electronic).

Koo:2014:CRB

[3792] Bonwook Koo, Dongyoung Roh, and Daesung Kwon. Converting random bits into random numbers. *The Journal of Supercomputing*, 70

(1):236–246, October 2014. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `http://link.springer.com/article/10.1007/s11227-014-1202-1`.

Korzen:2014:PPP

[3793] Marcin Korzeń and Szymon Jaroszewicz. PaCAL: A Python package for arithmetic computations with random variables. *Journal of Statistical Software*, 57(10):??, May 2014. CODEN JSSOBK. ISSN 1548-7660. URL `http://www.jstatsoft.org/v57/i10`.

Langr:2014:APP

[3794] Daniel Langr, Pavel Tvrdík, Tomás Dytrych, and Jerry P. Draayer. Algorithm 947: Paraperm — parallel generation of random permutations with MPI. *ACM Transactions on Mathematical Software*, 41(1):5:1–5:26, October 2014. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

LEcuyer:2014:LSS

[3795] Pierre L'Ecuyer and Richard Simard. On the lattice structure of a special class of multiple recursive random number generators. *INFORMS Journal on Computing*, 26(3):449–460, 2014. ISSN 1091-9856 (print), 1526-5528 (electronic).

Ling:2014:MDN

[3796] San Ling, Igor Shparlinski, and Huaxiong Wang. On the multidimensional distribution of the Naor–Reingold pseudo-random function. *Mathematics of Computation*, 83(289):2429–2434, 2014. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL `http://www.ams.org/journals/mcom/2014-83-289/S0025-5718-2014-02794-4; http://www.ams.org/journals/mcom/2014-83-289/S0025-5718-2014-02794-4/S0025-5718-2014-02794-4.pdf`.

Liu:2014:LFP

[3797] Huaning Liu. Large family of pseudorandom subsets of the set of the integers not exceeding N. *International Journal of Number Theory*, 10(5):1121–1141, August 2014. ISSN 1793-0421 (print), 1793-7310 (electronic). URL `https://www.worldscientific.com/doi/10.1142/S1793042114500183`.

Mascagni:2014:HPC

[3798] Michael Mascagni, Yue Qiu, and Lin-Yee Hin. High performance computing in quantitative finance: A review from the pseudo-random number generator perspective. *Monte Carlo Methods and Applications*, 20(2):

101–120, June 2014. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://www.degruyter.com/view/j/mcma.2014.20.issue-2/mcma-2013-0020/mcma-2013-0020.xml.

Mohamed:2014:MCS

[3799] N. M. A. Mohamed. Monte Carlo sampling of Maxwell and Gaussian distributions using a single random number. *Theory of Probability and its Applications*, 58(4):698–704, ???? 2014. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).

Mortari:2014:MAV

[3800] Daniele Mortari. Memory adaptive k-vector. In Roby S. Wilson, Renato Zanetti, Donald L. Mackison, and Ossama Abdelkhalik, editors, *Spaceflight mechanics 2014: proceedings of the 24th AAS/AIAA Space Flight Mechanics Meeting held January 26–30, 2014, Santa Fe, New Mexico, U.S.A*, pages 1461–1474. Published for the American Astronautical Society by Univelt, San Diego, CAS, USA, 2014. ISBN 0-87703-611-X (hardcover + CD ROM), 0-87703-612-8 (CD ROM version). ISSN 1081-6003. LCCN TL787.A6 A2 vol. 152. URL http://www.univelt.com/book=4731; https://www.researchgate.net/publication/288734831_Memory_adaptive_K-vector. Paper number AAS 14-302.

Raaphorst:2014:CSC

[3801] Sebastian Raaphorst, Lucia Moura, and Brett Stevens. A construction for strength-3 covering arrays from linear feedback shift register sequences. *Designs, Codes, and Cryptography*, 73(3):949–968, December 2014. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-013-9835-2.

Rivest:2014:SSR

[3802] Ronald L. Rivest and Jacob C. N. Schuldt. Spritz —- a spongy RC4-like stream cipher and hash function. Report, MIT CSAIL and Research Institute for Secure Systems, Cambridge, MA 02139, USA and AIST, Japan, October 27, 2014. 30 pp. URL http://people.csail.mit.edu/rivest/pubs/RS14.pdf.

Saito:2014:XV

[3803] M. Saito and M. Matsumoto. XSadd (version 1.1). Web document., February 15, 2014. URL http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/XSADD/.

Sanguinetti:2014:QRN

[3804] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Physical Review X*, 4(3):031056:1–031056:6, September 2014. CODEN PRXHAE. ISSN 2160-3308. URL `http://link.aps.org/doi/10.1103/PhysRevX.4.031056`.

Sileshi:2014:AHG

[3805] B. G. Sileshi, C. Ferrer, and J. Oliver. Accelerating hardware Gaussian random number generation using Ziggurat and CORDIC algorithms. In IEEE, editor, *IEEE SENSORS 2014: proceedings: Valencia Conference Centre, Valencia, Spain, November 2-5, 2014*, pages 2122–2125. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2014. ISBN 1-4799-0160-1 (paperback), 1-4799-0161-X (USB). ISSN 1930-0395. LCCN TA165 .I338 2014. URL `http://ieeexplore.ieee.org/document/6985457/?arnumber=6985457`.

Sobol:2014:QMC

[3806] Ilya M. Sobol and Boris V. Shukhman. Quasi-Monte Carlo: A high-dimensional experiment. *Monte Carlo Methods and Applications*, 20(3): 167–171, September 2014. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2014.20.issue-3/mcma-2013-0022/mcma-2013-0022.xml`.

Steele:2014:FSP

[3807] Guy L. Steele, Jr., Doug Lea, and Christine H. Flood. Fast splittable pseudorandom number generators. *ACM SIGPLAN Notices*, 49(10):453–472, October 2014. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Thomas:2014:FGR

[3808] David B. Thomas. FPGA Gaussian random number generators with guaranteed statistical accuracy. In IEEE, editor, *2014 IEEE 22nd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM): 11–13 May 2014, Boston, Massachusetts, USA*, pages 149–156. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2014. ISBN 1-4799-5111-0, 1-4799-5112-9, 1-4799-5110-2. LCCN ???? URL `http://ieeexplore.ieee.org/document/6861609/`.

Zhu:2014:SER

[3809] Yan Zhu, Di Ma, Changjun Hu, Gail-Joon Ahn, and Hongxin Hu. Secure and efficient random functions with variable-length output.

Journal of Network and Computer Applications, 45(??):121–133, October 2014. CODEN JNCAF3. ISSN 1084-8045 (print), 1095-8592 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1084804514001817`.

Andersen:2015:MEL

[3810] Timothy D. Andersen and Michael Mascagni. Memory efficient lagged-Fibonacci random number generators for GPU supercomputing. *Monte Carlo Methods and Applications*, 21(2):163–174, June 2015. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `http://www.degruyter.com/view/j/mcma.2015.21.issue-2/mcma-2014-0017/mcma-2014-0017.xml`.

Astor:2015:ADI

[3811] Eric P. Astor. Asymptotic density, immunity and randomness. *Computability*, 4(2):141–158, ???? 2015. CODEN ???? ISSN 2211-3568 (print), 2211-3576 (electronic).

Barabesi:2015:UMG

[3812] L. Barabesi and L. Pratelli. Universal methods for generating random variables with a given characteristic function. *Journal of Statistical Computation and Simulation*, 85(8):1679–1691, 2015. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Berman:2015:NAA

[3813] Itay Berman and Iftach Haitner. From non-adaptive to adaptive pseudorandom functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):297–311, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9169-2`.

Beznosko:2015:HSH

[3814] Dmitriy Beznosko. High-speed hardware random number generator. 21 lecture slides from PhotoDet 2015: International Conference on New Photo-detectors, 6–9 July 2015, Moscow, Troitsk, Russia, July 2015. URL `https://indico.inr.ru/event/4/session/13/contribution/1/material/slides/0.pptx`.

Beznosko:2015:PPF

[3815] Dmitriy Beznosko, T. Beremkulov, A. Duspayev, A. Iakovlev, A. Tailakov, and M. Yessenov. A physical principle for fast and miniature random number hardware generator using MPPC photo detector. *Journal of Advances in Physics: JAP*, 7(3):1970–1975, June 2015. ISSN

2347-3487. URL http://cirworld.org/journals/index.php/jap/article/view/243n.

Carlet:2015:EBF

[3816] Claude Carlet and Deng Tang. Enhanced Boolean functions suitable for the filter model of pseudo-random generator. *Designs, Codes, and Cryptography*, 76(3):571–587, September 2015. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL http://link.springer.com/article/10.1007/s10623-014-9978-9.

Claessen:2015:GCR

[3817] Koen Claessen, Jonas Duregård, and Michal H. Palka. Generating constrained random data with uniform distribution. *Journal of Functional Programming*, 25:e8, ???? 2015. CODEN JFPRES. ISSN 0956-7968 (print), 1469-7653 (electronic). URL https://www.cambridge.org/core/journals/journal-of-functional-programming/article/generating-constrained-random-data-with-uniform-distribution/567438B9A7FABDD0F191FF65DAEA7005.

Deng:2015:URN

[3818] L.-Y. Deng and J.-J. H. Shiau. Uniform random numbers. In N Balakrishnan, Theodore Colton, and Brian Everitt, editors, *Wiley StatsRef: Statistics Reference Online*, pages 1–14. Wiley, New York, NY, USA, 2015. ISBN 1-118-44511-2 (e-book). LCCN QA276.

Fog:2015:PRN

[3819] Agner Fog. Pseudo-random number generators for vector processors and multicore processors. *Journal of Modern Applied Statistical Methods*, 14(1):308–334, May 5, 2015. ISSN 1538-9472. URL http://digitalcommons.wayne.edu/jmasm/vol14/iss1/23; https://www.agner.org/random/theory/randomvector.pdf.

Guyeux:2015:ECS

[3820] Christophe Guyeux, Raphaël Couturier, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on GPU. *The Journal of Supercomputing*, 71(10):3877–3903, October 2015. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL http://link.springer.com/article/10.1007/s11227-015-1479-8.

Haeupler:2015:SFD

[3821] Bernhard Haeupler. Simple, fast and deterministic gossip and rumor spreading. *Journal of the ACM*, 62(6):47:1–47:??, December 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Hare:2015:MDR

[3822] Eric Hare, Andreas Buja, and Heike Hofmann. Manipulation of discrete random variables with `discreteRV`. *The R Journal*, 7(1):185–194, June 2015. CODEN ???? ISSN 2073-4859. URL `http://journal.r-project.org/archive/2015-1/RJournal_2015-1_hare-buja-hofmann.pdf`.

Hill:2015:PRN

[3823] David R. C. Hill. Parallel random numbers, simulation, and reproducible research. *Computing in Science and Engineering*, 17(4):66–71, July/August 2015. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366X (electronic). URL `http://csdl.computer.org/csdl/mags/cs/2015/04/mcs2015040066-abs.html`.

Jessa:2015:QRS

[3824] M. Jessa. On the quality of random sequences produced with a combined random bit generator. *IEEE Transactions on Computers*, 64(3):791–804, March 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Langley:2015:CPC

[3825] A. Langley, N. Mavrogiannopoulos W. Chang, J. Strombergson, and S. Josefsson. ChaCha20–Poly1305 cipher suites for transport layer security (TLS). Report, Internet Research Task Force (IRTF), 2015. URL `https://tools.ietf.org/html/rfc7905`. RFC 7905.

LEcuyer:2015:RNP

[3826] P. L'Ecuyer, D. Munger, B. Oreshkin, and R. Simard. Random numbers for parallel computers: requirements and methods, with emphasis on GPUs. Report, DIRO, Pavillon Aisenstadt, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal, QC, Canada H3C 3J7, April 17, 2015. 32 pp. URL `http://www.iro.umontreal.ca/~lecuyer/myftp/papers/parallel-rng-imacs.pdf`.

Leetmaa:2015:KER

[3827] Mikael Leetmaa and Natalia V. Skorodumova. KMCLib 1.1: Extended random number support and technical updates to the KMCLib general framework for kinetic Monte-Carlo simulations. *Computer Physics Communications*, 196(??):611–613, November 2015. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465515002611`.

LoRe:2015:SRN

[3828] Giuseppe Lo Re, Fabrizio Milazzo, and Marco Ortolani. Secure random number generation in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 27(15):3842–3862, October 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Lubicz:2015:TOB

[3829] D. Lubicz and N. Bochard. Towards an oscillator based TRNG with a certified entropy rate. *IEEE Transactions on Computers*, 64(4):1191–1200, April 2015. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Maitra:2015:CIC

[3830] Subhamoy Maitra. Chosen IV cryptanalysis on reduced round ChaCha and Salsa. Preprint, IACR Cryptology ePrint Archive, 2015. 13 pp. URL `http://eprint.iacr.org/2015/698`.

Malik:2015:RCL

[3831] Jamshaid Sarwar Malik, Ahmed Hemani, Jameel Nawaz Malik, B. Silmane, and N. D. Gohar. Revisiting central limit theorem: Accurate Gaussian random number generation in VLSI. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 23(5):842–855, May 2015. CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL `http://ieeexplore.ieee.org/document/6834810/`.

Malkiel:2015:RWW

[3832] Burton Gordon Malkiel. *A random walk down Wall Street: the time-tested strategy for successful investing*. W. W. Norton & Co., New York, NY, USA, revised and updated edition, 2015. ISBN 0-393-24611-6. 447 pp. LCCN HG4521 M251r 2015; HG4521 .M284 2015.

Miles:2015:CCP

[3833] Eric Miles and Emanuele Viola. On the complexity of constructing pseudorandom functions (especially when they don't exist). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):509–532, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9161-x`.

Miles:2015:SPN

[3834] Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *Journal of the ACM*, 62(6):

46:1–46:??, December 2015. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Mortari:2015:VAS

[3835] Daniele Mortari and J. A. Rogers. k-vector approach to sampling, interpolation, and approximation. *Journal of the Astronautical Sciences*, 60(3–4):686–706, December 2015. CODEN JALSA6. ISSN 0021-9142 (print), 2195-0571 (electronic). URL `http://ireal.gatech.edu/wp-content/themes/twentytwelve-child/pdfs/JAS_K-vector.pdf; https://link.springer.com/article/10.1007%2Fs40295-015-0065-x`.

Moufek:2015:MCB

[3836] Hamza Moufek and Kenza Guenda. McEliece cryptosystem based on punctured convolutional codes and the pseudo-random generators. *ACM Communications in Computer Algebra*, 49(1):21, March 2015. CODEN ???? ISSN 1932-2232 (print), 1932-2240 (electronic).

NIST:2015:SSP

[3837] NIST. SHA-3 standard: Permutation-based hash and extendable-output functions. FIPS PUB 202, National Institute for Standards and Technology, Gaithersburg, MD, USA, 2015. viii + 29 pp.

Nuida:2015:MPS

[3838] Koji Nuida, Takuro Abe, Shizuo Kaji, Toshiaki Maeno, and Yasuhide Numata. A mathematical problem for security analysis of hash functions and pseudorandom generators. *International Journal of Foundations of Computer Science (IJFCS)*, 26(2):169–??, February 2015. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Passerat-Palmbach:2015:TSS

[3839] Jonathan Passerat-Palmbach, Claude Mazel, and David R. C. Hill. TaskLocalRandom: a statistically sound substitute to pseudorandom number generation in parallel Java tasks frameworks. *Concurrency and Computation: Practice and Experience*, 27(13):3383–3398, September 10, 2015. CODEN CCPEBO. ISSN 1532-0626 (print), 1532-0634 (electronic).

Pollack:2015:SNN

[3840] Paul Pollack and Joseph Vandehey. Some normal numbers generated by arithmetic functions. *Canadian mathematical bulletin = Bulletin canadien de mathématiques*, 58(1):160–??, March 2015. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

Potter:2015:MUE

[3841] Bruce Potter and Sasha Wood. Managing and understanding entropy usage. Slides for Black Hat 2015 conference talk., July 20, 2015. URL `http://www.blackhat.com/docs/us-15/materials/us-15-Potter-Understanding-And-Managing-Entropy-Usage.pdf`.

Raitza:2015:RRN

[3842] Michael Raitza, Markus Vogt, Christian Hochberger, and Thilo Pionteck. RAW 2014: Random number generators on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 9(2):15:1–15:??, December 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Romano:2015:AGR

[3843] Paul K. Romano. An algorithm for generating random variates from the Madland–Nix fission energy spectrum. *Computer Physics Communications*, 187(??):152–155, February 2015. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465514003713`.

Ruckert:2015:MSS

[3844] Martin Ruckert. *The MMIX supplement: supplement to* The Art of Computer Programming, volumes 1, 2, 3 *by Donald E. Knuth*. Addison-Wesley, Reading, MA, USA, 2015. ISBN 0-13-399231-4 (paperback), 0-13-399289-6. xxi + 193 pp. LCCN QA76.6 .K64 2005 Suppl. 1. URL `http://mmix.cs.hm.edu/`.

Sarkar:2015:FNR

[3845] Santanu Sarkar. Further non-randomness in RC4, RC4A and VMPC. *Cryptography and Communications*, 7(3):317–330, September 2015. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s12095-014-0119-0`.

Savvidy:2015:MRN

[3846] Konstantin G. Savvidy. The MIXMAX random number generator. *Computer Physics Communications*, 196(??):161–165, November 2015. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465515002489`.

Schaathun:2015:ESP

[3847] Hans Georg Schaathun. Evaluation of splittable pseudo-random generators. *Journal of Functional Programming*, 25:e6, ???? 2015. CODEN JFPRES. ISSN 0956-7968 (print), 1469-7653 (electronic). URL `https://www.cambridge.org/core/journals/journal-of-functional-programming/article/evaluation-of-splittable-pseudorandom-generators/3EBAA9F14939C5BB5560E32D1A13`

Thomas:2015:THG

[3848] David B. Thomas. The table-Hadamard GRNG: an area-efficient FPGA Gaussian random number generator. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 8(4):23:1–23:??, October 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Urano:2015:DRE

[3849] Ryo Urano and Yuko Okamoto. Deterministic replica-exchange method without pseudo random numbers for simulations of complex systems. *Computer Physics Communications*, 197(??):128–135, December 2015. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465515003069`.

Wang:2015:SDB

[3850] Yongge Wang and Tony Nicol. On statistical distance based testing of pseudo random sequences and experiments with PHP and Debian OpenSSL. *Computers & Security*, 53(??):44–64, September 2015. CODEN CPSEDU. ISSN 0167-4048 (print), 1872-6208 (electronic). URL `https://www.sciencedirect.com/science/article/pii/S0167404815000693`.

Yu:2015:PGR

[3851] Yu Yu, Xiangxue Li, and Jian Weng. Pseudorandom generators from regular one-way functions: New constructions with improved parameters. *Theoretical Computer Science*, 569(??):58–69, March 2, 2015. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397514010123`.

Zhong:2015:NLM

[3852] Jianghua Zhong and Dongdai Lin. A new linearization method for nonlinear feedback shift registers. *Journal of Computer and System Sciences*, 81(4):783–796, June 2015. CODEN JCSSBM. ISSN 0022-0000 (print), 1090-2724 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0022000014002001`.

Ahmadi-Javid:2016:EAR

[3853] Amir Ahmadi-Javid and Asghar Moeini. An economical acceptance-rejection algorithm for uniform random variate generation over constrained simplexes. *Statistics and Computing*, 26(3):703–713, May 2016. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (electronic). URL `http://link.springer.com/article/10.1007/s11222-015-9553-x`.

Baccini:2016:RVG

[3854] Alberto Baccini, Lucio Barabesi, and Luisa Stracqualursi. Random variate generation and connected computational issues for the Poisson–Tweedie distribution. *Computational Statistics*, 31(2):729–748, June 2016. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `http://link.springer.com/article/10.1007/s00180-015-0623-5`.

Balkova:2016:APN

[3855] L'ubomíra Balková, Michelangelo Bucci, Alessandro De Luca, Jiří Hladký, and Svetlana Puzynina. Aperiodic pseudorandom number generators based on infinite words. *Theoretical Computer Science*, 647 (??):85–100, September 27, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397516303875`.

Bayon:2016:FME

[3856] Pierre Bayon, Lilian Bossuet, Alain Aubert, and Viktor Fischer. Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators. *Journal of Cryptographic Engineering*, 6(1):61–74, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0113-2`.

Chang-Fong:2016:CSC

[3857] N. Chang-Fong and A. Essex. The cloudier side of cryptographic end-to-end verifiable voting: A security analysis of Helios. In ACM, editor, *Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC 16: 5–9 December 2016, Hilton Los Angeles Universal City, Los Angeles, CA, USA)*. ACM Press, New York, NY 10036, USA, 2016. ISBN 1-4503-4771-1.

Chattopadhyay:2016:ETS

[3858] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. Report TR15-119, Hasso–Plattnet-Institut,

Universität Pottsdam, Pottsdam, Germany, March 20, 2016. URL http://eccc.hpi-web.de/report/2015/119/.

Chen:2016:PEP

[3859] Yu Chen and Zongyang Zhang. Publicly evaluable pseudorandom functions and their applications. *Journal of Computer Security*, 24(2):289–320, ???? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Choudhuri:2016:DCS

[3860] Arka Rai Choudhuri and Subhamoy Maitra. Differential cryptanalysis of Salsa and ChaCha — an evaluation with a hybrid model. *IACR Cryptology ePrint Archive*, 377:1–21, 2016. URL https://eprint.iacr.org/2016/377.

