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: http://www.math.utah.edu/~beebe/

06 October 2018
Version 1.295

Title word cross-reference

#14 [2264]. #15949 [868]. #4059 [1238]. #8373 [2087].

(0, 1) [1050]. (0, s) [2519, 2902]. (a^n - 1)/(a - 1) [914]. (j, c) [727]. (n^2) [2472]. (n^k) [2473]. (na) [2472]. (t, m, s) [2031, 2862, 2037, 2336]. (t, s) [2614, 2031, 2327, 2862, 2037]. (X^2 - Y^2)^1/2 [489]. 0.1(0 \times 1)0 \times 9 [139]. 1 [734, 872, 2815, 171, 709, 2937, 2939]. 1, 2, 3 [3448]. 1.13198824... [2496]. 10,000 [282]. $10.00 [168]. 10^{2857} [2467]. 10^{325} [2029]. 1200\mu [3096]. 128 [3121]. 13 [270]. 16 [270]. 2 [2815, 2106, 926, 3061, 2481, 2795, 2941]. 2, 000 [86]. $24.95 [2074]. 2^{-31} - 1 [834, 927]. 2^{15} [2124]. 2^{31} - 1 [3498, 799, 970, 1063, 1191, 1192]. 2^{31} - 69 [3344]. 2^{32} - 1 [1083]. 2^a [1468, 2224]. 2^b [1311, 1474, 1720]. 2^k [2595]. 2^{k-1} [2595]. 2^p [3208]. 2^p - 1 [2257]. 3 [1774, 3624]. 32 [3579]. 4 [270]. 48 [245]. 5 [270]. $52.95 [3548]. 64
\[ \beta = 48 \pm 32 \pm 1 \]
0.57pJ [3221]. 0.57pJ/bit [3221]. '05 [3879, 3883]. '07 [3889]. '08 [3893].
1 [744, 1039, 1909, 1910, 3238, 3236]. 1.04 [3155]. 1.1 [3644]. 1.6 [3580]. '10
[3736, 3900, 3816]. 12 [2813]. 120 [2441, 3114]. 12th [3883].
'13 [3926]. 133 [265, 266, 303, 309]. 134 [872]. 13th [3852]. 14th
[3890, 3819]. 153 [925, 1081, 1082]. 155 [922, 1082]. 157 [973]. 16
2 [194, 219, 2242, 3329]. 2.4GHz [3339]. 20 [2074, 2408]. 200 [298, 359].
[3916]. 2014 [3657]. 204 [1080]. 205 [1091]. 20MHz [2524]. 20th
29th [3797, 3781]. 2nd [3754, 3767].
3 [3066, 3652, 1930, 3330]. 3-Key [2844]. 3.0 [2616]. 3.x [2263]. 30 [3459].
[1208, 2921, 2991, 1728, 3343]. 32-bit-word [533]. 334 [426, 471]. 33rd
[505, 607]. 38th [3839]. 39th [3889].
4 [457, 656, 3331]. 4086 [2829]. 40th [3803]. 41st [3860]. 42 [675, 676].
48-Bit [1017]. 488 [658]. 4Gbps [3221].
5.0 [1628]. 5.2 [2732]. 500 [3273, 318]. 51st [3910]. 52 [868]. 52nd [3925].
5th [3894].
60th [3927]. 61 [1227]. 623-dimensionally [2321]. 64-bit


= [3733, 3743].
Advancing [3898].

AES [2702, 2453, 2534, 2844].

Ahrens [2702, 2453, 2534, 2844].

Alternating [2401, 1195, 162, 49].

Alternatives [2900, 3507, 1444].

Almost All-Optical [2900, 3507, 1444].

Almost Algebraic-Geometry [2900, 3507, 1444].

alignments [1841].


algorithmic [1706, 554, 1545, 3843].

algorithmische [554].

algorithmischer [1706].


Arias [2873, 1365, 975, 894].

alignments [1841].

All-Digital [3221, 3339].

All-Optical [3522].

alla [461].

Alley [1942, 1828, 1949].

Allocation [627, 670, 710, 2603, 3293].

Almost [2900, 3507, 1444].

Along [3722].

Alternating [3006].

Alternative [3403, 802, 1893, 2551, 2727].

Alternatives [2401, 1195, 162, 49].

Alto [3926, 3845].

Amer [1238, 1008].

America [3548].

American [3736, 3801, 3731].

Amiel [315].

Among [2370, 1492, 282, 823, 1855, 2025, 2026, 2397, 2426].

Amplification [2558, 2724].

Amplified [3355, 3496].

amplifier [3368, 3369].

Amsterdam [3774].

Anal [908].

analiz [346].

Analog [349].

Analog-Digital [349].

Analogue [195, 1093, 540].

analyse [3743].

Analyses [1770, 2957].

Analysis [3029, 3693, 3032, 2263, 2082, 918, 919, 737, 3390, 963, 1178, 3667, 1858, 398,
analysis [2927, 2853, 3432, 765, 1698, 2714, 2858, 3303, 2647, 984, 1051, 3308, 3207, 1710, 1213, 1268, 2561, 3687, 3212, 1931, 646, 450, 2050, 724, 261, 2055, 2580, 2586, 2956, 3016, 207, 1541, 2346, 2347, 3236, 3465, 19, 234].

Analytic [1979, 1054].

Analytical [2521, 351, 3927].

Analyzing [2179, 2204, 1332, 2128].

anaylsis [488, 600].

Andersen [235].

Anderson [1011, 2466].

Android [3565].

Angeles [3729, 3776, 90].

angen¨aherten [275].

Angle [505, 607].

animals [1846].

Ann [675, 676].

Annealing [3615, 2949].

Annual [3870, 3874, 3879, 3889, 3893, 3926, 3904, 3797, 3758, 3793, 3803, 3826, 3835, 3839, 3860, 3910, 3925, 3767, 3891, 3869, 3856, 3808, 3749, 3817, 3763, 3768, 3773, 3779, 3784, 3789, 3800, 3818, 3823, 3832, 3850, 3857, 3819, 3859, 3755, 3766, 3781, 3877].

ANSI [2844, 2545, 2641, 2926, 2994].

Anthanasios [384].

Antithetic [703, 710, 2018].

Antony [3858].

ANTS [3843].

ANTS-III [3843].

any [344, 2383, 75, 599].

Aperiodic [3665, 2700, 3574, 3112, 1553].

APG [1816].

apparent [815].

Appearing [1500].

Appears [1317].

Appendix [2844].

Appl [2242, 3549].

Apple [1116, 1230].

Applesoft [1316].

applicability [1124].

Application [3365, 827, 3032, 3764, 878, 2756, 3774, 299, 2696, 2625, 3068, 1583, 2226, 2459, 2306, 43, 3096, 3539, 2953, 860, 287, 3124, 3233, 3150, 2823, 1970, 3393, 2758, 3908, 3286, 2703, 3421, 3422, 3295, 1095, 3524, 2041, 1160, 2800, 685, 949, 724, 1220, 2411, 135, 3127, 1548, 3138, 2678, 7].

Application-based [1583, 3524].


Applied [3740, 3736, 3731, 3169, 3907, 1136, 3928, 3804, 2159, 487, 316, 41, 239, 473, 2237, 3749, 3852].

Applying [3376, 2040, 3600].


approaches [2675].


Approximately [498, 1788].

Approximating [2442, 3427].

Approximation [2189, 2368, 2386, 1414, 1499, 2810, 2499, 1843, 3056, 1252, 1097, 1220, 729].

Approximations [143, 2769, 1046, 475, 999, 2989, 1221, 2958, 3019].

April [3764, 3736, 3774, 3908, 3745, 3862, 3747, 3808, 3782, 3783].

Arbitrary
Archimedean [3253]. Architecture [2817, 2764, 3333, 2061, 3244, 3505, 3708, 1542].
Architectures [1445, 3680, 3593]. Area [238, 1879, 3661, 3029, 197, 1684, 3454, 1280, 692, 3499].
Area-Efficient [3661, 3029]. areas [3890, 3859, 2712]. Argument [667]. arguments [425].
Arisen [1]. Arising [1241, 1513, 3471, 3549].
Arizona [3758, 3799]. Arlington [3817, 3851, 3866, 3760, 3807]. ARM7 [3055].
Arnold [2891].
arrival [2693]. Art [1702, 1724, 310, 3751]. Artefacts [1559].
Arthur [3009]. article [868, 2242]. Artifacts [2692].
Artificial [145, 64, 73]. Ascending [2714]. aSHIIP [3349]. ASIC [2761].
Aspects [3740, 3767]. Asperger [2944]. ASR [1227]. Assembler [2213].
assembly [3697]. assess [1900]. Assessing [2128, 2398]. Assessment [1363, 2082, 2756, 2612, 1286, 1443, 2293].
Assignment [838, 843, 845, 857, 858, 859]. Assoc [1238, 1008]. Associated [1244, 2731, 3136, 2815, 1002, 21, 253, 419].
Association [1796, 165, 3548, 949, 7]. associées [1002]. Assumption [3490].
assumptions [1483]. Astronomical [1396]. Asymmetric [684, 3669].
Asymptotic [563, 101, 3633, 667, 1522, 781, 2252, 1550, 55, 2255, 399, 3160, 2443, 2539, 1738].
Asymptotical [2834]. Asymptotically [3293, 1424, 2325, 650, 3003].
Asymptotics [2988]. asymptotiques [781]. Atari [1425]. AT [3398].
Attacks [3258, 2303, 3015, 3666, 3698, 3435, 1427, 164]. Attraction [1529, 366, 726].
Attractor [1655]. Auburn [3797]. auctions [3177]. Audio [3393].
Auditorium [3845]. August [3890, 3801, 3731, 3819, 3859, 3845, 3865, 3865, 3891, 3744, 3804, 2601].
Austria [3754, 3812, 3848, 3804, 3840]. Authentication [1968, 3712, 3230, 3231, 3198].
autism [2944]. Autocorrelated [1603, 982, 1835]. Autocorrelation [1571, 324, 634, 774, 775, 1668, 301, 430, 463].
Autocorrelations [325, 962]. Autocorrelazioni [962]. Autokorrelation [463]. Autokorrelation [430].
automata-based [1399]. Automated [1816].
Automatically [2359]. Automation [3185, 3915]. automaton [2814, 3723].
automorphisms [361]. Autonomous [3349]. Autoregressive [1691].
available [3113]. Avalanche [3226]. Average


Cryptology

Cryptosystem [3227, 1335, 3651]. cryptosystems [2388, 1349, 3127].

Crystal [3851, 53, 3866, 3760, 3807]. crystallography [3189].

cuda [3479, 3068, 3195, 3541].

Cumulant [1657]. Cumulative [3512, 3513, 2713, 1961, 561]. CURAND [3479, 3541].

Current [3078, 1150, 3079]. Current-Mode [3078, 3079].

Curve [2969, 2779, 3010, 34]. Curves [3383, 1998, 2840, 2577, 2982, 1585, 1260, 33].

Customer [2686]. Cusum [1169]. Cusum-Shewhart [1169].

cut [2526].


