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/

09 October 2019
Version 1.320

Title word cross-reference

#14 [2275]. #15949 [870]. #4059 [1241]. #8373 [2098].

(0, 1) [1052]. (0, s) [2533, 2920]. (a^n - 1)/(a - 1) [916]. (j, c) [729]. (n^2α) [2486]. (n^kα) [2487]. (να) [2486]. (t, m, s) [2042, 2879, 2048, 2348]. (t, s) [2628, 2042, 2339, 2879, 2048]. (X^2 - Y^2)^1/2 [489]. 0.1(0 × 1)0 × 9 [139]. 1 [736, 874, 128, 3141]. 13 [270]. 16 [270]. 2 [2832, 2117, 3079, 2495, 2811, 2957]. 1, 2, 3 [3472]. 1.13198824... [2510]. 10, 000 [282]. $10.00 [168]. 10^{2857} [2481]. 10^{4355} [2040]. 1200µ [3115]. 128 [3141]. 13 [270]. 16 [270]. 2 [2832, 2117, 928, 2879, 2495, 2811, 2957]. 2, 000 [86]. $24.95 [2085]. 2^-31 - 1 [836, 929]. 2^{15} [2135], 2^{31} - 1

0.57pJ [3242]. 0.57pJ/bit [3242]. '05 [3941, 3945]. '07 [3951]. '08 [3955].


5.0 [1634]. 5.2 [2748]. 500 [3294, 317]. 51st [3972]. 52 [870]. 52nd [3987]. 5th [3956].

6 [3603]. 60th [3788]. 61 [1230]. 623-dimensionally [2333]. 64-bit
Advanced [1451, 1915, 3806, 3970, 3924, 2429, 2504]. Advances [3818, 3836, 3854, 1066, 3904, 3916, 2653, 3875, 2672, 3826, 3828, 3881, 3953, 3839].


Approximations
[143, 2785, 1048, 475, 1001, 3007, 1224, 2976, 3037]. April
[3826, 3797, 3836, 3859, 3970, 3807, 3924, 3809, 3870, 3844, 3845]. Arbitrary
[2196, 812, 1529, 3041, 963, 3753, 3774, 2988, 197, 1691, 3478, 1284, 694, 3523].
Archimedean [3274]. Architecture
[2834, 2780, 3778, 3355, 2072, 3265, 3529, 3740, 1548]. Architectures
[1451, 3711, 3618]. Area
[219x574][238, 1888, 3691, 3047, 2190]. Area-Efficient
[3691, 3047]. areas
[3952, 3921, 2726]. Argument
[669]. arguments
[425]. Arisen [1]. Arising
[1244, 1519, 3495, 3573]. Arithmetical
[293]. Arithmétiques [3]. Arizona
[3820, 3861]. Arlington
[3879, 3913, 3928, 3822, 3869]. ARM7
[3073]. Arnold [2908]. arranged [21]. arrangements [58]. Array
[1378, 3283, 2570, 1364]. Arrays
[1478, 914, 3651, 789]. arrival
[3533, 2553, 3490, 3261]. arrivals [2707]. Art
[1709, 1731, 3687, 342, 3813]. Artefacts
[1565]. Arthur
[3027]. article
[870, 2253]. Artifacts
[2706]. Ascending
[2728]. aSHIIP
[3372]. ASIC
[2777]. Aspects
[3501, 3829]. Asperger
[2962]. ASR
[1230]. Assembler
[2224]. assembly
[3729]. assess [1909]. Assessing
[2139, 2410]. Assessment
[1367, 2093, 2772, 2626, 1290, 1449, 2304]. Assignment
[2093, 2772, 2626, 1290, 1449, 2304]. Associative
[1247, 2746, 3156, 2832, 1004, 21, 253, 419]. Association
[1804, 3805, 165, 3572, 951, 7]. associées [1004]. Assumption
[3514]. assumptions [1489]. Astronomical
[1401]. Asymmetric
[686, 3700]. Asymptotic
[564, 101, 3660, 669, 1528, 783, 2263, 1556, 55, 2266, 399, 3180, 2457, 2553, 1746].
Asymptotically
[2851]. Asymptotiques
[783]. Autocorrelated
[1609, 984, 1844]. Autocorrelation
[1577, 323, 635, 776, 777, 1675, 301, 430, 463]. Autocorrelations
[324, 964]. Autonome
[964]. Autokorrelation
[463]. Automata
[1404]. Automated
[1825]. Automates
[1548]. Automatic
[168, 1186, 2463, 2784, 2479, 768, 161, 2462, 3761, 135, 174, 3791, 2914, 2990].
[1713]. Beta [655, 735, 736, 872, 874, 822, 953, 524, 870, 1236, 313, 830, 832, 3631, 326, 2943, 767, 2047, 1064, 952, 696, 1847]. beta- [326].


Bibliography [593, 480, 612, 863, 1225, 908, 950]. bicompositional [3511].

Biennial [3805]. billion [1890]. billion-record [1890]. Biltmore [3861].

bimodal [3700]. Binomial [655, 2522, 2222, 1333, 1409, 1506, 3558, 1161, 918, 870, 1788, 1212, 606]. Binomial-Truncated [1506].


Black-Box [2843]. Block [2550, 1266, 2489, 2884, 3203, 2717, 1596, 3128].


bodies [32]. body [2811, 1278]. Bonferroni [1183, 762]. BonGCL [1341].