Choudhuri:2016:SIM

[3861] A. R. Choudhuri and S. Maitra. Significantly improved multi-bit differentials for reduced round Salsa and ChaCha. *IACR Transactions on Symmetric Cryptology*, 2016(2):261–287, 2016. ISSN 2519-173X. URL https://tosc.iacr.org/index.php/ToSC/article/view/574.

deAndrade:2016:RNG

[3862] B. B. de Andrade, H. Bolfarine, and A. N. Siroky. Random number generation and estimation with the bimodal asymmetric power-normal distribution. *Journal of Statistical Computation and Simulation*, 86(3):460–476, 2016. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Dorre:2016:ELO

[3863] Felix Dörre and Vladimir Klebanov. Entropy loss and output predictability in the Libgcrypt PRNG. Report CVE-2016-6313, Karlsruhe Institute of Technology, Karlsruhe, Germany, August 18, 2016. 2 pp. URL http://formal.iti.kit.edu/~klebanov/pubs/libgcrypt-cve-2016-6313.pdf.

Drineas:2016:RRN

[3864] Petros Drineas and Michael W. Mahoney. RandNLA: randomized numerical linear algebra. *Communications of the ACM*, 59(6):80–90, June 2016. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://cacm.acm.org/magazines/2016/6/202647/fulltext.

Guskova:2016:RPL

[3865] M. S. Guskova, L. Yu. Barash, and L. N. Shchur. RNGAVXLIB: Program library for random number generation, AVX realization. *Computer Physics Communications*, 200(??):402–405, March 2016. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465515004117`.

Herbert:2016:LIV

[3866] Ian Herbert. Lowness for integer-valued randomness. *Computability*, 5 (2):103–109, ???? 2016. CODEN ???? ISSN 2211-3568 (print), 2211-3576 (electronic).

Karney:2016:SEN

[3867] Charles F. F. Karney. Sampling exactly from the normal distribution. *ACM Transactions on Mathematical Software*, 42(1):3:1–3:14, February 2016. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). See improvement in [**?**].

Koerner:2016:REB

[3868] Brendan I. Koerner. Russians engineer a brilliant slot machine cheat — and casinos have no fix. Web news story, February 6, 2016. URL `https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/`. This story reports how attackers were able to use live-video-recorded observations of slot-machine behavior to predict future output of the pseudo-random-number generator, and make substantial wins on bets.

Lao:2016:BFD

[3869] Yingjie Lao, Qianying Tang, Chris H. Kim, and Keshab K. Parhi. Beat frequency detector-based high-speed true random number generators: Statistical modeling and analysis. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1):9:1–9:??, December 2016. CODEN ???? ISSN 1550-4832 (print), 1550-4840 (electronic).

Lecuyer:2016:ALB

[3870] Pierre L'Ecuyer and David Munger. Algorithm 958: Lattice Builder: a general software tool for constructing rank-1 lattice rules. *ACM Transactions on Mathematical Software*, 42(2):15:1–15:30, June 2016. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Li:2016:ITS

[3871] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. Report TR15-125, Hasso–Plattnet-Institut, Universität Pottsdam, Pottsdam, Germany, February 3, 2016.

Li:2016:MUN

[3872] Jie Li, Jianliang Zheng, and Paula Whitlock. MaD0: an ultrafast nonlinear pseudorandom number generator. *ACM Transactions on Modeling and Computer Simulation*, 26(2):13:1–13:??, January 2016. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Liu:2016:PBG

[3873] Lingfeng Liu, Suoxia Miao, Mengfan Cheng, and Xiaojing Gao. A pseudorandom bit generator based on new multi-delayed Chebyshev map. *Information Processing Letters*, 116(11):674–681, November 2016. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019016300953`.

Losego:2016:SMW

[3874] A. Losego. Super Mario world random number generation. YouTube video (14m4s), 2016. URL `https://youtu.be/q15yNrJHOak`.

Malik:2016:GRN

[3875] Jamshaid Sarwar Malik and Ahmed Hemani. Gaussian random number generation: a survey on hardware architectures. *ACM Computing Surveys*, 49(3):53:1–53:??, November 2016. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic).

Mandal:2016:DIW

[3876] Kalikinkar Mandal, Xinxin Fan, and Guang Gong. Design and implementation of Warbler family of lightweight pseudorandom number generators for smart devices. *ACM Transactions on Embedded Computing Systems*, 15(1):1:1–1:??, February 2016. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Mandal:2016:FRI

[3877] Kalikinkar Mandal and Guang Gong. Feedback reconstruction and implementations of pseudorandom number generators from composited De Bruijn sequences. *IEEE Transactions on Computers*, 65(9):2725–2738, ???? 2016. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

McFarland:2016:MZA

[3878] Christopher D. McFarland. A modified ziggurat algorithm for generating exponentially and normally distributed pseudorandom numbers. *Journal of Statistical Computation and Simulation*, 86(7):1281–1294, 2016. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Miller:2016:RPS

[3879] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM*, 63(4):33:1–33:??, November 2016. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Nekrutkin:2016:CBF

[3880] Vladimir Nekrutkin. On the complexity of binary floating point pseudorandom generation. *Monte Carlo Methods and Applications*, 22(2):109–??, June 2016. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `https://www.degruyter.com/view/j/mcma.2016.22.issue-2/mcma-2016-0105/mcma-2016-0105.xml`.

NIST:2016:SDR

[3881] NIST. SP 800-90B: Draft recommendation for the entropy sources used for random bit generation. Web document, January 27, 2016. URL `http://csrc.nist.gov/publications/PubsDrafts.html#800-90B`.

Ohsaka:2016:DIA

[3882] Naoto Ohsaka, Takuya Akiba, Yuichi Yoshida, and Ken ichi Kawarabayashi. Dynamic influence analysis in evolving networks. *Proceedings of the VLDB Endowment*, 9(12):1077–1088, August 2016. CODEN ???? ISSN 2150-8097.

Raitza:2016:RRN

[3883] Michael Raitza, Markus Vogt, Christian Hochberger, and Thilo Pionteck. RAW 2014: Random number generators on FPGAs. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 9(2):15:1–15:??, February 2016. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Savvidy:2016:ACS

[3884] G. K. Savvidy. Anosov C-systems and random number generators. *Theoretical and Mathematical Physics*, 188(2):1155–1171, August 2016. CODEN TMPHAH. ISSN 0040-5779 (print), 1573-9333 (electronic). URL `http://arxiv.org/abs/1507.06348`.

Savvidy:2016:SEC

[3885] Konstantin Savvidy and George Savvidy. Spectrum and entropy of C-systems MIXMAX random number generator. *Chaos, Solitons & Fractals*, 91:33–38, October 2016. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic). URL `https://arxiv.org/abs/1510.06274`.

VanBever:2016:SBT

[3886] Germain Van Bever. Simplicial bivariate tests for randomness. *Statistics & Probability Letters*, 112(??):20–25, May 2016. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167715216000092`.

Vanhoef:2016:AYB

[3887] Mathy Vanhoef and Frank Piessens. All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS. In ????, editor, *24th USENIX Security Symposium (USENIX Security 15), August 12–14, 2015, Washington D.C.*, page 17. USENIX, Berkeley, CA, USA, 2016. ISBN 1-939133-11-4. LCCN ???? URL `https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-vanhoef.pdf`.

Vigna:2016:EEM

[3888] Sebastiano Vigna. An experimental exploration of Marsaglia's `xorshift` generators, scrambled. *ACM Transactions on Mathematical Software*, 42 (4):30:1–30:23, July 2016. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `http://dl.acm.org/citation.cfm?id=2845077`.

Yamakami:2016:PGA

[3889] Tomoyuki Yamakami. Pseudorandom generators against advised context-free languages. *Theoretical Computer Science*, 613(??):1–27, February 1, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0304397515009196`.

Yu:2016:GPR

[3890] Qiqing Yu and Junyi Dong. Generation of pseudo random numbers and estimation under Cox models with time-dependent covariates. *Journal of Statistical Computation and Simulation*, 86(14):2727–2739, 2016. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Aljahdali:2017:FIS

[3891] Asia Aljahdali and Michael Mascagni. Feistel-inspired scrambling improves the quality of linear congruential generators. *Monte Carlo Methods and Applications*, 23(2):89–??, June 2017. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `https://www.degruyter.com/view/j/mcma.2017.23.issue-2/mcma-2017-0105/mcma-2017-0105.xml`.

Anonymous:2017:DAD

[3892] Anonymous. The DUHK attack: Don't use hard-coded keys. Web site., October 25, 2017. URL `https://duhkattack.com/`. From the introduction: "DUHK (Don't Use Hard-coded Keys) is a vulnerability that affects devices using the ANSI X9.31 Random Number Generator (RNG) in conjunction with a hard-coded seed key. The ANSI X9.31 RNG is an algorithm that until recently was commonly used to generate cryptographic keys that secure VPN connections and web browsing sessions, preventing third parties from reading intercepted communications." See [3900] for details of the attack.

Artemenko:2017:PGO

[3893] Sergei Artemenko and Ronen Shaltiel. Pseudorandom generators with optimal seed length for non-Boolean poly-size circuits. *ACM Transactions on Computation Theory*, 9(2):6:1–6:??, May 2017. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic).

Bacher:2017:GRP

[3894] Axel Bacher, Olivier Bodini, Hsien-Kuei Hwang, and Tsung-Hsi Tsai. Generating random permutations by coin tossing: Classical algorithms, new analysis, and modern implementation. *ACM Transactions on Algorithms*, 13(2):24:1–24:43, May 2017. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic).

Barmpalias:2017:PCO

[3895] George Barmpalias, Douglas Cenzer, and Christopher P. Porter. The probability of a computable output from a random oracle. *ACM Transactions on Computational Logic*, 18(3):18:1–18:??, August 2017. CODEN ???? ISSN 1529-3785 (print), 1557-945X (electronic).

Barmpalias:2017:RNP

[3896] George Barmpalias, Douglas Cenzer, and Christopher P. Porter. Random numbers as probabilities of machine behavior. *Theoretical Computer Science*, 673(??):1–18, April 18, 2017. CODEN TCSCDI. ISSN 0304-3975

(print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397517301032.

Beebe:2017:MFC

[3897] Nelson H. F. Beebe. *The Mathematical-Function Computation Handbook: Programming Using the MathCW Portable Software Library*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2017. ISBN 3-319-64109-3 (hardcover), 3-319-64110-7 (e-book). xxxvi + 1114 pp. LCCN QA75.5-76.95. URL http://www.springer.com/us/book/9783319641096.

Bernardini:2017:MRP

[3898] Riccardo Bernardini and Roberto Rinaldo. Making random permutations from physically unclonable constants. *International Journal of Information Security*, 16(3):249–261, June 2017. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL http://link.springer.com/article/10.1007/s10207-016-0324-2.

Chalk:2017:CIR

[3899] Cameron T. Chalk, Bin Fu, Eric Martinez, Robert Schweller, and Tim Wylie. Concentration independent random number generation in tile self-assembly. *Theoretical Computer Science*, 667(??):1–15, March 8, 2017. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397516307496.

Cohney:2017:PSR

[3900] Shaanan Cohney, Matthew D. Green, and Nadia Heninger. Practical state recovery attacks against legacy RNG implementations. Report, University of Pennsylvania and The Johns Hopkins University, College Park, PA and Baltimore, MD, October 23, 2017. 15 pp. URL https://duhkattack.com/paper.pdf.

Deng:2017:DPR

[3901] Lih-Yuan Deng and Dale Bowman. Developments in pseudo-random number generators. *WIREs Computational Statistics*, 9(5):e1404:1–e1404:??, September/October 2017. CODEN ???? ISSN 1939-0068 (print), 1939-5108 (electronic).

Devroye:2017:EBC

[3902] Luc Devroye and Claude Gravel. The expected bit complexity of the von Neumann rejection algorithm. *Statistics and Computing*, 27(3):699–710, May 2017. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375

(electronic). URL http://link.springer.com/accesspage/article/10.1007/s11222-016-9648-z.

Dodis:2017:HEY

[3903] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too: Optimal recovery strategies for compromised RNGs. *Algorithmica*, 79(4):1196–1232, December 2017. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Fog:2017:PRN

[3904] Agner Fog. Pseudo random number generators: uniform and non-uniform distributions. Web site, 2017. URL http://www.agner.org/random/.

Ghersi:2017:CQR

[3905] Dario Ghersi, Abhishek Parakh, and Mihaly Mezei. Comparison of a quantum random number generator with pseudorandom number generators for their use in molecular Monte Carlo simulations. *Journal of Computational Chemistry*, 38(31):2713–2720, December 5, 2017. CODEN JCCHDD. ISSN 0192-8651 (print), 1096-987X (electronic).

Hamza:2017:NPR

[3906] Rafik Hamza. A novel pseudo random sequence generator for image-cryptographic applications. *Journal of Information Security and Applications (JISA)*, 35(??):119–127, August 2017. CODEN ???? ISSN 2214-2126. URL http://www.sciencedirect.com/science/article/pii/S2214212617303174.

Herrero-Collantes:2017:QRN

[3907] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004:1–015004:48, January 2017. CODEN RMPHAT. ISSN 0034-6861 (print), 1538-4527 (electronic), 1539-0756. URL http://journals.aps.org/rmp/abstract/10.1103/RevModPhys.89.015004.

Kuhl:2017:HRV

[3908] M. E. Kuhl. History of random variate generation. In Ören et al. [4110], pages 231–242. ISBN ???? LCCN QA76.5 W78 1980.

Lampropoulos:2017:BLL

[3909] Leonidas Lampropoulos, Diane Gallois-Wong, Catalin Hritcu, John Hughes, Benjamin C. Pierce, and Li yao Xia. Beginner's luck: a language for property-based generators. *ACM SIGPLAN Notices*, 52(1):

114–129, January 2017. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

LEcuyer:2017:HRN

[3910] Pierre L'Ecuyer. History of random number generation. In *Proceedings of the Winter Simulation Conference*, pages 231–242. ????, ????, 2017.

Lenstra:2017:TPR

[3911] Arjen K. Lenstra and Benjamin Wesolowski. Trustworthy public randomness with sloth, unicorn, and trx. *International Journal of Applied Cryptography. IJACT*, 3(4):330–343, 2017. CODEN ???? ISSN 1753-0563 (print), 1753-0571 (electronic). URL `https://www.inderscienceonline.com//doi/pdf/10.1504/IJACT.2017.089354`.

Liu:2017:ESG

[3912] Chuanhai Liu, Ryan Martin, and Nick Syring. Efficient simulation from a gamma distribution with small shape parameter. *Computational Statistics*, 32(4):1767–1775, December 2017. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `https://link.springer.com/article/10.1007/s00180-016-0692-0`.

Monroe:2017:NPR

[3913] Don Monroe. News: Pure randomness extracted from two poor sources. *Communications of the ACM*, 60(1):13–15, January 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/1/211100/fulltext`.

Nordrum:2017:TRN

[3914] Amy Nordrum. A true random-number generator built from carbon nanotubes. *IEEE Spectrum*, ??(??):??, August 9, 2017. CODEN IEESAM. ISSN 0018-9235 (print), 1939-9340 (electronic). URL `http://spectrum.ieee.org/nanoclast/computing/hardware/a-true-random-number-generator-built-from-carbon-nanotubes-promises-better-security-for-flexible-electronics`.

Obratil:2017:ATR

[3915] L. Obratil. The automated testing of randomness with multiple statistical batteries. Master's thesis, Masaryk University, Brno, Czechia, 2017. URL `https://is.muni.cz/th/uepbs/`.

Pandian:2017:AAN

[3916] K. K. Soundra Pandian and K. C. Ray. An algorithm and architecture for non-recursive pseudorandom sequence generation using sequence

folding technique. *International Journal of Computers and Applications*, 39(1):45–56, 2017. CODEN IJCAFW. ISSN 1206-212X (print), 1925-7074 (electronic). URL `https://www.tandfonline.com/doi/full/10.1080/1206212X.2016.1262165`.

Pomeranz:2017:CSL

[3917] Irith Pomeranz. Computation of seeds for LFSR-based n-detection test generation. *ACM Transactions on Design Automation of Electronic Systems*, 22(2):29:1–29:??, March 2017. CODEN ATASFO. ISSN 1084-4309 (print), 1557-7309 (electronic).

Popov:2017:DTP

[3918] Serguei Popov. On a decentralized trustless pseudo-random number generation algorithm. *Journal of Mathematical Cryptology*, 11(1):37–43, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Sibidanov:2017:RSB

[3919] Alexei Sibidanov. A revision of the subtract-with-borrow random number generators. *Computer Physics Communications*, 221(??):299–303, December 2017. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0010465517302916`.

Sutar:2017:DPI

[3920] Soubhagya Sutar, Arnab Raha, Devadatta Kulkarni, Rajeev Shorey, Jeffrey Tew, and Vijay Raghunathan. D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation. *ACM Transactions on Embedded Computing Systems*, 17(1):1–31, December 2017. ISSN 1539-9087 (print), 1558-3465 (electronic).

Sys:2017:AON

[3921] Marek Sýs, Zdenek Říha, and Vashek Matyáš. Algorithm 970: Optimizing the NIST Statistical Test Suite and the Berlekamp–Massey algorithm. *ACM Transactions on Mathematical Software*, 43(3):27:1–27:11, January 2017. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

Thorup:2017:FPH

[3922] Mikkel Thorup. Fast and powerful hashing using tabulation. *Communications of the ACM*, 60(7):94–101, July 2017. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `http://cacm.acm.org/magazines/2017/7/218878/fulltext`.

Vigna:2017:FSM

[3923] Sebastiano Vigna. Further scramblings of Marsaglia's `xorshift` generators. *Journal of Computational and Applied Mathematics*, 315(??):175–181, May 1, 2017. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042716305301`.

Ye:2017:VCS

[3924] Katherine Q. Ye, Matthew Green, Naphat Sanguansin, Lennart Beringer, Adam Petcher, and Andrew W. Appel. Verified correctness and security of mbedTLS HMAC-DRBG. In ACM, editor, *Proceedings of CCS 17, October 30–November 3, 2017, Dallas, TX, USA*, pages 1–14. ACM Press, New York, NY 10036, USA, 2017. ISBN 1-4503-4946-3. LCCN ???? URL `http://www.cs.princeton.edu/~appel/papers/verified-hmac-drbg.pdf`.

Aletti:2018:GDR

[3925] Giacomo Aletti. Generation of discrete random variables in scalable frameworks. *Statistics & Probability Letters*, 132(??):99–106, January 2018. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-2103 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0167715217302900`.

Anderson:2018:IP

[3926] David F. Anderson, Timo O. Seppäläinen, and Benedek Valkó. *Introduction to Probability*. Cambridge mathematical textbooks. Cambridge University Press, Cambridge, UK, 2018. ISBN 1-108-41585-7 (hardcover). xv + 429 pp. LCCN QA273 .A5534 2018.

Antoniadis:2018:EDC

[3927] Karolos Antoniadis, Peva Blanchard, and Julien Stainer. The entropy of a distributed computation random number generation from memory interleaving. *Distributed Computing*, 31(5):389–417, October 2018. CODEN DICOEB. ISSN 0178-2770 (print), 1432-0452 (electronic). URL `https://link.springer.com/article/10.1007/s00446-017-0311-5`.

Arnas:2018:NFI

[3928] David Arnas and Daniele Mortari. Nonlinear function inversion using k-vector. *Applied Mathematics and Computation*, 320(??):754–768, March 1, 2018. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300317306987`.

Bernardini:2018:GES

[3929] Riccardo Bernardini and Roberto Rinaldo. Generalized Elias schemes for efficient harvesting of truly random bits. *International Journal of Information Security*, 17(1):67–81, February 2018. CODEN ???? ISSN 1615-5262 (print), 1615-5270 (electronic). URL `http://link.springer.com/article/10.1007/s10207-016-0358-5`.

Blackman:2018:SLP

[3930] David Blackman and Sebastiano Vigna. Scrambled linear pseudorandom number generators. *arXiv.org*, ??(??):??, May 3, 2018. URL `https://arxiv.org/abs/1805.01407`. See also Web site with source code [3931].

Blackman:2018:XXG

[3931] David Blackman and Sebastiano Vigna. xoshiro / xoroshiro generators and the PRNG shootout. Web site, 2018. URL `http://prng.di.unimi.it/`. See also research paper [3930]. The site includes implementations in C, C++, and Java.

Bradbury:2018:RSR

[3932] Jonathan D. Bradbury, Steven R. Carlough, Brian R. Prasky, and Eric M. Schwarz. Reproducible stochastic rounding for out of order processors. U.S. Patent US10209958B2, July 23, 2018. Patent granted 19 February 2019; expired (fee related).

Cai:2018:VHA

[3933] Ruizhe Cai, Ao Ren, Ning Liu, Caiwen Ding, Luhao Wang, Xuehai Qian, Massoud Pedram, and Yanzhi Wang. VIBNN: Hardware acceleration of Bayesian neural networks. *ACM SIGPLAN Notices*, 53(2):476–488, February 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Chang:2018:CSL

[3934] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong Wang. The cycle structure of LFSR with arbitrary characteristic polynomial over finite fields. *Cryptography and Communications*, 10(6): 1183–1202, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0273-2`.

Checkoway:2018:WDL

[3935] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. Where did I leave my

keys?: lessons from the Juniper Dual EC incident. *Communications of the ACM*, 61(11):148–155, November 2018. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL `https://cacm.acm.org/magazines/2018/11/232227/fulltext`.

Deng:2018:SFE

[3936] Lih-Yuan Deng, Jyh-Jen Horng Shiau, Henry Horng-Shing Lu, and Dale Bowman. Secure and Fast Encryption (SAFE) with classical random number generators. *ACM Transactions on Mathematical Software*, 44(4): 45:1–45:17, August 2018. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `https://dl.acm.org/citation.cfm?id=3212673`.