2954, 3629, 2495, 2071, 2258, 784, 3235. Dimensionality [2899].
dimensionally [2321]. dimensions [2173, 672, 708]. Diode [3580]. Dipole
[1846, 1898, 2248, 1950]. Directions [3747]. Dirichlet [3487, 3605, 2352].
Disappearance [2340]. discarding [2426]. DISCO [3812]. discontinuous
[2181, 1133, 188]. Discr´epance [1002, 529]. Discrepancies
Discrete-Event [3817, 1962, 1068, 2079, 2507, 2816, 3255, 1126].
Discrete-Time [2189, 3035]. discreteRV [3640]. discret [1542]. Discriminating [2763].
Disorder [53, 2944]. Dispersion [1073, 1346, 2250]. dissipative [3552, 3376, 3443]. Dissociated [2368]. dissociation [2944]. Distance
[3490, 2619, 3578, 1508, 3208, 719]. Distance-Bounding [3490]. distances
[3376, 1658, 1659]. Distanz [719]. Distinct [1472, 929]. Distinguishers
[3340, 2703]. Distinguishing [2530, 2544]. DistMe [3110, 3539].
Distributed [393, 2174, 3904, 3262, 1652, 1971, 194, 618, 2285, 319, 2211, 1882, 199, 3510, 2769, 3616, 1688, 1691, 589, 548, 2244, 3535, 1158, 363, 1108, 2499, 3595, 615, 312, 1449, 3031, 176, 2965, 314, 212, 3161, 1465, 42, 1466, 2373, 1313, 2699, 666, 1199, 1320, 469, 301, 3290, 327, 1256, 3292, 978, 1419, 2714, 2858, 1700, 224, 3683, 2557, 1936, 783, 1166, 1831, 691, 1441].
[1287, 2262, 3375, 3256, 3562, 3384, 1072, 2512, 3159, 194, 2437, 2827, 3052, 3497, 2192, 3609, 2612, 2110, 2698, 3638, 2983, 3064, 2116, 199, 3510, 3068, 1401, 3193, 978, 1208, 1338, 2991, 3198, 2854, 1419, 637, 1153, 1512, 1604, 3441, 2558, 2724, 1516, 2330, 1356, 1616, 2947, 3724, 2574, 1533, 3451, 2249, 1108, 862, 2955, 1621, 1109, 3661, 2422, 2672, 1112, 1167, 1627, 825, 1022, 1114, 1227, 3363, 3274, 3552, 961, 3029, 3632, 2175, 3561, 3718, 2362, 2608, 2687, 1186, 571, 2517, 1579, 3416, 2703, 3437, 3582, 2238, 1436, 3337, 2875, 2956, 1166, 2885, 3499].
Final [986, 2397]. Finalist [2490]. Finalists [2453, 2534]. finalizer [3456].
Frequency [2001, 2115, 3675, 2869, 1019, 610, 541, 1322, 3202, 2663, 692].
Frequency-Modulated [2869]. frog [2284]. frontiers [3898, 3877].
frustration [3235]. FTN77 [1883]. Fukuoka [3796]. Full
[3154, 1079, 1004, 3225, 2741]. Full-Length [1079]. Fully [3154, 1079, 1004, 3225, 2741].
Function-based [3249].
function [2967, 3153, 1599, 2347].
Functionality [2537, 2408]. functioning [2944].

G [530, 2896, 579, 621, 1910, 1052, 259, 69]. G5
gambler [3082]. Gambling [2427, 2593, 3596]. Game [2797, 3069].
gaming [480]. Gamma [654, 733, 798, 882, 1244, 895, 2317, 2468, 1018, 523, 863, 864, 990, 693, 785, 3594, 868, 873, 1233, 831, 372, 2763, 1203, 327, 936, 765, 807, 1051, 2036, 601, 856, 955, 728, 991, 824, 729, 694, 993, 742, 466].
gamma-distributed [327, 666]. Gamma-distribution [742]. gamma-rays [1051].
gammaverteilten [327]. gas [793, 661, 2249].
GASPRNG [3567]. Gate [3066, 2556, 2962]. Gates [3023, 3283]. Gateway [3866, 3760, 3807]. Gathering [2597].
Gauss [1808]. Gaussian [3027, 2596, 873, 994, 658, 1073, 3158, 2437, 3606, 1570, 2979, 3170, 294, 345, 2761, 3505, 2218, 3614, 2220, 2456, 3292, 2635, 2778, 2851, 2927, 2928, 3089, 3430, 3519, 3438, 3582, 3647, 3680, 635, 1598, 443, 1012, 3623, 852, 360, 2943, 3332, 3333, 3628, 523, 391, 3017, 3125, 3631, 3661, 1831, 3351, 865, 2884, 2255, 2348].
Gaussian-distributed [3292]. Gbit [3459]. Gbit/s [3459]. GCD
[1234, 1784, 1157, 1269, 1943, 1946, 2055, 1834]. GCDs [3092]. GECCO
Gen2 [3155, 3335]. généateurs [3725]. General
Generalised [2122, 873]. Generalization [436, 235]. generalizations [3500]. Generalized [3718, 1181, 1298, 1660, 2758, 3171, 1339, 632, 383, 3209,
2671, 994, 1849, 3154, 1756, 3606, 1874, 2693, 405, 433, 1321, 2763, 3614, 1895,
2013, 3088, 3430, 1806, 1268, 2949, 2668, 1035]. 
Generate [1290, 997, 1069, 1848, 2530, 1490, 3595, 1841, 2358, 752, 2118, 1201, 1548, 1835, 1631, 1961].
Generated [3144, 3254, 264, 241, 1042, 597, 3655, 368, 3473, 1284, 1744, 567, 
736, 1659, 430, 463, 570, 3500, 1848, 2530, 1490, 3595, 1841, 2358, 752, 2118, 1201, 1548, 1835, 1631, 1961].
Generated [3144, 3254, 264, 241, 1042, 597, 3655, 368, 3473, 1284, 1744, 567, 
736, 1659, 430, 463, 570, 3500, 1848, 2530, 1490, 3595, 1841, 2358, 752, 2118, 1201, 1548, 1835, 1631, 1961].
Generation [3366, 992, 1367, 2356, 3717, 1232, 2749, 3598, 827, 530, 733, 734, 869, 870, 
871, 872, 3375, 2264, 2817, 2892, 1292, 2180, 1453, 2269, 2433, 2271, 2091, 3389, 829, 738, 2510, 798, 1073, 1241, 740, 214, 535, 461, 1300, 1978, 1465, 
2438, 1075, 1184, 2097, 2688, 2897, 618, 3169, 1033, 1305, 1188, 1988, 3609, 
2370, 1079, 2286, 2902, 90, 91, 2617, 1879, 2289, 579, 2290, 2694, 3178, 621, 
436, 2291, 2528, 321, 2218, 1682, 1891, 2768, 3510, 3068, 581, 1327, 2630, 
326, 2632, 2122, 2633, 1045, 1329, 3512, 3513, 1903, 1587, 756, 804, 1498].
Generation [2226, 1418, 2544, 2776, 2924, 3085, 806, 3619, 1147, 246, 3580, 
674, 1596, 1700, 3680, 3522, 2138, 1802, 2784, 2023, 2024, 2931, 443, 2142, 
2789, 637, 591, 715, 1154, 3001, 130, 185, 1052, 2480, 3532, 3686, 592, 1715, 
2034, 2148, 642, 680, 225, 1054, 647, 3709, 257, 1938, 3215, 1356, 1616, 987, 
2869, 3627, 1531, 3010, 2487, 284, 820, 855, 951, 952, 953, 954, 989, 1065, 
1164, 3338, 1944, 1825, 2873, 611, 861, 1222, 1732, 3121, 556, 2252, 3014, 3459, 
3712, 863, 864, 990, 2585, 163, 1736, 3018, 3125, 1831, 3127, 3128, 2168, 421].
Generation [1112, 1167, 526, 527, 1627, 693, 2425, 1551, 3550, 3690, 3475, 3664, 615, 1230, 
2430, 1449, 1745, 3031, 3145, 1845, 1291, 2891, 3376, 3377, 3557, 3558, 3559, 
3600, 1233, 1846, 2080, 2964, 3482, 344, 962, 2518, 3561, 828, 2088, 3037, 796, 
1028, 1847, 180, 1456, 1378, 921, 881, 1652, 396, 1751, 3697, 397, 2362, 2273, 
2970, 1975, 2275, 460, 1299, 1301, 964, 1566, 1662, 2758, 3272, 965, 966, 999, 
1077, 1185, 1663, 1764, 2193, 3165, 3606, 969, 1125, 1385, 216, 1990, 2107, 
318, 1389, 2373, 745, 541, 1037, 1251, 1391, 1477, 2905, 543, 183, 1253, 1320].
geneneration [623, 2762, 3569, 3285, 3671, 3638, 2914, 2005, 1041, 1780, 2449, 2628, 2706,


Generators [1930, 1055, 1725, 3657, 414, 1433, 3328, 3319, 3330, 3331, 2048, 3111, 782, 2572, 3113, 1618, 3332, 2049, 3218, 1063, 2408, 2574, 2951, 2163, 555, 2416, 2418, 524, 2582, 2583, 2342, 2806, 1361, 1539, 1735, 1954, 1109, 3347, 558, 2743, 3021, 1624, 1625, 2169, 1832, 2746, 3688, 785, 1282, 2066, 2427, 2593, 422, 1629, 423, 484, 3594, 826, 1633, 2355, 1024, 1116, 1170, 1284, 1286, 1443, 3552, 2595, 1840, 2429, 3028, 3029, 1231, 1369, 1289, 3632, 488, 3553, 2075, 3480, 2077, 1638, 3031, 1640, 2262, 3374, 3556, 3665, 2265, 3481, 3559, 1026, 2964, 3482, 3601, 3256].


generators [1768, 1995, 3701, 431, 1005, 272, 2288, 837, 972, 2834, 2981, 3702, 1318, 3611,
Goodness-of-Fit [2859, 1133, 1144, 608].

GPGPU [3541].

GPU [3600, 3392, 3643].

Graduate [3855].

Greedy [3340].

Grenoble [3748].

Gretl [3550].

Grid [1184, 2782, 3141].

GRNG [3661].

Guest [2275, 3022].

Guidelines [1679, 1532].

Guide [2275, 3022].

Hard-coded [3691].

Hardware-based [3227, 2778].

Hardware-optimized [3170].

Hash [3489, 3419, 2323, 3652, 3653, 1618, 3451, 3315, 3109, 3625].

Hashing [2098, 3563, 2028, 3714].

HASPENG [3199].

Havens [4796, 443, 929, 252].

Hawaii [3852].

Heads [2751].

help [2334].

HEMT [1448].

