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
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

05 August 2024
Version 1.393

Title word cross-reference

#14 [2315]. #15949 [892]. #4059 [1266]. #8373 [2137].

(0, 1) [1077]. (0, s) [2578, 2979]. (a^n – 1)/(a – 1) [939]. (j, c) [746]. (n^2 alpha) [2529]. (n^k alpha) [2530]. (nalpha) [2529]. (t, m, s) [2081, 2936, 2087, 2388]. (t, s) [2674, 2081, 2379, 2936, 2087]. (X, Y) [3695]. (X^2 – Y^2)^1/2 [499].
\[ \frac{a \pm j^2}{x^{\frac{a}{m}} (j + \tau)^2} \equiv 32 \mod 1 \]
0.57pJ [3314]. 0.57pJ/bit [3314]. '05 [4159, 4163]. '07 [4169]. '08 [4174].


5.0 [1668]. 5.2 [2800]. 500 [3367, 322]. 51st [4193]. 52 [892]. 52nd [4208]. 5th [4175].

6 [3685]. 60th [4210]. 61 [1255]. 623-dimensionally [2373]. 64-bit
4


9th [4191]. = [4010, 4021].

Black [2900]. Black-Box [2900]. Block [2595, 1291, 2532, 2942, 3271, 2766, 1629, 3192]. Blockcipher [2681].

Combinatorial [634, 3672, 203, 2366, 1555, 2127, 238, 3511, 770].
Combinatorialics [4070, 2762].
Combiner [2394].
Combiners [1746].
combinés [2647].
Combination [947, 2242, 1107, 1108, 1109, 3080, 2099, 427, 2410, 3269, 2281, 1654, 1248, 2886].
Combinations [398, 515, 484, 368, 1801, 1116, 2844, 447, 448, 62].
Combined [398, 515, 484, 368, 1801, 1116, 2844, 447, 448, 62].
Combining [903, 904, 1604, 3257, 2585, 3133, 3729].
Comment [295, 1601, 170, 2579, 860, 1066, 956, 1032, 1625, 959, 866, 964, 2926, 965, 869, 2629, 972, 883, 876].
Commentary [2180].
Comments [2821, 3118, 1150, 721, 786, 601, 1771].
Commitment [1553, 1645].
Commodore [1144].
Common [1208, 3904, 511, 1287, 1727, 3075, 1751, 1567, 808, 2171, 1119, 3634, 1856, 1085, 750, 3594, 2570, 2240, 1114, 1720, 911, 774, 729, 917, 1362, 2438, 1855, 2082, 940, 1476, 1672].
Commun [2048, 2170].
Communicating [1310].
Communication [584, 4167, 1310, 1327, 2491, 2833, 3521].
Communications [505, 4163, 4092, 2741].
Comp [2137].
Compact [2011, 2811, 3039, 3105, 1413, 2509, 3072, 600].
Comparative [1337, 401, 502, 3529, 2112].
Comparing [1223, 911, 1827, 2178, 3340].
Comparison [669, 578, 1054, 3245, 3838, 3681, 1727, 3165, 2079, 204, 2290, 610, 1081, 700, 2205, 2799, 1672, 1485, 1684, 1493, 591, 592, 1721, 2923, 2519, 3317, 2738, 462, 809].
Comparisons [1855, 2082, 1476, 1397, 1751, 1856].
compatibility [3663].
Compatible [1514, 1544, 3612].
Competing [186].
compiled [70].
Complete [1291, 1015, 3113, 935, 2398, 2823, 2823].
Completed [953].
Compete [1906, 2696, 3015, 3014, 3016].
Component [2696, 3015, 3014, 3016].
components [2773].
Composite [3246, 30, 2696, 871, 1574, 2103, 3203, 2146, 1700, 1443, 2102, 1869].
Composited [3811].
Composition [1934, 2208, 3708, 1238, 846].
Composition-Alias [2208].
Compound [1270, 2420, 1915, 2039, 2153, 2154, 2247, 2249, 2332, 2949, 3483, 1803, 2038, 2248, 2157, 2158, 2608, 2927, 2621, 80, 2223].
compressed [2077].
compression [4070].
Compromise [3104, 3008].
Compromised [3720, 3836].
COMPSTAT [4059].
Comptes [4010].
Compton [377].
Comput [2048, 1066, 2170].
Computability [4203, 2454, 3301].
Computable [3828].
Computation [4005, 3830, 4161, 4089, 2141, 2900, 1699, 854, 30, 142, 4198, 330, 1946, 4106,
3998, 4091, 2086, 2089, 3850, 4148, 3228, 941, 4007, 3860, 1262, 2413, 1900, 2590, 2507, 2994, 3986, 1852, 1757, 1990, 890, 4173.

Computational
[4210, 4182, 2573, 948, 4206, 2453, 2709, 4074, 344, 3915, 4173, 424, 3790, 2897, 1059, 4059, 3902, 4155, 1515, 557, 1738, 4214].

Computationally
[4083, 3971, 4062].

Computations
[1150, 413, 1168, 3733, 700, 2546, 2133, 2410, 2490, 724, 1430, 1371, 159, 1559].

compute
[2775].

Computer
[576, 670, 986, 1017, 892, 752, 893, 894, 895, 542, 4044, 2749, 1329, 3599, 1154, 4031, 505, 1513, 244, 413, 4024, 4034, 4037, 4040, 4055, 4060, 4066, 4072, 4082, 4105, 4114, 4118, 4139, 4143, 4193, 4208, 1170, 1171, 865, 776, 825, 867, 1535, 729, 1951, 827, 1373, 601, 337, 359, 1037, 4163, 4046, 1079, 4016, 3635, 4212, 1563, 1081, 4038, 4093, 1467, 1086, 3780, 2544, 1659, 4095, 887, 888, 4026, 1139, 712, 428, 539, 1261, 1682, 850, 1263, 759, 1023, 4137, 3132, 990, 991, 472, 994, 761, 762, 764, 2430, 4125, 1006, 1034, 2065, 1237, 1961, 311].

computer
[385, 1124, 454, 830, 1241, 615, 227, 1040, 4025, 1189, 1985, 3644, 1771, 374, 1309, 846, 2430, 4036].

Computes
[4203].

Computing
[4042, 4047, 4052, 4058, 4063, 4068, 4079, 4097, 4102, 4111, 4129, 4136, 4149, 4154, 4159, 4169, 4174, 4186, 4195, 4202, 4209, 2817, 892, 3040, 2970, 375, 467, 3365, 678, 152, 1800, 1812, 953, 2429, 2499, 1287, 960, 4199, 3174, 119, 1038, 1765, 2801, 4167, 3555, 4094, 3566, 4062, 2558, 212, 3243, 2756, 2166, 4197, 4207, 118, 1119, 96, 129, 3394, 2853, 3738, 3183, 4092, 4107, 1587, 139, 4061].

column [469].

Concept [384, 386, 37]. conception [1580].

Conceptual
[3466, 3984].

Concerning [355, 80, 2765, 188]. concert [3019].

Conclusion
[3273, 2449].

Concrete
[2019, 3244, 2947, 2134].

Conditional
[2074, 2075, 2449, 3187]. conditionally [3570]. conditions [2023]. cone [2548].

Conference
[4110, 4057, 4103, 4116, 4011, 4064, 4130, 4069, 4161, 4112, 4203, 4076, 4191, 4050, 4176, 4198, 4140, 4214, 4199, 4067, 4163, 4126, 4172, 4141, 4078, 4030, 4145, 4093, 4416, 4173, 4094, 4164, 4100, 4148, 4086, 4101, 4109, 4357, 4087, 4051, 4048, 4113, 4029, 4098, 4077, 4151, 4175, 4162, 4017, 4244, 4133, 4015, 4107, 427, 4134, 4156, 4128].

Confidence [1727, 39, 86, 1627]. Configurable [3945, 2557]. configuration [1188].


Congruential
[293, 2963, 267, 543, 2020, 2899, 1610, 1611, 1612, 1615, 1711, 2033, 2153, 2249, 2251, 2977, 3137, 820, 995, 1028, 1110, 1509, 3507, 1113, 858, 768, 769, 2434, 2838, 2047, 2591, 2914, 862, 327, 2177, 1538, 1369, 1370, 2442, 1732, 2929, 603, 654, 794, 613, 874, 2456, 2937, 658, 2099, 427, 1050, 1198, 1395, 3824, 2137, 1489, 1055, 1409, 2413, 632, 1691, 3240, 1600, 718, 2021, 320,
Correcting [3973, 4131]. Correction [1266, 3048, 1535, 2402, 1142, 221].
Corrections [270, 2843, 923]. correctly [1925]. Correctness [3857, 1781].
Correlated [2815, 2133, 1097, 141, 640, 3727, 596, 919, 2367, 697, 1, 2561,
431, 349, 1201, 1239, 3178, 2376, 227, 2381, 1983, 2803, 1884]. Correlation
[3466, 2236, 216, 52, 995, 244, 1746, 735, 840, 813, 1786, 497, 677, 1797, 952,
2265, 2345, 557, 481, 2850, 2703, 1126, 1460, 40, 655, 3188, 1760, 663, 1570, 51].
Correlational [813, 677, 462]. Correlations [755, 2569, 676, 2422, 2051, 2876, 1603,
1332, 1498, 2029, 549, 1420, 2425, 141, 1816, 2270, 1830, 1385, 1867, 2299, 3204, 2301, 2480]. Correspondence
[672, 2056, 1847, 2098]. corresponding [708, 1135]. Corrigenda [2137].
Corrigendum [2261, 1034, 2528, 1376, 1420, 2425, 141, 1816, 2270, 1830,
1385, 1867, 2299, 3204, 2301, 2480]. Cosmological [3685, 3540].
Cost [3307, 3228, 1008, 3693, 3542, 2460, 3317]. cost-effectiveness [3317].
Costruzione [469]. Countable [3]. Counter [3137]. Counter-Dependent
[3137]. Counting [2830, 1834, 1737, 2207, 3092, 1888, 1831]. Counts
[3319, 1352]. Couple [2038]. Coupled [3504, 3207, 3503, 3157, 3409, 3206].
Coupling [3391]. Coupon [144, 140]. courbe [35]. course [4080, 4023].
Courses [3257, 265]. Covariance [421, 53]. covariates [3823]. covering
[3741]. coverings [429]. covers [3627]. Cox [3823]. CPU [3871]. CPUs
[3895, 3712, 1769]. crack [2838]. cracked [605]. Cracking
[927, 3425, 3426, 3427, 3428, 838]. Cramér [294]. Crash [3927]. CRAY
[2421, 1386]. CRAY-System [2421]. Create [2749, 1758]. created [2296].
Creating [2870]. creation [2372]. Criteria
[1394, 1477, 2979, 520, 1461, 102, 2362, 2606, 3316]. Criterion [1]. Critical
[2749, 1700, 3944, 3048, 1699]. Crofton [2775]. Cross
[1786, 3504, 3206, 3207, 3503, 557]. Cross-correlation [1786, 557].
Cross-Coupled [3504, 3207, 3503]. cryogenic [1482]. Cryptanalysis
[2743, 2894, 3588, 1325, 1689, 3052, 3053, 3256, 2981, 2676, 2680, 2685, 2840,
2716, 2898]. Cryptanalytic [2354]. CRYPTO
[4045, 4098, 4172, 4056, 3104, 2993, 2592, 3969, 3956, 4004, 4035, 4071].
Crytoanalysis [2686]. Cryptographic
[1257, 1316, 3936, 3350, 2231, 4043, 3119, 3793, 4053, 3249, 1909, 3134,
2331, 1162, 2837, 2990, 3680, 3163, 2929, 1962, 2375, 2625, 1655, 2632,
3429, 3553, 3030, 3315, 3209, 1047, 3992, 2124, 3923, 3116, 3237, 2748,
3667, 3269, 3839, 2766, 1434, 2482, 2512, 3390, 1737, 1238, 2186, 3305,
2458, 2873, 3989, 3991, 3463, 4183, 4144]. Cryptographically
[3231, 3347, 3474, 1022, 1096, 1365, 3418, 3023, 1092, 2742, 3957, 3758, 3983,
1305, 1892]. cryptographically-secure [3983, 1892].
cryptographiquement [1892]. Cryptography
[4065, 2320, 902, 1695, 2666, 3050, 2984, 912, 2505, 2611, 3006, 3401, 1641,
2541, 2206, 2210, 4167, 2638, 4168, 1673, 2418, 4201, 4170, 2432, 4138, 3279,
1724, 1539, 2288, 1973, 2384, 2539, 3424, 2465, 3559, 2640, 3326, 3220, 4164].
Cryptology
[1146, 4045, 4035, 4053, 4054, 4074, 1131, 4084, 4043, 4098, 4071, 4172, 4056].
deployed [3424]. deposition
enhancements [3958]. Enhancing [3992, 3981, 1458]. ENIAC [3726, 87].
Equidistributed [509, 3873, 219, 1169, 2182, 2446, 2697, 2373]. Equidistribution [3475, 1804, 2155, 2253, 2332, 2248, 2671, 184, 1063]. equilibria [3149].
Erratum [497, 2964, 432, 1220, 2048, 687, 2170, 598, 2293, 933].
evaluations [2059]. even [3708, 3574]. even-distribution [3574]. Event [1095, 2129, 2564, 2890, 3348, 2827, 1154, 636, 855, 3483, 553, 1355, 1947].
Events [784, 2902, 1214]. everyone [3612]. Evidence [2850, 3359, 82, 2765, 3021]. evolution [3113, 3221]. Evolutionary [4161, 2575, 3172, 3642, 4148, 3341, 2590, 2958]. Evolvable [2652]. Evolved [2999]. evolving [3816, 2214]. Exact [3595, 550, 1161, 3697, 2307, 1395, 1792, 549, 3960, 1124, 3026, 2463, 51, 2121].