Ermakov:2018:RRQ

[3937] Sergej M. Ermakov and Svetlana N. Leora. Remarks on randomization of quasi-random numbers. *Monte Carlo Methods and Applications*, 24(2): 139–145, June 2018. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL `https://www.degruyter.com/view/j/mcma.2018.24.issue-2/mcma-2018-0012/mcma-2018-0012.xml`.

Ferreira:2018:WLS

[3938] L. S. Ferreira, L. N. Jorge, S. A. Leão, and A. A. Caparica. Wang–Landau sampling: Saving CPU time. *Journal of Computational Physics*, 358(??):130–134, April 1, 2018. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S002199911830007X`.

Gopalan:2018:PDF

[3939] Parikshit Gopalan, Daniel M. Kane, and Raghu Meka. Pseudorandomness via the discrete Fourier transform. *SIAM Journal on Computing*, 47 (6):2451–2487, ???? 2018. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).

Harase:2018:IBM

[3940] Shin Harase and Takamitsu Kimoto. Implementing 64-bit maximally equidistributed F_2-linear generators with Mersenne prime period. *ACM Transactions on Mathematical Software*, 44(3):30:1–30:11, April 2018. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `https://dl.acm.org/citation.cfm?id=3159444`.

Lin:2018:FCB

[3941] Zhiqiang Lin, Dingyi Pei, Dongdai Lin, and Xiaolei Zhang. Fast construction of binary ring FCSRs for hardware stream ciphers. *Designs,*

Codes, and Cryptography, 86(4):939–953, April 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0370-4`.

Lin:2018:RNG

[3942] Y. Lin, F. Wang, and B. Liu. Random number generators for large-scale parallel Monte Carlo simulations on FPGA. *Journal of Computational Physics*, 360(??):93–103, May 1, 2018. CODEN JCTPAH. ISSN 0021-9991 (print), 1090-2716 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0021999118300391`.

Liu:2018:SFS

[3943] Weihua Liu, Andrew Klapper, and Zhixiong Chen. Solving the FCSR synthesis problem for multi-sequences by lattice basis reduction. *Designs, Codes, and Cryptography*, 86(5):1023–1038, May 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0375-z`.

Merai:2018:PAS

[3944] László Mérai and Arne Winterhof. On the pseudorandomness of automatic sequences. *Cryptography and Communications*, 10(6):1013–1022, November 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0260-7`.

Mista:2018:BPQ

[3945] Agustín Mista, Alejandro Russo, and John Hughes. Branching processes for QuickCheck generators. *ACM SIGPLAN Notices*, 53(7):1–13, July 2018. CODEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic).

Mullner:2018:RSS

[3946] Clemens Müllner. The Rudin–Shapiro sequence and similar sequences are normal along squares. *Canadian Journal of Mathematics = Journal canadien de mathématiques*, 70(5):1096–??, October 2018. CODEN CJMAAB. ISSN 0008-414X (print), 1496-4279 (electronic).

Nguyen:2018:QMC

[3947] Nguyet Nguyen, Linlin Xu, and Giray Ökten. A quasi-Monte Carlo implementation of the ziggurat method. *Monte Carlo Methods and Applications*, 24(2):93–99, June 2018. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL

https://www.degruyter.com/view/j/mcma.2018.24.issue-2/mcma-2018-0008/mcma-2018-0008.xml.

Nir:2018:CPI

[3948] Y. Nir and A. Langley. ChaCha20 and Poly1305 for IETF protocols. Technical report, Check Point Software Technologies, Ltd. and Google, Inc., 5 Hasolelim St., Tel Aviv 6789735, Israel, 2018. URL https://datatracker.ietf.org/doc/html/rfc7539. RFC 7539.

Petrica:2018:FOC

[3949] Lucian Petrica. FPGA optimized cellular automaton random number generator. *Journal of Parallel and Distributed Computing*, 111 (??):251–259, January 2018. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731517301892.

Riesinger:2018:NSP

[3950] Christoph Riesinger, Tobias Neckel, and Florian Rupp. Non-standard pseudo random number generators revisited for GPUs. *Future Generation Computer Systems*, 82(??):482–492, May 2018. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL https://www.sciencedirect.com/science/article/pii/S0167739X16307993.

Sanders:2018:EPR

[3951] Peter Sanders, Sebastian Lamm, Lorenz Hübschle-Schneider, Emanuel Schrade, and Carsten Dachsbacher. Efficient parallel random sampling-vectorized, cache-efficient, and online. *ACM Transactions on Mathematical Software*, 44(3):29:1–29:14, April 2018. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL https://dl.acm.org/citation.cfm?id=3157734.

Sutar:2018:DPI

[3952] Soubhagya Sutar, Arnab Raha, Devadatta Kulkarni, Rajeev Shorey, Jeffrey Tew, and Vijay Raghunathan. D-PUF: an intrinsically reconfigurable DRAM PUF for device authentication and random number generation. *ACM Transactions on Embedded Computing Systems*, 17(1):17:1–17:??, January 2018. CODEN ???? ISSN 1539-9087 (print), 1558-3465 (electronic).

Tajvidi:2018:GAG

[3953] N. Tajvidi and B. A. Turlach. A general approach to generate random variates for multivariate copulae. *Australian & New Zealand Journal of*

Statistics, 60(1):140–155, March 2018. CODEN ???? ISSN 1369-1473 (print), 1467-842X (electronic).

Teng:2018:KPA

[3954] Sheng-Hua Teng. 2018 Knuth Prize is awarded to Johan Håstad. *ACM SIGACT News*, 49(3):78–79, September 2018. CODEN SIGNDM. ISSN 0163-5700 (print), 1943-5827 (electronic).

Turan:2018:RES

[3955] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, and Mike Boyle. Recommendation for the entropy sources used for random bit generation. NIST Special Publication 800-90B, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, USA, January 2018. URL `https://csrc.nist.gov/publications/detail/sp/800-90b/final`.

Viktorin:2018:MPR

[3956] Adam Viktorin, Roman Senkerik, Michal Pluhacek, and Tomas Kadavy. Modified progressive random walk with chaotic PRNG. *International Journal of Parallel, Emergent and Distributed Systems: IJPEDS*, 33(5): 450–459, 2018. CODEN ???? ISSN 1744-5760 (print), 1744-5779 (electronic).

Wang:2018:LBA

[3957] Li-Ping Wang and Daqing Wan. On lattice-based algebraic feedback shift registers synthesis for multisequences. *Cryptography and Communications*, 10(3):455–465, May 2018. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `http://link.springer.com/article/10.1007/s12095-017-0230-0`.

Xu:2018:SCM

[3958] Jun Xu, Santanu Sarkar, Lei Hu, Zhangjie Huang, and Liqiang Peng. Solving a class of modular polynomial equations and its relation to modular inversion hidden number problem and inversive congruential generator. *Designs, Codes, and Cryptography*, 86(9):1997–2033, September 2018. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-017-0435-4`.

Achiha:2019:GKW

[3959] Taku Achiha, Hiroshi Sugita, Kenta Tonohiro, and Yuto Yamamoto. Generation of k-wise independent random variables with small randomness. *Monte Carlo Methods and Applications*, 25(3):259–??, September 2019. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961

(electronic). URL https://www.degruyter.com/view/j/mcma.2019.25.issue-3/mcma-2019-2046/mcma-2019-2046.xml.

Alhadawi:2019:DPB

[3960] Hussam S. Alhadawi, Mohamad Fadli Zolkipli, Saba M. Ismail, and Dragan Lambić. Designing a pseudorandom bit generator based on LFSRs and a discrete chaotic map. *Cryptologia*, 43(3):190–211, 2019. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.tandfonline.com/doi/full/10.1080/01611194.2018.1548390.

Arnas:2019:RSU

[3961] D. Arnas, C. Leake, and D. Mortari. Random sampling using k-vector. *Computing in Science and Engineering*, 21(1):94–107, January/February 2019. CODEN CSENFA. ISSN 1521-9615 (print), 1558-366x (electronic).

Bernard:2019:PSM

[3962] Florent Bernard, Patrick Haddad, Viktor Fischer, and Jean Nicolai. From physical to stochastic modeling of a TERO-based TRNG. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):435–458, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9291-2; https://link.springer.com/content/pdf/10.1007/s00145-018-9291-2.pdf.

Biebl:2019:RBS

[3963] Michael Biebl et al. [RDRAND broken on some AMD CPUs]. Debian Bug Tracking System report, May 19, 2019. URL https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=929215.

Blanco:2019:AIP

[3964] Jesús Blanco, Andrés García, and Valentín Cañas. Analysis and improvements of the pseudorandom number generation in passive UHF-RFID tags. *Future Generation Computer Systems*, 99(??):115–123, October 2019. CODEN FGSEVI. ISSN 0167-739X (print), 1872-7115 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167739X18317849.

Chang:2019:BBS

[3965] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong Wang. On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials. *Designs, Codes, and Cryptography*, 87(5):1137–1160, May 2019. CODEN DCCREC. ISSN 0925-1022 (print),

1573-7586 (electronic). URL https://link.springer.com/article/10.1007/s10623-018-0509-y.

Ciglaric:2019:OLP

[3966] Tadej Ciglaric, Rok Cesnovar, and Erik Strumbelj. An OpenCL library for parallel random number generators. *The Journal of Supercomputing*, 75(7):3866–3881, July 2019. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic).

Datta:2019:CPF

[3967] Pratish Datta, Ratna Dutta, and Sourav Mukhopadhyay. Constrained pseudorandom functions for Turing machines revisited: How to achieve verifiability and key delegation. *Algorithmica*, 81(9):3245–3390, September 2019. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic).

Deon:2019:PTG

[3968] Aleksei F. Deon and Yulian A. Menyaev. Poisson twister generator by cumulative frequency technology. *Algorithms (Basel)*, 12(6), June 2019. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL https://www.mdpi.com/1999-4893/12/6/114.

Downey:2019:AR

[3969] Rod Downey and Denis R. Hirschfeldt. Algorithmic randomness. *Communications of the ACM*, 62(5):70–80, May 2019. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.birs.ca/cmo-workshops/2016/16w5072/files/; https://cacm.acm.org/magazines/2019/5/236411/fulltext.

Falcon:2019:CAG

[3970] Raúl M. Falcón, Víctor Álvarez, and Félix Gudiel. A computational algebraic geometry approach to analyze pseudo-random sequences based on Latin squares. *Advances in Computational Mathematics*, 45(4):1769–1792, August 2019. CODEN ACMHEX. ISSN 1019-7168 (print), 1572-9044 (electronic). URL https://link.springer.com/article/10.1007/s10444-018-9654-0.

Frank:2019:RWT

[3971] Buddy Frank. RNGs what are they, and are they random? CDC Gaming Reports, Inc. Web site, September 4, 2019. URL https://www.cdcgamingreports.com/rngs-what-are-they-and-are-they-random/.

Gorder:2019:RSN

[3972] Bjürn Görder and Michael Kolonko. Ranking and selection: a new sequential Bayesian procedure for use with common random numbers. *ACM Transactions on Modeling and Computer Simulation*, 29(1):2:1–2:24, February 2019. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

Guidi:2019:FOS

[3973] Federico Amadio Guidi, Sofia Lindqvist, and Giacomo Micheli. Full orbit sequences in affine spaces via fractional jumps and pseudorandom number generation. *Mathematics of Computation*, 88(318):2005–2025, April 2019. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL https://www.ams.org/journals/mcom/2019-88-318/S0025-5718-2018-03400-7; https://www.ams.org/journals/mcom/2019-88-318/S0025-5718-2018-03400-7/S0025-5718-2018-03400-7.pdf; https://www.ams.org/mathscinet/search/authors.html?authorName=Amadio%20Guidi%2C%20Federico; https://www.ams.org/mathscinet/search/authors.html?mrauthid=1078793; https://www.ams.org/mathscinet/search/authors.html?mrauthid=1177141.

Impagliazzo:2019:PS

[3974] Russell Impagliazzo, Raghu Meka, and David Zuckerman. Pseudorandomness from shrinkage. *Journal of the ACM*, 66(2):11:1–11:??, April 2019. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/ft_gateway.cfm?id=3230630.

Intel:2019:IAM

[3975] Intel. *Intel Architecture Memory Encryption Technologies Specification*. Intel Corporation, ????, 336907-002us (revision 1.2) edition, April 2019. URL https://software.intel.com/sites/default/files/managed/a5/16/Multi-Key-Total-Memory-Encryption-Spec.pdf.

Kim:2019:GBA

[3976] HyungGyoon Kim, Hyungmin Cho, and Changwoo Pyo. GPU-based acceleration of the Linear Complexity Test for random number generator testing. *Journal of Parallel and Distributed Computing*, 128(??):115–125, June 2019. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519300784.

Kissel:2019:KRC

[3977] Zachary A. Kissel. Key regression from constrained pseudorandom functions. *Information Processing Letters*, 147(??):10–13, July 2019. CODEN

IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0020019019300493`.

Lemire:2019:FRI

[3978] Daniel Lemire. Fast random integer generation in an interval. *ACM Transactions on Modeling and Computer Simulation*, 29(1):3:1–3:12, February 2019. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). See replication report [3983].

Lemire:2019:XXX

[3979] Daniel Lemire and Melissa E. O'Neill. Xorshift1024*, xorshift1024+, xorshift128+ and xoroshiro128+ fail statistical tests for linearity. *Journal of Computational and Applied Mathematics*, 350(??):139–142, April 2019. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042718306265`.

Liu:2019:LFP

[3980] Huaning Liu. Large families of pseudorandom binary lattices by using the multiplicative inverse modulo P. *International Journal of Number Theory*, 15(3):527–546, April 2019. ISSN 1793-0421 (print), 1793-7310 (electronic). URL `https://www.worldscientific.com/doi/10.1142/S1793042119500271`.

Martirosyan:2019:STM

[3981] Narek Martirosyan, Konstantin Savvidy, and George Savvidy. Spectral test of the MIXMAX random number generators. *Chaos, Solitons & Fractals*, 118:242–248, January 2019. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).

Poudel:2019:MTU

[3982] Prawar Poudel, Biswajit Ray, and Aleksandar Milenkovic. Microcontroller TRNGs using perturbed states of NOR flash memory cells. *IEEE Transactions on Computers*, 68(2):307–313, ???? 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic). URL `https://ieeexplore.ieee.org/document/8443106/`.

Quaglia:2019:RCR

[3983] Francesco Quaglia. Replicated computational results (RCR) report for "Fast Random Integer Generation in an Interval". *ACM Transactions on Modeling and Computer Simulation*, 29(1):4:1–4:3, February 2019. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). See [3978].

SoltaniPanah:2019:CDG

[3984] A. Soltani Panah, A. Yavari, R. van Schyndel, D. Georgakopoulos, and X. Yi. Context-driven granular disclosure control for Internet of Things applications. *IEEE Transactions on Big Data*, 5(3):408–422, September 2019. ISSN 2332-7790.

Steele:2019:UBP

[3985] Guy L. Steele Jr. and Jean-Baptiste Tristan. Using butterfly-patterned partial sums to draw from discrete distributions. *ACM Transactions on Parallel Computing (TOPC)*, 6(4):22:1–22:??, November 2019. CODEN ???? ISSN 2329-4949 (print), 2329-4957 (electronic).

Ueno:2019:TBP

[3986] R. Ueno, M. Suzuki, and N. Homma. Tackling biased PUFs through biased masking: a debiasing method for efficient fuzzy extractor. *IEEE Transactions on Computers*, 68(7):1091–1104, July 2019. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Viola:2019:CEP

[3987] Emanuele Viola. Constant-error pseudorandomness proofs from hardness require majority. *ACM Transactions on Computation Theory*, 11(4): 19:1–19:??, September 2019. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3322815`.

Xu:2019:NPF

[3988] Xiaofang Xu, Chunlei Li, and Xiangyong Zeng. Nonsingular polynomials from feedback shift registers. *International Journal of Foundations of Computer Science (IJFCS)*, 30(3):469–487, 2019. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Zhang:2019:REU

[3989] Jun Zhang, Rui Hou, Wei Song, Sally A. Mckee, Zhen Jia, Chen Zheng, Mingyu Chen, Lixin Zhang, and Dan Meng. RAGuard: an efficient and user-transparent hardware mechanism against ROP attacks. *ACM Transactions on Architecture and Code Optimization*, 15(4):50:1–50:??, January 2019. CODEN ???? ISSN 1544-3566 (print), 1544-3973 (electronic). URL `https://dl.acm.org/ft_gateway.cfm?id=3280852`.

Anonymous:2020:X

[3990] Anonymous. Xorshift. Web site., 2020. URL `https://en.wikipedia.org/wiki/Xorshift`. This article discusses Marsaglia's Xorshift family

of generators, including 32-bit, 64-bit, and 128-bit variants, plus xorwow, xorshift+, xoshiro, and xoroshiro, with comments about which common test suites they pass or fail. Lua 5.4 changed from the previous default of C's rand() or random() to a new one based on xoshiro256** (256-bit state, 32- or 64-bit result). The period of xoshiro256** is 2**256 - 1 (about 10**77). See [3930, 3931].

Ayubi:2020:DCG

[3991] Peyman Ayubi, Saeed Setayeshi, and Amir Masoud Rahmani. Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application. *Journal of Information Security and Applications (JISA)*, 52(??):??, June 2020. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212619304958`.

Barani:2020:NPR

[3992] Milad Jafari Barani, Peyman Ayubi, Milad Yousefi Valandar, and Behzad Yosefnezhad Irani. A new pseudo random number generator based on generalized Newton complex map with dynamic key. *Journal of Information Security and Applications (JISA)*, 53(??):??, August 2020. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212619309512`.

Goualard:2020:GRF

[3993] Frédéric Goualard. Generating random floating-point numbers by dividing integers: a case study. In Krzhizhanovskaya et al. [4295], pages 15–28. ISBN 3-030-50416-6, 3-030-50417-4 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/book/10.1007/978-3-030-50417-5`.

Gurjar:2020:PBO

[3994] Rohit Gurjar and Ben Lee Volk. Pseudorandom bits for oblivious branching programs. *ACM Transactions on Computation Theory*, 12(2):8:1–8:12, May 2020. CODEN ???? ISSN 1942-3454 (print), 1942-3462 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3378663`.

Hurley-Smith:2020:QLC

[3995] Darren Hurley-Smith and Julio Hernandez-Castro. Quantum leap and crash: Searching and finding bias in quantum random number generators. *ACM Transactions on Privacy and Security (TOPS)*, 23(3):16:1–16:25, July 2020. CODEN ???? ISSN 2471-2566 (print), 2471-2574 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3398726`.

James:2020:RHQ

[3996] Frederick James and Lorenzo Moneta. Review of high-quality random number generators. *Computing and Software for Big Science*, 4 (1):2:1–2:12, December 2020. CODEN ???? ISSN 2510-2036 (print), 2510-2044 (electronic). URL `https://link.springer.com/article/10.1007/s41781-019-0034-3`.

Jeong:2020:PRN

[3997] Young-Seob Jeong, Kyo-Joong Oh, and Ho-Jin Choi. Pseudo-random number generation using LSTMs. *The Journal of Supercomputing*, 76 (10):8324–8342, October 2020. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-020-03229-7`.

LEcuyer:2020:SAM

[3998] Pierre L'Ecuyer, Paul Wambergue, and Erwan Bourceret. Spectral analysis of the MIXMAX random number generators. *INFORMS Journal on Computing*, 32(1):135–144, Winter 2020. CODEN ???? ISSN 1091-9856 (print), 1526-5528 (electronic). URL `/doi/pdf/10.1287/ijoc.2018.0878`.

Li:2020:NAM

[3999] Yubo Li, Zhichao Yang, Kangquan Li, and Longjiang Qu. A new algorithm on the minimal rational fraction representation of feedback with carry shift registers. *Designs, Codes, and Cryptography*, 88(3): 533–552, March 2020. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-019-00695-w`.

Lorek:2020:TPG

[4000] Paweł Lorek, Grzegorz Loś, Karol Gotfryd, and Filip Zagórski. On testing pseudorandom generators via statistical tests based on the arcsine law. *Journal of Computational and Applied Mathematics*, 380(??): Article 112968, December 15, 2020. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042720302594`.

Merai:2020:DSS

[4001] László Mérai and Igor E. Shparlinski. Distribution of short subsequences of inversive congruential pseudorandom numbers modulo 2^t. *Mathematics of Computation*, 89(322):911–922, April 2020. CODEN MCMPAF.

ISSN 0025-5718 (print), 1088-6842 (electronic). URL https://www.ams.org/AMSMathViewer; https://www.ams.org/journals/mcom/2020-89-322/S0025-5718-2019-03467-1; https://www.ams.org/journals/mcom/2020-89-322/S0025-5718-2019-03467-1/S0025-5718-2019-03467-1.pdf; https://www.ams.org/mathscinet/search/authors.html?authorName=Merai%2C%20Laszlo; https://www.ams.org/mathscinet/search/authors.html?mrauthid=192194.

Mikaitis:2020:SRA

[4002] Mantas Mikaitis. Stochastic rounding: Algorithms and hardware accelerator. *arXiv.org*, ??(??):1–6, June 29, 2020. URL https://arxiv.org/abs/2001.01501#.

Stpiczynski:2020:ALB

[4003] Przemysław Stpiczyński. Algorithmic and language-based optimization of Marsa-LFIB4 pseudorandom number generator using OpenMP, OpenACC and CUDA. *Journal of Parallel and Distributed Computing*, 137(??):238–245, March 2020. CODEN JPDCER. ISSN 0743-7315 (print), 1096-0848 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0743731519304885.