Hermite
[2979, 1138]. Herstellung [174]. Heston [3583]. Heterogeneous
[3271, 2769, 3156, 3214]. Heuristic [71, 2038, 2990, 2734, 3342].
Heuristic-Based [2038]. heuristics [2957]. HI [309]. Hidden [1676].
Hiding [3286]. hierarchical [3070, 2928]. Hierarchy [2138, 3349, 1564].
High [2356, 3367, 2085, 3635, 2603, 3047, 3183, 3184, 3191, 3074, 3675, 3916, 2464, 635, 2022, 3622, 3529, 3318, 1162, 3018, 3020, 100, 3470, 1030, 1296, 2602, 2685, 2608, 2687, 2974, 3057, 3170, 2517, 2761, 3284, 2982, 1684, 1896, 2120, 117, 3084, 3195, 128, 3432, 1914, 3437, 3438, 1921, 772, 2328, 225, 2944, 2870, 2954, 1165, 3629, 3460, 121, 2421, 2495, 3472, 2885]. High-density
[2603]. high-dimensional [2608, 2687, 2328, 2954, 3629]. High-entropy
[3047]. high-functioning [2944]. high-order [2982]. High-Performance
[3074, 3191, 3529, 3432]. high-period [2974]. High-Quality
[2085, 2517, 1896, 2120, 1914, 2421, 2495]. High-Speed
[2356, 3184, 3675, 3318, 3635, 2464, 1162, 2685, 3170, 1684, 117, 128, 772, 225]. Higher
[1657, 2382, 3153, 3422, 1218, 2879]. Higher-Order [1657]. Highly
Histogram [3392, 1580]. Histograms [3589, 1279]. Historical [2674].
History [70, 88, 701, 2705, 2723, 67, 1351, 369]. Hit [1746, 1979, 1752].
Hit-and-Run [1746, 1752]. Hitachi [2070]. Hitting [2379]. HK97 [3475].
Hlawka [848, 455]. HMAC [3716]. HMAC-DRBG [3716]. Hoare [3858].
Hoeffding [2244]. Homer [2450]. homogeneous [12, 1581].
Homomorphism [506, 2362]. homomorphisms [3143]. Hong [3872].
Honolulu [3852, 3009]. honor [3898, 3927]. honour [3858]. Hopfield [3348].
Hörmann [2896]. Horner [2498, 239]. Horseshoes [2304]. Horton [1867].
Hot [3845]. HotBits [2811]. Hotel
[3790, 3736, 3833, 3788, 3760, 3762, 3807, 3822, 3873, 3772, 3847]. Houston
[3757]. Huge [2998]. hundred [1196]. Hurst [2288]. HW [3091]. Hyatt
[3851, 3925, 3847]. Hybrid [3167, 349, 2494, 3227, 3028, 3153, 545].
hyperbolas [2068, 2349]. Hyperbolic [2731, 873, 994, 1756, 1905, 1937].
Hypercube [3771, 908, 909, 1326]. Hypercubes [3875]. Hypergeometric
[1328, 1143]. hyperplane [2195]. Hyperplanes [2197]. hyperspheres
[3251, 2954]. Hypotheses [173]. Hypothesis [434].
I. [867]. IBM [3734, 702, 793, 661, 1393, 1479, 470, 2533, 153, 1507, 482, 454].
IBM-Compatible [1479, 1507]. ibre [1024]. IC
[2685, 3403, 3283, 3284, 2332, 2482, 3346]. ICCMSE [3892]. ICGA [3869].
identical [929]. Identically [2499, 3290]. Identification [1422].
Identifying [3188]. identities [1358]. identity [2509, 1905]. IEEE
[3864, 3909, 3910, 3925]. If [1454]. IFIP [3908]. II
[3854, 1230, 3261, 1606, 1759, 2206, 1776, 1886, 1203, 251, 1923, 2026, 2398, 637, 1605, 678, 1434, 521, 2581, 864, 2169, 1547, 2071]. II.5 [744]. IIASA
Iterate [3414]. Iterated [2803, 2171, 244, 2785]. Iterating [1721].
iteration [111]. Iterations [2527, 3239, 3286, 1905, 3315]. Iterative
[1932, 1634, 1677]. IV [911]. ix [168, 3830].

[2752, 2365, 3508, 2781, 3654, 3007]. Java-implemented [3007]. JavaTalk
[3810, 3834, 3750, 3729, 3827, 3848, 3902, 3744, 3869, 3816]. Jump
[2983, 3064, 3065]. June [3823, 3874, 3889, 3903, 3912, 3926, 3740, 3881, 3843,
3920, 3798, 3754, 3729, 3909, 3738, 3828, 3855, 3902, 3867, 3816, 3829, 3856].
Jungles [2331]. Justification [2191, 985].

Kakutani [3209]. kappa [3595]. KASUMI [2536]. Keccak [3488]. KENO
[2046]. KENO-Va [2046]. kernel [2937]. Kernels [2938, 1950]. Key
[3367, 3258, 2269, 3045, 3276, 888, 2450, 2844, 2929, 1602, 2027, 1514, 2484,
1938, 1629, 3037, 3386, 2388, 3307, 1927, 3108]. Key-Stream [3367]. Keys
[3691, 3506, 1602, 3684, 2874]. keystream [3180, 3450]. keystreams [1766].
Kloosterman-type [1763]. KMCLib [3644]. Known
[1807, 3272, 2283, 781]. Knoxville [3771]. Knuth [1698, 677, 714]. Kochen
[63, 399, 71, 1133, 767, 2715, 97, 816, 188, 3453]. Kong [3872]. Kongruenz
[1024]. Kongruenz-Generatoren [1024]. konvexe [32]. konvexer [719].
Korea [3882]. Körper [32]. kriging [3492]. krivoi [34]. Kronescher [3491].
KY [3894].

L [530, 579, 621]. Laboratory [3728, 3730]. Lag [594]. Lagged
[2072, 2174, 1917, 2022, 2023, 2024, 1930, 3632, 2202, 1130, 1922, 2787, 1921].
Lagged-Fibonacci [1917, 2022, 2023, 2024, 3632, 1922, 2787, 1921].
Landau [689, 1107]. language [3705]. languages [3689]. Laning [168].
Laplace [2521, 667, 3002, 3216]. laptops [2270]. Large
[3728, 3262, 3497, 3498, 839, 667, 26, 2554, 2145, 185, 3213, 1529, 2965, 2827,
3053, 3164, 1321, 64, 73, 244, 95, 3721, 1053, 605, 230]. Large-Order
[3497, 3498]. Large-Scale [3728, 185, 2145, 2965, 95, 3721]. large-size [73].
largely [961]. Laser [3215, 3285, 3300, 3460, 3242]. Lasers
[3101, 3128, 3233]. Last [2166]. Latin [2328]. LatMRG [2131]. Lattice
[531, 567, 1972, 2895, 2436, 700, 2612, 2831, 2298, 2918, 2636, 3620, 3676, 2711,
Linear-Algebra [1813], linear-complexity [1517], linear-size [3601].
LLL [2915]. LLL-spectral [2915]. LLRANDOM [630]. Lmcgrid [3141].
Load [2206]. loaded [2455]. Loads [3046].
Low-Dimensionality [2899]. Low-Discrepancy [2617, 2149, 2326, 1540, 1848, 1215, 1346, 1712, 877, 1646, 2914, 2463, 2712, 1711, 3538, 2057].


Mixed [390, 326, 815, 943]. Mixing [1262, 552, 1677, 1201, 3456].
MIXMAX [3660]. Mixture [1452, 1093, 2073, 1014, 3120].
Mixtures [1499]. ML [1656]. ML-sequences [1656]. Mobile
Model [2817, 3615, 184, 53, 2953, 3141, 790, 2265, 3666, 3381, 1119,
2603, 3637, 2094, 2095, 1487, 2989, 1698, 3583, 3311, 1937, 2247, 2248, 3120,
2419, 1550, 3139, 1552]. Model-Based [3615]. Modeling
[1559, 2185, 3871, 3675, 3006, 1723, 3596, 1009, 1591, 2458, 2923, 226, 1542].
Modelling [2735, 3840, 1127, 1186]. Models [495, 1691, 1810, 2073, 3569, 930, 3070,
1786, 2712, 3751, 956, 2250, 2064, 3690, 1960]. Modern
[3367, 3740, 3693, 1126, 2380, 3299, 3600, 3744]. modification [1965, 1561].
Modified [992, 3269, 2106, 414, 2670, 993, 316, 2224, 3683, 191].
Modified-Logistic [3269]. Modular
[2096, 2913, 1155, 2488, 1394, 2128, 3092, 2791]. Modulated [2869].
modulator [3048]. Module [2916, 3150]. Modules [2566, 3727]. moduli
[2361, 2096, 1659, 1304, 1321, 2319, 2786, 3208]. Modulo
[2900, 247, 364, 368, 229, 2075, 926, 1251, 1314, 301, 709, 2637, 2849, 2481,
2941, 1720, 1438, 5, 2934]. Modulus [3498, 799, 970, 1003, 1083, 1474, 2049,
555, 2876, 2595, 1468, 1574, 1578, 1671, 1672, 1759, 1872, 1873, 2105, 2106,
2277, 2278, 1310, 834, 927, 1191, 1192, 1311, 2124, 2224, 762, 3299, 2477, 2864,
1734, 2740, 3343, 3344, 3131, 3132, 3353, 2257]. Molecular [2503, 3702, 1890].
molecular-dynamics [1890]. Moment [1850, 1032, 1567, 2239, 718].
Moment-Generating [1850]. Moments [752, 3413, 3422, 2123, 1218].
Monaco [3867]. Monica [3731]. monitoring [3218]. Monkey [1801, 2041].
Monkeying [2859]. Monographs [3548]. Monotone
Monte [3740, 176, 2433, 111, 3906, 3872, 1583, 3895, 629, 3901, 3296, 2789,
3828, 3848, 3855, 3876, 3886, 2242, 2046, 98, 187, 2950, 3867, 1825, 1739, 1171,
2076, 3034, 343, 2082, 176, 177, 2965, 210, 3485, 1558, 2181, 1559, 1293, 1645,
2183, 2184, 2599, 3260, 232, 1375, 877, 2090, 1122, 89, 193, 492, 3395, 1858,
150, 1981, 3398, 3054, 1245, 3921, 1186, 3502, 195, 3277, 2204, 2284, 2372,
2442, 574, 3872, 1249, 3278, 1676, 2111, 2208, 1085, 705, 2290, 2694, 3702,
1197, 196, 346, 218, 1774, 3612, 499, 127, 221, 322, 886, 1777, 501, 2295, 2447].
Monte Carlo [629, 176, 1559, 232, 1186, 3644]. Monterey
[3785, 3830, 3856, 3749]. Montgomery [2009, 2128, 2791, 2488]. monthly
Nonnegative