[1892, 322, 1580, 1500, 1001, 622, 890, 759, 1517, 1531, 1532, 1304, 2973, 3049].

generator
[2309, 2960, 1884, 3498, 3601, 2002, 1215, 459, 461, 3215, 3330]. Generatoren
[1050, 1052]. Generators
[1394, 2559, 2310, 2816, 293, 3976, 2122, 2225, 2963, 3346, 1479, 3658, 3826, 3233, 3110, 2658, 2314, 3112, 2745, 2967, 578, 2132, 3350, 4002, 2476, 3098, 3326, 3449, 3650, 3217, 3218, 3452, 3567, 3568, 1585, 3036, 3220, 3335, 3222, 1784, 3574, 3225, 3457, 3039, 3226, 3890, 2740, 2887, 3576, 3460, 2959, 3975, 3706, 1256, 1592].

Generators
[769, 1815, 2759, 2760, 2909, 3607, 3672, 3981, 3675, 2047, 2050, 2165, 3060, 3144, 3873, 3061, 2266, 2591, 2056, 2914, 862, 3384, 3965, 279, 327, 3927, 3928, 2694, 2554, 2177, 3683, 2596, 558, 2597, 1538, 1236, 1369, 1370, 1733, 2183, 2283, 2359, 2365, 2442, 2443, 2444, 2551, 2516, 2517, 2604, 2700, 2701, 3003, 3070, 3072, 3286, 3529, 3735, 3930, 4003, 3803, 1732, 3290, 3170, 2702, 2928, 2929, 3173, 3624, 3396, 2366, 3998, 1633, 2453, 3688, 358, 3810, 3811, 1178, 1180, 1845, 1847, 2780, 2710, 3179, 1640, 2714, 3692, 1461, 1549, 1551, 1748, 1292, 2196, 2617, 2788, 1854, 2624].

 generators
[3657, 2125, 3582, 2127, 1678, 3109, 1680, 2313, 3473, 3660, 3791, 2316, 3583, 3663, 1052, 3041, 3584, 3713, 3349, 3234, 2566, 2014, 3792, 3114, 1684, 1147, 1053, 1406, 2895, 3864, 1054, 2896, 1203, 2016, 1688, 2661, 2747, 2971, 3045, 2413, 905, 1491, 1691, 2897, 1205, 718, 3123, 3717, 1902, 3126, 3898, 3667, 3494, 1903, 2145, 2237, 546, 2388, 1907, 2024, 2146, 2239, 1023, 1908, 3249, 2327, 1342, 1497, 1498, 3251, 1415, 1494, 1495, 3497, 1604, 1702, 2750, 2901, 3132, 3252, 3834, 1334, 1416, 633, 2902, 3254, 3255, 1608, 406, 1417, 2753, 2245, 246, 2495, 1501, 3258, 1419, 1420].

generators
generators
[1830, 2174, 2273, 2274, 2352, 3524, 1002, 3157, 1442, 2844,
Goodness-of-Fit
Gossip
Gossip
Graduate
Grand
Grande
Granular
Graph
Graphic
Graphical
Graphics
Graphs
greater
Greatest
Greece
Greedy
Green
grenades
Grenoble
gretl
Grid
GRNG
Group
Grouped
grouping
Groups
growth
Guangdong
Guarantee
guaranteed
Guarantees
Guest
Guide
Guideline
Guidelines
Guitar
H
H2PEC
Haar
H˚astad
Hadamard
Halcomb
Halftoning
Halton
Hamburg
Hamiltonian
Hammersley
Hamming
Hand
Handbook
hand
Handel
Handel-C
Hard
Hard/soft
hardcore
Hardness
hardnesses
Hardware
Hardware-based
Hardware-optimized
Harmonic
Harvard
harvesting
Harshard
Hash
Hash3
Hashing
HASHPRNG
Hastings
HAVEGE
Having
Hawaii
Heads
heap
heap-ordered
heat
heavy-tailed
Heavy
Hecke
Held
Helios
Helmholtz
Hermite
[3056, 1166]. **Herstellung** [176]. **Heston** [3691]. **Heterogeneous**
[3365, 3961, 2842, 3243, 3307]. **Heuristic** [72, 2088, 3068, 2802, 3441].
**Heuristic-Based** [2088]. **heuristics** [3034]. **HI** [4192]. **Hidden** [1717, 3890].
**hiding** [3381]. **hierarchical** [3150, 3005]. **Hierarchy** [2188, 3448, 2969, 1603].
**High-density** [2663]. **high-dimensional** [2668, 2750, 2380, 3031, 3746].
**High-efficiency** [3985]. **High-entropy** [3126]. **high-functioning** [3021].
**high-order** [3059]. **High-Performance** [3154, 3280, 3633, 3532].
**high-period** [3051]. **High-Quality**
[2135, 3928, 2576, 1941, 2170, 1960, 2475, 2552]. **High-Speed**
[2408, 3272, 3803, 3415, 3754, 2520, 1190, 2748, 3258, 1725, 118, 129, 792, 227].
**Higher** [2019, 3244, 1698, 2434, 3240, 3522, 1246, 2954]. **Higher-Order**
[1698]. **Highly** [1618, 3017]. **highly-uniform** [3017]. **Hilbert** [3014].
**Hill** [170, 4152, 891, 1797, 3181]. **Hilton** [4073, 4067]. **Hirschberg** [1886].
**Histogram** [3491, 1619]. **Histograms** [3698, 1308]. **Historical** [2737].
**History** [71, 89, 720, 2768, 3841, 3843, 2787, 68, 1382, 374, 3221]. **Hit**
[1788, 2027, 3995, 1794]. **Hit-and-Run** [1788, 1794]. **Hitachi** [2120].
**Hitting** [2431]. **HK97** [3577]. **Hlawka** [872, 463]. **HMAC** [3857].
**HMAC-DRBG** [3857]. **Hoare** [4137]. **Hoeffding** [2295]. **Home** [2505].
**homogeneous** [12, 1620]. **Homomorphism** [517, 2414]. **homomorphisms**
[3230]. **Hong** [4151]. **Honolulu** [4131, 4192]. **honor** [4181, 4210]. **honour**
[4137]. **Hopfield** [3447]. **H"{o}rmann** [2973]. **Horner** [2555, 242]. **Horseshoes**
[2355]. **Horton** [1912]. **Hot** [4124]. **HotBits** [2885]. **Hotel**
[4069, 4013, 4112, 4067, 4039, 4022, 4041, 4086, 4101, 4051, 4126].
**Houston** [4036]. **Huge** [3076]. **hundred** [1224]. **Hurst** [2339]. **HW** [3173].
**Hyatt** [4130, 4208, 4126]. **Hybrid**
[3255, 3981, 354, 2551, 3320, 3106, 3240, 557]. **hyperbolas** [2118, 2401].
**Hyperbolic** [2797, 897, 1019, 1799, 1950, 1983]. **Hypercube**
[4050, 933, 934, 1356]. **Hypercubes** [4064]. **Hypergeometric** [1358, 1171].
**hyperplane** [2245]. **Hyperplanes** [2247]. **Hyperrectangles** [1798].
**hyperspheres** [3344, 3031]. **Hypotheses** [175]. **Hypothesis** [442].

I. [891]. **IBM** [4011, 721, 813, 677, 1426, 1514, 478, 2592, 155, 1544, 492, 462].
**IBM-Compatible** [1514, 1544]. **ibre** [1050]. **IC**
[2748, 3502, 3378, 3379, 2384, 2539, 3445]. **ICCMSE** [4173]. **ICCS** [4214].
**ICGA** [4148]. **ICGA-2001** [4148]. **ICICTA** [4198]. **icosahedral** [167].
**ideal** [813, 677]. **identical** [954]. **Identically** [2556, 3385]. **Identification**
[1455]. **Identifying** [3277]. **identities** [1389]. **identity** [2567, 1950]. **IEEE**
[4143, 4192, 4193, 4208]. **If** [1488]. **IFIP** [4191]. **II**
[4133, 1258, 3355, 1707, 1802, 2256, 1819, 1931, 1231, 4214, 254, 1969, 2075,
Investigation [2678, 3984]. Investigations [1665, 1670, 2143, 1747].
investing [3768]. invitation [4018]. Invited [2500, 1633]. Inviting [299, 1633].