Vigna:2020:POR

[4004] Sebastiano Vigna. On the probability of overlap of random subsequences of pseudorandom number generators. *Information Processing Letters*, 158(??):Article 105939, June 2020. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0020019020300260.

AlmarazLuengo:2021:RSR

[4005] Elena Almaraz Luengo and Luis Javier García Villalba. Recommendations on statistical randomness test batteries for cryptographic purposes. *ACM Computing Surveys*, 54(4):80:1–80:34, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL https://dl.acm.org/doi/10.1145/3447773.

Arroyo:2021:ARI

[4006] Daisy Arroyo and Xavier Emery. Algorithm 1013: an R implementation of a continuous spectral algorithm for simulating vector Gaussian random fields in Euclidean spaces. *ACM Transactions on Mathematical Software*, 47(1):8:1–8:25, January 2021. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL https://dl.acm.org/doi/10.1145/3421316.

Blackman:2021:SLP

[4007] David Blackman and Sebastiano Vigna. Scrambled linear pseudorandom number generators. *ACM Transactions on Mathematical Software*, 47(4):36:1–36:32, December 2021. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `https://dl.acm.org/doi/10.1145/3460772`.

Deng:2021:ERC

[4008] L.-Y. Deng, D. Bowman, C.-C. Yang, and H. H.-S. Lu. Extending RC4 to construct secure random number generators. In Cristina Ruiz Martin, Maria Julia Blas, and Alonso Inostrosa Psijas, editors, *Proceedings of the 2021 Annual Modeling and Simulation Conference (ANNSIM '21), July 19–22, 2021, Virtual Event*, pages 1–12. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2021. ISBN 1-56555-375-6. LCCN QA76.9.C65 .I578 2021. URL `https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9552088`.

Even:2021:SRA

[4009] Guy Even, Reut Levi, Moti Medina, and Adi Rosén. Sublinear random access generators for preferential attachment graphs. *ACM Transactions on Algorithms*, 17(4):28:1–28:26, October 2021. CODEN ???? ISSN 1549-6325 (print), 1549-6333 (electronic). URL `https://dl.acm.org/doi/10.1145/3464958`.

Hofert:2021:RNG

[4010] Marius Hofert. Random number generators produce collisions: Why, how many and more. *The American Statistician*, 75(4):394–402, 2021. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL `http://www.tandfonline.com/doi/full/10.1080/00031305.2020.1782261`.

Hughes:2021:BEM

[4011] James Prescott Hughes. *BadRandom: the effect and mitigations for low entropy random numbers in TLS*. Ph.D. dissertation, University of California, Santa Cruz, Santa Cruz, CA, 2021. xv + 101 pp. URL `https://escholarship.org/uc/item/9528885m`.

Kietzmann:2021:GPN

[4012] Peter Kietzmann, Thomas C. Schmidt, and Matthias Wählisch. A guideline on pseudorandom number generation (PRNG) in the IoT. *ACM Computing Surveys*, 54(6):112:1–112:38, July 2021. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3453159`.

Kim:2021:MPU

[4013] Kyungduk Kim, Stefan Bittner, Yongquan Zeng, Stefano Guazzotti, Ortwin Hess, Qi Jie Wang, and Hui Cao. Massively parallel ultrafast random bit generation with a chip-scale laser. *Science*, 371(6532):948–952, February 2021. CODEN SCIEAS. ISSN 0036-8075 (print), 1095-9203 (electronic).

Lakshmanan:2021:CRN

[4014] Ravie Lakshmanan. A critical random number generator flaw affects billions of IoT devices. The Hacker News Web site., August 9, 2021. URL `https://thehackernews.com/2021/08/a-critical-random-number-generator-flaw.html`.

Peetermans:2021:DAC

[4015] Adriaan Peetermans, Vladimir Rozić, and Ingrid Verbauwhede. Design and analysis of configurable ring oscillators for true random number generation based on coherent sampling. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 14(2):7:1–7:20, July 2021. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL `https://dl.acm.org/doi/10.1145/3433166`.

Petro:2021:YDI

[4016] Dan Petro and Allan Cecil. You're doing IoT RNG. BishopFox Labs Web site., August 5, 2021. URL `https://labs.bishopfox.com/tech-blog/youre-doing-iot-rng`.

Qu:2021:RVG

[4017] Yan Qu, Angelos Dassios, and Hongbiao Zhao. Random variate generation for exponential and gamma tilted stable distributions. *ACM Transactions on Modeling and Computer Simulation*, 31(4):19:1–19:21, October 2021. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `https://dl.acm.org/doi/10.1145/3449357`.

Ryabko:2021:PRG

[4018] Boris Ryabko. A pseudo-random generator whose output is a normal sequence. *International Journal of Foundations of Computer Science (IJFCS)*, 32(08):981–989, December 2021. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic). URL `https://www.worldscientific.com/doi/10.1142/S0129054121500325`.

Shoup:2021:NLD

[4019] Victor Shoup. NTL: a library for doing number theory. Web site, 2021.

Steele:2021:PLB

[4020] Guy L. Steele Jr. and Sebastiano Vigna. LXM: better splittable pseudorandom number generators (and almost as fast). *Proceedings of the ACM on Programming Languages (PACMPL)*, 5(OOPSLA):148:1–148:31, October 2021. CODEN ???? ISSN 2475-1421 (electronic). URL https://dl.acm.org/doi/10.1145/3485525.

Trejo:2021:NQR

[4021] José Manuel Agüero Trejo and Cristian S. Calude. A new quantum random number generator certified by value indefiniteness. *Theoretical Computer Science*, 862(??):3–13, March 16, 2021. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0304397520304679.

Ullah:2021:ESS

[4022] Ikram Ullah, Naveed Ahmed Azam, and Umar Hayat. Efficient and secure substitution box and random number generators over Mordell elliptic curves. *Journal of Information Security and Applications (JISA)*, 56(??):??, February 2021. CODEN ???? ISSN 2214-2126. URL http://www.sciencedirect.com/science/article/pii/S2214212620307845.

Zhandry:2021:HCQ

[4023] Mark Zhandry. How to construct quantum random functions. *Journal of the ACM*, 68(5):33:1–33:43, October 2021. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL https://dl.acm.org/doi/10.1145/3450745.

AlmarazLuengo:2022:NAA

[4024] Elena Almaraz Luengo, Marcos Brian Leiva Cerna, Luis Javier García Villalba, and Julio Hernandez-Castro. A new approach to analyze the independence of statistical tests of randomness. *Applied Mathematics and Computation*, 426(??):1–16, August 1, 2022. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0096300322002004.

Chen:2022:LCL

[4025] Shilin Chen, Shang Ma, Zhuo Qin, Bixin Zhu, Ziqian Xiao, and Meiqing Liu. A low complexity and long period digital random sequence generator based on residue number system and permutation polynomial. *IEEE Transactions on Computers*, 71(11):3008–3017, November 2022. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Cheon:2022:ACD

[4026] Jung Hee Cheon, Wonhee Cho, Jeong Han Kim, and Jiseung Kim. Adventures in crypto dark matter: attacks, fixes and analysis for weak pseudorandom functions. *Designs, Codes, and Cryptography*, 90(8): 1735–1760, August 2022. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-022-01071-x`.

DiMauro:2022:DIN

[4027] Juan Di Mauro, Eduardo Salazar, and Hugo D. Scolnik. Design and implementation of a novel cryptographically secure pseudorandom number generator. *Journal of Cryptographic Engineering*, 12(3):255–265, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-022-00297-8`.

Donenfeld:2022:RNG

[4028] Jason A. Donenfeld. Random number generator enhancements for Linux 5.17 and 5.18. Web document, March 18, 2022. URL `https://www.zx2c4.com/projects/linux-rng-5.17-5.18/`.

Doron:2022:NOP

[4029] Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Nearly optimal pseudorandomness from hardness. *Journal of the ACM*, 69 (6):43:1–43:??, December 2022. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic). URL `https://dl.acm.org/doi/10.1145/3555307`.

Du:2022:IES

[4030] Yusong Du, Baoying Fan, and Baodian Wei. An improved exact sampling algorithm for the standard normal distribution. *Computational Statistics*, 37(2):721–737, April 2022. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `https://link.springer.com/article/10.1007/s00180-021-01136-w`. See [3867].

Ernstsson:2022:DPP

[4031] August Ernstsson, Nicolas Vandenbergen, and Christoph Kessler. A deterministic portable parallel pseudo-random number generator for pattern-based programming of heterogeneous parallel systems. *International Journal of Parallel Programming*, 50(3-4):319–340, August 2022. CODEN IJPPE5. ISSN 0885-7458 (print), 1573-7640 (electronic). URL `https://link.springer.com/article/10.1007/s10766-022-00726-5`.

Goualard:2022:DRF

[4032] Frédéric Goualard. Drawing random floating-point numbers from an interval. *ACM Transactions on Modeling and Computer Simulation*, 32(3): 16:1–16:24, July 2022. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic). URL `https://dl.acm.org/doi/10.1145/3503512`.

Gutierrez:2022:ALC

[4033] Jaime Gutierrez. Attacking the linear congruential generator on elliptic curves via lattice techniques. *Cryptography and Communications*, 14(3):505–525, May 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-021-00535-6`.

Haramoto:2022:UPX

[4034] Hiroshi Haramoto, Makoto Matsumoto, and Mutsuo Saito. Unveiling patterns in xorshift128+ pseudorandom number generators. *Journal of Computational and Applied Mathematics*, 402(??):??, March 1, 2022. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0377042721004131`.

Hughes:2022:CIT

[4035] James P. Hughes and Whitfield Diffie. The challenges of IoT, TLS, and random number generators in the real world: Bad random numbers are still with us and are proliferating in modern systems. *ACM Queue: Tomorrow's Computing Today*, 20(3):18–40, May 2022. CODEN AQCUAE. ISSN 1542-7730 (print), 1542-7749 (electronic). URL `https://dl.acm.org/doi/10.1145/3546933`.

Lim:2022:AAP

[4036] Zhao Ging Lim, Chen-Tuo Liao, and Yi-Ching Yao. Asymptotic analysis of Peres' algorithm for random number generation. *Probability in the Engineering and Informational Sciences*, 36(2):341–356, April 2022. CODEN ???? ISSN 0269-9648 (print), 1469-8951 (electronic). URL `https://www.cambridge.org/core/journals/probability-in-the-engineering-and-informational-sciences/article/asymptotic-analysis-of-peres-algorithm-for-random-number-generation/3B02FFEA433E0788CFD05B30974E83D3`. See Yuval Peres, *Iterating von Neumann's Procedure for Extracting Random Bits*, Annals of Statistics **20**(1) 590–597, March 1992, doi:10.1214/aos/1176348543.

Merai:2022:PSD

[4037] László Mérai and Arne Winterhof. Pseudorandom sequences derived from automatic sequences. *Cryptography and Communications*, 14(4): 783–815, July 2022. CODEN ???? ISSN 1936-2447 (print), 1936-2455 (electronic). URL `https://link.springer.com/article/10.1007/s12095-022-00556-9`.

Muller:2022:DAL

[4038] Stephan Müller, Sebastian Mayer, Caroline Holz auf der Heide, and Andreas Hohenegger. Documentation and analysis of the Linux random number generator. Report, Federal Office for Information Security, Post Box 20 03 63, D-53133 Bonn, Germany, November 25, 2022. 103 pp. URL `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/LinuxRNG/LinuxRNG_EN_V5_2.pdf`. Version 5.2.

Saarinen:2022:DRV

[4039] Markku-Juhani O. Saarinen, G. Richard Newell, and Ben Marshall. Development of the RISC-V entropy source interface. *Journal of Cryptographic Engineering*, 12(4):371–386, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-021-00275-6`.

Serrano:2022:UPC

[4040] Ronaldo Serrano, Ckristian Duran, Marco Sarmiento, Tuan-Kiet Dang, Trong-Thuc Hoang, and Cong-Kha Pham. A unified PUF and crypto core exploiting the metastability in latches. *Future Internet*, 14(10):298, October 17, 2022. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/14/10/298`.

Sharma:2022:PRB

[4041] Madhu Sharma, Ranjeet Kumar Ranjan, and Vishal Bharti. A pseudorandom bit generator based on chaotic maps enhanced with a bit-XOR operation. *Journal of Information Security and Applications (JISA)*, 69 (??):??, September 2022. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212622001521`.

Steele:2022:CES

[4042] Guy L. Steele, Jr. and Sebastiano Vigna. Computationally easy, spectrally good multipliers for congruential pseudorandom number generators. *Software — Practice and Experience*, 52(2):443–458, February 2022. CODEN SPEXBL. ISSN 0038-0644 (print), 1097-024X (electronic).

Sulewski:2022:TMC

[4043] Piotr Sulewski. Two methods of conjoint summands of generating bivariate and trivariate normal pseudo-random numbers. *Journal of Statistical Computation and Simulation*, 92(8):1714–1739, 2022. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.

Sys:2022:BDH

[4044] Marek Sýs, Lubomír Obrátil, Vashek Matyás, and Dusan Klinec. A bad day to die hard: Correcting the Dieharder Battery. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-021-09414-y`.

Xiaohui:2022:AGR

[4045] Zhou Xiaohui and Gu Guiding. An algorithm of generating random number by wavelet denoising method and its application. *Computational Statistics*, 37(1):107–124, March 2022. CODEN CSTAEB. ISSN 0943-4062 (print), 1613-9658 (electronic). URL `https://link.springer.com/article/10.1007/s00180-021-01117-z`.

Zheng:2022:BCS

[4046] Jun Zheng and Hanping Hu. Bit cyclic shift method to reinforce digital chaotic maps and its application in pseudorandom number generator. *Applied Mathematics and Computation*, 420(??):Article 126788, May 1, 2022. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S0096300321008705`.

AlmarazLuengo:2023:GPR

[4047] Elena Almaraz Luengo. Gamma pseudo random number generators. *ACM Computing Surveys*, 55(4):85:1–85:33, May 2023. CODEN CMSVAN. ISSN 0360-0300 (print), 1557-7341 (electronic). URL `https://dl.acm.org/doi/10.1145/3527157`.

Chatterjee:2023:FFT

[4048] Swetaki Chatterjee, Nikhil Rangarajan, Satwik Patnaik, Dinesh Rajasekharan, Ozgur Sinanoglu, and Yogesh Singh Chauhan. FerroCoin: Ferroelectric tunnel junction-based true random number generator. *IEEE Transactions on Emerging Topics in Computing*, 11(2):541–547, April/June 2023. ISSN 2168-6750 (print), 2376-4562 (electronic).

Cicek:2023:NRW

[4049] Ihsan Cicek and Ahmad Al Khas. A new read-write collision-based SRAM PUF implemented on Xilinx FPGAs. *Journal of Cryptographic Engineering*, 13(1):19–36, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-021-00281-8`.

Dupin:2023:AIR

[4050] Aurélien Dupin, Pierrick Méaux, and Mélissa Rossi. On the algebraic immunity-resiliency trade-off, implications for Goldreich's pseudorandom generator. *Designs, Codes, and Cryptography*, 91(9):3035–3079, September 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01220-w`.

Giles:2023:AIC

[4051] Michael Giles and Oliver Sheridan-Methven. Approximating inverse cumulative distribution functions to produce approximate random variables. *ACM Transactions on Mathematical Software*, 49(3):26:1–26:??, September 2023. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL `https://dl.acm.org/doi/10.1145/3604935`.

Gulic:2023:EMO

[4052] Marko Gulić and Martina Zuskin. Enhancing metaheuristic optimization: a novel nature-inspired hybrid approach incorporating selected pseudorandom number generators. *Algorithms (Basel)*, 16(9), September 2023. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/16/9/413`.

Hanlon:2023:FHP

[4053] James Hanlon and Stephen Felix. A fast hardware pseudorandom number generator based on `xoroshiro128`. *IEEE Transactions on Computers*, 72(5):1518–1524, May 2023. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Koshiba:2023:TPS

[4054] Takeshi Koshiba, Behrouz Zolfaghari, and Khodakhast Bibak. A tradeoff paradigm shift in cryptographically-secure pseudorandom number generation based on discrete logarithm. *Journal of Information Security and Applications (JISA)*, 73(??):??, March 2023. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212623000157`.

Kuyu:2023:CIE

[4055] Yigit Çagatay Kuyu and Fahri Vatansever. A conceptual investigation of the effect of random numbers over the performance of metaheuristic algorithms. *The Journal of Supercomputing*, 79(13):13971–14038, September 2023. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-023-05111-8`.

Lu:2023:HET

[4056] Yingchun Lu, Yun Yang, Rong Hu, Huaguo Liang, Maoxiang Yi, Huang Zhengfeng, Yuanming Ma, Tian Chen, and Liang Yao. High-efficiency TRNG design based on multi-bit dual-ring oscillator. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 16(4):64:1–64:??, December 2023. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic). URL `https://dl.acm.org/doi/10.1145/3624991`.

Luengo:2023:STS

[4057] Elena Almaraz Luengo, Bittor Alaña Olivares, Luis Javier García Villalba, Julio Hernandez-Castro, and Darren Hurley-Smith. StringENT test suite: ENT battery revisited for efficient P value computation. *Journal of Cryptographic Engineering*, 13(2):235–249, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00313-5`.

McCurdy:2023:SNS

[4058] Jonathan McCurdy. *SAFE-NET: Secure and Fast Encryption Using Network of Pseudo-Random Number Generators*. Ph.D. dissertation, The University of Memphis, Memphis, TN, USA, August 2023. 79 pp. URL `https://digitalcommons.memphis.edu/cgi/viewcontent.cgi?article=4125&context=etd`.

Pandit:2023:LBQ

[4059] Anupama Arjun Pandit, Atul Kumar, and Arun Mishra. LWR-based quantum-safe pseudo-random number generator. *Journal of Information Security and Applications (JISA)*, 73(??):??, March 2023. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212623000169`.

Pratihar:2023:BSF

[4060] Kuheli Pratihar, Urbi Chatterjee, Manaar Alam, Rajat Subhra Chakraborty, and Debdeep Mukhopadhyay. Birds of the same feather flock together: a dual-mode circuit candidate for strong PUF-TRNG

functionalities. *IEEE Transactions on Computers*, 72(6):1636–1651, June 2023. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

Saini:2023:CNF

[4061] A. Saini, A. Tsokanos, and R. Kirner. CryptoQNRG: a new framework for evaluation of cryptographic strength in quantum and pseudorandom number generation for key-scheduling algorithms. *The Journal of Supercomputing*, 79(11):12219–12237, July 2023. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-023-05115-4`.

Shparlinski:2023:FPS

[4062] Igor E. Shparlinski. Fixed points of the subset sum pseudorandom number generators. *Designs, Codes, and Cryptography*, 91(7):2473–2479, July 2023. CODEN DCCREC. ISSN 0925-1022 (print), 1573-7586 (electronic). URL `https://link.springer.com/article/10.1007/s10623-023-01209-5`.

Yao:2023:LOT

[4063] Liang Yao, Huaguo Liang, and Yingchun Lu. Low-overhead TRNG based on MUX for cryptographic protection using multiphase sampling. *The Journal of Supercomputing*, 79(15):17170–17186, October 2023. CODEN JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL `https://link.springer.com/article/10.1007/s11227-023-05349-2`.

Alawida:2024:ELC

[4064] Moatsum Alawida. Enhancing logistic chaotic map for improved cryptographic security in random number generation. *Journal of Information Security and Applications (JISA)*, 80(??):??, February 2024. CODEN ???? ISSN 2214-2126. URL `http://www.sciencedirect.com/science/article/pii/S2214212623002697`.

Baran:2024:AIP

[4065] Klaudia Baran, Mateusz Sitko, and Lukasz Madej. Analysis of the influence of a pseudo-random number generator type on the kinetics of the cellular automata recrystallization model. *Journal of Computational Science*, 75(??):??, January 2024. CODEN ???? ISSN 1877-7503 (print), 1877-7511 (electronic). URL `http://www.sciencedirect.com/science/article/pii/S1877750323002533`.

Chen:2024:NND

[4066] Yucong Chen, Yanshan Tian, Rui Zhou, Diego Martínez Castro, Deke Guo, and Qingguo Zhou. NDSTRNG: Non-deterministic sampling-based

true random number generator on SoC FPGA systems. *IEEE Transactions on Computers*, 73(5):1313–1326, May 2024. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (electronic).

deCurto:2024:ECS

[4067] J. de Curtò, I. de Zarzà, Juan-Carlos Cano, and Carlos T. Calafate. Enhancing communication security in drones using QRNG in frequency hopping spread spectrum. *Future Internet*, 16(11):412, November 8, 2024. CODEN ???? ISSN 1999-5903. URL `https://www.mdpi.com/1999-5903/16/11/412`.

Devroye:2024:RVG

[4068] Luc Devroye and John P. Nolan. Random variate generation for the first hit of a ball for the symmetric stable process in $\mathbf{R}^d$. *Journal of Statistical Theory and Practice*, 18(1):??, March 2024. CODEN ???? ISSN 1559-8608 (print), 1559-8616 (electronic). URL `https://link.springer.com/article/10.1007/s42519-023-00364-1`.

Dziala:2024:CWG

[4069] Tomasz R. Dziala. Collatz–Weyl generators: High quality and high throughput parameterized pseudorandom number generators. *[submitted to [unspecified] Elsevier journal]*, ??(??):1, January 29, 2024. URL `https://arxiv.org/pdf/2312.17043`.

Hoza:2024:LIN

[4070] William M. Hoza, Edward Pyne, and Salil Vadhan. Limitations of the Impagliazzo–Nisan–Wigderson pseudorandom generator against permutation branching programs. *Algorithmica*, 86(10):3153–3185, October 2024. CODEN ALGOEJ. ISSN 0178-4617 (print), 1432-0541 (electronic). URL `https://link.springer.com/article/10.1007/s00453-024-01251-2`.