Nonnormal

Nonoverlapping

Nonparametric

Nonprobabilistic

Nonrandom

Nonrecursive

nonskewed

nonsuccessive

Nonuniform

nonuniformly

Norfolk

N¨orlund

Normal

Normale

Normali

Normalisation

Normality

Normalizing

Normally

normally-distributed

normalverteilter

NORTA

North

Norway

Note

Notes

November

Num

Num

NSWC

Nuclear

ns-2

ns2

On-the-Fly [3217]. on/off [2693]. One
[1962, 3554, 734, 3382, 2097, 2209, 2383, 3571, 2625, 1585, 1149, 1261, 1594,
439, 440, 475, 2467, 717, 2038, 2156, 1618, 3229, 3473, 1552, 3480, 872, 3287,
1403, 3069, 1406, 186, 2586, 1166, 5, 3247, 3663]. One-chip [3229]. one-class
[3530]. one-dependent [1406]. One-Dimensional [3473, 186]. One-line
[439, 440]. one-shot [3069]. One-Sided [475]. One-Table [162].
One-Time [3382, 2209, 2156]. One-Way
[3554, 3571, 1594, 2383, 1585, 1149, 1261, 3480, 3287, 1403, 3663]. Ones
[1353, 2044]. Online [3724, 2574, 3586, 3004]. Only
[2686, 3272, 3283, 3509, 2453]. Ontario [3859, 3816]. OpenBSD [2366].
openssl [3036]. Operating [3031]. operation [3031]. operations [3802]. operator
[1965]. operators [111, 2347]. opinion [277]. Optimal
[1028, 2091, 2361, 1304, 3607, 3700, 1665, 1666, 578, 668, 627, 670, 710, 1265, 3103,
1434, 1361, 1380, 2287, 2531, 2451, 3293, 2010, 3095, 3003, 813, 2804, 1665, 1666].
Optimality [578, 1087, 1057]. optimisation [3530]. Optimised
[3402, 3518, 3347]. Optimization [3402, 2517, 3913, 2386, 1909, 1910, 2056,
1442, 3769, 3147, 3257, 2967, 2516, 2704, 3804, 3538]. Optimized
[3210, 3333, 3170, 3723]. Optimizing [3713, 3243]. Optimum
[644, 610]. Oracle [3694]. Orbits [2096, 2891]. Order
[2357, 1657, 1865, 3497, 3498, 2901, 624, 1340, 1691, 2854, 3099, 53, 683, 2590,
1235, 1377, 2827, 3053, 3164, 1034, 2982, 1323, 2628, 45, 3225, 3344, 3462].
Order-Disorder [53]. Ordered
[2619, 1745, 148, 1854, 1001, 3058, 1129, 40]. ordering [2539]. Orders
[2382, 1036, 2586, 2879]. ordinal [429].
orangier [740]. Oregon [3857, 3843]. organic [3395]. Oriented
[2609, 3309, 3310, 3114, 1767, 2638, 3432]. Origin [1769]. origins [3922].
Orlando [3861, 3751]. Orleans [3870]. Orono [3801]. ors [3228].
orthogonal [1232]. Oscillation [2869]. Oscillator
[3378, 3483, 3405, 3646, 3137, 3360, 3368, 3369, 3666, 2685, 3404, 3181, 3202, 3206,
3352]. Oscillator-Based
[3378, 3368, 3369, 3666, 2685, 3552]. Oscillators
[3522, 3284, 206]. Other
[1445, 2860, 173, 576, 577, 116, 1491, 2463, 2547, 260, 958, 728, 3727, 3247].
Otherwise [2182]. Ottawa [3890]. outage [3311]. Output
[3694, 2689, 3670, 3652, 3588, 3466]. Overview [2674, 2366, 2849]. Oxford
[3858, 3750].
Polyominoes [2080]. Poor [735, 127, 3706]. Popular [2128, 639].
Population [1940, 8, 17, 134]. Populations [24, 12, 39]. Portability [972].
Problem
[2089, 3264, 51, 2833, 299, 1422, 383, 3653, 1732, 1560, 2753, 923, 3187, 933, 1866].
problème [2753]. Problems
[195, 575, 109, 1091, 26, 767, 337, 338, 1813, 1611, 1629, 2823, 193, 1855, 1179, 1190, 221, 201, 1717, 3587, 187, 2800, 686, 419, 164, 1545]. procédé [318].

Procedure
[1072, 1180, 925, 1081, 971, 436, 304, 277, 1721, 1555, 1636, 318, 1813, 1611, 1629, 2823, 193, 1855, 1179, 1190, 750, 221, 1717, 3587, 187, 2800, 686, 419, 164, 1545]. Proceedings [3763, 3784, 3809, 3832, 3919, 3926, 3730, 3785, 3766, 3774, 3731, 3798, 3752, 3757, 3771, 3853, 3729, 3793, 3794, 3916, 3827, 3751, 3866, 3867, 3892, 3816, 3747, 3829, 3830, 3783, 3749, 3782, 3743, 3831, 3879, 3893, 3778, 3824, 3769, 3790, 3748, 3764, 3765, 3736, 3810, 3833, 3756, 3834, 3858, 3825, 3750, 3780, 3872, 3792, 3754, 3859, 3803, 3860, 3864, 3854, 3861, 3788, 3883, 3847, 3799, 3828, 3848, 3855, 3876, 3744, 3804, 3760, 3762, 3869, 3822, 3849, 3772, 3841, 3817, 3768, 3773, 3779, 3789, 3800, 3818, 3823, 3850, 3857, 3870, 3874, 3903, 3912, 3837, 3728, 3734, 3796, 3900, 3920, 3797, 3745].

Processes

Produce
[1086]. Producing [333, 354, 74, 75, 380, 2875]. Product
[2535, 2989, 205, 3119, 874, 1130, 1891, 1211].

Products
[2934, 390, 523, 1994, 3426, 2744]. Professor [3858]. Profile
[2888, 2759, 2701, 2721, 2999, 1708, 1517, 2879, 1837]. Program
[3377, 3559, 2085, 1187, 3671, 223, 3133, 998, 2324, 599, 1352, 1104, 911]. Programmable
[2220, 1785, 2556]. Programmed
[876, 1650, 2885]. Programmierung
[866]. Programming
[3696, 2922, 2038, 1611, 3869, 866, 3750, 1190, 2119, 2647, 596, 2164].

Programs
[1450, 3263, 3603, 3264, 370, 459, 1000, 689, 1107, 1439, 3574, 897, 1936, 1848].

Project
[2526]. Projections
[3071]. Proof
[1963, 2748, 2429, 698, 399].

Proofs
[1910, 3526, 3650, 2380, 2047]. Proper
[2078, 1316, 2178]. Properties
[566, 829, 1977, 536, 2281, 2286, 2832, 836, 496, 184, 2552, 438, 412, 721, 1832, 2814, 3481, 2361, 1852, 2188, 293, 1761, 2105, 2198, 2203, 2282, 2611, 2108, 704, 2287, 141, 2700, 1325, 889, 755, 2301, 1007, 3083, 1593, 3299, 1696, 1705, 1520, 98, 781, 2801, 2948, 3010, 2741, 1738, 2172].

Property
[179, 3136, 3376, 1120, 3167, 3705, 1266, 783]. property-based
[3705].


Pseudo-random
52


pseudorandom

pseudorandom

pseudorandom-number
[2595]. Pseudorandomness
[2887, 2176, 3264, 3491, 704, 2621, 2445, 3511, 2453, 2534, 2629, 2536, 2546, 2136, 3303, 2475, 1606, 2590, 2505, 2083, 2350, 3022, 2675, 2074].

pseudorandom-sequence
[1320]. Pseudozufallszahlenfolgen
[606].

psevdosluchainykh
[346]. PSI
[1392]. PUB
[1816]. Public
[2269, 888, 2450, 1927, 2484, 3187, 2388]. Public-Key
[888, 2450, 2484].

Publications
[259, 389]. Publicly
[3050]. PUF
[3712]. Pulse
[3405, 1785, 600, 3406]. Pulse-Excited
[3405]. Pulse/Data
[1785]. Pulses
[508, 509, 3242]. punched
[35]. punctured
[3651]. Pure
[3706]. Purpose
[1054]. Purposes
[2855]. PVT
[3339]. PVT-variation
[3339]. pW
[3273]. pyramids
[1426]. Python
[3618, 3519, 2317, 2318].

Q.R.N.G.
[3371]. Qs
[3506]. Quadratic

Quadrature
[891, 766, 713, 1012, 391, 2447]. Quality
[2085, 3395, 1782, 2630, 3642, 2022, 1063, 3018, 3126, 2882, 3147, 3257, 1863, 2517, 1892, 1806, 2120, 3084, 3195, 1914, 3437, 1921, 591, 2409, 2410, 2421, 2495, 2883, 2885].

quanta
[1186]. Quantendynamik
[11]. Quantifiers
[3163]. Quantis
[3545]. Quantitative
[3034, 720, 3905, 3622]. quantity
[225]. Quantum
[3365, 3366, 3476, 2749, 3370, 3389, 3041, 3609, 3280, 3704, 1584, 3076, 3294, 3515, 3581, 3522, 3684, 1938, 3446, 3627, 519, 2579, 3013, 3457, 3021, 3242, 3250, 3477, 3265, 3564, 372, 3057, 3566, 3702, 3288, 3290, 2454, 3423, 3075, 11, 3527, 3586, 3325, 3336, 2736, 2492, 3223, 3460, 3229, 3233, 3547, 3466, 2959, 3240].

Quantum-Mechanical
[519]. Quantumlike
[686]. quark
[3838]. 'quasi'
[311]. Quasi-Monte
Random

Random

Random

Random

Random

Random
[3674]. RV [1204].

S [3039, 315, 974, 1039, 437, 389, 3580, 2070, 3459]. S-3800 [2070].
Saarbrücken [3767]. SAC [3890, 2530, 2766]. SAC’99 [3859]. Safari [2331].
SAFE [3719, 2049]. Salford [1883]. Salt [3829]. Salzburg [3848].
same [365]. Sample [697, 1073, 3495, 619, 2905, 58, 781, 35].
samplers [1752]. Samples [1182, 1947, 8, 828, 64, 73, 17, 39, 134, 33, 230].
Saturday [3881]. Saturday-Wednesday [3881]. Saunders [3088]. Savage [2466]. SC’11 [3916]. Scalable [3164, 3199, 3717, 3610, 3567, 2780, 2470, 2471, 2270, 3086]. Scale [2173, 3728, 767, 185, 10, 2965, 14, 1666, 95, 3721, 1424, 2145, 1053].
School [2756, 3749, 630]. School-Based [2756]. Schwinger [2265]. Sci [1039]. Science [3752, 3863, 3757, 3745, 3755, 3758, 3761, 3776, 3781, 3787, 3793, 3803, 3826, 3835, 3839, 3860, 3864, 3910, 3925, 3917, 3767, 3759, 3814, 3887, 3892, 3878, 3747, 3782, 3783, 3765, 3858, 3846, 3877, 3746, 3539, 3805].
sciences [3868]. Scientific [3740, 2894, 1122, 3739, 1140, 1140, 1724, 2489, 3815, 3174, 2717, 3828, 3744].
Scientists [626, 274, 1200]. scores [429]. Scrambled [3209, 3688, 3115].
Scrambling [2614]. scramblings [2727, 3715]. screening [3224, 2586].
second-order [3225]. Secondary [2882]. Secret [2825, 1276, 2425]. Secure [3375, 2682, 3258, 1453, 3490, 2110, 2533, 2634, 3077, 3645, 3096, 3015, 1112, 1167, 2679, 3638, 3421, 1401, 2300, 1335, 3091, 3321, 3108, 2946, 2337, 1276, 3547, 2678, 3719, 1847]. Securely [3684]. sécuritaire [1847]. Security [3851, 3378, 3667, 3267, 1868, 2829, 3172, 3503, 2696, 2764, 2629, 3883, 2558,


simulation [3384, 211, 1858, 1460, 464, 1034, 271, 1252, 1088, 3573, 3739, 2449, 1487, 2221, 
1142, 1255, 1890, 3288, 2123, 1334, 3194, 2850, 2016, 3432, 3530, 1710, 1914, 
3521, 2328, 3443, 2333, 3539, 2051, 2249, 2422, 3662, 1956, 1957, 3363, 1961]. 
simulative [1706]. simultaneously [1744]. Sin [3485, 1126, 1570, 3612, 3613, 1343, 2782, 1428, 3320, 3535, 3110, 1531, 2808, 
423, 3595, 3028, 3596, 3256, 2965, 3395, 2095, 3398, 3054, 1676, 2288, 3702, 
1135, 1774, 3569, 1325, 2988, 1902, 1413, 2850, 2061, 3412, 3530, 1710, 1914, 
3521, 2328, 3443, 2333, 3539, 2051, 2249, 2422, 3662, 1956, 1957, 3363, 1961]. 
simultaneously [1744]. SiN [3384, 211, 1858, 1460, 464, 1034, 271, 1252, 1088, 3573, 3739, 2449, 1487, 2221, 
1142, 1255, 1890, 3288, 2123, 1334, 3194, 2850, 2016, 3432, 3530, 1710, 1914, 
3521, 2328, 3443, 2333, 3539, 2051, 2249, 2422, 3662, 1956, 1957, 3363, 1961]. 
simultaneously [1744]. Sin [3485, 1126, 1570, 3612, 3613, 1343, 2782, 1428, 3320, 3535, 3110, 1531, 2808, 
423, 3595, 3028, 3596, 3256, 2965, 3395, 2095, 3398, 3054, 1676, 2288, 3702, 
1135, 1774, 3569, 1325, 2988, 1902, 1413, 2850, 2061, 3412, 3530, 1710, 1914, 
3521, 2328, 3443, 2333, 3539, 2051, 2249, 2422, 3662, 1956, 1957, 3363, 1961].
space-bounded

trapezoidal 

Treatment

Trees

Trends

Trial

Trials

Triangle

triangles

Trident

Trier

trigamma

Trinomials

Triple

triples

TRNG

TRNGs

Trojans

True

Triangular

Trident

Trier

trigamma

Trinomials

Triple

triples

TRNG

TRNGs

Trojans

True

Trees

Triangles

uniform [1224, 2958, 3019, 3593, 911, 5, 1835, 2676, 3274, 2985, 2924, 420, 1275].


unpublished [2966]. unreasonable [3801]. unrestricted [1734, 2740].


using [1124, 3276, 1249, 1195, 2526, 2624, 3416, 2915, 1400, 976, 1203, 2843].
VARIATES

VARIATIONAL
[2144, 3221, 3160, 3339].