L [541, 594, 637]. Laboratory [4005, 4007]. Lag [610]. Lagged
3147, 3941, 3390, 1008, 1449, 2519, 2775, 2853, 3176, 3693, 3542, 1752, 2294, 3642, 2107, 2121. low-cost [3693, 3542]. Low-Degree [3396].
Luby [2124, 1850, 3187]. Luc [248x1304]. Lucas [3512, 2403]. luck [3842].
Lyapunov [2850, 1842]. lying [1314]. LZSS [3360].
multi-stage [159]. multicomputer [1835]. multicyclic [662].
Multidimensional [2914, 2272, 3736, 1244, 1584, 494, 901, 2828, 2501, 2912].
multidimensionally [1169]. Multigroup [290]. Multiloop [1906].
Multimedia [3205]. Multinomial [1099]. Multiparty [1401, 1680, 2900].
multiphase [3991]. Multiple [2415, 241, 152, 3131, 3599, 3600, 2422, 996,
2909, 638, 1283, 508, 1430, 2828, 2501, 2912, 2198, 930, 3430, 2880, 1476, 1672, 3230, 3583, 3123, 3241, 2901, 3132, 3252, 1276, 278, 1527, 2273, 2274, 2353, 3524, 2921, 3068, 1838, 2179, 2181, 2280, 2360, 1454, 1751, 1856, 2082, 2732, 2808, 2809, 2950, 2952, 3033, 3034, 3318, 3441, 3443, 3564, 2647, 3222].
Multiple-Comparison [1672]. Multiple-Recursive [277x299, 2083, 2085].
Multiple-Valued [241]. multiples [2647]. Multiplexed [2683].
Multiplication [2178, 1183, 1590]. Multiplications [2990]. Multiplicative
[267, 543, 406, 820, 995, 1028, 1110, 1341, 1509, 3278, 2177, 1732, 654, 2099, 569, 535, 2308, 2137, 905, 1600, 718, 320, 1699, 438, 1420, 856, 952, 1219, 1220, 555, 1427, 2174, 3912, 2187, 2860, 1010, 3300, 927, 3038]. multiplicatively
[471]. multiplicatively-generated [471]. Multiplicators [496]. Multiplier
[4000, 1776, 2808, 3094, 3563, 2308]. Multipliers [2442, 2516, 1055, 2413,
1898, 1334, 2246, 2495, 685, 3524, 2998, 782, 2877, 3971, 2732, 2950, 3033].
multiplikativ [438, 471]. Multiply [742, 2655, 2239, 2761, 639].
multiply-with-carry [2239, 2761]. Multiprocessor [1484, 1911, 1674].
multiprocessors [4050, 1741]. multiprogrammed [981].
multiprogramming [1152]. multisequences [3889]. mutispin [1300].
Multistep [1294, 1481]. multithreading [3621]. multivariable [223].
Multivariate [2815, 578, 1788, 2972, 1337, 2586, 1934, 1284, 2276, 2774,
3411, 3304, 3430, 3431, 3210, 431, 2892, 3044, 2244, 1176, 2613, 790, 2866,
3412, 3413, 1564, 981, 3885]. Murmur [3558]. musical [3708]. mutual
[923, 924]. Mutually [861]. MUX [3991]. mV [3367]. my [3868].

[3847]. Naor [3736, 2637]. Nash [3149]. National
[4007, 4130, 4156, 134, 4018, 91]. NATO [4023]. Natural
[2149, 1345, 3630, 3770, 524, 2219, 2097]. Nature [3981, 786].
NDSS [4187]. NDSTRNG [3994]. near [2590, 4015]. nearby [2184].
[726]. Negative [2262, 842, 349, 1237]. nei [987]. neighbor [1356].
neighborhood [2635, 2727]. neighborhood-of-four [2635, 2727]. Nested
[996, 2476]. net [2081, 2233]. Netherlands [4053, 4214]. Nets
[2975, 2379, 2936, 2087, 2388, 4189, 2793, 2463, 625]. Netscape [2162].
Network [4187, 2022, 3270, 3610, 2694, 3407, 3327, 2111, 2230, 3499].
networked [3265]. Networking [4199]. Networks
Neuere [631]. Neumann

Normal [398, 634, 323, 368, 43, 1500, 3812, 2616]. notional-distributed [1500]. normalverteilter [1500]. NORTA [2569]. North [4066, 4087].


Number [2354, 2177, 2919, 866, 3942, 2596, 1447, 2276, 332, 480, 2696, 1288, 1631, 1733, 2183, 2283, 2359, 2365, 2443, 2444, 2515, 2603, 2604, 2700, 2701, 2849, 3001, 3003, 3070, 3072, 3165, 3286, 3529, 3735, 3930, 4003, 3944, 3619].
46

1621, 224, 382, 202, 1169, 3681, 1231, 2436, 154, 1523, 1524, 1525, 1941, 2170, 356, 383, 2482, 1070, 2509, 3929, 3523, 2171, 118, 1118, 1172, 2917, 3387, 1830, 1440, 2174, 2273, 2274, 2352, 2353, 3524, 1002, 2175, 2176, 3155, 3156, 3159, 2512, 1442, 2844, 3908, 916, 1004, 1234, 1444, 1726, 779, 3163, 1445, 1628, 1446, 2920, 2440, 3983, 598, 599, 248, 2921, 2998, 3068, 826, 1365, 3389, 1368, 1632, 1838, 1957, 2179, 2184, 2279, 2280, 2281, 2360, 2361, 2362, 2363, 2364, 2600, 2602, 2698, 2846, 2848, 2923, 3071.

3393, 3620, 3843, 3283, 1539, 1174, 3390, 1122, 3164, 3284, 782, 2850, 783, 3633, 3405, 3013, 611, 1010, 655, 1128, 1297, 1647, 1754, 1755, 2083, 2535, 2620, 2720, 3190, 3016, 3303, 3409, 2867, 3410, 3411, 616, 659, 3191, 876, 3697, 3082, 2538, 2869, 2939, 3414, 2203, 3305, 3775, 1463, 1130, 491, 525, 1080, 1299, 1464, 1760, 2091, 968, 1386, 3192, 3881, 2539, 2092, 564, 3545, 2094, 1300, 3419, 800, 3019, 3851, 1131, 618, 2540, 1981, 3422, 260, 1132, 620, 367, 839, 3548, 2385, 1654, 3882, 3021, 1087, 1565, 3023, 1088, 2726, 3086, 1656, 931.

[346, 455, 830, 3694, 793, 3296, 1078, 1127, 3403, 921, 832, 3298, 609, 3633, 3405, 3013, 611, 1010, 655, 1128, 1297, 1647, 1754, 1755, 2083, 2535, 2620, 2720, 3190, 3016, 3303, 3409, 2867, 3410, 3411, 616, 659, 3191, 876, 3697, 3082, 2538, 2869, 2939, 3414, 2203, 3305, 3775, 1463, 1130, 491, 525, 1080, 1299, 1464, 1760, 2091, 968, 1386, 3192, 3881, 2539, 2092, 564, 3545, 2094, 1300, 3419, 800, 3019, 3851, 1131, 618, 2540, 1981, 3422, 260, 1132, 620, 367, 839, 3548, 2385, 1654, 3882, 3021, 1087, 1565, 3023, 1088, 2726, 3086, 1656, 931.

3322, 167, 2954, 3951, 2476, 1663, 1308, 985, 3098, 2812, 3952, 3449, 3451, 1093, 2112, 1094, 3651, 3935, 2553, 3568, 232, 1587, 1878, 3036, 3569, 1782, 2652, 3333, 2117, 2223, 3335, 2065, 462, 2958, 3102, 2554, 3222, 3453, 3573, 3653, 1784, 2406, 2308, 2654, 2739, 3038, 3455, 3225, 3974, 3457, 3093, 3226, 3890, 2740, 2887, 2741, 3339, 3340, 3460, 2959, 3975, 3462, 3706, 1256, 1592, 575, 2960, 3796, 3498, 3601]. **Number-theoretic** [2289]. **Numbers**


[225, 1729, 1537, 558, 645, 1540, 2601, 1731, 27, 249, 691, 1962, 1373, 651, 449,
54

3284, 2441, 2927, 2612, 1841, 3394, 3397, 1634, 3293, 3177, 3691, 3738, 2373, 284, 3542, 2786, 2865, 455, 793, 3772, 3012, 1750, 3404, 2289, 695, 797, 798.

Pseudorandom

Pseudorandomness

Pseudozufallsvektoren

Pseudozufallszahlenfolgen

Pseudosluchainykh

PSI

PSO

PUF

Publications

Publicly

Published

Public-Key

Public-Key-Number

Pseudorandom

Pseudorandom-Number

Public-Key

Public-Key-Number

Pseudozufallsvektoren

Pseudozufallszahlenfolgen

Pseudosluchainykh

PSI

PSO

PUF
PUF-TRNG \[3988\]. PUFs \[3918\]. Pulse \[3504, 1828, 676, 3505\]. Pulse-Excited \[3504\]. Pulse/Data \[1828\]. Pulses \[519, 520, 3335\]. punched \[36\]. punctured \[3772\]. Pure \[3846\]. Purpose \[1081\]. Purposes \[3936, 2929\]. PVT \[3438\]. PVT-variation \[3438\]. pW \[3367\]. pyramids \[1459\]. Python \[3733, 3623, 2369, 2370, 4212\].


Quasirandom \[2560, 1324, 2140, 3490, 1222, 2200, 2871, 1773, 3243, 2771, 1371, 1857, 1860, 1871, 2104, 574\]. Quaternion \[3450\]. quatrième \[4010\]. Quebec \[4097, 4149\]. Query \[449\]. Quest \[1347, 3471\]. questions \[85\]. Queue \[988, 1955, 1956, 1020, 2756, 963, 3329\]. Queueing \[1402, 1241\]. Queueing \[1484, 620, 802\]. Quick \[2031\]. QuickCheck \[3878\]. Quickly \[1926\]. Quicksort \[2493\]. Quinary \[925\]. Quincunx \[3420\]. Quintessential \[3420\]. quintic \[3056\]. quotient \[1239\]. quotients \[3602, 1242\].

R \[2137, 3937, 3718, 3169, 3291\]. R16 \[806\]. R18 \[769\]. R24 \[862\]. R52 \[1108\]. R53 \[1109\]. R57 \[1167\]. R58 \[1181\]. Rabin \[1318\]. Racah \[424\]. Rackoff \[1850\]. Radial \[348\]. Radiation \[338, 11\]. Radical \[324\]. Radical-inverse \[324\]. radio \[497, 481\]. radioactive \[2885\]. Radisson
Randomizer [1505]. Randomly [863, 2087, 664, 2207, 1474, 22, 1834, 3392].
randomly-shifted [3392]. Randomness
[3464, 671, 3936, 3708, 2965, 1021, 127, 3586, 2318, 3423, 3547, 3641, 2633, 3646, 175, 2469, 2547, 1872, 3649, 2955, 2555, 3579, 3891, 3954, 2819, 3471, 3751, 466, 2969, 436, 1687, 213, 3359, 104, 3048, 1327, 3598, 1602, 3251, 42, 3901, 81, 1715, 3670, 440, 143, 117].
randoms [899]. ‘RANDU’ [721].
RANEXP [1932]. RANF [1118]. Range
[2422, 8, 404, 1332, 1498, 1797, 1420, 2339, 1385]. RANGEN [2673]. ranges
[2466]. Rank [1021, 1353, 2995, 3804, 3014, 3016, 3089]. rank-
[3014, 3016]. Rank-1 [2995, 3804]. Rank-based [1353]. Ranking
[2136, 3904, 2163, 3634]. ranks [2368]. ranlip [2892]. RANLUX [2263, 2264, 1941, 2170, 2390].
ranshi [2164]. RANTEST [936]. ranut [2661]. Rapid [1653]. rapides
[2647]. rapidly [74]. rapprochés [2184]. Rare [2827, 3483, 2902].
raspredelenija [35]. Rate [2240, 3766, 626, 3405, 3697]. Rates
[1938, 2172, 1667, 1393, 2521]. Rational
[169, 3079, 2199, 2795, 3613, 1036, 3931]. Ratios [339, 3695, 1504]. RAW
RC6 [2508, 2593]. RCR [3915]. RDRAND [3895]. Re [2706, 3419].
Re-seeding [3419]. reactor [4013, 3505]. read [3978]. read-write [3978].
Reading [10]. Real [3659, 2150, 3139, 3384, 3965, 3562, 728, 2195, 2945].
Real-Time [3384]. Real-Valued [3139]. realistic [3670]. realization
[3476, 3799, 3421, 2804, 2641]. Reasonably [1]. Reasoning [2824, 3201].
receiver [3275]. Rechenautomaten [176]. recherche [1367]. Recipes
[1765, 2312, 2229]. Reciprocal [376, 378, 412, 390, 420, 421, 1365, 2305].
Recommendation [2967, 3041, 3584, 3124, 3636, 3815, 3887].
Recommendations [3936, 2132, 1913, 2903]. Recommended [2918].
Reconfigurable [3054, 3141, 3853, 3884, 3210, 2581, 2931, 3498].
Reconfiguration [3384]. Reconstructing [1342]. Reconstruction [3811].
Record [316, 1926, 4124, 2725]. Recovery [3720, 3836, 3833, 3192].
recrystallization [3993]. rectangle [1395]. Rectangles
[2366, 3655, 2127, 1545]. Recurrence [373, 3652, 951, 1280, 1344, 926].