Kannan:2024:EPS

[4071] Shiva Kumar Kannan and Urmila Diwekar. An enhanced particle swarm optimization (PSO) algorithm employing quasi-random numbers. *Algorithms (Basel)*, 17(5), May 2024. CODEN ALGOCH. ISSN 1999-4893 (electronic). URL `https://www.mdpi.com/1999-4893/17/5/195`.

kumar:2024:QRN

[4072] Vaishnavi kumar and Padmapriya Pravinkumar. Quantum random number generator on IBM QX. *Journal of Cryptographic Engineering*, 14(2):253–259, June 2024. CODEN ???? ISSN 2190-8508 (print),

2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00341-1.

Li:2024:PER

[4073] Shuaiyu Li, Yunpei Wu, and Yuzhong Cheng. Parameter estimation and random number generation for student Lévy processes. *Computational Statistics & Data Analysis*, 194(??):??, June 2024. CODEN CSDADW. ISSN 0167-9473 (print), 1872-7352 (electronic). URL http://www.sciencedirect.com/science/article/pii/S0167947324000173.

Lubicz:2024:ECO

[4074] David Lubicz and Viktor Fischer. Entropy computation for oscillator-based physical random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09494-6.

Merai:2024:DRM

[4075] László Mérai and Igor E. Shparlinski. Distribution of recursive matrix pseudorandom number generator modulo prime powers. *Mathematics of Computation*, 93(347):1355–1370, July 2024. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL https://www.ams.org/journals/mcom/2024-93-347/S0025-5718-2023-03895-9.

Sasmal:2024:AMD

[4076] Mrinmay Sasmal, Tresa Joseph, and Bindiya T. S. Approximate multiplier design with LFSR-based stochastic sequence generators for edge AI. *IEEE Computer Architecture Letters*, 23(1):91–94, 2024. ISSN 1556-6056 (print), 1556-6064 (electronic).

Soler:2024:PPK

[4077] David Soler, Carlos Dafonte, Manuel Fernández-Veiga, Ana Fernández Vilas, and Francisco J. Nóvoa. A privacy-preserving key transmission protocol to distribute QRNG keys using zk-SNARKs. *Computer Networks (Amsterdam, Netherlands: 1999)*, 242(??):??, April 2024. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (electronic). URL http://www.sciencedirect.com/science/article/pii/S1389128624000914.

Deng:2025:DSR

[4078] Lih-Yuan Deng, Nirman Kumar, Henry Horng-Shing Lu, and Ching-Chi Yang. Developments in secure random number generators. *WIREs Computational Statistics*, 17(1):e70011:1–e70011:??, March 2025. CODEN

???? ISSN 1939-0068 (print), 1939-5108 (electronic). URL https://wires.onlinelibrary.wiley.com/doi/epdf/10.1002/wics.70011.

Feng:2025:HTT

[4079] Yongkang Feng, Liang Yao, Hongli Zhou, Minjie Wu, Shuai Xiang, Wanting Sun, Xiumin Xu, and Yingchun Lu. High-throughput TRNG design with novelty adjustable TDC based on STR. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, 18(2):29:1–29:??, June 2025. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).

Liu:2025:CRU

[4080] Minzhao Liu, Ruslan Shaydulin, Pradeep Niroula, Matthew DeCross, Shih-Han Hung, Wen Yu Kon, Enrique Cervero-Martín, Kaushik Chakraborty, Omar Amer, Scott Aaronson, Atithi Acharya, Yuri Alexeev, K. Jordan Berg, Shouvanik Chakrabarti, Florian J. Curchod, Joan M. Dreiling, Neal Erickson, Cameron Foltz, Michael Foss-Feig, David Hayes, Travis S. Humble, Niraj Kumar, Jeffrey Larson, Danylo Lykov, Michael Mills, Steven A. Moses, Brian Neyenhuis, Shaltiel Eloul, Peter Siegfried, James Walker, Charles Lim, and Marco Pistoia. Certified randomness using a trapped-ion quantum processor. *Nature*, 640 (8058):343–348, April 10, 2025. CODEN NATUAS. ISSN 1476-4687. URL https://www.nature.com/articles/s41586-025-08737-1.

Xu:2025:DQT

[4081] Guobin Xu, Oluwole Adetifa, Jianzhou Mao, Eric Sakk, and Shuangbao Wang. Developing quantum trusted platform module (QTPM) to advance IoT security. *Future Internet*, 17(5):193, April 26, 2025. CODEN ???? ISSN 1999-5903. URL https://www.mdpi.com/1999-5903/17/5/193.

Basuyaux:20xx:RNG

[4082] Jean Philippe Basuyaux. Random number generators (généateurs de nombres aléatoires), ≪RNG≫ou ≪REG≫. World-Wide Web site., 20xx. URL http://perso.wanadoo.fr/basuyaux/liens/rng.html.

LEcuyer:20xx:PNG

[4083] P. L'Ecuyer. Pseudorandom number generators. In Eckhart Platen and Peter Jaeckel, editors, *Simulation Methods in Financial Engineering*, Encyclopedia of Quantitative Finance. Wiley, New York, NY, USA, 20xx. Forthcoming.

Wagner:20xx:WRS

[4084] David Wagner. Writings on randomness; source code for generating randomness; source code for testing randomness; hardware for generating randomness; source code to other useful crypto modules; miscellaneous. World-Wide Web site., 20xx. URL `http://www.cs.berkeley.edu/~daw/rnd/`.

Anonymous:1951:PSS

[4085] Anonymous, editor. *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery, Harvard University Computation Laboratory, 13–16 September 1949*, volume 26 of *Annals of the Computation Laboratory of Harvard University*. Harvard University Press, Cambridge, MA, USA, 1951. ISSN ???? LCCN QA75 .S9 1949.

Householder:1951:MCM

[4086] Alston S. Householder, George E. Forsythe, and Hallett-Hunt Germond, editors. *Monte Carlo method. Proceedings of a Symposium Held June 29, 30 and July 1, 1949 in Los Angeles, California*, volume 12 of *Applied Mathematics Series / National Bureau of Standards*. United States Government Printing Office, Washington, DC, USA, 1951.

Anonymous:1954:ADC

[4087] Anonymous, editor. *Automatic digital computation: [Proceedings of a symposium held at the National Physical Laboratory on March 25, 26, 27 and 28, 1953]*. Her Majesty's Stationary Office, London, England, 1954. LCCN QA76 .T4 1953.

Curtiss:1956:NAP

[4088] John H. Curtiss, editor. *Numerical Analysis: Proceedings of the Sixth Symposium in Applied Mathematics of the American Mathematical Society, held at the Santa Monica City College, August 26–28, 1953*, volume 6. McGraw-Hill, New York, NY, USA, 1956. LCCN ????

Meyer:1956:SMC

[4089] Herbert A. Meyer, editor. *Symposium on Monte Carlo Methods: held at the University of Florida, March 16 and 17, 1954*. Wiley, New York, NY, USA, 1956. LCCN QA273 U577.

Macphail:1959:PFC

[4090] M. S. Macphail, editor. *Proceedings of the fourth Canadian Mathematical Congress: Banff, 1957 = Comptes rendus du quatrième Congrès canadien de mathématiques: Banff, 1957*. University of Toronto Press, Toronto, ON, Canada, 1959. LCCN QA7 .C37 1957.

Anonymous:1960:PFI

[4091] Anonymous, editor. *Proceedings of the first IBM Conference on Statistics: data processing statistical seminar: May 2, 1960 through May 4, 1960*. IBM Corporation, Poughkeepsie, NY, USA, 1960. LCCN ????

Ralston:1960:MMD

[4092] Anthony Ralston and Herbert S. Wilf, editors. *Mathematical methods for digital computers*. Wiley, New York, NY, USA, 1960–1977. ISBN 0-471-70690-6. various pp. LCCN QA39 .R26. Three volumes.

Birkhoff:1961:NRT

[4093] Garrett Birkhoff and Eugene P. (Eugene Paul) Wigner, editors. *Nuclear reactor theory: [proceedings of the 11th Symposium in Applied Mathematics of the American Mathematical Society held at the Hotel New Yorker, April 23–25, 1959]*, volume 11 of *Proceedings of symposia in applied mathematics*. American Mathematical Society, Providence, RI, USA, 1961. LCCN QC787.N8 S9 1959.

Taub:1963:JNCa

[4094] A. H. Taub, editor. *John von Neumann: Collected Works. Volume V: Design of Computers, Theory of Automata and Numerical Analysis*. Pergamon, New York, NY, USA, 1963. ix + 784 pp. LCCN ????

Kozesnik:1964:TTP

[4095] Jaroslav Kožešník, editor. *Transactions of the third Prague conference on information theory, statistical decision functions, random processes held at Liblice near Prague, from June 5 to 13, 1962*. Czechoslovak Academy of Science, Prague, Czechoslovakia, 1964. LCCN ???? In memory of RNDr. Antonin Spacek.

Hollingdale:1967:DSO

[4096] S. H. Hollingdale, editor. *Digital simulation in operational research: a conference under the aegis of the Scientific Affairs Division of N.A.T.O., Hamburg, September 6–10th, 1965*. English Universities Press, London, UK, 1967. LCCN QA76.5 D55 1965.

Naylor:1968:CST

[4097] T. H. Naylor, J. L. Balintfy, D. S. Burdick, and K. Chu. *Computer Simulation Techniques*. Wiley, New York, NY, USA, 14th edition, 1968. xiii + 352 pp. LCCN QA76.5 .N36.

Anonymous:1969:CPP

[4098] Anonymous, editor. *A collection of papers presented by invitation at the Symposia on Applied Probability and Monte Carlo Methods and Modern Aspects of Dynamics / sponsored by the Air Force Office of Scientific Research at the 1967 national meeting of SIAM in Washington, DC, June 11–15, 1967*, volume 3 of *SIAM Studies in Applied Mathematics*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1969. LCCN QA1 S565 v. 3.

Bose:1970:EPS

[4099] R. C. (Raj Chandra) Bose and Samarendra Nath Roy, editors. *Essays in probability and statistics*, volume 3 of *University of North Carolina monograph series in probability and statistics*. University of North Carolina Press, Chapel Hill, NC, USA, 1970. ISBN 0-8078-1109-2. xviii + 750 pp. LCCN QA273 .E78.

Rice:1971:MS

[4100] John R. Rice, editor. *Mathematical Software*. Academic Press, New York, NY, USA, 1971. ISBN 0-12-587250-X. LCCN QA1 .M26. Based on the proceedings of the Mathematical Software Symposium held at Purdue University, Lafayette, Indiana, USA, April 1–3, 1970.

Zaremba:1972:ANT

[4101] S. K. Zaremba, editor. *Applications of Number Theory to Numerical Analysis = Applications de la théorie des nombres à l'analyse numérique. Proceedings of the symposium at the Centre for Research in Mathematics, University of Montreal, September 9–14, 1971*. Academic Press, New York, NY, USA, 1972. ISBN 0-12-775950-6. LCCN QA297 .A67.

Schaffner:1974:PPB

[4102] Kenneth F. Schaffner and Robert S. Cohen, editors. *PSA 1972: proceedings of the 1972 Biennial Meeting Philosophy of Science Association (Olds Plaza Hotel, East Lansing, Michigan, October 27–29, 1972)*, volume 20 of *Boston Studies in the Philosophy of Science*. D. Reidel, Dordrecht, The Netherlands; Boston, MA, USA; Lancaster, UK; Tokyo, Japan, 1974. ISBN 90-277-0408-2, 90-277-0409-0, 94-010-2140-6 (e-book). ISSN 0068-0346. LCCN Q175 .B7312. URL `https://link.springer.com/book/10.1007/978-94-010-2140-1`.

Patil:1975:MCS

[4103] Ganapati P. Patil, Samuel Kotz, and J. K. Ord, editors. *A modern course on statistical distributions in scientific work: proceedings of the NATO*

Advanced Study Institute held at the University of Calgary, Calgary, Alberta, Canada, July 29–August 10, 1974, volume 17 of *NATO Advanced Study Institutes series: Series C, mathematical and physical sciences*. D. Reidel, Dordrecht, The Netherlands; Boston, MA, USA; Lancaster, UK; Tokyo, Japan, 1975. ISBN 90-277-0609-3. LCCN QA273.6 .N37 1974.

Hoaglin:1976:PNI

[4104] David C. Hoaglin and Roy E. Welsch, editors. *Proceedings of the Ninth Interface Symposium on Computer Science and Statistics, Harvard University, Massachusetts Institute of Technology, April 1–2, 1976*. Rindle, Weber & Schmidt, Inc., Boston, MA, USA, 1976. ISBN 0-87150-237-2. LCCN QA276.A1 I53 1976.

Ralston:1976:ECS

[4105] Anthony Ralston and Chester L. Meek, editors. *Encyclopedia of computer science*. Petrocelli/Charter, New York, NY, USA, 1976. ISBN 0-88405-321-0. xxviii + 1523 pp. LCCN QA76.15 .E55 1976.

Traub:1976:ACR

[4106] J. F. Traub, editor. *Algorithms and Complexity: Recent Results and New Directions: [Proceedings of a Symposium on New Directions and Recent Results in Algorithms and Complexity held by the Computer Science Department, Carnegie-Mellon University, April 7–9, 1976]*. Academic Press, New York, NY, USA, 1976. ISBN 0-12-697540-X. ix + 523 pp. LCCN QA76.6 .S9195 1976.

Barra:1977:RDS

[4107] Jean René Barra, F. Brodeau, G. Romier, and B. Van Cutsem, editors. *Recent developments in statistics: proceedings of the European Meeting of Statisticians, Grenoble, 6–11 September, 1976*. North-Holland, Amsterdam, The Netherlands, 1977. ISBN 0-7204-0751-6. LCCN QA276.A1 E89 1976.

Wang:1979:ILB

[4108] Peter C. C. Wang, editor. *Information linkage between applied mathematics and industry: Proceedings of the First Annual Workshop on the Information Linkage between Applied Mathematics and Industry, held at the Naval Postgraduate School, Monterey, California, February 23–25, 1978*. Academic Press, New York, NY, USA, 1979. ISBN 0-12-734250-8. LCCN TA329 .W67 1978.

Dempster:1980:SPP

[4109] M. A. H. Dempster, editor. *Stochastic programming: proceedings of an international conference sponsored by the Institute of Mathematics and*

Its Applications, Mathematical Institute, Oxford, 15–17 July 1974. Academic Press, New York, NY, USA, 1980. ISBN 0-12-208250-8. LCCN T57.79 .I54 1974. US$97.00.

Oren:1980:SDM

[4110] Tuncer I. Ören, Charles M. Shub, and Paul F. Roth, editors. *Simulation with discrete models: a state-of-the-art view: Proceedings of the 1980 Winter Simulation Conference, December 3–5, 1980, Orlando Marriott, Orlando, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1980. ISBN ???? LCCN QA76.5 W78 1980.

Eddy:1981:CSS

[4111] William F. Eddy, editor. *Computer Science and Statistics: Proceedings of the 13 Symposium on the Interface, Pittsburgh, PA, USA*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1981. ISBN 3-540-90633-9. LCCN QA276.4. .C58 1981.

Rubinstein:1981:SMC

[4112] Reuven Y. Rubinstein. *Simulation and the Monte Carlo method*. Wiley series in probability and statistics. Wiley, New York, NY, USA, 1981. ISBN 0-470-31651-9, 0-470-31722-1 (e-book). xv + 278 pp. LCCN QA298 .R8. URL `http://www.gbv.de/dms/bowker/toc/9780471089179.pdf`.

Grossmann:1982:PSI

[4113] Wilfried Grossmann, Georg Ch. Pflug, and Wolfgang Wertz, editors. *Probability and statistical inference: proceedings of the 2nd Pannonian Symposium on Mathematical Statistics, Bad Tatzmannsdorf, Austria, June 14–20, 1981*. D. Reidel, Dordrecht, The Netherlands; Boston, MA, USA; Lancaster, UK; Tokyo, Japan, 1982. ISBN 90-277-1427-4. LCCN QA276.A1 P36 1981.

IEEE:1982:ASF

[4114] IEEE, editor. *23rd annual Symposium on Foundations of Computer Science, November 3–5, 1982, Chicago, Illinois*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1982. CODEN ASFPDV. ISBN ???? ISSN 0272-5428. LCCN QA76.6 .S95 1982. IEEE catalog number 82CH1806-9. IEEE Computer Society order number 440.

Chaum:1983:ACP

[4115] David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors. *Advances in Cryptology: proceedings of CRYPTO 82*. Plenum Press, New

York, NY, USA; London, UK, 1983. ISBN 1-4757-0604-9 (print), 1-4757-0602-2. LCCN QA76.9.A25 C79 1982.

Gentle:1983:CSS

[4116] James E. Gentle, editor. *Computer Science and Statistics: Proceedings of the Fifteenth Symposium on the Interface, Houston, Texas, March 1983*. North-Holland, Amsterdam, The Netherlands, 1983. ISBN 0-444-86688-4. LCCN QA276.4 .S95 1983.

IEEE:1983:ASF

[4117] IEEE, editor. *24th Annual Symposium on Foundations of Computer Science: November 7–9, 1983, Tucson, Arizona*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. CODEN ASFPDV. ISBN 0-8186-0508-1. ISSN 0272-5428. LCCN QA76.6 .S95 1983. IEEE catalog number 83CH1938-0.

Ralston:1983:ECS

[4118] Anthony Ralston and Edwin D. Reilly, Jr., editors. *Encyclopedia of Computer Science and Engineering*. Van Nostrand Reinhold, New York, NY, USA, second edition, 1983. ISBN 0-442-24496-7. xxix + 1664 pp. LCCN QA76.15 .E48 1983.

Roberts:1983:WSC

[4119] Stephen D. Roberts, Jerry Banks, and Bruce Schmeiser, editors. *1983 Winter Simulation Conference proceedings: December 12–14, 1983, Marriott Crystal Gateway Hotel, Arlington, Virginia*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1983. ISBN ???? LCCN QA76.9.C65 W56 1983.

IEEE:1984:ASF

[4120] IEEE, editor. *25th annual Symposium on Foundations of Computer Science, October 24–26, 1984, Singer Island, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1984. CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-8186-4591-1 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1984. IEEE catalog number 84CH2085-9.

Sheppard:1984:WSC

[4121] Sallie Sheppard, Udo W. Pooch, and Claude Dennis Pegden, editors. *1984 Winter Simulation Conference proceedings: November 28–30, 1984, Sheraton Dallas Hotel, Dallas, Texas*. Society for Computer Simulation, San Diego, CA, USA, 1984. ISBN 0-911801-04-9 (SCS), 0-444-87605-7

(North Holland). LCCN QA76.9.C65 W56 1984. IEEE order number 84CH2098-2.

ACM:1985:PSA

[4122] ACM, editor. *Proceedings of the seventeenth annual ACM Symposium on Theory of Computing, Providence, Rhode Island, May 6–8, 1985*. ACM Press, New York, NY 10036, USA, 1985. ISBN 0-89791-151-2 (paperback). LCCN QA 76.6 A13 1985. ACM order number 508850.

Beth:1985:ACP

[4123] Thomas Beth, N. Cot, and I. Ingemarsson, editors. *Advances in cryptology: proceedings of EUROCRYPT 84, a Workshop on the Theory and Application of Cryptographic Techniques, Paris, France, April 9–11, 1984*, volume 209 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-16076-0 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 E951 1984. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0209.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=209`. Held at the University of Paris, Sorbonne.

Billard:1985:CSS

[4124] L. (Lynne) Billard, editor. *Computer science and statistics: proceedings of the Sixteenth Symposium on the Interface, Atlanta, Georgia, March 1984*. Elsevier Science Publishers B.V., Amsterdam, The Netherlands, 1985. ISBN 0-444-87725-8. LCCN QA276.4 .S95 1984.

Blakley:1985:ACP

[4125] George Robert Blakley and David Chaum, editors. *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-15658-5, 3-540-39568-7. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1984; QA267.A1 L43 no.196. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0196.htm`; `http://www.springerlink.com/content/cemajg0qmeev/`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=196`. CRYPTO 84: a Workshop on the Theory and Application of Cryptographic Techniques, held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.

Mehlhorn:1985:SAS

[4126] Kurt Mehlhorn, editor. *STACS 85: 2nd Annual Symposium on Theoretical Aspects of Computer Science, Saarbrücken, January 3–5, 1985*, volume 182 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1985. CODEN LNCSD9. ISBN 0-387-13912-5 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.182. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0182.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=182`.

ACM:1986:PEA

[4127] ACM, editor. *Proceedings of the Eighteenth annual ACM Symposium on Theory of Computing, Berkeley, California, May 28–30, 1986*. ACM Press, New York, NY 10036, USA, 1986. ISBN 0-89791-193-8. LCCN QA 76.6 A13 1986. ACM order number 508860.

Arkin:1986:SOP

[4128] V. I. Arkin, A. Shiraev, and R. Wets, editors. *Stochastic optimization: proceedings of the international conference, Kiev, 1984*, volume 81 of *Lecture notes in control and information sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1986. ISBN 0-387-16659-9. LCCN QA402.3.S778 1986.

DAgostino:1986:GFT

[4129] Ralph B. D'Agostino and Michael A. Stephens, editors. *Goodness-of-fit techniques*, volume 68 of *Statistics, textbooks and monographs*. Marcel Dekker, Inc., New York, NY, USA, 1986. ISBN 0-8247-7487-6. xviii + 560 pp. LCCN QA277 .G645 1986.