VARIATIONAL
[243].

VARIATIONS
[2519].

VARIOUS
[683, 2823, 765, 99].

VARYING
[1528, 2978].

VAVILOV
[689, 1107].

VAX
[1305].

VAX-11
[1305].

VECTOR
[1445, 395, 2271, 2034, 2148, 1531, 2819, 1387, 2107, 1487, 1488, 244, 1416, 1596, 716, 1217, 1608, 1713, 1714, 1926, 2035, 3533, 646].

VECTORIAL
[3486].

VECTORIZED
[3724, 1177, 1473, 1355].

VECTORS
[531, 2185, 2510, 700, 2281, 505, 284, 1018, 3338, 1284, 2358, 567, 2087, 3605, 1753, 2282, 1131, 1199, 1253, 1320, 2228, 1520, 2476, 2802, 607, 1944, 2669].

VEGAS
[3823, 3864, 3910, 3828].

VERIFIABLE
[3667, 3050].

VERIFICATION
[2764].

VERIFIED
[2359, 3716].

VERMONT
[3835].

VERSATILE
[508].

VERSCHLÜSSELUNGSABBILDUNGEN
[1005].

VERSION
[3553, 996, 1090, 2601, 2994, 3626].

VERSIONS
[2530, 1017, 2824, 2017, 720].

VERSUS
[713, 2426].

attered
[1838].

VERTICAL
[2226].

VERWERFUNG
[1838].

VERY
[1165, 1283, 1321, 979, 1920, 2029, 2328, 651].

VERY-LONG-CYCLE
[1283].

VERY-LONG-PERIOD
[1920].

VI
[2473].

VIA
[1924, 1838, 2086, 2435, 2970, 3271, 1459, 2189, 3054, 2098, 3169, 2368, 2442, 3413, 3577, 2462, 2928, 3201, 1012, 2244, 2940, 3112, 951, 2668, 2806, 1627, 2065, 3362, 3364].

VICTORIA
[3800, 3893].

VIENNA
[3798, 3840].

VIEW
[1504, 1150, 1954, 755, 3751].

VIGENÈRE
[1861].

VIRGINIA
[3851, 3883, 3807, 3782, 3760].

VIRTUAL
[3327].

VISIT
[2166].

VISTA
[3822].

VISUAL
[3007].

VLSI
[3909, 1400, 3647, 1617, 1953, 1623, 1548].

VMPC
[3659].

VOL.
[637].

VOLATILITY
[3583].

VOLTAGE
[3221].

VOLUME
[3737].

VOTING
[3667].

VS
[881, 162].

VULNERABILITIES
[3327].

VYCHISLITELNYKH
[346].

W
[2087, 3066, 3155].

WA
[3916, 1504, 1908].

WADSWORTH
[259].

Wahrscscheinlichkeit
[554].

Wahrscheinlichkeitstheorie
[554].

WAKE
[3206].

WAKE-UP
[3206].

WALK
[2338, 2353, 193, 3648, 2147, 2248, 2253, 2254, 2341].

WALKING
[3555].

WALKS
[1241, 2039, 2798, 2190, 2525, 1774, 1888, 2843].

WALL
[3648].

WALSH
[1885, 2053, 1278, 826].

WALSH-SPECTRAL
[1278].

WALT
[3822].

WANG
[2794].

WARBLER
[3681].

WARNING
[1322, 2794].

WARP
[1581].

WASHINGTON
[2686].

WAY
[3554, 839, 3506, 2929, 2558, 2724, 1297, 3242].

WEAKLY
[1602, 1839].

WEAKNESS
[2623].

WEB
[2686, 3113, 2584].

WEBCAM
[2720].

WEDNESDAY
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.


REFERENCES

75


REFERENCES


REFERENCES


REFERENCES


[34] 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 (Matematičeskii Sbornik)*, N.S., 6(48):3–26, ????. 1939. CODEN MATSAB. ISSN 0368-8666.

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Anonymous:1954:RDc


Anonymous:1954:RDd


Bartholomew:1954:NUS


Hammersley:1954:PMM


Lehmer:1954:DRN


Meyer:1954:GTR


Moshman:1954:GPR


Page:1954:MCS


[139] 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.*


REFERENCES

http://www.rand.org/pubs/research_memoranda/RM1237.html. Also appeared as AECU 3259.


REFERENCES


REFERENCES


[185] Mervin E. Muller. An inverse method for the generation of random normal deviates on large-scale computers. *Mathematical Tables and Other
REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


[230] Donald D. Wall. A random number test for large samples. In Anonymous [3734], pages 7–11. LCCN ???.


REFERENCES


[243] Edmund Hlawka. Funktionen von beschränkter Variation in der Theorie der Gleichverteilung. (German) [Functions of bounded variation in the

**Kiefer:1961:LDE**


**Kuehn:1961:BPR**


**Liniger:1961:MDH**


**Mamangakis:1961:MNR**


**Manelis:1961:GRN**


**Marsaglia:1961:ERV**


**Marsaglia:1961:GER**


REFERENCES


REFERENCES


REFERENCES


Marsaglia:1962:RVC


Marsaglia:1962:SPG


MendesFrance:1962:CMF


Pathria:1962:SSR


Richtmyer:1962:CFE


Scheuer:1962:GNR


Shanks:1962:CD


Sibuya:1962:FCN

REFERENCES


REFERENCES


REFERENCES


Kolmogorov:1963:TRN

Laughlin:1963:RAR

MacLaren:1963:FPG

Magleby:1963:SNF

Marsaglia:1963:GDR

Marsaglia:1963:RNF

Moses:1963:TRP

Poore:1963:CAR


[324] 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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[399] Miklós Csörgö. A new proof of some results of Rényi and the asymptotic distribution of the range of his Kolmogorov–Smirnov type random


[405] 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 (Gen-
REFERENCES


[409] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3739], pages 64–68. LCCN QA76.5 D55 1965.


REFERENCES


REFERENCES


REFERENCES


[460] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3740], pages 70–111. LCCN QA1 S565 v. 3.


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Anonymous:1970:FVP


Behboodian:1970:ERV


Blaisdell:1970:RSP


Butler:1970:AAG


Cenacchi:1970:PRN


Dixon:1970:NSE


Downham:1970:SAA

REFERENCES


Hastings algorithm, a generalization of the work in [118]. See [2705, page 255].


REFERENCES


Marsaglia:1970:RV1


McShane:1970:RSE


Murry:1970:GAG


Payne:1970:FTP


Prasad:1970:PDA


REFERENCES


REFERENCES


[554] 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.,
REFERENCES


Ahrens:1972:CMS


Alam:1972:AVM


Barr:1972:CMN


Basu:1972:ITF


Behboodian:1972:CNS


Beyer:1972:LSR


Cenacchi:1972:QRS

REFERENCES


REFERENCES

CS-TR-72-254, Stanford University, Department of Computer Science, Stanford, CA, USA, January 1972. 21 pp.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hamming:1973:NMS


Holland:1973:GAO


Knop:1973:AAR


Kozlov:1973:EEM


Learmonth:1973:NPS


Levin:1973:NRS


Lewis:1973:GFS

REFERENCES


[639] Frank Neuman, Robert Merrick, and Clyde F. Martin. The correlation structure of several popular pseudorandom number generators. Report
REFERENCES


[646] P. Pohl. The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and al-


REFERENCES


REFERENCES


[677] 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


[Chay:1975:MUB]
REFERENCES


Kleijnen:1975:AVC


Levin:1975:UDSa

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

Levin:1975:UDSb

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

Malcolm:1975:LVG


MendesFrance:1975:SNA


Miyatake:1975:GPR


Monroe:1975:CIT

Nance:1975:IFR


Newman:1975:MIF


Niederreiter:1975:DDM


Niederreiter:1975:QVR


Pohl:1975:MFP


Pollard:1975:MCM

REFERENCES


REFERENCES

Witsenhausen:1975:SPD


Yao:1975:ASA


Anderson:1976:PRR


Atkinson:1976:CGB


Atkinson:1976:SAG


Bays:1976:IPR


Blood:1976:CPR

REFERENCES

Brent:1976:ABE

[737] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3747], 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 \(O\left(0.705 \log N\right)\) for large \(N = \max(|u|, |v|)\). See [2434] for an update, and a repair to an incorrect conjecture in this paper. See also [2360], where the worst case complexity is shown to be \(O(\log N)\), and the number of right shifts at most \(2 \log(N)\).

Chamayou:1976:DAG


Chambers:1976:MSS


Claustriaux:1976:GCN


Enison:1976:PTB

REFERENCES


REFERENCES


Niederreiter:1976:CSL


Niederreiter:1976:DPR


Niederreiter:1976:SIL


Niederreiter:1976:SNE


Pohl:1976:DMP


Rouault:1976:PAE


Rudolph:1976:RNG

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[839] Nancy L. Geller. Some examples of the weak and strong laws of large numbers for averages of mutually independent random variables. *The
REFERENCES


Hoaglin:1978:SAR


Hollander:1978:TDU


Holmlid:1978:UCP


Kiefer:1978:PNA


Li:1978:EMN

REFERENCES


REFERENCES


[857] 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


REFERENCES


REFERENCES


REFERENCES


[Bright:1979:QRN]


[Brown:1979:CPNa]


[Brown:1979:CPNb]


[Burford:1979:AVM]


[Cheng:1979:SSG]


[delJunco:1979:HLV]


REFERENCES


REFERENCES


Tripathi:1979:RFI


vanLint:1979:PRA


Wang:1979:MND


Williams:1979:SPF


Wright:1979:ECR


Ahrens:1980:SBP


Atkinson:1980:TPR


Basu:1980:RAEa

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Lindley:1980:RAE


Marsaglia:1980:GRV


OBrien:1980:PIR


Peskun:1980:TTC


Petkovic:1980:RRV

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


Rice:1980:DQF

S. O. Rice. Distribution of quadratic forms in normal random variables—evaluation by numerical integration. *SIAM Journal on Scientific and
REFERENCES


[953] B. W. Schmeiser. Random variate generation: a survey. Technical report, School of Industrial Engineering, Purdue University, West Lafayette, IN,
REFERENCES


REFERENCES


REFERENCES


Greenwood:1981:PFA


Ide:1981:EZM


Kaplan:1981:ERS


Kemp:1981:EGL


Kirkpatrick:1981:VFS


Kozlov:1981:ECI


Kronmal:1981:VAR


[989] 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.