SIMD-Oriented [3198]. Similar [3879]. Similarity [2323, 4167].
SIMPL [763]. SIMPL/1 [763]. Simple
[1478, 580, 1683, 1202, 1606, 1607, 3759, 1074, 2525, 2374, 2076, 829, 3549, 2636, 2946, 1249, 3463, 2561, 850, 1148, 1795, 1103, 2425, 4117, 1281, 75, 3064, 2181, 2609, 3174, 621, 2473, 3208]. simplest [3198]. simplexes [3879].
Structures

Subgroup

Subharmonic

Sublattice

Sublinear

Subroutine

Subsequence

Subset

Subsets

Subspace

Substitute

Substitution

Substitution-Permutation

Substream

Substructure

Subtle

Subtract

Subtract-with-Borrow

Subtraction

Such

Suggestions

Suitable

Suite

Suites

Summer

Sums

Super

Supercomputer

Supercomputers

Supercomputing

Supercube

Superconductive

Superior

Superior

Supplement

Support

Supported

Supposed

Suppression

Surface

Survey

Survival

SWAC

Swan

Swarm

SWB

Swendsen

Switched

Switched-Capacitor

Switching

Switzerland

SX

Symbolic

Symbolic-Numerical

Symmetric

Symmetrical
3467, 3468, 3792, 3116, 3117, 3237, 3238, 3239, 3268, 3269, 3271, 3279, 2520, 3039, 3114, 3862, 2748, 3724, 2583, 600, 3631, 3694, 573, 629, 668. **Truncated** [2899, 1537, 417, 1474, 853, 1342].

**trust** [2346].**trustless** [3851].**Trustworthy** [3844].**trx** [3844].**Tsallis** [3026].**Tucson** [4037].**Tunable** [3270, 2842].**Tuning** [2810, 2883].**Tunnel** [3977].**tuples** [2441].**Turán** [2052, 656].**Turbo** [3648, 1608, 1364].**TURBO RAND** [1225].**Turbulence** [1909, 1446].**turbulent** [2682].**Turing** [4203, 3043, 3586, 3899, 4205].**turn** [2510].**Tutorial** [1398, 1154, 1615, 1451, 1086].**Tweedie** [3790].**Twelfth** [4088].**twenty** [2510].**Two** [3104, 2010, 1099, 988, 427, 808, 714, 497, 1485, 1054, 401, 1617, 1712, 1713, 1917, 1918, 2155, 2328, 2329, 1340, 1280, 1344, 2684, 478, 3729, 1119, 3524, 777, 2921, 3068, 1632, 481, 186, 2066, 3394, 2187, 1239, 2784, 735, 3846, 2938, 1085, 2298, 34, 2646, 3033, 3441, 3564, 1472, 2552, 2738, 2309].**Two-bit** [3523].**Two-Dimensional** [3151, 3154, 1842, 54, 714, 2298, 2552, 2309].**Two-Queue** [988].**Two-Sided** [3555].**Two-Source** [3794, 3805].**Two-Stage** [1099].**two-term** [3524, 2921, 3068, 3033, 3441, 3564].**Twofish** [2508].**Type** [2689, 155, 2595, 787, 2942, 886, 2220, 3229, 3993, 404, 1806, 1161, 1518, 356, 699, 3213, 3573, 3653].**Types** [3624, 575].

**Übertragungsprinzip** [33].**UHF** [3896].**UHF-RFID** [3896].**UK** [4203, 4164].**uklonenijah** [35].**Ukraine** [4089].**Ulam** [3605].**Ulrich** [892].**Ultimate** [2256, 3544].**Ultra** [3455].**Ultra-lightweight** [3455].**ultracomputers** [1299].**Ultrafast** [3722, 3806, 3281, 3943, 3568].**Ultrahigh** [3308].**Ultrahigh-Speed** [3308].**Unavoidable** [1061].**Unbiased** [1097, 1327, 1201, 586].**Unbounded** [2980, 2832, 3063].**uncertain** [3267].**uncertainty** [4150, 1218, 3298].**unclonable** [3831].**Unconditional** [3176].**Unconstrained** [2088].**Uncorrelated** [1486, 298].**Uncovering** [2457].**Underlying** [863].**Understanding** [2996, 3777].**unequal** [140].**unicorn** [3844].**Unified** [2010, 2039, 1541, 3969, 290, 2000, 567, 3100].**Uniform** [811, 1398, 1787, 1688, 403, 1415, 1495, 2751, 1273, 680, 1429, 825, 516, 690, 2997, 1451, 1957, 2283, 2364, 2365, 2444, 2603, 3529, 1074, 783, 2702, 3292, 358, 1544, 1077, 1642, 3079, 2084, 1572, 2110, 3096, 3446, 427, 3337, 3342, 3789, 1397, 2224, 1786, 1261, 1052, 2661, 905, 401, 3047, 3757, 2326, 1023, 1499, 1702, 1703, 2668, 2750, 1213, 1922, 2043, 3837, 764, 1433, 3377, 1351, 1519, 685, 2991, 246, 1825, 382, 2271, 1232, 777, 85, 2282, 3528, 730, 731, 2610, 252, 2373, 607, 656, 739, 923, 924, 3017, 121, 1386, 661, 367, 970, 623, 3700, 1660].


References

[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.


80 REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[94] Preston C. Hammer. The mid-square method of generating digits. In Householder et al. [4006], page 33.


REFERENCES


REFERENCES


REFERENCES


[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 × 1)0 × 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.


REFERENCES


REFERENCES


REFERENCES


178 J. Bass and J. Guilloud. Méthode de Monte-Carlo et suites uniformément denses. (French) [The Monte Carlo Method and sequences of uniformly-
REFERENCES


[Bolshev:1959:TRV]


[Cashwell:1959:PMM]


[Cook:1959:RRP]

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

[Ehrlich:1959:MCS]


[Golenko:1959:DCS]


[Golenko:1959:FRN]

REFERENCES

527–537, October 1959. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[232] Donald D. Wall. A random number test for large samples. In Anonymous [4011], pages 7–11. LCCN ???


REFERENCES


REFERENCES


REFERENCES


REFERENCES

December 1962. CODEN NUMMA7. ISSN 0029-599X (print), 0945-3245 (electronic).


[295]
REFERENCES

119


Barnes:1963:CEG


Bolshev:1963:APT


DeMatteis:1963:SAP


Firestone:1963:CNU


Fisher:1963:STB


Franklin:1963:DSR


Gabai:1963:DCSa

REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
</table>
REFERENCES


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


REFERENCES

Kronmal:1964:EPN


Liu:1964:MFS


MacLaren:1964:FPG


Marsaglia:1964:CMG


Marsaglia:1964:FPG


Marsaglia:1964:MPR


Marsaglia:1964:RDA


Marsaglia:1964:RNV

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

Marsaglia:1964:RVC


Marsaglia:1964:SPIa


Marsaglia:1964:SPIb


Onicescu:1964:NSA


Poore:1964:CPG


Sobol:1964:PPR


Stockmal:1964:CPR

REFERENCES


REFERENCES


REFERENCES

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See certification [628] and remarks [380, 391].

Pike:1965:ARN


Pike:1965:CAGb


Potter:1965:CNS


Pyke:1965:S


Reeves:1965:AUR


Rosenberg:1965:CNN


Scheinok:1965:DFR


Seshadri:1965:RVW

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

Shapiro:1965:DAA


Stoneham:1965:SDT


Tausworthe:1965:RNG


Teichroew:1965:HDS


Chaitin:1966:LPC


Chiang:1966:ERR


Dyadkin:1966:SRE

REFERENCES


REFERENCES


REFERENCES


Shreider:1966:MCM


Spitzer:1966:RPP


Springer:1966:DPI


Stroud:1966:GQF


Zaremba:1966:GLP


Albert:1967:CNN


Azorin:1967:BRB

REFERENCES


Behboodian:1967:EAV


Canavos:1967:CAT


Chambers:1967:RNG


Coveyou:1967:FAU


Csorgo:1967:NPS


deBalbine:1967:NRP


Downham:1967:MCP

REFERENCES


REFERENCES


[414] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [4017], pages 64–68. LCCN QA76.5 D55 1965.


VanGelder:1967:SNR


Westlake:1967:URN


White:1967:EDC


Wyner:1967:RPC


Adhikari:1968:DMS


Anonymous:1968:GCM


Ayoub:1968:EEK

REFERENCES


REFERENCES


REFERENCES


Miller:1968:ACP


Muller:1968:RN


Pillai:1968:NEI


Polljak:1968:APN


Show:1968:AGR


Sibuya:1968:GDE


REFERENCES


[468] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [4018], pages 70–111. LCCN QA1 S565 v. 3.


REFERENCES


REFERENCES


REFERENCES


REFERENCES

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See remark [618].


Dixon:1970:NSE


Downham:1970:SAA


Fuchs:1970:EDR


Good:1970:RPM


Gustavson:1970:FRN


Haber:1970:NEM

149


REFERENCES

995, November 1970. CODEN AMMYAE. ISSN 0002-9890 (print), 1930-0972 (electronic).


REFERENCES


REFERENCES


Vincent:1970:CGT


Vincent:1970:GTR


White:1970:FDC


Zaremba:1970:DII


Ashford:1971:BRG


Berman:1971:GGD


Beyer:1971:LSM

REFERENCES


REFERENCES


[568] 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.,


Ahrens:1972:CMS

Alam:1972:AVM

Barr:1972:CMN

Basu:1972:ITF

Behboodian:1972:CNS

Beyer:1972:LSR

Broemeling:1972:BPD


REFERENCES


REFERENCES


Forsythe:1972:NCMa


Forsythe:1972:NCMb


Frazer:1972:BOM


Garside:1972:BRBa


Heathcote:1972:TGF


Hurst:1972:AAG


Kirschmann:1972:CR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[626] Nathan O. Sokal. Optimum choice of noise frequency band and sampling rate for generating random binary digits from clipped white noise.