Heath:1986:HMP

[4130] M. T. Heath, editor. *Hypercube multiprocessors, 1987: Proceedings of the Second Conference on Hypercube Multiprocessors, Knoxville, Tennessee, September 29–October 1, 1986*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1986. ISBN 0-89871-215-7. LCCN QA76.5 .C61921 1986.

Wilson:1986:WSC

[4131] James R. Wilson, James O. Henriksen, and Stephen D. Roberts, editors. *1986 Winter Simulation Conference proceedings: December 8–10, 1986, Radisson Mark Plaza Hotel, Washington, DC*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,

1986. ISBN 0-911801-11-1. LCCN QA76.9.C65 W56 1986. URL `http://www.acm.org/pubs/contents/proceedings/simulation/318242/`.

ACM:1987:PNA

[4132] ACM, editor. *Proceedings of the nineteenth annual ACM Symposium on Theory of Computing, New York City, May 25–27, 1987*. ACM Press, New York, NY 10036, USA, 1987. ISBN 0-89791-221-7 (paperback). LCCN QA 76.6 A13 1987. ACM order number 508870.

Chaum:1987:ACE

[4133] David Chaum and Wyn L. Price, editors. *Advances in Cryptology–EUROCRYPT '87: Workshop on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987: Proceedings*, volume 304 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. ISBN 0-387-19102-X (New York), 3-540-19102-X (Berlin). LCCN QA76.9.A25 E963 1987.

Deavours:1987:CYT

[4134] Cipher A. Deavours, David Kahn, Louis Kruh, and Greg Mellen, editors. *Cryptology yesterday, today, and tomorrow*. The Artech House communication and electronic defense library. Artech House Inc., Norwood, MA, USA, 1987. ISBN 0-89006-253-6. xi + 519 pp. LCCN Z103.C76 1987. US$60.00. First volume of selected papers from issues of Cryptologia.

IEEE:1987:ASF

[4135] IEEE, editor. *28th annual Symposium on Foundations of Computer Science, October 12–14, 1987, Los Angeles, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1987. CODEN ASFPDV. ISBN 0-8186-0807-2, 0-8186-4807-4 (microfiche), 0-8186-8807-6 (casebound). ISSN 0272-5428. LCCN QA 76 S979 1987. IEEE Catalog no. 87CH2471-1. Computer Society order number 807.

Odlyzko:1987:ACC

[4136] Andrew Michael Odlyzko, editor. *Advances in cryptology: CRYPTO '86: proceedings*, volume 263 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1987. CODEN LNCSD9. ISBN 3-540-18047-8, 0-387-18047-8. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791 1986. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0263.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=263`. Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.

Abrams:1988:WSC

[4137] Michael A. Abrams, Peter L. Haigh, John Craig Comfort, et al., editors. *1988 Winter Simulation Conference proceedings: December 12–14, 1988, the San Diego Marriott, San Diego, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. ISBN 0-911801-42-1. LCCN QA76.9.C65 W56 1988. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5817`. IEEE catalog number 88CH2659-1.

ACM:1988:PTA

[4138] ACM, editor. *Proceedings of the twentieth annual ACM Symposium on Theory of Computing, Chicago, Illinois, May 2–4, 1988*. ACM Press, New York, NY 10036, USA, 1988. ISBN 0-89791-264-0. LCCN QA 76.6 A13 1988. ACM order number 508880.

Edwards:1988:CPC

[4139] D. (David) Edwards and N. E. (Niels E.) Raun, editors. *COMPSTAT: proceedings in computational statistics, 8th symposium held in Copenhagen 1988*. Physica-Verlag, Vienna, Austria, 1988. ISBN 3-7908-0411-8. LCCN QA276.4 .C57 1988. URL `http://catalog.hathitrust.org/api/volumes/oclc/19564603.html`.

IEEE:1988:ASF

[4140] IEEE, editor. *29th annual Symposium on Foundations of Computer Science, October 24–26, 1988, White Plains, New York*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1988. CODEN ASFPDV. ISBN 0-8186-0877-3 (paperback), 0-8186-4877-5 (microfiche), 0-8186-8877-7 (hard). ISSN 0272-5428. LCCN QA 76 S979 1988. IEEE catalog number 88CH2652-6. Computer Society order no. 877.

Wegman:1988:CSS

[4141] Edward J. Wegman, Donald T. Gantz, and John J. Miller, editors. *Computing Science and Statistics Proceedings of the 20th Symposium on the Interface Fairfax, Virginia, April 1988*. American Statistical Association, Alexandria, VA, USA, 1988. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a208838.pdf`.

Wegman:1988:SIC

[4142] Edward J. Wegman, editor. *20th Symposium on the Interface: Computing Science and Statistics: Theme: Computationally Intensive Methods in Statistics April 20–23, 1988*. Interface Foundation of North America,

Inc., P.O. Box 7460, Fairfax Station, VA 22039-7460, USA, 1988. URL `http://www.dtic.mil/dtic/tr/fulltext/u2/a205068.pdf`.

ACM:1989:PTF

[4143] ACM, editor. *Proceedings of the twenty-first annual ACM Symposium on Theory of Computing, Seattle, Washington, May 15–17, 1989*. ACM Press, New York, NY 10036, USA, 1989. ISBN 0-89791-307-8. LCCN QA 76.6 A13 1989. ACM order number 508890.

Anonymous:1989:PFC

[4144] Anonymous, editor. *Proceedings of the Fourth Conference on Hypercubes, Concurrent Computers and Applications, 6–8 March 1989, Monterey, CA, USA*. Golden Gate Enterprises, Los Altos, CA, USA, 1989. ISBN ???? LCCN QA76.5.C619215 1989. Two volumes.

Beker:1989:CC

[4145] Henry Beker and F. C. Piper, editors. *Cryptography and coding*, The Institute of Mathematics and Its Applications conference series; new ser., 20. Oxford University Press, Walton Street, Oxford OX2 6DP, UK, 1989. ISBN 0-19-853623-2. LCCN QA268.C74 1989. UK£35.00, US$52.00. Held in December 1986. Based on the proceedings of a conference organized by the Institute of Mathematics and its Applications on cryptography and coding, held at the Royal Agricultural College, Cirencester on 15th–17th December 1986.

IEEE:1989:ASF

[4146] IEEE, editor. *30th annual Symposium on Foundations of Computer Science, October 30–November 1, 1989, Research Triangle Park, North Carolina*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. CODEN ASFPDV. ISBN 0-8186-1982-1 (casebound), 0-8186-5982-3 (microfiche). ISSN 0272-5428. LCCN QA 76 S979 1989; TK7885.A1 S92 1989. Formerly called the Annual Symposium on Switching and Automata Theory. IEEE catalog number 89CH2808-4. Computer Society order number 1982.

MacNair:1989:WSC

[4147] Edward A. MacNair, Kenneth J. Musselman, and Philip Heidelberger, editors. *1989 Winter Simulation Conference proceedings: December 4–6, 1989, the Capital Hilton Hotel, Washington, DC*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1989. ISBN 0-911801-58-8. LCCN QA76.9.C65 W56 1989. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=5823`. IEEE order number 89CH2778-9.

ACM:1990:PTS

[4148] ACM, editor. *Proceedings of the twenty-second annual ACM Symposium on Theory of Computing, Baltimore, Maryland, May 14–16, 1990*. ACM Press, New York, NY 10036, USA, 1990. ISBN 0-89791-361-2. LCCN QA76.A15 1990. ACM order number 508900.

Balci:1990:WSC

[4149] Osman Balci, Richard E. Nance, and Randall P. Sadowski, editors. *1990 Winter Simulation Conference proceedings, 9–12 December 1990, The Fairmont Hotel, New Orleans, Louisiana*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-911801-72-3. LCCN QA76.5.W56 1990.

Capocelli:1990:SCC

[4150] Renato M. Capocelli, editor. *Sequences: Combinatorics, compression, security, and transmission*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. ISBN 3-540-97186-6 (Berlin), 0-387-97186-6 (New York). LCCN QA292 A38 1988.

Goldwasser:1990:ACC

[4151] S. Goldwasser, editor. *Advances in cryptology — CRYPTO '88: proceedings*, volume 403 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1990. CODEN LNCSD9. ISBN 0-387-97196-3 (USA). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1988. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0403.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=403`.

IEEE:1990:PAS

[4152] IEEE, editor. *Proceedings: 31st Annual Symposium on Foundations of Computer Science: October 22–24, 1990, St. Louis, Missouri*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. CODEN ASFPDV. ISBN 0-8186-2082-X (paperback), 0-8186-6082-1 (microfiche), 0-8186-9082-8 (case). ISSN 0272-5428. LCCN TK7885.A1 S92 1990. Formerly called the Annual Symposium on Switching and Automata Theory. IEEE catalog number 90CH29256. Computer Society order number 2082.

IEEE:1990:PSN

[4153] IEEE, editor. *Proceedings, Supercomputing '90: November 12–16, 1990, New York Hilton at Rockefeller Center, New York, New York*. IEEE

Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1990. ISBN 0-8186-2056-0 (paperback) (IEEE Computer Society), 0-89791-412-0 (paperback) (ACM). LCCN QA 76.88 S87 1990. ACM order number 415903. IEEE Computer Society Press order number 2056. IEEE catalog number 90CH2916-5.

Pomerance:1990:CCNb

[4154] Carl Pomerance and S. Goldwasser, editors. *Cryptology and Computational Number Theory*, volume 42 of *Proceedings of symposia in applied mathematics. AMS short course lecture notes*. American Mathematical Society, Providence, RI, USA, 1990. ISBN 0-8218-0155-4. ISSN 0160-7634. LCCN QA76.9.A25 C84 1990; QA1 .A56 v.42 1990. Lecture notes prepared for the American Mathematical Society short course, Cryptology and computational number theory, held in Boulder, Colorado, August 6–7, 1989.

Anonymous:1991:PIS

[4155] Anonymous, editor. *Proceedings of the International Symposium on Supercomputing: Fukuoka, Japan, November 6–8, 1991*. Kyushu University Press, Fukuoka, Japan, 1991. ISBN 4-87378-284-8. LCCN QA76.88.I1991.

Day:1991:PAA

[4156] William Day, editor. *Proceedings / 29th Annual [ACM] Southeast Regional Conference, Auburn, Alabama, April 10–12, 1991*. ACM Press, New York, NY 10036, USA, 1991. ISBN 0-89791-388-4. LCCN ????

Dorninger:1991:CGA

[4157] D. Dorninger, editor. *Contributions to general algebra, Proceedings of the Vienna conference, June 14–17, 1990: 40 Algebra*, volume 7. Hölder-Pichler-Tempsky, Wien, Austria, 1991. ISBN 3-209-01380-2 (HPT), 3-519-02766-6 (Teubner). LCCN QA150 .C666 1991.

Nelson:1991:WSC

[4158] Barry L. Nelson, W. David Kelton, and Gordon M. Clark, editors. *1991 Winter Simulation Conference proceedings: December 8–11, 1991, the Arizona Biltmore, Phoenix, Arizona*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. CODEN WSCPDK. ISBN 0-7803-0181-1. ISSN 0275-0708, 0743-1902. LCCN QA 76.9 C65 W56 1991. IEEE catalog number 91CH3050-2.

ACM:1992:PTF

[4159] ACM, editor. *Proceedings of the twenty-fourth annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 4–6, 1992*. ACM Press, New York, NY 10036, USA, 1992. ISBN 0-89791-511-9. LCCN QA76.A15 1992. ACM order number 508920.

Burr:1992:UEN

[4160] Stefan A. Burr, editor. *The unreasonable effectiveness of number theory: American Mathematical Society short course, August 6–7, 1991, Orono, Maine*, volume 46 of *Proceedings of symposia in applied mathematics*. American Mathematical Society, Providence, RI, USA, 1992. ISBN 0-8218-5501-8. LCCN QA241 .U67 1992.

Gritzmann:1992:ORE

[4161] Peter Gritzmann, R. Hettich, R. Horst, and E. Sachs, editors. *Operations research '91: extended abstracts of the 16th Symposium on Operations Research, held at the University of Trier at September, 9–11, 1991*. Physica-Verlag, Vienna, Austria, 1992. ISBN 0-387-91431-5 (New York), 3-7908-0608-0 (Heidelberg). LCCN T57.6 .S95 1991.

IEEE:1992:ASF

[4162] IEEE, editor. *33rd Annual Symposium on Foundations of Computer Science: October 24–27, 1992, Pittsburgh, Pennsylvania: proceedings [papers]*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. CODEN ASFPDV. ISBN 0-8186-2901-0 (microfiche), 0-8186-2900-2 (paperback). ISSN 0272-5428. LCCN QA 76 S979 1992. IEEE Catalog Number 92CH3188-0. IEEE Computer Society Press Order Number 2900.

Pflug:1992:SOP

[4163] Georg Ch. Pflug and Ulrich Dieter, editors. *Simulation and optimization: proceedings of the International Workshop on Computationally Intensive Methods in Simulation and Optimization, held at the International Institute for Applied Systems Analysis (IIASA), Laxenburg, Austria, August 23–25, 1990*, volume 374 of *Lecture notes in economics and mathematical systems*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1992. ISBN 3-540-54980-3 (Berlin), 0-387-54980-3 (New York). LCCN QA402.5 .I525 1990.

Simmons:1992:CCS

[4164] Gustavus J. Simmons, editor. *Contemporary Cryptology: the science of information integrity*. IEEE Computer Society Press, 1109 Spring Street,

Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-87942-277-7. xv + 640 pp. LCCN QA76.9.A25 C6678 1992. US$79.95. IEEE order number: PC0271-7.

Steele:1992:PA

[4165] John Michael Steele and William F. Eddy, editors. *Probability and Algorithms*. National Academy Press, Washington, DC, USA, 1992. ISBN 0-309-04776-5. ix + 178 pp. LCCN QA273.P7953 1992. URL `http://site.ebrary.com/lib/stanford/Doc?id=10056784`; `http://www.nap.edu/books/0309047765/html/`.

Swain:1992:PWS

[4166] James J. Swain, editor. *Proceedings of the Winter Simulation Conference. Crystal Gateway Marriott Hotel, Arlington, Virginia, December 13–16, 1992*, volume 24. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1992. ISBN 0-7803-0797-6 (softbound), 0-7803-0798-4 (casebound), 0-7803-0799-2 (microfiche). LCCN T57.62 .W787 1992. IEEE catalog number 92CH3202-9.

Vouk:1992:PAS

[4167] Mladen A. Vouk, Douglas S. Reeves, and Cherri M. Pancake, editors. *Proceedings of the 30th Annual Southeast Regional Conference: 1992, Raleigh, North Carolina, April 8–10, 1992*. ACM Press, New York, NY 10036, USA, 1992. ISBN 0-89791-506-2. LCCN QA75.5 .S69a 1992.

ACM:1993:PPT

[4168] ACM, editor. *PODS '93. Proceedings of the Twelfth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems: May 25–28, 1993, Washington, DC*, volume 12 of *Proceedings of the ACM SIGACT SIGMOD SIGART Symposium on Principles of Database Systems*. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-593-3. LCCN QA 76.9 D3 A26 1993.

Bronstein:1993:IPI

[4169] Manuel Bronstein, editor. *ISSAC'93: proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, July 6–8, 1993, Kiev, Ukraine*. ACM Press, New York, NY 10036, USA, 1993. ISBN 0-89791-604-2. LCCN QA 76.95 I59 1993. ACM order number: 505930.

Lenstra:1993:DNF

[4170] A. K. Lenstra and H. W. Lenstra, Jr. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993.

ISBN 0-387-57013-6 (New York), 3-540-57013-6 (Berlin). viii + 131 pp. LCCN QA3 .L35 v.1554.

Miola:1993:DIS

[4171] A. Miola, editor. *Design and Implementation of Symbolic Computation Systems International Symposium. DISCO '93 Gmunden, Austria, September 15–17, 1993: Proceedings*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1993. ISBN 3-540-57235-X. LCCN QA76.9.S88I576 1993.

Mullen:1993:FFC

[4172] Gary L. Mullen and Peter Jau-Shyong Shiue, editors. *Finite fields, coding theory, and advances in communications and computing*, volume 141 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, NY, USA, 1993. ISBN 0-8247-8805-2. LCCN QA247.3 .F56 1993. URL `http://www.loc.gov/catdir/enhancements/fy0745/92023503-d.html`. Proceedings of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing held at the University of Nevada, Las Vegas, August 7–10, 1991.

Ralston:1993:ECS

[4173] Anthony Ralston and Edwin D. Reilly, Jr., editors. *Encyclopedia of Computer Science and Engineering*. Van Nostrand Reinhold, New York, NY, USA, third edition, 1993. ISBN 0-442-27679-6. xxv + 1558 pp. LCCN QA76.15 .E48 1993.

Sincovec:1993:PSS

[4174] Richard F. Sincovec, David E. Keyes, L. M. R., L. R. Petzold, and D. A. Reed, editors. *Proceedings of the Sixth SIAM Conference on Parallel Processing for Scientific Computing, held March 22–24, 1993, in Norfolk, VA, USA*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1993. ISBN 0-89871-315-3. LCCN QA76.58 .S55 1993 v.1-2. Two volumes.

Swartzlander:1993:PSC

[4175] Earl Swartzlander, Jr., Mary Jane Irwin, and Graham Jullien, editors. *Proceedings: 11th Symposium on Computer Arithmetic, June 29–July 2, 1993, Windsor, Ontario*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1993. ISBN 0-7803-1401-8 (softbound), 0-8186-3862-1 (casebound), 0-8186-3861-3 (microfiche). ISSN 0018-9340 (print), 1557-9956 (electronic). LCCN QA 76.9 C62 S95 1993. IEEE Transactions on Computers **43(8)**, 1994.

ACM-SIAM:1994:ASD

[4176] *Proceedings of the fifth annual ACM-SIAM Symposium on Discrete Algorithms, Arlington, VA, USA*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1994. ISBN 0-89871-329-3. LCCN QA76.6 .A278 1994.

ACM:1994:PTS

[4177] ACM, editor. *Proceedings of the twenty-sixth annual ACM Symposium on the Theory of Computing: Montreal, Quebec, Canada, May 23–25, 1994*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-663-8. LCCN QA76 .A15 1994. ACM order number 508930.

Desmedt:1994:ACC

[4178] Yvo G. Desmedt, editor. *Advances in cryptology, CRYPTO '94: 14th annual international cryptology conference, Santa Barbara, California, USA, August 21–25, 1994: proceedings*, volume 839 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1994. CODEN LNCSD9. ISBN 3-540-58333-5 (Berlin), 0-387-58333-5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C79 1994. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t0839.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=839`.

IEEE:1994:PSW

[4179] IEEE, editor. *Proceedings, Supercomputing '94: Washington, DC, November 14–18, 1994*, Supercomputing. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-8186-6605-6 (paper), 0-8186-6606-4 (microfiche), 0-8186-6607-2 (case). ISSN 1063-9535. LCCN QA76.5 .S894 1994. URL `http://sc94.ameslab.gov/AP/contents.html`. IEEE catalog number 94CH34819.

Snodgrass:1994:PAS

[4180] Richard T. Snodgrass and Marianne Winslett, editors. *Proceedings of the 1994 ACM SIGMOD International Conference on Management of Data / SIGMOD '94, Minneapolis, Minnesota, May 24–27, 1994*, volume 23(2) of *SIGMOD Record (ACM Special Interest Group on Management of Data)*. ACM Press, New York, NY 10036, USA, 1994. ISBN 0-89791-639-5. ISSN 0163-5808 (print), 1943-5835 (electronic). LCCN QA 76.9 D3 S53 v.23 no.2 1994.

Tew:1994:WSC

[4181] Jeffrey D. Tew, Mani S. Manivannan, and Deborah A. Sadowski, editors. *1994 Winter Simulation Conference proceedings: Walt Disney World Swan Hotel, Lake Buena Vista, Florida, December 11–14, 1994*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1994. ISBN 0-7803-2109-X (casebound), 0-7803-2108-1 (paperback), 0-7803-2110-3 (microfiche). LCCN QA76.9.C65 W56 1994. IEEE catalog number 94CH35705.

ACM:1995:PTS

[4182] ACM, editor. *Proceedings of the twenty-seventh annual ACM Symposium on Theory of Computing: Las Vegas, Nevada, May 29–June 1, 1995*. ACM Press, New York, NY 10036, USA, 1995. ISBN 0-89791-718-9. LCCN QA 76.6 A13 1995. ACM order number 508950.

Alexopoulos:1995:WSC

[4183] C. Alexopoulos, K. Kang, W. R. Lilegdon, and D. Goldsman, editors. *1995 Winter Simulation Conference: proceedings, December 3–6, 1995. San Diego, CA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1995. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56 1995. URL `http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=3475`. IEEE Catalog No. 95CB35865.

DePietro:1995:PNP

[4184] G. De Pietro, A. Giordano, M. Vajtersic, and P. Zinterhof, editors. *Parallel Numerics '95: proceedings of the international workshop, Sorrento, Italy, September 27–29, 1995*. Zaccaria, Naples, Italy, 1995. ISBN ???? LCCN ????

IEEE:1995:ASF

[4185] IEEE, editor. *36th Annual Symposium on Foundations of Computer Science: October 23–25, 1995, Milwaukee, Wisconsin*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1995. CODEN ASFPDV. ISBN 0-7803-3121-4 (casebound), 0-8186-7183-1 (softbound), 0-8186-7184-X (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1995. IEEE catalog number 95CB35834.

Levelt:1995:IPI

[4186] A. H. M. Levelt, editor. *ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation: July 10–12, 1995, Montréal, Canada*, ISSAC -PROCEEDINGS- 1995. ACM Press, New

York, NY 10036, USA, 1995. ISBN 0-89791-699-9. LCCN QA 76.95 I59 1995. ACM order number 505950.