[995] F. Baccelli and E. G. Coffman. A data base replication analysis using an M/M/m queue with service interruptions. *ACM SIGMETRICS Perfor-
REFERENCES

...mance Evaluation Review, 11(4):102–107, December 1982. CODEN ????
ISSN 0163-5999 (print), 1557-9484 (electronic).

Bartels:1982:RVN

[996] Robert Bartels. The rank version of von Neumann’s ratio test for ran-
March 1982. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X

Blum:1982:HGC

[997] Manuel Blum and Silvio Micali. How to generate cryptographically
strong sequences of pseudo-random bits. In IEEE [3755], pages 112–117.
IEEE catalog number 82CH1806-9. IEEE Computer Society
order number 440.

Crigler:1982:RCP

[998] 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. vi + 41 + 3 pp. URL http://www.dtic.mil/dtic/
tr/fulltext/u2/a118412.pdf.

Devroye:1982:NAR

1982. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic),
1563-5163.

DiDonato:1982:FSP

[1000] A. R. DiDonato. Five statistical programs in Basic for desktop com-
puters. Report NSWC TR 83-13, Naval Surface Weapons Center (Code
K104), Dahlgren, VA 22448, USA, November 1982. vi + 96 + 4 pp. URL

Dykstra:1982:MLE

functions of stochastically ordered random variables. Journal of the American
JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic). URL http://
REFERENCES


REFERENCES


REFERENCES

Plumstead:1982:ISG


Rizzi:1982:GPB


Roberts:1982:ITN


Schmeiser:1982:BGR


Shen:1982:FAD


Tracht:1982:RAN


Vahle:1982:BPR


REFERENCES


REFERENCES


Fushimi:1983:DGF


Fushimi:1983:IOE


Fushimi:1983:RTR


Gokhale:1983:EBG


Helstrom:1983:CDQ


Hopkins:1983:SAAAb

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1083] George S. Fishman and Louis R. Moore III. An exhaustive analysis of multiplicative congruential random number generators with


REFERENCES


REFERENCES


REFERENCES

Rasmussen:1984:FPS


Ronse:1984:FSR


Scholtz:1984:GS


Schorr:1984:PLV


Smith:1984:EMC


Thesen:1984:SER

REFERENCES


REFERENCES


Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


REFERENCES

held at the University of California, Santa Barbara, August 19–22, 1984, sponsored by the International Association for Cryptologic Research.


REFERENCES


REFERENCES


[1153] A. Ian McLeod. Statistical algorithms: Remark AS R58: a remark on Algorithm AS 183. an efficient and portable pseudo-random number gen-
Monahan:1985:ARN


Montgomery:1985:MMT


Niederreiter:1985:STP


Norton:1985:EBG


Percus:1985:PBS


Pierchala:1985:IMU


Reichert:1985:LLT

REFERENCES


REFERENCES


Vitter:1985:RSR


Yashchin:1985:ADC


Afflerbach:1986:SLS


Anderson:1986:MMC


Anon:1986:IRN


Blum:1986:IUC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Shore:1986:AID


Shore:1986:SGA


Sowey:1986:TCB


Stephens:1986:TBE


Stephens:1986:TUD


Wolfram:1986:RSG


Wolfram:1986:TAC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

1613-9798 (electronic). URL http://www.springerlink.com/content/q7885421202m6565/.


[1292] 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
REFERENCES


REFERENCES


[1312] Alan M. Frieze, Johan Håstad, Ravi Kannan, Jeffrey C. Lagarias, and Adi Shamir. Reconstructing truncated integer variables satisfying linear


REFERENCES


LEcuyer:1988:GLC


LEcuyer:1988:LCG


Levitan:1988:QSN


Luby:1988:HCP


Mactutus:1988:CSN


Matsumoto:1988:FPS

[1344] 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.

Monahan:1988:CAG


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Chassaing:1989:ORN


Dagpunar:1989:CPP


Danilowicz:1989:DDP


Deak:1989:URN


Devroye:1989:RVG


Durst:1989:ULC


Edgeman:1989:RNG

REFERENCES


REFERENCES


REFERENCES


Impagliazzo:1989:ECS


Impagliazzo:1989:HRR


Impagliazzo:1989:PRG


Kachitvichyanukul:1989:ABS


Kahaner:1989:NMS


Kamps:1989:CPL

[1406] U. Kamps. Chebyshev polynomials and least squares estimation based on one-dependent random variables. Linear Algebra and its Applications,
REFERENCES


REFERENCES


REFERENCES


Mertsch:1989:PAS


Niederreiter:1989:STC


Paul:1989:IRN


Percus:1989:RNG


Pickover:1989:PRG


Reber:1989:PNG


Rhee:1989:OPIa

[1434] Wansoo T. Rhee and Michel Talagrand. Optimal bin packing with items of random sizes. II. SIAM Journal on Computing, 18(1):139–151, Febru-
ary 1989. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).


REFERENCES


REFERENCES

Dagpunar:1990:SMD


Deak:1990:RNG


Deak:1990:URN


DeArman:1990:IRN


DeMatteis:1990:CPR


DeMatteis:1990:LRC


Deng:1990:GUV


Doring:1990:ENZ

[1466] H. Döring. Erzeugung normalverteilter Zufallszahlen mit 16-bit-PC. (German) Generation of normally-distributed random numbers on an
REFERENCES


REFERENCES


Goldreich:1990:NCI


Goldreich:1990:SPD


Golland:1990:BRB


Haastad:1990:PRG


Hildebrand:1990:RCS


Hormann:1990:AMG


Hortensius:1990:CAC

REFERENCES


REFERENCES


Kelton:1990:BRB


Kemp:1990:BRB


Kemp:1990:NAG


Kemp:1990:PRA


Kinderman:1990:CCG


Korolev:1990:ADR
REFERENCES


Macomber:1990:DUR


Marsaglia:1990:DBR


Marsaglia:1990:RNG


Marsaglia:1990:TUR


Maurer:1990:PLR


Micali:1990:EPR

REFERENCES


90-012, University of Tokyo, Faculty of Science, Dept. of Information Science, Tokyo, Japan, April 1990. 6 pp.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Dunweg:1991:BDS


Eichenauer-Herrmann:1991:ASI


Eichenauer-Herrmann:1991:CCP


Eichenauer-Herrmann:1991:CIC


Eichenauer-Herrmann:1991:DIC


Eichenauer-Herrmann:1991:DQC


Eichenauer-Herrmann:1991:ICPa


REFERENCES


REFERENCES


REFERENCES

[1616] 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


Walsh:1991:MFR


Wheeler:1991:PMN


Wheeler:1991:SIC


Yamamoto:1991:NEM


Yang:1991:UCR


Zeng:1991:PBG


Baker:1992:PPT


Bays:1992:IRN


Bellido:1992:SBR


Berdnikov:1992:RNG


Binder:1992:MCS


Bratley:1992:ITL

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Ishikawa:1992:MHS

Kleijnen:1992:PNG

Kleijnen:1992:RMS

Ko:1992:GPB

Kolonko:1992:GUD

Krawczyk:1992:HPC

Lagarias:1992:PN


REFERENCES


REFERENCES


Szyszkowicz:1992:GRP


Tang:1992:SDA


Tezuka:1992:AAC


Tezuka:1992:FGL


Traub:1992:MCA


Tsai:1992:AFT

vonHanxleden:1992:CDP


Warford:1992:GPR


Wikramaratna:1992:TBA


Wollan:1992:PRN


Won:1992:USN


Anderson:1993:CCB


Atkinson:1993:UGR

REFERENCES


REFERENCES


REFERENCES


REFERENCES

[1805] 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,

[1806] Ueli M. Maurer. A simplified and generalized treatment of Luby–Rackoff
pseudorandom permutation generators. Lecture Notes in Computer Sci-
ence, 658:239–??, 1993. CODEN LNCSDC. ISSN 0302-9743 (print),
service/series/0558/bibs/0658/06580239.htm; http://link.springer-

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.

with support for signature functions. In Miosa [3812], pages 81–94. ISBN

[1809] H. N. Book review: Random Number Generators and Simulation, by
CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic).

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).
REFERENCES


[1817] 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 [1353, 1458, 1803, 1827]. The authors report that they would now recommend the MCG \( x_{n+1} = 48\,271x_n \mod (2^{31} - 1) \) over their original \( x_{n+1} = 16\,807x_n \mod (2^{31} - 1) \).


REFERENCES


[1827]

---


---


---


---


---


---

Yang:1993:NBS


Zechner:1993:EBV


Zurbenko:1993:WCR


Aiello:1994:PPP


Allison:1994:UHA


Angus:1994:PIT


Annan:1994:RAA

REFERENCES


REFERENCES


[1861] 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.


Cuccaro:1994:TTQ


Davis:1994:CRA


DeArmon:1994:RLO


Deng:1994:DIR


Devroye:1994:NHS


Eastlake:1994:RRR


REFERENCES


REFERENCES


REFERENCES


[1903] 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.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1979] Asit Dan, Philip S. Yu, and Jen Yao Chung. Characterization of database access pattern for analytic prediction of buffer


REFERENCES


Eichenauer-Herrmann:1995:IUB


Eichenauer-Herrmann:1995:NPE


Eichenauer-Herrmann:1995:PNG


Eichenauer-Herrmann:1995:QCP


Eichenauer-Herrmann:1995:RCM


Eichenauer-Herrmann:1995:UAA

REFERENCES


Entacher:1995:IPN


Entacher:1995:PSS


Feige:1995:RGP


Fleischer:1995:TTP


Gardy:1995:DAS


Gutbrod:1995:FRN

REFERENCES

Hallgren:1995:LCG


Hamilton:1995:EBU


Hamilton:1995:UGR


Han:1995:PGF


Hellekalek:1995:CBP


Hellekalek:1995:GDE


Hellekalek:1995:IPN


REFERENCES


REFERENCES


[2022] Michael Mascagni, Steven A. Cuccaro, Daniel V. Pryor, and M. L. Robinson. A fast, high quality, and reproducible parallel lagged-

Mascagni:1995:PPNa


Mascagni:1995:PPNb


Matus:1995:CIAa


Matus:1995:CIAb


Micali:1995:SMG


Miller:1995:RAC

REFERENCES


REFERENCES


Ong:1995:CBG


Owen:1995:RPN


Palubeckis:1995:HBB


Pattanaik:1995:AER


Penrice:1995:AEP


Percus:1995:TAM


REFERENCES


REFERENCES


[2068] Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inverse congruential pseudorandom numbers? Journal of Computational


REFERENCES


REFERENCES


REFERENCES


Beyer:1996:CLS


Bland:1996:SRN


Boppana:1996:BCP


Bromley:1996:QNG


Brunner:1996:PCO


Bryc:1996:BRB

REFERENCES


[2098] Martin Dietzfelbinger. Universal hashing and k-wise independent random variables via integer arithmetic without primes. Lecture Notes in
REFERENCES


REFERENCES


George S. Fishman. Monte Carlo: concepts, algorithms, and applications. Springer series in operations research. Springer-Verlag, Berlin,
REFERENCES


REFERENCES


[2124] Chiang Kao and J. Y. Wong. An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus


LUBY:1996:PCA


LUO:1996:TDS


MARINI:1996:CHR


MARSAGLIA:1996:DBT


MASUDA:1996:PPR


MATSUMOTO:1996:SDR


MATTHEWS:1996:SRN

REFERENCES


Niederreiter:1996:LDS


Niederreiter:1996:QPG


Nisan:1996:ERH


Ogawa:1996:RRP


Paplinski:1996:HIL


Petrov:1996:LTP


Radovic:1996:QMC

[2155] Igor Radović, Ilya M. Sobol, and Robert F. Tichy. Quasi-Monte Carlo methods for numerical integration: Comparison of different low discrep-

Rubin:1996:OTP


Sanchis:1996:PAC


Schervish:1996:VWT


Schneier:1996:ACP


Sethumadhavan:1996:NPE


Sezgin:1996:RNG

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Bellare:1997:PRN


Berblinger:1997:MCI


Berg:1997:CNF


Binder:1997:AMC


Binder:1997:MCS


Cario:1997:MGR

report, Department of Industrial Engineering and Management Sciences, Northwestern University, Evanston, IL, USA, 1997.