Sowey:1972:CCB


Sullins:1972:CAP


Vincent:1972:CPA


Ahrens:1973:EFM


Ahrens:1973:NME


Burford:1973:BAC

REFERENCES


[646] 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 [754] algorithm: see [1485] for a comparison, both mathematical, and graphical.


[653] E. J. McGrath and D. C. Irving. Techniques for efficient Monte Carlo simulation. Vol. II. Random number generation for selected probabil-

Neave:1973:MUB


Neuman:1973:CSS


Niederreiter:1973:BEB


Niederreiter:1973:MTD


Overstreet:1973:QCM


Overstreet:1973:RNG

REFERENCES


Tsuda:1973:NIF


Vincent:1973:RGT


Adam:1974:CLS


Ahrens:1974:CMS


Alam:1974:SNT


Beasley:1974:CSR


Block:1974:CBE

REFERENCES


Brent:1974:AAG


Chen:1974:GRV


Cohn:1974:CRP


Coldwell:1974:CDS


Collins:1974:CTE


Dahlquist:1974:NM


Dieter:1974:URN

REFERENCES


REFERENCES


[694] 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 ???


REFERENCES


REFERENCES

[709] 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.

numbers with floating-point representation. Electronics Letters,
10(25–26):533–534, December 12, 1974. CODEN ELLEAK. ISSN 0013-5194
stamp/stamp.jsp?tp=&arnumber=4245313.

with arbitrary frequency distributions. Electronics Letters,
10(8):127–128, April 18, 1974. CODEN ELLEAK. ISSN 0013-5194 (print), 1350-
jsp?tp=&arnumber=4245054.

[712] 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).

[713] J. Whittaker. Miscellanea: Generating gamma and beta random vari-
ables with non-integral shape parameters. Applied Statistics,
23(2):210–214, 1974. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (elec-
tronic).

[714] Y. Akeda and M. Hori. Numerical test of Palásti’s conjecture on two-
March 27, 1975. CODEN NATUAS. ISSN 0028-0836 (print), 1476-4687 (elec-
tronic). URL http://www.nature.com/nature/journal/v254/n5498/
pdf/254318a0.pdf.

variables. Canadian mathematical bulletin = Bulletin canadien de
REFERENCES


REFERENCES


REFERENCES

M. B. Levin. On the uniform distribution of the sequence $\alpha \lambda$. *Mat. Sb. (N.S.)*, 98(??):??, 1975. CODEN ????, ISSN ???.

M. B. Levin. On the uniform distribution of the sequence $\alpha \lambda$. *Math. USSR-Sb.* 27(??):183–197, 1975. CODEN ????, ISSN ???.


REFERENCES

Newman:1975:MIF


Niederreiter:1975:DDM


Niederreiter:1975:QVR


Pohl:1975:MFP


Pollard:1975:MCM


Rosenblatt:1975:MSS


Schaufele:1975:API

REFERENCES


REFERENCES

Anderson:1976:PRR


Atkinson:1976:CGB


Atkinson:1976:SAG


Bays:1976:IPR


Blood:1976:CPR


Brent:1976:ABE

complexity is shown to be $O(lg N)$, and the number of right shifts at most $2 lg(N)$.


REFERENCES

1976. CODEN SIMUD5. ISSN 0163-6103. URL http://www.or.unc.edu/research/temp/tech70b.html.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[860] Donald P. Gaver. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments: Comment.
REFERENCES


[Geller:1978:SEW]


[Hoaglin:1978:SAR]


[Hollander:1978:TDU]


[Holmlid:1978:UCP]


[Kemp:1978:CGB]

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Schrage:1979:MPF

Sobol:1979:ESS

Sobol:1979:SSH

Tanemura:1979:RCP

Tripathi:1979:RFI

vanLint:1979:PRA

Wang:1979:MND


REFERENCES


REFERENCES

216

Marsaglia:1980:GRV


OBrien:1980:PIR


Peskun:1980:TTC


Petkovic:1980:RRV


Ribeiro:1980:MOS


Rice:1980:DQF


Rubin:1980:RAE


REFERENCES


[987] F. Battaglia. Riproduzione delle autocorrelazioni nei metodi di generazione di numeri pseudo-casuali normali. (Italian) [Reproduction of

Calo:1981:DAT


Deak:1981:EMR


Devroye:1981:CGP


Devroye:1981:CGR


Diaconis:1981:GRP


Dudewicz:1981:EBT


REFERENCES

Landauer:1981:RNF


Menzefricke:1981:BAC


Nekrutkin:1981:JSM


Preece:1981:DFD


Rubinstein:1981:RNG


Schatte:1981:RVL

223

REFERENCES

[1014] 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.


REFERENCES


REFERENCES


REFERENCES


[1054] Lenore Blum, Manuel Blum, and Michael Shub. Comparison of two pseudorandom number generators. In Chaum et al. [4035], pages 61–


REFERENCES


REFERENCES


REFERENCES


Plumstead:1983:ISPb

Pokhodzei:1983:OMM

Purdy:1983:CFA

Ripley:1983:CGR

Ripley:1983:LSP

Rosenbaum:1983:RNG

Sakasegawa:1983:SRS


REFERENCES


REFERENCES


[1110] George S. Fishman and Louis R. Moore III. An exhaustive analysis of multiplicative congruential random number generators with
REFERENCES


REFERENCES


Marsaglia:1984:EAM


Marsaglia:1984:FEI


Marsaglia:1984:GCM


Modianos:1984:RNG


Niederreiter:1984:PSP


Papoulis:1984:PRV


Paulsen:1984:IRN

REFERENCES


REFERENCES


REFERENCES


[1162] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. On the cryptologic applications of random functions (extended abstract). In
REFERENCES


REFERENCES


Reichert:1985:LLT


Riesel:1985:PNC


Saito:1985:HSS


Sawitzki:1985:ARN


Shanthikumar:1985:DRV


Smith:1985:VHP


Thesen:1985:EGU


REFERENCES


REFERENCES


[1227] H. Grothe. Matrixgeneratoren zur Erzeugung gleichverteilter Zufallsvektoren. (German) Matrix generators for generating uniformly distributed
REFERENCES


REFERENCES


Nicola:1986:QAF


Niederreiter:1986:DFS


Niederreiter:1986:LDP


Niederreiter:1986:MNI


Niederreiter:1986:PVG


Panny:1986:NHM


Santha:1986:GQR

REFERENCES


Zeisel:1986:SAR


Zielinski:1986:QRN


Agnew:1987:RSC


Aldridge:1987:CRR


Allender:1987:SCE


Anderson:1987:GRO


Barbu:1987:NFM

Gh. Barbu. A new fast method for computer generation of gamma and beta random variables by transformations of uniform variables. *Statisti-
REFERENCES

260


REFERENCES

Chiu:1987:SRS

Chung:1987:RWA

Collings:1987:CRN

Compagner:1987:MLS

Dagpunar:1987:NMS

Diaconis:1987:SAG
Doolen:1987:MCW


Edgington:1987:RT


Eichenauer:1987:MRN


Eichenauer:1987:SQC


Federickson:1987:PMC


Fullerton:1987:NPN


Fushimi:1987:MAP


REFERENCES


Beauchemin:1988:GRN


Binder:1988:MCS


Bratley:1988:AIS


Brickell:1988:CSR


Brillhart:1988:FHP


Chor:1988:UBS

[1328] Bruce Jay Collings and G. Barry Hembree. Addendum to “Initializing
generalized feedback shift register pseudorandom number generators”.
0004-5411 (print), 1557-735X (electronic). See [1209].

of t and normal distributions. *Communications in Statistics: Simulation
and Computation*, 17(2):653–661, 1988. CODEN CSSCDB. ISSN 0361-
0918.

catdir/enhancements/fy0638/88003212-d.html; http://www.loc.gov/catdir/
enhancements/fy0638/88003212-t.html.

[1331] A. De Angelis. A class of N-dimensional probability density func-
tions suitable for random generation. *Computer Physics Communications*,
52(1):61–64, December 1988. CODEN CPHCBZ. ISSN 0010-4655
science/article/pii/0010465588901725.

[1332] A. De Matteis and S. Pagnutti. Parallelization of random number gener-
ators and long-range correlations. *Numerische Mathematik*, 53(5):595–
608, August 1988. CODEN NUMMA7. ISSN 0029-599X (print), 0945-
3245 (electronic).

In Wegman et al. [4061], pages 624–626. URL http://www.dtic.mil/
dtic/tr/fulltext/u2/a208838.pdf.

[1334] V. Denzer and A. Ecker. Optimal multipliers for linear congruential
pseudo-random number generators with prime moduli. *BIT (Nordisk tid-
skrift for informationsbehandling)*, 28(4):803–808, December 1988. CO-
DEN BITTEL, NBITAB. ISSN 0006-3835 (print), 1572-9125 (elec-
REFERENCES


[1341] G. S. Fishman. Multiplicative congruential random number generators with modulus $2^\beta$: An exhaustive analysis for $\beta = 32$ and a partial anal-


[1348] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. In IEEE [4060], pages 12–24. CODEN ASF-
REFERENCES


[1367] 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, Qu´ebec, Canada, 1988.


REFERENCES


[1395] Lothar Afflerbach and Rainer Weibächer. The exact determination of rectangle discrepancy for linear congruential pseudorandom numbers.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Paul:1989:IRN


Percus:1989:RNG


Pickover:1989:PRG


Reber:1989:PNG


Rhee:1989:OPIa

REFERENCES


REFERENCES


REFERENCES


[1500] H. Döring. Erzeugung normalverteilter Zufallszahlen mit 16-bit-PC. (German) |Generation of normally-distributed random numbers on an


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Vinogradova:1990:ECF


Wallace:1990:PRG


Wang:1990:DRV


Wang:1990:VDC


Williamson:1990:PAN


Wolf:1990:AFM


Wong:1990:RNG


Michael Berblinger and Christoph Schlier. Monte Carlo integration with quasi-random numbers: some experience. *Computer Physics Communication*...
Berndnicov:1991:MCS


Bittner:1991:NSP


Chambers:1991:SEM


Clementson:1991:CRN


Compagner:1991:DR


Compagner:1991:HCR


REFERENCES
REFERENCES


314

REFERENCES


Kao:1991:CRN


Kemp:1991:PRV


Koen:1991:ACB


Komo:1991:DPR


Lai:1991:PNB


Law:1991:SMA


[2036, 1875] about the extremely bad lattice structure in high dimensions of the generators proposed in this paper.