Niederreiter:1995:MCQ

[4187] Harald Niederreiter and Peter Jau-Shyong Shiue, editors. *Monte Carlo and quasi-Monte Carlo methods in scientific computing: proceedings of a conference at the University of Nevada, Las Vegas, Nevada, USA, June 23–25, 1994*, volume 106 of *Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1995. ISBN 0-387-94577-6 (softcover). LCCN Q183.9 .M66 1995.

USENIX:1995:PFUa

[4188] USENIX, editor. *Proceedings of the fifth USENIX UNIX Security Symposium: June 5–7, 1995, Salt Lake City, Utah, USA*. USENIX, Berkeley, CA, USA, 1995. ISBN 1-880446-70-7. LCCN QA76.8.U65 U55 1992(3)-1995(5). URL `http://www.usenix.org/publications/library/proceedings/security95/index.html`.

USENIX:1995:PNS

[4189] USENIX, editor. *Proceedings of the Ninth Systems Administration Conference (LISA IX): September 17–22, 1995, Monterey, CA, USA*. USENIX, Berkeley, CA, USA, 1995. ISBN 1-880446-73-1. LCCN QA 76.76 O63 S97 1995. URL `http://www.usenix.org/publications/library/proceedings/lisa95/index.html`.

ACM:1996:FCP

[4190] ACM, editor. *FCRC '96: Conference proceedings of the 1996 International Conference on Supercomputing: Philadelphia, Pennsylvania, USA, May 25–28, 1996*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-803-7. LCCN QA76.5 I61 1996. ACM order number 415961.

ACM:1996:PTE

[4191] ACM, editor. *Proceedings of the twenty-eighth annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, May 22–24, 1996*. ACM Press, New York, NY 10036, USA, 1996. ISBN 0-89791-785-5. LCCN QA 76.6 A13 1996. ACM order number 508960. Also known as Federated Computing Research Conference (FCRS '96).

Charnes:1996:WSC

[4192] John M. Charnes, D. J. Morice, D. T. Brunner, and J. J. Swain, editors. *1996 Winter Simulation Conference: proceedings, Hotel Del Coronado, Coronado, California, 8–11 December 1996*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA,

1996. ISBN 0-7803-3383-7. LCCN QA76.9.C65 W56 1996. URL `http://ieeexplore.ieee.org/servlet/opac?punumber=6969`; `http://www.acm.org/pubs/contents/proceedings/simulation/256562/`. IEEE catalog number 96CB35957.

Cohen:1996:FFA

[4193] S. (Stephen) Cohen and Harald Niederreiter, editors. *Finite fields and applications: proceedings of the third international conference, Glasgow, July 1995*, volume 233 of *London Mathematical Society lecture note series*. Cambridge University Press, Cambridge, UK, 1996. ISBN 0-521-56736-X (paperback). LCCN QA247.3 .F535 1996.

IEEE:1996:ASF

[4194] IEEE, editor. *37th Annual Symposium on Foundations of Computer Science: October 14–16, 1996, Burlington, Vermont*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1996. CODEN ASFPDV. ISBN 0-7803-3762-X (casebound), 0-8186-7594-2 (softbound), 0-8186-7596-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 1996. IEEE catalog number 96CH35973. IEEE Computer Society Press order number PR07594.

Trobec:1996:PIW

[4195] Roman Trobec, M. Vajteršič, Jurij Šilc, Borut Robič, et al., editors. *Proceedings of the International Workshop Parallel Numerics '96, Gozd Martuljek, Slovenia, September 11–13, 1996*. Institut "Jožef Stefan", Ljubljana, Slovenia, 1996. ISBN 86-80023-25-6. LCCN ????

Andradottir:1997:PWS

[4196] Sigrún Andradóttir, editor. *Proceedings of the 1997 Winter Simulation Conference: Renaissance Waverly, Atlanta, Georgia, 7–10 December 1997*. ACM Press, New York, NY 10036, USA, 1997. ISBN 0-7803-4278-X. LCCN QA76.5 W78 1997.

Gell-Mann:1997:QJA

[4197] Murray Gell-Mann. *The quark and the jaguar: adventures in the simple and the complex*. W. H. Freeman and Company, New York, NY, USA, 1997. ISBN 0-7167-2725-0 (paperback). xviii + 392 pp. LCCN QC774.G45 A3 1994. URL `http://www.gbv.de/dms/bowker/toc/9780716725817.pdf`; `http://www.zentralblattmath.org/zmath/en/search/?an=0833.00011`.

IEEE:1997:ASF

[4198] IEEE, editor. *38th Annual Symposium on Foundations of Computer Science: October 20–22, 1997, Miami Beach, Florida*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1997. CODEN ASFPDV. ISBN 0-8186-8197-7 (paperback), 0-8186-8198-5 (casebound), 0-8186-8199-3 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 .S92 1997. IEEE catalog number 97CB36150. IEEE Computer Society Press order number PR08197.

Troch:1997:PSI

[4199] I. Troch and F. Breitenecker, editors. *Proceedings of the Second IMACS Symposium on Mathematical Modelling: February 5–7, 1997, Technical University Vienna, Austria*, volume 11 of *ARGESIM report*. ARGESIM, Vienna, 1997. ISBN 3-901608-11-7. LCCN ????

Wyrzykowski:1997:PNP

[4200] R. Wyrzykowski, Jurij Šilc, Roman Trobec, et al., editors. *Parallel Numerics '97: proceedings of the International Workshop, Zakopane, Poland, September 5–7, 1997*. Institute of Mathematics and Computer Science, Czñestochowa, Poland, 1997. ISBN 83-7098-365-0. LCCN ????

Banks:1998:HSP

[4201] Jerry Banks, editor. *Handbook of simulation: principles, methodology, advances, applications, and practice*. Wiley, New York, NY, USA, 1998. ISBN 0-471-13403-1 (hardcover). xii + 849 pp. LCCN T57.62 .H37 1998. URL `http://www.loc.gov/catdir/bios/wiley044/97051533.html`; `http://www.loc.gov/catdir/description/wiley037/97051533.html`; `http://www.loc.gov/catdir/toc/onix01/97051533.html`.

Buhler:1998:ANT

[4202] Joe P. Buhler, editor. *Algorithmic number theory: third international symposium, ANTS-III, Portland, Oregon, USA, June 21–25, 1998: proceedings*, volume 1423 of *Lecture notes in computer science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 3-540-64657-4 (softcover). LCCN QA241 .A43 1998.

Hellekalek:1998:RQR

[4203] Peter Hellekalek and Gerhard Larcher, editors. *Random and quasi-random point sets*, volume 138 of *Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 0-387-98554-9. xii + 332 pp. LCCN QA298 .P82 1998. URL `http://www.loc.gov/catdir/enhancements/fy0816/98030563-d.html`; `http://www.loc.gov/catdir/enhancements/fy0816/98030563-t.html`.

IEEE:1998:HCC

[4204] IEEE, editor. *Hot chips 10: conference record: August 16–18, 1998, Memorial Auditorium, Stanford University, Palo Alto, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN ???? LCCN ????

Kent:1998:ECS

[4205] Allen Kent, James G. Williams, and Carolyn M. Hall, editors. *Encyclopedia of computer science and technology*, volume 39 (supplement 24). Marcel Dekker, Inc., New York, NY, USA, 1998. ISBN 0-8247-2292-2 (hardcover). vii + 360 pp. LCCN QA76.15 .E5 v.39.

Medeiros:1998:WSC

[4206] D. J. Medeiros, Edward F. Watson, John S. Carson, and Mani S. Manivanan, editors. *1998 Winter Simulation Conference proceedings: Simulation in the 21st century. December 13–16, 1998, Washington, DC, Grand Hyatt Hotel*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1998. ISBN 0-7803-5133-9 (softbound), 0-7803-5102-9 (casebound), 0-7803-5103-7 (microfiche). LCCN QA76.9.C65 W562 1998. IEEE catalog number 98CH36274.

Niederreiter:1998:MCQ

[4207] Harald Niederreiter, Peter Hellekalek, Gerhard Larcher, and Peter Zinterhof, editors. *Monte Carlo and Quasi-Monte Carlo methods 1996: proceedings of a conference at the University of Salzburg, Austria, July 9–12, 1996*, volume 127 of *Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1998. ISBN 0-387-98335-X (softcover). LCCN Q183.9 .M67 1998. URL `http://www.loc.gov/catdir/enhancements/fy0815/97034133-d.html`; `http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html`.

USENIX:1998:SUS

[4208] USENIX, editor. *Seventh USENIX Security Symposium proceedings: conference proceedings: San Antonio, Texas, January 26–29, 1998*. USENIX, Berkeley, CA, USA, 1998. ISBN 1-880446-92-8. LCCN QA76.9.A25 U83 1998. URL `http://db.usenix.org/publications/library/proceedings/sec98`.

ACM:1999:PTF

[4209] ACM, editor. *Proceedings of the thirty-first annual ACM Symposium on Theory of Computing: Atlanta, Georgia, May 1–4, 1999*. ACM Press, New York, NY 10036, USA, 1999. ISBN 1-58113-067-8. LCCN QA75.5 .A14 1999. ACM order number 508990.

Anonymous:1999:NIS

[4210] Anonymous, editor. *22nd National Information Systems Security Conference: Hyatt Regency Crystal City, Arlington, Virginia, October 18–21, 1999*. National Institute for Standards and Technology, Gaithersburg, MD, USA, 1999. LCCN ????

Fossorier:1999:AAA

[4211] Marc P. C. Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors. *Applied algebra, algebraic algorithms, and error-correcting codes: 13th international symposium, AAECC-13, Honolulu, Hawaii, USA, November 15–19, 1999: proceedings*, volume 1719 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66723-7. LCCN QA268 .A35 1999. URL `http://www.loc.gov/catdir/enhancements/fy0812/99054502-d.html`.

Heath:1999:APP

[4212] Michael T. Heath, Abhiram Ranade, and Robert S. Schreiber, editors. *Algorithms for parallel processing: Proceedings of the Workshop on Algorithms for Parallel Processing, held September 16–20, 1996, at the IMA, University of Minnesota*, volume 105 of *The IMA volumes in mathematics and its applications*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 0-387-98680-4. LCCN QA76.58 .A543 1999. URL `http://www.loc.gov/catdir/enhancements/fy0817/98033425-t.html`.

Iliev:1999:RAN

[4213] O. P. (Oleg P.) Iliev et al., editors. *Recent advances in numerical methods and applications II: proceedings of the fourth international conference, NMA '98, Sofia, Bulgaria 19–23 August, 1998*. World Scientific Publishing Co. Pte. Ltd., P. O. Box 128, Farrer Road, Singapore 9128, 1999. ISBN 981-02-3827-4. xv + 907 pp. LCCN QA297 .R37 1999.

Niederreiter:1999:MCQ

[4214] Harald Niederreiter and Jerome Spanier, editors. *Monte Carlo and quasi-Monte Carlo methods, 1998: proceedings of a conference held at the Claremont Graduate University, Claremont, California, USA, June 22–26, 1998*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 1999. ISBN 3-540-66176-X (softcover). LCCN Q183.9 .M672 1999. URL `http://www.loc.gov/catdir/enhancements/fy0815/99047502-d.html`.

USENIX:1999:UAT

[4215] USENIX, editor. *Usenix Annual Technical Conference. June 6–11, 1999. Monterey, California, USA*. USENIX, Berkeley, CA, USA, 1999. ISBN 1-880446-33-2. LCCN QA76.8.U65 U84 1999. URL `http://db.usenix.org/publications/library/proceedings/usenix99`.

ACM:2000:PTS

[4216] ACM, editor. *Proceedings of the thirty second annual ACM Symposium on Theory of Computing: Portland, Oregon, May 21–23, [2000]*. ACM Press, New York, NY 10036, USA, 2000. ISBN 1-58113-184-4. LCCN QA76.6 .A13 2000. ACM order number 508000.

Davies:2000:MPC

[4217] Jim Davies, A. W. Roscoe, and Jim Woodcock, editors. *Millennial perspectives in computer science: proceedings of the 1999 Oxford–Microsoft Symposium in honour of Professor Sir Antony Hoare*. Palgrave, Basingstoke, UK, 2000. ISBN 0-333-92230-1. LCCN QA75.5 .O8 2000.

Heys:2000:SAC

[4218] Howard Heys and Carlisle Adams, editors. *Selected areas in cryptography: 6th annual international workshop, SAC'99, Kingston, Ontario, Canada, August 9–10, 1999: proceedings*, volume 1758 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2000. ISBN 3-540-67185-4. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA267.A1 L43 no.1758.

IEEE:2000:ASF

[4219] IEEE, editor. *41st Annual Symposium on Foundations of Computer Science: proceedings: 12–14 November, 2000, Redondo Beach, California*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2000. CODEN ASFPDV. ISBN 0-7695-0850-2, 0-7695-0851-0 (case), 0-7695-0852-9 (microfiche). ISSN 0272-5428. LCCN TK7885.A1 S92 2000. IEEE Computer Society Order Number PR00850.

Joines:2000:WSC

[4220] Jeffrey A. Joines, R. R. Barton, K. Kang, and P. A. Fishwick, editors. *2000 Winter Simulation Conference proceedings: Wyndham Palace Resort and Spa, Orlando, FL, USA, 10–13 December, 2000*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2000. ISBN 0-7803-6579-8 (softcover), 0-7803-6580-1 (casebound), 0-7803-6581-X (microfiche). LCCN QA76.9.C65 W568 2000. IEEE Catalog Number 00CH37165.

NIST:2000:TAE

[4221] NIST, editor. *The Third Advanced Encryption Standard Candidate Conference, April 13–14, 2000, New York, NY, USA*. National Institute for Standards and Technology, Gaithersburg, MD, USA, 2000. ISBN ???? LCCN ???? URL `http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-2.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-3.pdf`; `http://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf`.

Gass:2001:EOR

[4222] Saul I. Gass and Carl M. Harris, editors. *Encyclopedia of Operations Research and Management Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2001. ISBN 0-7923-7827-X. xxxviii + 917 pp. LCCN T57.6. E53 2000. URL `http://www.loc.gov/catdir/enhancements/fy1004/00025363-d.htm`.

IEEE:2001:ISF

[4223] IEEE, editor. *42nd IEEE Symposium on Foundations of Computer Science: proceedings: October 14–17, 2001, Las Vegas, Nevada, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2001. CODEN ASFPDV. ISBN 0-7695-1390-5, 0-7695-1391-3 (case), 0-7695-1392-1 (microfiche). ISSN 0272-5428. LCCN TK7885 .I61 2001. IEEE Computer Society order number PR01390.

Koc:2001:CHEa

[4224] Çetin K. Koç and Christof Paar, editors. *Cryptographic hardware and embedded systems — CHES 2000: Second International Workshop, Worcester, MA, USA, August 17–18, 2000: Proceedings*, volume 1965 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2001. CODEN LNCSD9. ISBN 3-540-41455-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.E42 C454 2000. URL `http://link.springer-ny.com/link/service/series/0558/tocs/t1965.htm`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=1965`.

Peters:2001:WPW

[4225] Brett A. Peters, J. S. Smith, D. J. Medeiros, and M. W. Rohrer, editors. *WSC'01: Proceedings of the 2001 Winter Simulation Conference: a Simulation Odyssey, Crystal Gateway Marriott, Arlington, VA, USA, 9–12*

December 2001. ACM Press, New York, NY 10036, USA, 2001. ISBN 0-7803-7307-3 (paperback), 0-7803-7308-1 (microfiche), 0-7803-7309-X. LCCN QA76.5 .W56 2001. IEEE catalog number 01CH37304.

Schueller:2001:MCS

[4226] Gerhart I. Schuëller and Pol D. Spanos, editors. *Monte Carlo Simulation: Proceedings of the International Conference on Monte Carlo Simulation (MCS 2000), Monte Carlo, Monaco, 18–21 June, 2001*. A. A. Balkema Publishers, Amsterdam, The Netherlands, 2001. ISBN 90-5809-188-0. LCCN QC20.7.M65.I584 2000. Contributions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Smelser:2001:IES

[4227] Neil J. Smelser and Paul B. Baltes, editors. *International encyclopedia of the social and behavioral sciences*. Elsevier, Amsterdam, The Netherlands, 2001. ISBN 0-08-043076-7 (set). lxxxvi + 16695 + 588 + 898 (26 volumes) pp. LCCN H41 .I58 2001. URL `http://www.loc.gov/catdir/enhancements/fy0612/2001044791-d.html`.

Spector:2001:GPG

[4228] Lee Spector, Erik D. Goodman, Annie Wu, W. B. Langdon, Hans-Michael Voigt, Mitsuo Gen, Sandip Sen, Marco Dorigo, Shahram Pezeshk, Max H. Garzon, and Edmund Burke, editors. *GECCO-2001: proceedings of the Genetic and Evolutionary Computation Conference: a joint meeting of the Sixth Annual Genetic Programming Conference (GP-2001) and the Tenth International Conference on Genetic Algorithms (ICGA-2001), July 7–11, 2001, San Francisco, California*. Morgan Kaufmann Publishers, San Francisco, CA, USA, 2001. ISBN 1-55860-774-9. LCCN QA76.623 .G46 2001.

ACM:2002:PTF

[4229] ACM, editor. *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing, Montréal, Québec, Canada, May 19–21, 2002*. ACM Press, New York, NY 10036, USA, 2002. ISBN 1-58113-495-9. LCCN QA75.5 .A22 2002. ACM order number 508020.

Dror:2002:MUE

[4230] Moshe Dror, Pierre L'Ecuyer, and Ferenc Szidarovszky, editors. *Modeling uncertainty: an examination of stochastic theory, methods, and applications*, volume 46 of *International series in operations research and management science*. Kluwer Academic Publishers, Norwell, MA, USA, and Dordrecht, The Netherlands, 2002. ISBN 0-7923-7463-0. xxviii

+ 770 pp. LCCN QA274.2 .M63 2002. URL http://www.loc.gov/catdir/enhancements/fy0820/2001050485-d.html; http://www.loc.gov/catdir/enhancements/fy0820/2001050485-t.html.

Fang:2002:MCQ

[4231] Kaitai Fang, Fred J. Hickernell, and Harald Niederreiter, editors. *Monte Carlo and quasi-Monte Carlo methods 2000: proceedings of a conference held at Hong Kong Baptist University, Hong Kong SAR, China, November 27–December 1, 2000*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2002. ISBN 3-540-42718-X (paperback). LCCN Q183.9 .M674 2002. URL http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.html.

USENIX:2002:PBF

[4232] USENIX, editor. *Proceedings of BSDCon 2002: February 11–14, 2002, Cathedral Hill Hotel, San Francisco, CA*. USENIX, Berkeley, CA, USA, 2002. ISBN 1-880446-02-2. LCCN QA76.76.O63 B736 2002. URL http://www.usenix.org/publications/library/proceedings/bsdcon02/tech.html.

Rudnicki:2003:OIP

[4233] Marek Rudnicki and Sławomir Wiak, editors. *Optimization and Inverse Problems in Electromagnetism*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2003. ISBN 1-4020-1506-2, 90-481-6375-7 (print), 94-017-2494-6 (e-book). xxii + 336 + 227 pp. LCCN QA76.9.M35; T57-57.97. URL http://www.springerlink.com/content/978-94-017-2494-4.

ACM:2004:PAA

[4234] ACM, editor. *Proceedings of the 36th Annual ACM Symposium on the Theory of Computing: Chicago, Illinois, USA, June 13–15, 2004*. ACM Press, New York, NY 10036, USA, 2004. ISBN 1-58113-852-0. LCCN QA75.5 .A22 2004.

Gentle:2004:HCS

[4235] James E. Gentle, Wolfgang Härdle, and Yuichi Mori, editors. *Handbook of computational statistics: concepts and methods*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 3-540-40464-3. xii + 1070 pp. LCCN QA276.4 .H36 2004. URL http://www.loc.gov/catdir/enhancements/fy0817/2004106523-d.html; http://www.loc.gov/catdir/enhancements/fy0817/2004106523-t.html.

Niederreiter:2004:MCQ

[4236] Harald Niederreiter, editor. *Monte Carlo and quasi-Monte Carlo methods 2002: proceedings of a conference held at the National University of Singapore, Republic of Singapore, November 25–28, 2002*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2004. ISBN 3-540-20466-0 (softcover). LCCN Q183.9 .I526 2002. URL `http://www.loc.gov/catdir/enhancements/fy0817/2004041328-d.html`.

Peitgen:2004:CFN

[4237] Heinz-Otto Peitgen, H. (Hartmut) Jürgens, and Dietmar Saupe. *Chaos and fractals: new frontiers of science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2004. ISBN 0-387-20229-3. xiii + 864 pp. LCCN Q172.5.C45 P45 2004. URL `http://www.loc.gov/catdir/enhancements/fy0818/2003063341-d.html`; `http://www.loc.gov/catdir/enhancements/fy0818/2003063341-t.html`.

Teugels:2004:EAS

[4238] Jozef L. Teugels and Bjørn Sundt, editors. *Encyclopedia of Actuarial Science*. Wiley, New York, NY, USA, 2004. ISBN 0-470-84676-3 (hardcover). xxxiv + 1842 pp. LCCN HG8781 .E47 2004. URL `http://www.loc.gov/catdir/description/wiley042/2004014696.html`; `http://www.loc.gov/catdir/toc/ecip0419/2004014696.html`. Three volumes.

ACM:2005:SPA

[4239] ACM, editor. *STOC '05: proceedings of the 37th Annual ACM Symposium on Theory of Computing: Baltimore, Maryland, USA, May 22–24, 2005*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-58113-960-8. LCCN QA75.5 A22 2005.