Coddington:1997:RNG


Compagner:1997:RER


Couture:1997:DPM


Dai:1997:RCD


Dai:1997:RRW


Deng:1997:SJC

REFERENCES


Eichenauer-Herrmann:1997:ADH


Eichenauer-Herrmann:1997:AEP


Eichenauer-Herrmann:1997:CCC


Eichenauer-Herrmann:1997:ICP


Eichenauer-Herrmann:1997:PSN


REFERENCES


Foster:1997:DOT


Gell-Mann:1997:ETZ


Grabner:1997:MSR


Hamilton:1997:AR


Hamilton:1997:ARP


Hellekalek:1997:CAP

REFERENCES


Hellekalek:1997:GRN

[2215] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [3840], page ?? ISBN 3-901608-11-7. LCCN ???

Hellekalek:1997:NPNa


Hellekalek:1997:NPNb


Herendi:1997:FGR


Heuer:1997:CCS


Imperiale:1997:PUG

REFERENCES


Kreckel:1997:PAM


LEcuyer:1997:BLS


LEcuyer:1997:EBT


LEcuyer:1997:ILS


LEcuyer:1997:RNG


LEcuyer:1997:TBS


LEcuyer:1997:URN


[2236] 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.”.


[2238] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In IEEE [3839], pages 458–467. CODEN ASF-


REFERENCES


Woodward:1997:ECD


Wu:1997:MCR


Zubkov:1997:PTD


Aiello:1998:DPP


Andreev:1998:NGD


Antoch:1998:RPN

REFERENCES


Bach:1998:EPM


Baldwin:1998:PAB


Baldwin:1998:PPR


Ballesteros:1998:TRN


Barni:1998:CPD

REFERENCES


[2274] Paul D. Coddington and Sung-Hoon Ko. Random number generator for parallel computers. In Greg Egan, Richard Brent, and Dennis Gan-
REFERENCES


**Couture:1998:GEI**


**DSouza:1998:SBD**


**Eichenauer-Herrmann:1998:IUB**


**Eichenauer-Herrmann:1998:LBD**


**Eichenauer-Herrmann:1998:SQI**


**Ellison:1998:CRN**


REFERENCES

Fuster-Sabater:1998:LPS


Gammel:1998:HRR


Garcia:1998:GCE


Gentle:1998:RNG


Gutmann:1998:SGP


Hamilton:1998:AEP

REFERENCES


Hellekalek:1998:ARQ


Hellekalek:1998:CAP


Hellekalek:1998:DTP


Hellekalek:1998:GRN


Hellekalek:1998:WST


Hickernell:1998:LRH

REFERENCES


Kolmogorov:1998:TRN


Larcher:1998:DPS


LEcuyer:1998:GPI


LEcuyer:1998:RNGa


LEcuyer:1998:RNGb


LEcuyer:1998:RNGc


LEcuyer:1998:RNGd

REFERENCES


REFERENCES


Miller:1998:BPG


Morohosi:1998:DAR

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


Niederreiter:1998:NSA


Owen:1998:LSS


Park:1998:AGC


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Falk:1999:SAG


Fernandez:1999:AER


Fernandez:1999:ANRa


Fernandez:1999:ANRb


Gartner:1999:PCP


Gartner:1999:RCZ

REFERENCES


[2385] Benjamin Jun and Paul Kocher. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Re-
REFERENCES


REFERENCES

informs.org/doi/abs/10.1287/opre.47.1.159; http://www.jstor.
org/stable/222902.

[2392] P. L’Ecuyer. Some recommendable uniform random number genera-
tors. 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.
1-56555-171-0 (vol. 1), 1-56555-172-9 (vol. 2). LCCN ????

[2393] Pierre L’Ecuyer. Tables of linear congruential generators of different
pdf.

[2394] Pierre L’Ecuyer. Tables of maximally equidistributed combined LFSR
1999. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (elec-

36A5FC62.17C9CC33@stat.fsu.edu. Posting to the sci.crypt.random-numbers,
thread/ca8682a4658a124d/.

[2396] M. Mascagni. Some methods of parallel pseudorandom number gen-
eration. In Heath et al. [3853], pages 277–288. ISBN 0-387-98680-

[2397] 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-
REFERENCES


REFERENCES

Presented at the ANSI X9F1 Meeting, Institute for Defense Analyses, Alexandria, VA.

Soto:1999:STRc


Stauffer:1999:IMT


Sudan:1999:PGX


Tomassini:1999:GHQ


Tretiakov:1999:EMC


Trevisan:1999:CEU

[2423] Luca Trevisan. Construction of extractors using pseudo-random generators (extended abstract). In ACM [3850], pages 141–148. ISBN 1-58113-
REFERENCES


[2428] 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


REFERENCES

31–36, January 2000. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Hickernell:2000:ELS


Hormann:2000:AAG


Hormann:2000:ARV


IEEE:2000:IPH


Impagliazzo:2000:EPR


Indyk:2000:SDP

REFERENCES


[2467] George Marsaglia. The monster, a random number generator with period over $10^{2637}$ times as long as the previously touted longest-period one. Technical report ?????, Florida State University, Tallahassee, FL, USA, ???? 2000.


REFERENCES


REFERENCES


Soto:2000:RTA


Stefanescu:2000:GUR


Stefanov:2000:OQR


Sugita:2000:RWS


Takashima:2000:HPR


Tomassini:2000:GHQ


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Fischer:2001:CLT


Fischer:2001:TRN


Folegati:2001:CLR


Gerosa:2001:FIB


Gonsalves:2001:PAS

The program contains code (near the end) for the portable ran
yu() 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.


REFERENCES

Hernandez:2001:FNO


Hernandez:2001:GAC


Howgrave-Graham:2001:PRN


Iwata:2001:PAF


Johnson:2001:CCO


Kang:2001:PMT

[2536] Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseudorandomness of MISTY-type transformations and the block ci-


REFERENCES


REFERENCES


www.rand.org/content/dam/rand/pubs/monograph_reports/2005/
digits.txt.zip; http://www.rand.org/pubs/monograph_reports/
MR1418.html. See also [146].

Rukhin:2001:STS

[2572] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker,
Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heck-
et, 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,
csrc.nist.gov/rng/sts-1.5.tar; http://csrc.nist.gov/rng/

Rukhin:2001:TRS

DEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL

Schindler:2001:EOT

[2574] W. Schindler. Efficient online tests for true random number gen-
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

FPGA implementation of neighborhood-of-four cellular automata ran-

Shaltiel:2001:SEA

[2576] Ronen Shaltiel and Christopher Umans. Simple extractors for all min-
entropies and a new pseudo-random generator. In IEEE [3864], pages


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Kunchenko:2002:PPE


Kuo:2002:CCC


LEcuyer:2002:CEG


LEcuyer:2002:OOR


LEcuyer:2002:RAR


LEcuyer:2002:SST

REFERENCES


McCullough:2002:RNG


Mita:2002:PBG


Moon:2002:IDC


Murray:2002:IYP


Niederreiter:2002:ADI


Niederreiter:2002:ICS


[2664] Barry Shackleford, Motoo Tanaka, Richard J. Carter, and Greg Snider. FPGA implementation of neighborhood-of-four cellular automata ran-

**Shparlinski:2002:DDH**


**Sugita:2002:RNI**


**Tan:2002:PPP**


**Tang:2002:CRN**


**Tang:2002:LBS**

REFERENCES


REFERENCES

Yaguchi:2002:CLP


Yao:2002:CBR


Aamodt:2003:CSP


Andem:2003:CTE


Anonymous:2003:DR

[2681] 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.”.


[2686] 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 fiasr 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).

REFERENCES


REFERENCES


REFERENCES


Intel:2003:IRN


Joe:2003:RAI


Kocarev:2003:CPR


LEcuyer:2003:CGC


Lemieux:2003:RPL


Li:2003:ULD

Lodwick:2003:EVC


Louchard:2003:ARS


Marsaglia:2003:EKD


Marsaglia:2003:RNG

Marsaglia:2003:TOS

Marsaglia:2003:XR


xorshift generators and the well-understood linear feedback shift register generators. See also [3448, 3541, 3630] for the failure of Marsaglia's xorwow() generator from this paper. See [2865, 3688] for detailed analysis.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Sugita:2004:SPR


Tang:2004:SGM


Tirler:2004:EKR


Tonon:2004:URS


Tsang:2004:TCT

REFERENCES


REFERENCES

Banks:2005:DES

Barak:2005:MAP

Beliakov:2005:CLR

Beliakov:2005:UNR

Benony:2005:CPC

Blackburn:2005:PNP
REFERENCES


[2826] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. Lecture Notes in Computer
Deng:2005:EPM


Dodge:2005:RNG


Eastlake:2005:RRR


Elsner:2005:IRN


Entacher:2005:BLP


Falcioni:2005:PMC


REFERENCES


REFERENCES


REFERENCES


Tang:2005:EER


Tang:2005:MLC


Tang:2005:RMR


Terpstra:2005:SIC


Topuzoglu:2005:LCP


Tu:2005:SRD

REFERENCES

Wichern:2005:GGP


Wiese:2005:IPN


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ

REFERENCES


REFERENCES


REFERENCES


Dickinson:2006:EEL


El-Mahassni:2006:DNC


Evans:2006:DOS


Faure:2006:SCR


Feige:2006:SIR


Finnigin:2006:CPN


REFERENCES

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


Hars:2006:MIA


Hartinger:2006:NUL


Hechenleitner:2006:PSG


Hong:2006:DRN


Indyk:2006:SDP

REFERENCES


LEcuyer:2006:ISB


LEcuyer:2006:TSL


Lee:2006:HGN


Lee:2006:IBH


Maffre:2006:WKT
REFERENCES


REFERENCES


[2949] Thomas Schanze. An exact $D$-dimensional Tsallis random number generator for generalized simulated annealing. *Computer Physics Communi-


generator [1022] developed for 16-bit arithmetic to a new four-part combination generator for 32-bit arithmetic with a period of $2^{121} \approx 10^{36}$.