Marsaglia:1991:NGR


Matus:1991:AFD


Maurer:1991:LRP


Maurer:1991:UST


McInnes:1991:IPK


Melamed:1991:TCM


Micali:1991:EPP

[1643] Silvio Micali and Claus-Peter Schnorr. Efficient, perfect polynomial random number generators. Journal of Cryptology: the journal of the Inter-
REFERENCES


Patarin:1991:NRP


Peterson:1991:NRN


Pickover:1991:PRG


Revello:1991:CEC


Ritter:1991:EGC

[1655] 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; Čebyshev 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.
REFERENCES


REFERENCES


REFERENCES


Aluru:1992:RNG


Anastasio:1992:OCL


Anderson:1992:CRN


Arno:1992:PSC


Atkinson:1992:GBT


Babai:1992:MPP


Baker:1992:PPT

REFERENCES

Bays:1992:IRN


Bellido:1992:SBR


Berdnikov:1992:RNG


Binder:1992:MCS


Bratley:1992:ITL


Brenner:1992:PRL


REFERENCES 326


Canfield:1992:RARb


Carroll:1992:CCE


Collins:1992:RNG


Dai:1992:BSD


DalleMolle:1992:HOC


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Louchard:1992:DAD


Maclaren:1992:LUL


Makino:1992:GSR


Marsaglia:1992:MRN


Mason:1992:ACA


Matsumoto:1992:TGG


Maurer:1992:UST


Sobol:1992:QSG


Sprugnoli:1992:GBT


Szyszkowicz:1992:GRP


Tang:1992:SDA


Tezuka:1992: AAC


Tezuka:1992:FGL


Traub:1992:MCA


Atkinson:1993:UGR


Belisle:1993:HRA


Brickell:1993:SRI


Browne:1993:CTC


Bshouty:1993:CFR


Bundschuh:1993:MEC


Cerecedo:1993:NIG

[1793] M. Cerecedo, T. Matsumoto, and H. Imai. Non-interactive generation of shared pseudorandom sequences. Lecture Notes in Computer Science,


REFERENCES


[1806] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Kloosterman-type sums and the discrepancy of nonoverlapping pairs of inversive

**Eichenauer-Herrmann:1993:LSN**


**Eichenauer-Herrmann:1993:SIN**


**Erdmann:1993:CMT**


**Fisher:1993:OOR**


**Flahive:1993:ICG**


**Galway:1993:ESCb**

REFERENCES


Hansen:1993:GPC

Hayes:1993:WF

Hildebrand:1993:RPF

Hormann:1993:GBR

Hormann:1993:PRN

Hormann:1993:QNU
Hormann:1993:TRM


Jebelean:1993:CSG


Kalkuhl:1993:PDC


Kanellakis:1993:IDM


Kankaala:1993:BLC

REFERENCES


REFERENCES


[Lee:1993:GRB]


[Li:1993:IKC]


[Lin:1993:NCP]


[Loparo:1993:LER]


[Makino:1993:SPR]


[Marsaglia:1993:LHR]


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


Morris:1993:NL


N:1993:BR


Nelson:1993:CVM


Nelson:1993:RMC


Niederreiter:1993:FFP

in Communications and Computing held at the University of Nevada, Las Vegas, August 7–10, 1991.


[1862] 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 [1384, 1492, 1847, 1872]. The authors report that they would now recommend the MCG $x_{n+1} = 48271x_n \mod (2^{31} - 1)$ over their original $x_{n+1} = 16807x_n \mod (2^{31} - 1)$.

REFERENCES


REFERENCES

December 1993. CODEN SIREAD. ISSN 0036-1445 (print), 1095-7200 (electronic).


REFERENCES


REFERENCES


REFERENCES


Cooperman:1994:RBC


Coppersmith:1994:SG


Corcoran:1994:MVC

[1906] 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 Vigenère 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


Cuccaro:1994:TTQ


Davis:1994:CRA

[1909] Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic randomness from air turbulence in disk drives. In Desmedt [4098], pages


Eichenauer-Herrmann:1994:DIP


Eichenauer-Herrmann:1994:DQC


Eichenauer-Herrmann:1994:EIC


Eichenauer-Herrmann:1994:GIC


Eichenauer-Herrmann:1994:ILB


Eichenauer-Herrmann:1994:SIN

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Karian:1994:RNG


Karloff:1994:CWI


Kenney:1994:HTI


Kreyszig:1994:MCM


Lavastre:1994:SAS


REFERENCES


Luscher:1994:PHQ


Ma:1994:IMC


MacLaren:1994:CPN


Makino:1994:LFR


Marsaglia:1994:MAR


Marsaglia:1994:REI


Marsaglia:1994:SPV

February 1994. CODEN CPHYE2. ISSN 0894-1866 (print), 1558-4208 (electronic).


D. V. Pryor, S. A. Cuccaro, M. Mascagni, and M. L. Robinson. Implementation of a portable and reproducible parallel pseudorandom num-
REFERENCES


ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content~content=a748639261~db=all~order=page.


REFERENCES


Zhang:1994:PEE


Zijp:1994:UTC


Ahrens:1995:OTM


Al-Hussaini:1995:UPT


Anguita:1995:CDP


Antipov:1995:COP

REFERENCES


Chou:1995:LTI


Chou:1995:PLI


Chow:1995:NRP


Compagner:1995:OCR


Couture:1995:LRC


Cusick:1995:PPN


REFERENCES


REFERENCES


REFERENCES

[Marsaglia:1995:MRN]

[Marsaglia:1995:RVI]


[Mascagni:1995:PPNa]


[Matus:1995:CIAa]

[Matus:1995:CIAb]


REFERENCES


Pattanaik:1995:AER


Penrice:1995:AEP


Percus:1995:TAM


Phatak:1995:LMP


Pickover:1995:GET


Pickover:1995:RNG

REFERENCES

Powell:1995:LEP


Ramon:1995:PKV


Regan:1995:PGM


Ross:1995:TCP


Sakamoto:1995:CMC


Savory:1995:UMA


Schmid:1995:EMC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2187] Ping Luo. The two-dimensional structure of the sequence of random numbers generated by multiplicative congruential generators. Journal
REFERENCES


REFERENCES


REFERENCES


Sipper:1996:CEP


Sipper:1996:GPR


Takashima:1996:HWT


Takashima:1996:LVT


Takashima:1996:STT


Ugrin-Sparac:1996:NAG


Ugrin-Sparac:1996:PET

[2220] G. Ugrin-Šparac and D. Ugrin-Šparac. On a possible error of type II in statistical evaluation of pseudo-random number genera-


REFERENCES


REFERENCES


Berblinger:1997:MCI


Berg:1997:CNF


Binder:1997:AMC


Binder:1997:MCS


Cario:1997:MGR


Coddington:1997:RNG

REFERENCES


Eichenauer-Herrmann:1997:CCC


Eichenauer-Herrmann:1997:ICP


Eichenauer-Herrmann:1997:PSN


Eichenauer-Herrmann:1997:QCP


Emmerich:1997:EPQ


[2266] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breiteneker [4119], page ?? ISBN 3-901608-11-7. LCCN ????


REFERENCES


REFERENCES


Marsaglia:1997:RNG

[2287] 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


Naor:1997:NTC


Pincus:1997:APR


Schaber:1997:DIC


Shchur:1997:CMC


Shchur:1997:SDR


Slone:1997:EBR


Woodward:1997:ECD


Wu:1997:MCR


Zubkov:1997:PTD


Aiello:1998:DPP


Andreev:1998:NGD


Antoch:1998:RPN

REFERENCES


REFERENCES


Emmerich:1998:SIP


Entacher:1998:BSW


Entacher:1998:LIP


Entacher:1998:LCG


Evans:1998:RVG


Fuster-Sabater:1998:LPS

A. Fuster-Sabater and L. J. Garcia-Villalba. Likelihood that a pseudorandom sequence generator has optimal properties. Electronics Let-
Gammel:1998:HRR


Garcia:1998:GCE


Gentle:1998:RNG


Gutmann:1998:SGP


Hamilton:1998:AEP


patent application number 08/648,553, filed 15 May 1996 by Intel Corporation.


[2356] Donald E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, third edi-
REFERENCES

Kolmogorov:1998:TRN


Larcher:1998:DPS


LECuyer:1998:GPI


LECuyer:1998:RNGa


LECuyer:1998:RNGb


LECuyer:1998:RNGb

REFERENCES


REFERENCES

(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


Mascagni:1998:PLC


Matsumoto:1998:DCP


Matsumoto:1998:MTD


REFERENCES

Mende:1998:MSP


Miller:1998:BPG


Morohosi:1998:DAR


Niederreiter:1998:AGA


Niederreiter:1998:NSA


Owen:1998:LSS


Park:1998:AGC

[2381] Chul Gyu Park and Dong Wan Shin. An algorithm for generating correlated random variables in a class of infinitely divisible distribu-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2430] Bernd Gärtner. Ein Reifall mit Computer-Zufallszahlen. (German) [A failure with computer random numbers]. *Mitteilungen der Deutschen
REFERENCES

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

[2431] 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

[2432] Oded Goldreich. Modern cryptography, probabilistic proofs, and pseudo-
randomness, volume 17 of Algorithms and combinatorics. Springer-Ver-
ISBN 3-540-64766-X. ISSN 0937-5511. xv + 182 pp. LCCN QA76.9.A25
G64 1999.

Gonzalez:1999:RNG

[2433] 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
science/article/pii/S0010465599002337.

Griffin:1999:DNR

[2434] Frances Griffin, Harald Niederreiter, and Igor Shparlinski. On the dis-
tribution of nonlinear recursive congruential pseudorandom numbers of
higher orders. In Fossorier et al. [4131], pages 87–93. ISBN 3-540-
enhancements/fy0812/99054502-d.html.

Haastad:1999:PGO

A pseudorandom generator from any one-way function. SIAM Journal
on Computing, 28(4):1364–1396, August 1999. CODEN SMJCAT. ISSN
org/sam-bin/dbq/article/24470.

Intel:1999:IRN

[2436] Intel Platform Security Division. The Intel random number generator. In-
intel.com/design/security/rng/techbrief.pdf.
REFERENCES


[2455] Moni Naor and Omer Reingold. Synthesizers and their application to the parallel construction of pseudo-random functions. *Journal of Com-
REFERENCES


REFERENCES

of-rsa.ppt. Presented at the 1999 RSA Data Security Conference, San Jose, CA.


REFERENCES


[2482] 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.


REFERENCES

Borkowf:2000:BRB


Brent:2000:TYA


Chen:2000:RRI


Couture:2000:LCR


Danger:2000:EFI


Deng:2000:RNG

REFERENCES


REFERENCES


REFERENCES


[2524] 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.


REFERENCES


[2534] Harald Niederreiter and Igor E. Shparlinski. Exponential sums and the
distribution of inversive congruential pseudorandom numbers with prime-
ISSN 0065-1036 (print), 1730-6264 (electronic).

[2535] H. Niederreiter and A. Winterhof. Incomplete exponential sums over
finite fields and their applications to new inversive pseudorandom num-
ber generators. *Finite Fields and their Applications*, 93(??):387–399,
???? 2000. CODEN FFTAFM. ISSN 1071-5797 (print), 1090-2465 (elec-
tronic).

[2536] Takuji Nishimura. Tables of 64-bit Mersenne twisters. *ACM Transac-
CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

[2537] NIST. Random number generation and testing. World-Wide Web site.,

[2538] 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 fac-
ulté des études supérieures en vue de l’obtention du grade de Maître es
sciences (M.Sc.) en informatique option recherche opérationnelle.

for applications in cryptography. *IEEE Journal of Solid-State Circuits*,
47(5):615–621, ????. 2000. CODEN IJSCBC. ISSN 0018-9200 (print),
1558-173X (electronic).

Physics Communications*, 124(2–3):125–131, February 2000. CODEN
CPHCBZ. ISSN 0010-4655 (print), 1879-2944 (electronic). URL http://


REFERENCES


REFERENCES


[2565] Lawrence Barker, Henry Rolka, Deborah Rolka, and Cedric Brown. Statistical practice — equivalence testing for binomial random variables:

[Battaglia:2001:GAP]


[Batu:2001:TRV]


[Chamayou:2001:PRN]


[Chen:2001:ING]


[Chick:2001:NPS]


[Chowdhury:2001:ESI]


[2584] 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 $A = 31167285 = 0x1db9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.