Armitage:2005:EB

[4240] Peter Armitage and Theodore Colton, editors. *Encyclopedia of biostatistics*. Wiley, New York, NY, USA, second edition, 2005. ISBN 0-470-01181-5 (e-book), 0-470-84907-X (hardcover). lxxxiv + 6022 (8 volumes) pp. LCCN QH323.5 .E53 2005. URL `http://mrw.interscience.wiley.com/emrw/9780470011812/home/`; `http://onlinelibrary.wiley.com/book/10.1002/0470011815`.

Beyer:2005:GEC

[4241] Hans-Georg Beyer et al., editors. *Genetic and Evolutionary Computation Conference: GECCO 2005, June 25–29, 2005 (Saturday-Wednesday) Washington, D.C., USA*. ACM Press, New York, NY 10036, USA, 2005.

ISBN 1-59593-010-8 (paperback). LCCN QA76.623 .G44 2005. ACM order number 910050.

Helleseth:2005:STA

[4242] Tor Helleseth, Dilip Sarwate, Hong-Yeop Song, and Kyeongcheol Yang, editors. *Sequences and their applications: SETA 2004: third international conference, Seoul, Korea, October 24–28, 2004. Revised selected papers*, volume 3486 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-26084-6 (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA292 .S48 2004. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3486`; `http://www.springerlink.com/openurl.asp?genre=volume&id=doi:10.1007/b136167`.

Meadows:2005:CPA

[4243] Catherine Meadows and Paul Syverson, editors. *CCS '05: proceedings of the 12th ACM Conference on Computer and Communications Security: November 7–11, 2005, Alexandria, Virginia, USA*. ACM Press, New York, NY 10036, USA, 2005. ISBN 1-59593-226-7. LCCN QA76.9.A25. ACM order number 459050.

Smart:2005:CCI

[4244] Nigel P. Smart, editor. *Cryptography and Coding: 10th IMA international Conference, Cirencester, UK, December 19–21, 2005. Proceedings*, volume 3796 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2005. CODEN LNCSD9. ISBN 3-540-30276-X (softcover). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL `http://www.springerlink.com/content/978-3-540-30276-6`; `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=3796`.

Henderson:2006:S

[4245] Shane G. Henderson and Barry L. Nelson, editors. *Simulation*, volume 13 of *Handbooks in operations research and management science*. Elsevier, Amsterdam, The Netherlands, 2006. ISBN 0-444-51428-7. xiii + 678 pp. LCCN HG176.7 .F56 2008.

Niederreiter:2006:MCQ

[4246] Harald Niederreiter and D. (Denis) Talay, editors. *Monte Carlo and Quasi-Monte Carlo methods 2004*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-

540-25541-9. LCCN Q183.9 .I526 2004. URL `http://www.loc.gov/catdir/enhancements/fy0663/2005930449-d.html`; `http://www.loc.gov/catdir/toc/fy0614/2005930449.html`.

Schroeder:2006:NTS

[4247] Manfred Robert Schroeder. *Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information, Computing, and Self-Similarity*, volume 7 of *Springer Series in Information Sciences*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., fourth edition, 2006. ISBN 3-540-26598-8, 3-540-26596-1. ISSN 0720-678X. xxvi + 367 pp. LCCN QA241.

Ytrehus:2006:CCI

[4248] Øyvind Ytrehus, editor. *Coding and Cryptography: International Workshop, WCC 2005, Bergen, Norway, March 14–18, 2005. Revised Selected Papers*, volume 3969 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2006. ISBN 3-540-35481-6. LCCN QA76.9.A25 I557 2005.

ACM:2007:SPA

[4249] ACM, editor. *STOC '07: proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11–13, 2007*. ACM Press, New York, NY 10036, USA, 2007. ISBN 1-59593-631-9. LCCN QA75.5 .A22 2007.

Adams:2007:SAC

[4250] Carlisle Adams, Ali Miri, and Michael Wiener, editors. *Selected areas in cryptography: 14th international workshop, SAC 2007, Ottawa, Canada, August 16–17, 2007; revised selected papers*, volume 4876 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-77360-6, 3-540-77359-2. ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 S22 2007eb.

Altiok:2007:SMA

[4251] Tayfur Altiok and Benjamin Melamed. *Simulation Modeling and Analysis with ARENA*. Elsevier, Amsterdam, The Netherlands, 2007. ISBN 0-12-370523-1 (hardcover), 0-12-374246-3. xxi + 440 pp. LCCN QA298.

Menezes:2007:ACC

[4252] A. J. (Alfred J.) Menezes, editor. *Advances in cryptology — CRYPTO 2007: 27th Annual International Cryptology Conference,*

Santa Barbara, CA, USA, August 19–23, 2007: proceedings, volume 4622 of *Lecture notes in computer science, 0302-9743*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2007. ISBN 3-540-74142-9 (paperback). LCCN QA76.9.A25 C79 2007. URL `http://www.springerlink.com/openurl.asp?genre=issue&issn=0302-9743&volume=4622`.

Simos:2007:CMS

[4253] Theodore E. Simos and George Maroulis, editors. *Computation in Modern Science and Engineering: Proceedings of the [Fifth] International Conference on Computational Methods in Science and Engineering 2007 (ICCMSE 2007), Corfu, Greece, 25–30 September 2007*, volume 2A, 2B of *AIP Conference Proceedings (#963)*. American Institute of Physics, Woodbury, NY, USA, 2007. ISBN 0-7354-0476-3 (set), 0-7354-0477-1 (vol. 1), 0-7354-0478-X (vol. 2). ISSN 0094-243X (print), 1551-7616 (electronic), 1935-0465. LCCN Q183.9 .I524 2007. URL `http://www.springer.com/physics/atoms/book/978-0-7354-0478-6`.

ACM:2008:SPA

[4254] ACM, editor. *STOC '08: proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17–20, 2008*. ACM Press, New York, NY 10036, USA, 2008. ISBN 1-60558-047-3. LCCN QA76.6 .A152 2008.

Golomb:2008:STA

[4255] Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors. *Sequences and their applications — SETA 2008: 5th international conference, Lexington, KY, USA, September 14–18, 2008: proceedings*, volume 5203 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-85912-8, 3-540-85911-X. LCCN QA292 .S48 2008eb.

IEEE:2008:ICA

[4256] IEEE, editor. *2008 International Conference on Application-Specific Systems, Architectures and Processors: Leuven, Belgium, 2–4 July 2008*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2008. ISBN 1-4244-1897-6 (paperback), 1-4244-1898-4. LCCN ???? URL `http://ieeexplore.ieee.org/servlet/opac?punumber=4569858`; `http://www.gbv.de/dms/tib-ub-hannover/631855815.pdf`. IEEE catalog number CFP08063-PRT.

Keller:2008:MCQ

[4257] Alexander Keller, Stefan Heinrich, and Harald Niederreiter, editors. *Monte Carlo and Quasi-Monte Carlo methods 2006*. Springer-Ver-

lag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-74495-9 (paperback), 3-540-74496-7. LCCN Q183.9 .I526 2006. URL `http://catdir.loc.gov/catdir/toc/fy0803/2007936240.htm`.

Nguyen:2008:GG

[4258] Hubert Nguyen, editor. *GPU gems 3*. Addison-Wesley, Reading, MA, USA, 2008. ISBN 0-321-51526-9. l + 942 pp. LCCN T385 .G6882 2008. URL `http://www.loc.gov/catdir/toc/ecip0720/2007023985.html`.

Robshaw:2008:NSC

[4259] Matt J. B. Robshaw and Olivier Billet, editors. *New Stream Cipher Designs: The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 3-540-68350-X (paperback), 3-540-68351-8 (e-book). viii + 295 pp. LCCN QA76.9.A25 N486 2008.

Rousseau:2008:MT

[4260] Christiane Rousseau and Yvan Saint-Aubin, editors. *Mathematics and Technology*. Springer Undergraduate Texts in Mathematics and Technology. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-69216-9. ISSN 1867-5506. 300 pp. LCCN QA37.3.R6814 2008.

Saint-Aubin:2008:MT

[4261] Yvan Saint-Aubin and Christiane Rousseau, editors. *Mathematics and Technology*. Springer Undergraduate Texts in Mathematics and Technology. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2008. ISBN 0-387-69216-9. ISSN 1867-5506. 300 pp. LCCN QA37.3.R6814 2008.

Alexopoulos:2009:AFS

[4262] Christos Alexopoulos, David Goldsman, and James R. Wilson, editors. *Advancing the frontiers of simulation: a Festschrift in honor of George Samuel Fishman*, volume 133 of *International series in operations research and management science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 1-4419-0816-1 (hardcover). xii + 329 pp. LCCN QA76.9.C65 A383 2009.

Belsley:2009:HCE

[4263] David A. Belsley and Erricos John Kontoghiorghes, editors. *Handbook of Computational Econometrics*. Wiley, New York, NY, USA, 2009. ISBN 0-470-74385-9. xviii + 496 pp. LCCN HB143.5 .H357

2009. URL http://catalogimages.wiley.com/images/db/jimages/9780470743850.jpg; http://www.loc.gov/catdir/enhancements/fy0913/2009025907-d.html; http://www.loc.gov/catdir/enhancements/fy0913/2009025907-t.html.

Clavier:2009:CHE

[4264] Christophe Clavier and Kris Gaj, editors. *Cryptographic Hardware and Embedded Systems — CHES 2009: 11th International Workshop Lausanne, Switzerland, September 6–9, 2009 Proceedings*, volume 5747 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. CODEN LNCSD9. ISBN 3-642-04137-X (print), 3-642-04138-8 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN ???? URL http://www.springerlink.com/content/978-3-642-04138-9.

LEcuyer:2009:MCQ

[4265] Pierre L'Ecuyer and Art B. Owen, editors. *Monte Carlo and Quasi-Monte Carlo Methods 2008*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2009. ISBN 3-642-04106-X, 3-642-04107-8 (e-book). LCCN Q183.9 .I526 2008.

Paredaens:2009:PTE

[4266] Jan Paredaens and Jianwen Su, editors. *Proceedings of the twenty-eighth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, PODS'09, Providence, Rhode Island, June 29–July 1, 2009*. ACM Press, New York, NY 10036, USA, 2009. ISBN 1-60558-553-X. LCCN ????

ACM:2010:PAI

[4267] ACM, editor. *Proceedings of the 2010 ACM International Symposium on Theory of Computing: June 5–8, 2010, Cambridge, MA, USA*. ACM Press, New York, NY 10036, USA, 2010. ISBN 1-60558-817-2. LCCN QA 76.6 .A152 2010. URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Anonymous:2010:NDS

[4268] Anonymous, editor. *17th Annual Network and Distributed System Symposium, NDSS '10, The Dana on Misson Bay, San Diego, California. February 28–March 3, 2010*. Internet Society, Reston, VA, USA, 2010. ISBN 1-891562-29-0, 1-891562-30-4. LCCN ???? URL http://www.isoc.org/isoc/conferences/ndss/10/proceedings.shtml.

Cont:2010:EQF

[4269] Rama Cont, editor. *Encyclopedia of quantitative finance*. Wiley, New York, NY, USA, 2010. ISBN 0-470-06160-X, 0-470-05756-4. xlv + 2037 pp. LCCN HG106 .E53 2010. Four volumes.

Dick:2010:DNS

[4270] J. (Josef) Dick and Friedrich Pillichshammer. *Digital nets and sequences: discrepancy and quasi-Monte Carlo integration*. Cambridge University Press, Cambridge, UK, 2010. ISBN 0-521-19159-9 (hardback). xvii + 600 pp. LCCN QA298 .D53 2010. URL `http://assets.cambridge.org/97805211/91593/cover/9780521191593.jpg`.

Feldman:2010:APS

[4271] Richard M. Feldman and Ciriaco Valdez-Flores. *Applied probability and stochastic processes*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2010. ISBN 3-642-05155-3, 3-642-05158-8. xv + 397 pp. LCCN QA274 .F45 2010. URL `http://swbplus.bsz-bw.de/bsz314370110inh.htm`; `http://swbplus.bsz-bw.de/bsz314370110kap.htm`; `http://swbplus.bsz-bw.de/bsz314370110vor.htm`; `http://www.gbv.de/dms/zbw/609423665.pdf`.

Gollmann:2010:SCR

[4272] Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors. *Smart card research and advanced application: 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14–16, 2010: proceedings*, volume 6035 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-12509-3 (paperback). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN TK7895.S62 C36 2010.

IEEE:2010:ISV

[4273] IEEE, editor. *2010 IEEE Symposium on VLSI Circuits, Honolulu, HI, June 16–18, 2010*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 1-4244-5454-9. LCCN ????

IEEE:2010:PIA

[4274] IEEE, editor. *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science: 23–26 October 2010, Las Vegas, Nevada, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2010. ISBN 0-7695-4244-1, 1-4244-8525-8. ISSN 0272-5428. LCCN QA76 .S95

2010. URL http://opac.ieeecomputersociety.org/opac?year=2010&volume=00&catalog=4244&acronym=focs. IEEE Computer Society order number P4244.

Peterson:2010:IEE

[4275] Penelope L. Peterson, Eva (Eva Lee) Baker, and Barry MacGaw, editors. *International Encyclopedia of Education*. Science direct. Elsevier, Amsterdam, The Netherlands, third edition, 2010. ISBN 0-08-044894-1 (e-book), 0-08-044893-3 (set), 0-08-044895-X (vol. 1), 0-08-044896-8 (vol. 2), 0-08-044897-6 (vol. 3), 0-08-044898-4 (vol. 4), 0-08-044899-2 (vol. 5), 0-08-044900-X (vol. 6), 0-08-044901-8 (vol. 7), 0-08-044902-6 (vol. 8). ???? pp. LCCN LB15 .I569 2010. URL http://sfx.metabib.ch/sfx_locater?sid=ALEPH:DSV01\%26isbn=0-08-044894-1. Eight volumes.

ACM:2011:PAI

[4276] ACM, editor. *Proceedings of the 2011 ACM International Symposium on Theory of Computing: June 6–8, 2011, San Jose, CA, USA*. ACM Press, New York, NY 10036, USA, 2011. ISBN ???? LCCN ???? URL http://www.gbv.de/dms/tib-ub-hannover/63314455x..

Gilli:2011:NMO

[4277] Manfred Gilli, Dietmar Maringer, and Enrico Schumann, editors. *Numerical Methods and Optimization in Finance*. Elsevier Academic Press, Amsterdam, The Netherlands, 2011. ISBN 0-12-375662-6. xv + 584 pp. LCCN HG106 .G55 2011.

Hwu:2011:GCG

[4278] Wen mei Hwu, editor. *GPU computing gems*. Elsevier, Amsterdam, The Netherlands, emerald edition, 2011. ISBN 0-12-384988-8. xx + 865 pp. LCCN T385 .G6875 2011.

IEEE:2011:ICI

[4279] IEEE, editor. *International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011: 28–29 March 2011, Shenzhen, Guangdong, China; proceedings*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 0-7695-4353-7, 1-61284-289-5. LCCN ???? URL http://ieeexplore.ieee.org/servlet/opac?punumber=5750113.

Lathrop:2011:SPI

[4280] Scott Lathrop, Jim Costa, and William Kramer, editors. *SC'11: Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis, Seattle, WA, November 12–18 2011*.

ACM Press and IEEE Computer Society Press, New York, NY 10036, USA and 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2011. ISBN 1-4503-0771-X. LCCN ????

Lovric:2011:IES

[4281] Miodrag Lovric, editor. *International Encyclopedia of Statistical Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2011. ISBN 3-642-04898-6. lvii + 1673 pp. LCCN QA276.14 .I58 2011.

vanTilborg:2011:ECS

[4282] Henk C. A. van Tilborg and Sushil Jajodia, editors. *Encyclopedia of Cryptography and Security*. Springer reference. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2011. ISBN 1-4419-5905-X (print), 1-4419-5906-8 (e-book). xl + 1416 pp. LCCN QA76.9.A25 E53 2011.

ACM:2012:SPA

[4283] ACM, editor. *STOC'12: Proceedings of the 2012 ACM International Symposium on Theory of Computing: May 19–22, 2012, New York, NY, USA*. ACM Press, New York, NY 10036, USA, 2012. ISBN 1-4503-1245-4. LCCN ???? URL `http://www.gbv.de/dms/tib-ub-hannover/63314455x.`.

Cooper:2012:HWC

[4284] S. Barry Cooper, Anuj Dawar, and Benedikt Löwe, editors. *How the World Computes: Turing Centenary Conference and 8th Conference on Computability in Europe, CiE 2012, Cambridge, UK, June 18–23, 2012. Proceedings*, volume 7318 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2012. ISBN 3-642-30869-4. LCCN ????

Dunn:2012:EMC

[4285] William L. (William Lee) Dunn and J. Kenneth Shultis, editors. *Exploring Monte Carlo methods*. Elsevier Academic Press, Amsterdam, The Netherlands, 2012. ISBN 0-444-51575-5 (hardcover). xvi + 384 pp. LCCN QA298 .D86 2012. URL `http://www.loc.gov/catdir/enhancements/fy1116/2010050137-d.html`.

Dyson:2012:TCO

[4286] George Dyson. *Turing's cathedral: the origins of the digital universe*. Pantheon Books, New York, NY, USA, 2012. ISBN 0-375-42277-3 (hardcover). xxii + 401 pp. LCCN QA76.17 .D97 2012.

Gentle:2012:HCS

[4287] James E. Gentle, Wolfgang Karl Härdle, and Yuichi Mori, editors. *Handbook of Computational Statistics: Concepts and Methods*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., second edition, 2012. ISBN 3-642-21550-5 (print), 3-642-21551-3 (e-book). xii + 1070 pp. LCCN QA276.4 .H36 2012. URL `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-b.html`; `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-d.html`; `http://www.loc.gov/catdir/enhancements/fy1316/2012938637-t.html`.

Hwu:2012:GCG

[4288] Wen mei Hwu, editor. *GPU computing gems*. Applications of GPU computing series. Morgan Kaufmann, Boston, MA, jade edition, 2012. ISBN 0-12-385963-8 (hardback). xvi + 541 + 16 pp. LCCN T385 .G6875 2012.

IEEE:2012:PIA

[4289] IEEE, editor. *Proceedings of the 2012 IEEE 52nd Annual Symposium on Foundations of Computer Science: 20–23 October 2012, Hyatt Regency, New Brunswick, New Jersey, USA*. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2012. ISBN 1-4673-4383-8. ISSN 0272-5428. LCCN QA76 .S95 2012. URL `http://dimacs.rutgers.edu/FOCS12/`; `http://theory.stanford.edu/~tim/focs12/`. IEEE Computer Society order number P????.

ACM:2013:SPF

[4290] ACM, editor. *STOC '13: Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing: June 1–4, 2013, Palo Alto, California, USA*. ACM Press, New York, NY 10036, USA, 2013. ISBN 1-4503-2029-5.

Bailey:2013:CAM

[4291] David H. Bailey, Heinz H. Bauschke, Peter Borwein, Frank Garvan, Michel Théra, Jon D. Vanderwerff, and Henry Wolkowicz, editors. *Computational and analytical mathematics: in honor of Jonathan Borwein's 60th Birthday*, volume 50 of *Springer proceedings in mathematics and statistics*. Springer, New York, NY, USA, 2013. ISBN 1-4614-7620-8, 1-4614-7621-6 (e-book). ISSN 2194-1009. xv + 701 pp. LCCN QA241. URL `http://public.eblib.com/choice/publicfullrecord.aspx?p=1466708`; `http://swb.eblib.com/patron/FullRecord.aspx?p=1466708`; `http://www.myilibrary.com?id=547562`.

Higham:2015:PCA

[4292] Nicholas J. Higham, Mark R. Dennis, Paul Glendinning, Paul A. Martin, Fadil Santosa, and Jared Tanner, editors. *The Princeton Companion to Applied Mathematics*. Princeton University Press, Princeton, NJ, USA, 2015. ISBN 0-691-15039-7 (hardcover). 994 (est.) pp. LCCN QA155 .P75 2015.

Osais:2017:CSF

[4293] Yahya E. Osais. *Computer Simulation: a Foundational Approach Using Python*, volume 101 of *Chapman and Hall/CRC computer and information science series*. Chapman and Hall/CRC, Boca Raton, FL, USA, 2017. ISBN 1-315-12029-1 (e-book), 1-351-63708-8 (e-book: Mobi), 1-4987-2682-8 (hardcover), 1-4987-2683-6 (e-book PDF). LCCN QA76.9.C65 O83 2017.

Rubinstein:2017:SMC

[4294] Reuven Y. Rubinstein and Dirk P. Kroese. *Simulation and the Monte Carlo Method*, volume 10 of *New York Academy of Sciences Series*. Wiley, New York, NY, USA, third edition, 2017. ISBN 1-118-63216-8 (hardcover), 978-111-863-2-2-0-8(PDF e-book), 1-118-63228-1 (Mobipocket e-book), 1-118-63238-9 (ePub e-book). xvii + 414 pp. LCCN QA298.R835 2017.

Krzhizhanovskaya:2020:CSI

[4295] Valeria V. Krzhizhanovskaya, Gábor Závodszky, Michael H. Lees, Jack J. Dongarra, Peter M. A. Sloot, Sérgio Brissos, and João Teixeira, editors. *Computational Science — ICCS 2020 20th International Conference, Amsterdam, The Netherlands, June 3–5, 2020, Proceedings, Part II*, volume 12138 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2020. ISBN 3-030-50416-6, 3-030-50417-4 (e-book). ISSN 0302-9743 (print), 1611-3349 (electronic). URL `https://link.springer.com/book/10.1007/978-3-030-50417-5`.