REFERENCES


[2978] Paul Dupuis, Kevin Leder, and Hui Wang. Importance sampling for sums of random variables with regularly varying tails. *ACM Transactions on
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Alimohammad:2008:CAG


Alimohammad:2008:EAH


Alioto:2008:APE


Alvarez:2008:ETR


Attya:2008:ROC


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Howes:2008:U


Inaltekin:2008:ANE


Jang:2008:CDH


Joe:2008:CSS


Jovanovic-Dolecek:2008:UMT


Kalos:2008:MCM


Wei Li, Kangshun Li, Wensheng Zhang, Chao Wang, and Ying Huang. A random number generator based on particle dynamical evolutionary


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Cao:2009:DSB

Cecen:2009:NHN

Chen:2009:FPM

Chen:2009:MTR

Chi:2009:PQN
REFERENCES


Arthur Dryver. Code snippet: The enhancement of teaching materials for applied statistics courses by combining random number generation and


REFERENCES


[3181] R. A. Guinee and M. Blaszczyk. A novel true random binary sequence generator based on a chaotic double scroll oscillator combi-


REFERENCES


REFERENCES


REFERENCES


Svozil:2009:TCQ


Tafazzoli:2009:PCE


Tang:2009:FPS


Tawfeeq:2009:RNG


Thamrin:2009:EHB


Tian:2009:PTE

REFERENCES


Umlauft:2009:GNS


vanMeel:2009:GFS


Verloop:2009:HTA


Volos:2009:IEP


vonzurGathen:2009:SSP


Wang:2009:NPR

REFERENCES


REFERENCES


[3250] Alistair A. Abbott, Cristian S. Calude, and Karl Svozil. A quantum random number generator certified by value indefiniteness. Re-


REFERENCES


[3262] A. A. Borovkov. Integro-local and local theorems on normal and large deviations of the sums of nonidentically distributed random variables in


REFERENCES


REFERENCES

Quantum Communications and Quantum Imaging VIII.


[3300] 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,
REFERENCES


Lovett:2010:PGC


Luan:2010:PRC


Luo:2010:PAE


Marsaglia:2010:SKR


Marton:2010:RDC


Meka:2010:PGP


REFERENCES


REFERENCES


Proschan:2010:BQQ


Qi:2010:DFR


Quantis:2010:RNG


Quantis:2010:RTR


Ristenpart:2010:WGR


Roper:2010:CRNa

Roper:2010:CRNb


Roper:2010:CRNc


Roper:2010:CRNd


Saiprasert:2010:MMM


Saiprasert:2010:OHA


Saito:2010:VMT


Segui:2010:AIP


[3352] B. Valtchanov, V. Fischer, A. Aubert, and F. Bernard. Characterization of randomness sources in ring oscillator-based true random number

Varbanets:2010:ICG


Wikramaratna:2010:TEC


Williams:2010:FPR


Wu:2010:ULT


Xiaohui:2010:DCR


Xin:2010:IEB

[3358] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In 2010
REFERENCES

Ying:2010:DRN


Yoo:2010:IRR


Yu:2010:NRN


Zafar:2010:GRN


Zhmurov:2010:EPR


Anonymous. Quantum random bit generator service. Project developed by Centre for Informatics and Computing, Ruđer Bošković Institute, Zagreb, Croatia, 2011. URL http://random.irb.hr/.


Anonymous. Quantum random bit generator service. Project developed by Centre for Informatics and Computing, Ruđer Bošković Institute, Zagreb, Croatia, 2011. URL http://random.irb.hr/.


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.”


Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of


\textbf{REFERENCES}}
REFERENCES

Bellovin:2011:FMI


Blackburn:2011:DSS


Blanchet:2011:ERE


Boerstler:2011:RNG


Bohl:2011:FAR


Bradley:2011:PTR


Brown:2011:DRN


REFERENCES


REFERENCES


[3412] Parikshit Gopalan, Raghu Meka, Omer Reingold, and David Zuckerman. Pseudorandom generators for combinatorial shapes. In ACM [3912],


Heam:2011:SEU


Hedayatpour:2011:HFB


Hofert:2011:SET


Hung:2011:DRD


Hwang:2011:SID


Jian:2011:TBQ

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
REFERENCES


REFERENCES

Mukherjee:2011:RGU


Phillips:2011:PRN


Qiu:2011:ATB


Quantis:2011:RRW


Ren:2011:QRN


Rose:2011:KBT

REFERENCES

[3448] 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. [3916], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ???.


REFERENCES


Symul:2011:RTD


Tang:2011:ESG


Tang:2011:PES


Taylor:2011:DR


Veillette:2011:TCP


Versolatto:2011:MPR

REFERENCES


REFERENCES


REFERENCES

Abbott:2012:SKS


Abbott:2012:TFA


Anonymous:2012:CTC


Applebaum:2012:PGL


Barash:2012:GSP


Barker:2012:RRN


Bayon:2012:CEA

[3483] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, and François Poucheret. Contactless electromagnetic active attack on ring oscillator

Becher:2012:TNN


Beisbart:2012:WMC


Berger:2012:CPR


Bergman:2012:GRV


Bertoni:2012:KSF


Boldyreva:2012:NPG

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

[3520] 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

Science, 7417:68–85, 2012. CODEN LNCS9. ISSN 0302-9743 (print),
1007/978-3-642-32009-5_5/.

[3527] Jaroslaw Adam Miszczak. Generating and using truly random quantum
states in Mathematica. Computer Physics Communications, 183(1):118–
dc124, January 2012. CODEN CPHCBZ. ISSN 0010-4655 (print), 1879-
article/pii/S0010465511002748.

Pseudorandom generator to strengthen cooperation in VANETs. Lecture
ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.
springer.com/content/pdf/10.1007/978-3-642-27579-1_47.

[3529] Nimalan Nandapalan, Richard P. Brent, Lawrence M. Murray, and Alis-
tair P. Rendell. High-performance pseudorandom number generation on
graphics processing units. Lecture Notes in Computer Science, 7203:609–
618, 2012. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http://link.springer.com/chapter/10.1007/978-3-
642-31464-3_62.

algorithms and an indifference-zone ranking and selection procedure un-
der common random numbers for simulation optimisation. Journal of
Simulation, 6(1):56–66, 2012. ISSN 1747-7778 (print), 1747-7786 (elec-
tronic).

[3531] 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 LNCS9. ISSN 0302-9743 (print),
1007/978-3-642-31464-3_10/.

[3532] NIST. Recommendation for random number generation using determin-
istic random bit generators. Special Publication 800-90, National Insti-


REFERENCES


REFERENCES


[3560] 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


Hu:2013:PSG


IBM:2013:IPC


Imai:2013:CRN


Khoshkenar:2013:NTR


Liberty:2013:THR


Liu:2013:ITT


REFERENCES

Ozkaynak:2013:SPP


Pae:2013:EOR


Sainudiin:2013:PER


Saito:2013:VMT


Schretter:2013:DIM


Sezgin:2013:FBP


REFERENCES

Barabesi:2014:NUR


Barash:2014:PGA


Baron:2014:LSP


Blacher:2014:PRN


Braverman:2014:PGR


Chen:2014:EES


Cheng:2014:GBR

[3605] Ching-Wei Cheng, Ying-Chao Hung, and Narayanaswamy Balakrishnan. Generating beta random numbers and Dirichlet random vectors


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
<th>Year</th>
<th>Authors</th>
<th>Journal</th>
<th>Volume</th>
<th>Issue</th>
<th>Pages</th>
<th>DOI</th>
</tr>
</thead>
</table>


Mohamed:2014:MCS


Raaphorst:2014:CSC


Rivest:2014:SSR


Saito:2014:XV


Sanguinetti:2014:QRN


Sileshi:2014:AHG


REFERENCES


REFERENCES


**Passerat-Palmbach:2015:TSS**


**Pollack:2015:SNN**


**Potter:2015:MUE**


**Raitza:2015:RRN**


**Romano:2015:AGR**


**Sarkar:2015:FNR**


REFERENCES

Bayon:2016:FME


Chang-Fong:2016:CSC


Chattopadhyay:2016:ETS


deAndrade:2016:RNG


Dorre:2016:ELO


Guskova:2016:RPL

Herbert:2016:LIV


Karney:2016:SEN


Koerner:2016:REB


Lao:2016:BFD


Lecuyer:2016:ALB


Li:2016:ITS


REFERENCES


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA


Vigna:2016:EEM


Yamakami:2016:PGA


Yu:2016:GPR

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 [3698] for details of the attack.


REFERENCES


[3715] 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-


REFERENCES

Mullner:2018:RSS


Petrica:2018:FOC


Sanders:2018:EPR


Basuyaux:20xx:RNG


LEcuyer:20xx:PNG


Wagner:20xx:WRS

[3727] 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


REFERENCES


Rice:1971:MS


Zaremba:1972:ANT


Patil:1975:MCS


Hoaglin:1976:PNI


Ralston:1976:ECS


Traub:1976:ACR

[3747] J. F. Traub, editor. Algorithms and Complexity: Recent Results and New Directions: [Proceedings of a Symposium on New Directions and
REFERENCES


REFERENCES


REFERENCES


REFERENCES
662


REFERENCES


REFERENCES


IEEE:1987:ASF


Odlyzko:1987:ACC


Abrams:1988:WSC


ACM:1988:PTA


Edwards:1988:CPC

REFERENCES


REFERENCES


IEEE:1990:PAS


IEEE:1990:PSN


Pomerance:1990:CCNb


Anonymous:1991:PIS

REFERENCES


REFERENCES


Pflug:1992:SOP


Simmons:1992:CCS


Steele:1992:PA


Swain:1992:PWS


Vouk:1992:PAS

REFERENCES


REFERENCES


[Sincovec:1993:PSS]


[Swartzlander:1993:PSC]


[ACM-SIAM:1994:ASD]


[ACM:1994:PTS]


[Desmedt:1994:ACC]

REFERENCES


REFERENCES


REFERENCES


Andradottir:1997:PWS


Gell-Mann:1997:QJA


IEEE:1997:ASF


Troch:1997:PSI


Wyrzykowski:1997:PNP


Banks:1998:HSP

REFERENCES

http://www.loc.gov/catdir/description/wiley037/97051533.html;
http://www.loc.gov/catdir/toc/onix01/97051533.html.

Buhler:1998:ANT


Hellekalek:1998:RQR


IEEE:1998:HCC


Kent:1998:ECS


Medeiros:1998:WSC


Niederreiter:1998:MCQ

[3848] 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,
REFERENCES


USENIX:1998:SUS


ACM:1999:PTF


Anonymous:1999:NIS


Fossorier:1999:AAA


Heath:1999:APP

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Beyer:2005:GEC


Helleseth:2005:STA


Meadows:2005:CPA


Smart:2005:CCI

REFERENCES

Henderson:2006:S


Niederreiter:2006:MCQ


Schroeder:2006:NTS


Ytrehus:2006:CCI1


ACM:2007:SPA


Adams:2007:SAC


REFERENCES


[3901] Pierre L’Ecuyer and Art B. Owen, editors. *Monte Carlo and Quasi-Monte Carlo Methods 2008*. Springer-Verlag, Berlin, Germany / Hei-


REFERENCES


REFERENCES


Cooper:2012:HWC


Dunn:2012:EMC


Dyson:2012:TCO


Gentle:2012:HCS


Hwu:2012:GCG


IEEE:2012:PIA

REFERENCES