[2589] Julio César Hernández, José María Sierra, Arturo Ribagorda, Benjamín Ramos, and J. C. Mex-Perera. Distinguishing TEA from a ran-

Hernandez:2001:FNO


Hernandez:2001:GAC


Howgrave-Graham:2001:PRN


Iwata:2001:PAF


Johnson:2001:CCO

REFERENCES


REFERENCES


REFERENCES


REFERENCES


RAND:2001:MRD


Raqab:2001:ELS


Rukhin:2001:STS


Rukhin:2001:TRS


Schindler:2001:EOT


[2647] 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.


REFERENCES


REFERENCES

CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).


REFERENCES


REFERENCES

Friedel:2002:FGR


Futschik:2002:EFE


Gangnon:2002:MDE


Gennaro:2002:CPG


Gilbert:2002:NRP


Gleeson:2002:TRN


Golic:2002:SWM


REFERENCES


Janke:2002:PRN


Jeruchim:2002:FRV


Jeruchim:2002:MCS


Jones:2002:KTP


Karras:2002:SPB


[2706] George Marsaglia. Re: *good* 64-bit random-number generator. Posting to the sci.crypt.random-numbers news group, September 3,


REFERENCES

McCullough:2002:ASP


McCullough:2002:DMF


McCullough:2002:RNG


Mita:2002:PBG


Moon:2002:IDC


Murray:2002:IYP


Niederreiter:2002:ADI


Niederreiter:2002:ICS


Niederreiter:2002:RAT


NIST:2002:ERN


Papoulis:2002:PRV


Philipp:2002:MTD

REFERENCES


REFERENCES


REFERENCES

494

Umans:2002:PRG


Wang:2002:HOL


Wang:2002:NCT


Wu:2002:BPR


Yaguchi:2002:CLP


Yao:2002:CBR

REFERENCES


[2744] 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.”.


[2749] 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).


Engel:2003:BLE


Epstein:2003:DIT


Galmes:2003:ACM


Gentle:2003:RNG


Gibbons:2003:NSI


Goldreich:2003:SME

Oded Goldreich and Vered Rosen. On the security of modular exponentiation with application to the construction of pseudorandom genera-
Gonnet:2003:RTT


Goresky:2003:EMC


Grabner:2003:CGD


Guimond:2003:SPI


Gutierrez:2003:LNC


Hellekalek:2003:EEC

REFERENCES


REFERENCES


Maaranen:2003:UQR


Marsaglia:2003:EKD


Marsaglia:2003:RNG


Marsaglia:2003:TOS


Marsaglia:2003:XR


Matsumoto:2003:SDT


Srinivasan:2003:TPR


Stipcevic:2003:NDR


Sugita:2003:DRW


Tang:2003:SDA


Tang:2003:SPM


Tsang:2003:TCT


[2816] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complex-


[Borwein:2004:MEP]


[Brent:2004:NMX]


[Brown:2004:TRV]


[Bucklew:2004:IRE]


[Conflitti:2004:MDS]

REFERENCES

Deng:2004:GMP


Dorfer:2004:CFE


Espejo:2004:ANR


Feige:2004:SIR


Fung:2004:AIH


Goubin:2004:CLF

REFERENCES

Guan:2004:PNG

Gupta:2004:DBG

Gutmann:2004:CSA

Haldir:2004:HCL

Hernandez:2004:STN

Hong:2004:DCT
Hormann:2004:ANR


Jeske:2004:TAM


Kim:2004:CNS


Kim:2004:CRN


Knight:2004:PDU


LEcuyer:2004:DLR

REFERENCES


REFERENCES


REFERENCES

Schmuland:2004:CLT


Sezgin:2004:MSS


Sugita:2004:SPR


Szczepanski:2004:BRN


Tang:2004:SGM


Tirler:2004:EKR

REFERENCES


REFERENCES


REFERENCES


[2898] Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of


REFERENCES


Falcioni:2005:PMC


Gennaro:2005:IPR


Gerlovina:2005:ABL


Gonnet:2005:MRG


Gonzalez:2005:SCM

REFERENCES


Gubernatis:2005:MRM


Hahn:2005:CLM


Hamano:2005:DSD


Hess:2005:LCM


Hill:2005:RDS


Horan:2005:NRN


Kang:2005:ETP

REFERENCES


REFERENCES


REFERENCES


Liang:2005:NPR


Lim:2005:EMT


Louchard:2005:MRU


Marsaglia:2005:MGF


Marsaglia:2005:RPO


REFERENCES


Jeff T. Terpstra. Some illustrative classroom examples regarding sums of discrete random variables with finite support. *The American Statistician*,

Topuzoglu:2005:LCP


Tu:2005:SRD


Wichmann:2005:GGP


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ


Aistleitner:2006:NZG


Alon:2006:MPF


Aly:2006:LCP


Anonymous:2006:E

REFERENCES

Barak:2006:ERU


Barash:2006:POE


Barker:2006:RRN


BenAtti:2006:BMA


Berkovitz:2006:EHR


Brent:2006:FRR


[2977] Edwin D. El-Mahassni, Igor E. Shparlinski, and Arne Winterhof. Distribution of nonlinear congruential pseudorandom numbers modulo al-

Evans:2006:DOS


Faure:2006:SCR


Feige:2006:SIR


Finnigin:2006:CPN


Galperin:2006:SSU


Gammel:2006:LFN

REFERENCES


[2990] Laszlo Hars. Modular inverse algorithms without multiplications for cryptographic applications. EURASIP Journal on Embedded Systems,
REFERENCES


REFERENCES


520, December 2006. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).

L’Ecuyer:2006:TSL


Lee:2006:HGN


Lee:2006:IBH


Maffre:2006:WKT


Marsaglia:2006:RCS


REFERENCES


REFERENCES


Schmidt:2006:BRJ


Schroeder:2006:RNG


Sezgin:2006:DLP


Simka:2006:MTR


Skoge:2006:PHH

REFERENCES


generator [1048] developed for 16-bit arithmetic to a new four-part combination generator for 32-bit arithmetic with a period of $2^{121} \approx 10^{36}$.


Bhatnagar:2007:ANB


Brent:2007:SLP


Brown:2007:SAN


Cheung:2007:HGA


Chiu:2007:CKC


Cowles:2007:BRB

REFERENCES

Delfs:2007:ICP


Doornik:2007:CHP


Dorrendorf:2007:CRNa


Dorrendorf:2007:CRNb


Drutarovsky:2007:RCB

REFERENCES


Hars:2007:PRS


Hasan:2007:FSU


Hormann:2007:ITD


Hormann:2007:SGD


Juneja:2007:AFS


Kang:2007:PFS

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
REFERENCES


Kundu:2007:CWG


Kung:2007:RFB


LEcuyer:2007:EPB


LEcuyer:2007:LRN


LEcuyer:2007:TCL


LEcuyer:2007:TSL

[3072] Pierre L’Ecuyer and Richard Simard. TestU01, a software library in ANSI C for empirical testing of random number generators: User’s guide,

Lim:2007:MCA


Liu:2007:NLR


Matsumoto:2007:CDI


Matsumoto:2007:FSC


Meidl:2007:LCP


Mislove:2007:DRV

REFERENCES


REFERENCES


Perez:2007:RJI


Rusu:2007:PRN


Santhanam:2007:CLB


Sathyanarayana:2007:GPS


Sinescu:2007:GIR


REFERENCES

“Special Issue: Field Programmable Technology. Guest Editors: Gordon Brebner, Samir Chakraborty, and Weng-Fai Wong”.


REFERENCES


REFERENCES


REFERENCES

Haramoto:2008:EJA


Haramoto:2008:FJA


Holleman:2008:WCT


Hou:2008:LPD


Howes:2008:U


Inaltekin:2008:ANE

[3149] Hazer Inaltekin and Stephen B. Wicker. The analysis of Nash equilibria of the one-shot random-access game for wireless networks and the behavior
REFERENCES


**Jang:2008:CDH**


**Joe:2008:CSS**


**Jovanovic-Dolecek:2008:UMT**


**Kalos:2008:MCM**


**Kang:2008:HPP**


**Kato:2008:QSC**

REFERENCES


[3172] 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
REFERENCES


REFERENCES


Petit:2008:BCB


Petit:2008:EPR


Reuillon:2008:RDS


Rousseau:2008:RNG


Rukhin:2008:TRA


Rumley:2008:PRN

REFERENCES


[Saito:2008:SOF]


[Schlier:2008:SHS]


[Schneier:2008:SSR]


[Shen:2008:RRL]


[Sinescu:2008:CLR]


[Sinescu:2008:GLR]

REFERENCES


REFERENCES


Varbanets:2008:ESS


Varbanets:2008:ICGa


Varbanets:2008:ICGb


Walker:2008:EPN


Wang:2008:DCP


Ware:2008:RIE


Wikramaratna:2008:ACR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

sciences, 367(1901):3281–3296, August 28, 2009. ISSN 1364-503x (print), 1471-2962 (electronic).


Devroye:2009:RVG


Devroye:2009:RVG


Dodson:2009:IGT


Dogaru:2009:HCA


Dorrendorf:2009:CRN

REFERENCES

Edrees:2009:HOZ


Faure:2009:GHS


Feldhofer:2009:HIS


Fischer:2009:SRF


Galassi:2009:GSL


Gao:2009:MPL

[3263] Zhi-Han Gao and Fang-Wei Fu. The minimal polynomial over $\mathbb{F}_q$ of linear recurring sequence over $\mathbb{F}_{q^m}$. *Finite Fields and their Applications,*
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Katti:2009:EHI


Ladd:2009:FRN


Langdon:2009:FHQ


Laracy:2009:RVG


LEcuyer:2009:LRN


LEcuyer:2009:TV

REFERENCES


REFERENCES


Nekrutkin:2009:STS


Nies:2009:CR


Okten:2009:GNK


Orlov:2009:ORN


Paindaveine:2009:MRT


Pareschi:2009:PAC


REFERENCES


[3340] Senhua Yu and D. Dasgupta. An empirical study of Conserved Self Pattern Recognition Algorithm: Comparing to other one-class classifiers and


REFERENCES


Anashin:2010:NAE


Anyanwu:2010:DCS


Banks:2010:DES


Barsegov:2010:EPR


Bassham:2010:STS


Bastos-Filho:2010:IRN

REFERENCES


Bellare:2010:PFP


Berger:2010:FFF


Binder:2010:MCS


Blacher:2010:PRN


Borovkov:2010:ILL


Braverman:2010:PGR


[3363] Shih-Liang Chen, TingTing Hwang, and Wen-Wei Lin. Randomness enhancement for a digitalized modified-logistic map based pseudo random
REFERENCES

Cheong:2010:ERE


Chi:2010:GPR


Derflinger:2010:RVG


DeRoover:2010:MPR


deSchryver:2010:NHE

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,
REFERENCES


REFERENCES

bw.de/bsz314370110vor.htm; http://www.gbv.de/dms/zbw/609423665.pdf.


REFERENCES


Murguia:2010:IAP


NanoOpticsGroup:2010:HBR


Navin:2010:CSR


Navin:2010:ETU


Ning:2010:GRO


REFERENCES


Pareschi:2010:ITH


Pashley:2010:GRN


Passerat-Palmbach:2010:RIG


Peris-Lopez:2010:CSP


Plesser:2010:RSI

[3419] Hans Ekkehard Plesser and Anders Grønvik Jahnsen. Re-seeding invalidates tests of random number generators. Applied Mathematics and
**REFERENCES**


REFERENCES


Saito:2010:VMT


Segui:2010:AIP


Seznec:2010:PCM


Shen:2010:PQR


Shi:2010:MED


Shin:2010:AFG


Srinivasan:2010:ADP

S. Srinivasan, S. Mathew, R. Ramanarayanan, F. Sheikh, M. Anders, H. Kaul, V. Erraguntla, R. Krishnamurthy, and G. Taylor. 2.4GHz


REFERENCES


REFERENCES

Wu:2010:ULT


Xiaohui:2010:DCR


Xin:2010:IEB


Ying:2010:DRN


Yoo:2010:IRR


Yu:2010:NRN

REFERENCES


Zafar:2010:GRN


Zhmurov:2010:EPR


Zimand:2010:SEC


Abbott:2011:NNS


Abbott:2011:QRN


Al-Abiachi:2011:CDN

REFERENCES


[3472] 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.”.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Hwang:2011:SID


Jian:2011:TBQ


Kao:2011:EAT


Kleimo:2011:RNG


Koucky:2011:PGG


LEcuyer:2011:AZV


REFERENCES


[3545] Carolyn L. Phillips, Joshua A. Anderson, and Sharon C. Glotzer. Pseudorandom number generation for Brownian Dynamics and Dissipative Par-


[3550] 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. [4199], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ???.

REFERENCES


Seyedzadeh:2011:IES


Shaolan:2011:EDE


Shparlinski:2011:ADP


Simard:2011:CTS


Sinescu:2011:ECS


Soucarros:2011:ITT


REFERENCES


REFERENCES


REFERENCES


Cesaratto:2012:PRK


Chen:2012:ECR


Chi:2012:ESN


Chiu:2012:MTR


Cohen:2012:SMI


Colbeck:2012:FRC

REFERENCES


REFERENCES


[3617] W. Kaczynski, L. Leemis, N. Loehr, and J. McQueston. Nonparametric random variate generation using a piecewise-linear cumulative distribu-


[3623] Y. Li, P. Chow, J. Jiang, M. Zhang, and S. Wei. Software/hardware framework for generating parallel Gaussian random numbers based on

[3624] 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/.


REFERENCES


QUANTIS: 2012: REQ


RAINVILLE: 2012: EOL


REUILLON: 2012: PSS


RIESEL: 2012: PNC


SAITO: 2012: DCS


SAITO: 2012: RGR


REFERENCES


[3664] 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.
REFERENCES

Beliakov:2013:EIBa


Beliakov:2013:EIBb


Claessen:2013:SPN


Deng:2013:FTQ


Ducklin:2013:ARN

REFERENCES


REFERENCES


REFERENCES

Khoshkenar:2013:NTR


Lang:2013:TRS


Leonenko:2013:BRD


Liberty:2013:THR


Liu:2013:ITT


Ma:2013:PQR

[3688] 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,
REFERENCES

Malik:2013:UCB


Martino:2013:EEG


Mascagni:2013:PPR


Meka:2013:PGP


Melia-Segui:2013:JPL


Miszczak:2013:EOQ


Colas Schretter and Harald Niederreiter. A direct inversion method for non-uniform quasi-random point sequences. *Monte Carlo Methods and


REFERENCES


REFERENCES

[3719] Luc Devroye. Random variate generation for the generalized inverse
2014. CODEN STACE3. ISSN 0960-3174 (print), 1573-1375 (elec-
tronic). URL http://link.springer.com/article/10.1007/s11222-
012-9367-2.

[3720] 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 Mathe-
matics, Weizmann Institute; Dept. of Computer Science, Northeastern
University, New York, NY, USA; Tel Aviv, Israel; Boston, MA, USA,


B. J. Sussman. Efficient Raman generation in a waveguide: A route to
104(5):051117:1–051117:4, ????. 2014. CODEN APPLAB. ISSN 0003-
6951 (print), 1077-3118 (electronic), 1520-8842. URL ????.

[3723] 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 Applica-
tions (JIISA)*, 19(1):78–87, February 2014. CODEN ????. ISSN 2214-
S221421261400012X.

[3724] Akio Fukushima, Takayuki Seki, Kay Yakushiji, Hitoshi Kubota, Hi-
roshi 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. CO-
DEN APEPC4. ISSN 1882-0778 (print), 1882-0786 (electronic).


REFERENCES

Kawai:2014:ADT


Koo:2014:CRB


Korzen:2014:PPP


Langr:2014:APP


LEcuyer:2014:LSS


Ling:2014:MDN

Liu:2014:LFP


Mascagni:2014:HPC


Mohamed:2014:MCS


Mortari:2014:MAV


Raaphorst:2014:CSC

REFERENCES


REFERENCES

Moufek:2015:MCB


NIST:2015:SSP


Nuida:2015:MPS


Passerat-Palmbach:2015:TSS


Pollack:2015:SNN


Potter:2015:MUE


Raitza:2015:RRN

REFERENCES

December 2015. CODEN ???? ISSN 1936-7406 (print), 1936-7414 (electronic).


REFERENCES


REFERENCES

Balkova:2016:APN


Bayon:2016:FME


Chang-Fong:2016:CSC


Chattopadhyay:2016:ETS


Chen:2016:PEP


deAndrade:2016:RNG

[3796] B. B. de Andrade, H. Bolfarine, and A. N. Siroky. Random number generation and estimation with the bimodal asymmetric power-normal


REFERENCES


Mandal:2016:DIW


Mandal:2016:FRI


McFarland:2016:MZA


Miller:2016:RPS


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA

REFERENCES


Raitza:2016:RRN


Savvidy:2016:ACS


Savvidy:2016:SEC


VanBever:2016:SBT


Vigna:2016:EEM


Yamakami:2016:PGA


[3825] 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 [3833] for details of the attack.


[3828] George Barmpalias, Douglas Cenzer, and Christopher P. Porter. The probability of a computable output from a random oracle. *ACM Trans-
REFERENCES


Barmpalias:2017:RNP


Beebe:2017:MFC


Bernardini:2017:MRP


Chalk:2017:CIR


Cohney:2017:PSR


Deng:2017:DPR

REFERENCES

e1404:??, September/October 2017. CODEN ???? ISSN 1939-0068 (print), 1939-5108 (electronic).


REFERENCES


REFERENCES


January 2017. CODEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic).


[3860] Karolos Antoniadis, Peva Blanchard, and Julien Stainer. The entropy of a distributed computation random number generation from memory


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3908] 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(??):
Kissel:2019:KRC


Lemire:2019:FRI


Lemire:2019:XXX


Liu:2019:LFP


Martirosyan:2019:STM


Poudel:2019:MTU

Quaglia:2019:RCR


SoltaniPanah:2019:CDG


Steele:2019:UBP


Ueno:2019:TBP


Viola:2019:CEP


Xu:2019:NPF


Zhang:2019:REU

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 [3863, 3864].


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Luengo:2023:STS

[3986] Elena Almaraz Luengo, Bittor Ala˜na Olivares, Luis Javier García Vil-

lalba, Julio Hernandez-Castro, and Darren Hurley-Smith. StringENT
test suite: ENT battery revisited for efficient P

Pandit:2023:LBQ

[3987] Anupama Arjun Pandit, Atul Kumar, and Arun Mishra. LWR-based quantum-safe pseudo-random number generator. Journal of Informa-
article/pii/S2214212623000169.

Pratihar:2023:BSF

[3988] Kuheli Pratihar, Urbi Chatterjee, Manaar Alam, Rajat Subhra

Saini:2023:CNF

[3989] A. Saini, A. Tsokanos, and R. Kirner. CryptoQNRG: a new frame-
work for evaluation of cryptographic strength in quantum and pseudo-
random number generation for key-scheduling algorithms. The Journal

Shparlinski:2023:FPS

[3990] Igor E. Shparlinski. Fixed points of the subset sum pseudorandom number
springer.com/article/10.1007/
s10623-023-01209-5.

Yao:2023:LOT

[3991] Liang Yao, Huaguo Liang, and Yingchun Lu. Low-overhead TRNG based
on MUX for cryptographic protection using multiphase sampling. The
JOSUED. ISSN 0920-8542 (print), 1573-0484 (electronic). URL https://


[4004] 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/.


REFERENCES


REFERENCES


REFERENCES


M. A. H. Dempster, editor. Stochastic programming: proceedings of an international conference sponsored by the Institute of Mathematics and


REFERENCES


REFERENCES


REFERENCES

Mehlhorn:1985:SAS


ACM:1986:PEA


Arkin:1986:SOP


DAgostino:1986:GFT


Heath:1986:HMP


Wilson:1986:WSC


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

719


[4084] Gustavus J. Simmons, editor. Contemporary Cryptology: the science of information integrity. IEEE Computer Society Press, 1109 Spring Street,
REFERENCES


REFERENCES

LCCN QA3 .L35 v.1554.


REFERENCES

ACM-SIAM:1994:ASD


ACM:1994:PTS


Desmedt:1994:ACC


IEEE:1994:PSW


Snodgrass:1994:PAS

REFERENCES


[4112] 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,
REFERENCES 725


Cohen:1996:FFA


IEEE:1996:ASF


Trobec:1996:PIW


Andradottir:1997:PWS


Gell-Mann:1997:QJA

IEEE:1997:ASF


Troch:1997:PSI


Wyrzykowski:1997:PNP


Banks:1998:HSP


Buhler:1998:ANT


Hellekalek:1998:RQR

REFERENCES


REFERENCES

Anonymous:1999:NIS


Fossorier:1999:AAA


Heath:1999:APP


Iliev:1999:RAN


Niederreiter:1999:MCQ

REFERENCES


REFERENCES


REFERENCES


Fang:2002:MCQ


USENIX:2002:PBF


Rudnicki:2003:OIP


ACM:2004:PAA


Gentle:2004:HCS


REFERENCES


REFERENCES


Schroeder:2006:NTS


Ytrehus:2006:CCI


ACM:2007:SPA


Adams:2007:SAC


Altiok:2007:SMA


Menezes:2007:ACC

REFERENCES


Simos:2007:CMS


ACM:2008:SPA


Golomb:2008:STA


IEEE:2008:ICA


Keller:2008:MCQ

[4177] Alexander Keller, Stefan Heinrich, and Harald Niederreiter, editors. Monte Carlo and Quasi-Monte Carlo methods 2006. Springer-Ver-
REFERENCES


REFERENCES


LEcuyer:2009:MCQ


Paredaens:2009:PTE


ACM:2010:PAI


Anonymous:2010:NDS


Cont:2010:EQF


Dick:2010:DNS

REFERENCES


REFERENCES

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).

on Theory of Computing: June 6–8, 2011, San Jose, CA, USA. ACM


[4198] IEEE, editor. International Conference on Intelligent Computation Tech-
nology 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
ieee.org/servlet/opac?punumber=5750113.

[4199] Scott Lathrop, Jim Costa, and William Kramer, editors. SC’11: Proceed-
ings 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 ????

ence. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / Lon-
REFERENCES

vanTilborg:2011:ECS


ACM:2012:SPA


Cooper:2012:HWC


Dunn:2012:EMC


Dyson:2012:TCO


Gentle:2012:HCS

REFERENCES


Hwu:2012:GCG


IEEE:2012:PIA


ACM:2013:SPF


Bailey:2013:CAM


Higham:2015:PCA

REFERENCES

Osais:2017:CSF


Rubinstein:2017:SMC


Krhizhanovskaya:2020:CSI