Borwein [3788, 3585, 3586]. both [1742, 2756]. Bound [2049, 1996].

carry-free [1060]. Carus [3572]. cascade [2095]. Case
[2191, 509, 1, 2837, 3180, 1762, 2115, 2295, 3538, 2946, 50, 3155]. cases
[2806, 2817, 2966]. Casinos [3705]. Casuali [964]. cat [2908]. Cathedral
[3935, 3984]. Cauchy [1291, 3519, 2535]. Cautionary [219]. Cautions
[2031]. Cebyshev [1684, 1204]. Cell [3050, 3621, 1326]. Cells
[3780, 2514, 3593]. cellulares [1548]. Cellular [2283, 3079, 1404, 1492, 3092,
1548, 1969, 1246, 3187, 2785, 1405, 1709, 2334, 3330, 3763, 2749, 2589,
2678, 2175, 2425, 2353, 1963, 2435, 2509, 1629, 1228, 1229]. Censored
[843]. Centenary [3982]. Center [3856]. Central
[1083, 2952, 3312, 3461, 3674, 2737, 1240, 2535, 2819]. Centre [3804]. centro
[3495, 3573]. centro-invertible [3495, 3573]. centroids [429]. Century
[2452, 3909, 2770]. Certain [41, 495, 669, 24, 425, 1292, 101, 1871, 2205, 171,
206, 297, 402, 219, 220, 1497, 2555, 1703, 1432, 1519, 689, 1548]. certains
[1548]. Certifiable [3571]. Certification [3389, 359, 309, 613]. Certified
[2200, 502, 3088, 645, 210, 3299, 692]. Chance [2369, 3469, 460, 244].
Change [1868, 3430, 3358, 986]. Changes [2535]. Changing [2696, 1828].
Channel [965, 3288, 1793, 2451, 2777, 3128, 3489]. Chaos [1643, 1661, 2995,
2549, 3096, 2723, 3454, 3939, 2813, 2594, 2595, 3160, 2692, 3053, 3419, 3097,
1806, 2734, 3127, 1531, 3233, 3346, 3369, 3147, 2366, 2830, 3384, 3620].
Chaos-Based [2995, 3454, 2594, 2595, 2692, 3053, 3419, 3233, 2830, 3620].
chao-s-type [3147]. Chaotic [3398, 1459, 3428, 2018, 2566, 2335, 3121, 3340,
3236, 2592, 3142, 3143, 3148, 2762, 3260, 1636, 3273, 3770, 3056, 3183, 3427,
2849, 2538, 2993, 3201, 3308, 3665, 3438, 1403, 3210, 3599, 2793, 3457, 3334,
3612, 1163, 3243, 3254, 3766, 3258, 3154, 3267]. Chapman [2300]. Chapter
[2915, 2942]. Character [2520, 2671]. characterisation [2017].
Characteristic [1186, 1269, 3753, 3774, 968, 1076, 760, 2811, 1961, 2070].
characteristics [196]. Characterization [1989, 862, 3375].
characterizations [1669]. Characterizing [3570]. Characters [2804].
Cheat [3705]. Chebyshev [1411, 3710]. check [886]. Checks [2644]. Chen
[3599, 3612]. Chernoff [2250, 2255]. CHES [3962, 3927]. Chi
[804, 43, 1268, 1349, 3331, 87, 1326, 1147]. Chi-Square [804, 3331, 87].
China [3934, 3977]. Chinese [105, 2682]. Chip [3073, 1454, 3065, 3250].
chips [3907]. chisel [346]. Choice [486, 676, 43, 611, 87, 2545, 2605].
Cholesky [951]. Choose [816]. Choosing [807, 588, 1812, 2731, 945].
CiE [3982]. Cipher
[1870, 2550, 3016, 907, 2592, 1639, 2717, 3093, 3128, 3652, 2500, 3154].
Ciphers
[1452, 2619, 2489, 2884, 3193, 3758, 3458, 1432, 1712, 3329, 1621, 2891].
Circuit [2706, 2886, 3027, 3056, 3159]. Circuits
Circulation [3642]. Cirencester [3946]. City [3835, 3913, 3792, 3891].
[2551, 1506, 96, 2422, 87, 1147, 1794, 1599, 3027]. Classical
[3725, 3280, 3755, 1887, 795, 662, 1692]. Classification [1886]. Classified
[612, 863, 1225]. classifiers [210x574]. Classroom
[393, 567, 294, 505, 383, 360, 363, 2895]. Clearer
[315x562]. Cleve
[2040, 2571]. client
[1941]. client-server
[1941]. Clipped
[611]. Clipper
[2038]. Clipper-like
[2038]. Clock
[1977]. Clock-controlled
[1977]. Close
[2473, 1145, 2649]. Close-Point
[2473]. Closer
[3527]. Cloudier
[3698]. clubs
[1289]. Cluster
[1831, 2258]. Cluster-flipping
[1831]. Clustered
[253]. clustered-rocket
[253]. Clustering
[3202, 887, 3199]. cm
[168]. CMOS
[3294, 3084, 3242, 525, 3141, 3497, 1644, 2768, 1305, 1469, 1773, 1785, 3207, 2130, 940, 1806, 1603, 1935, 2341, 1941, 3768, 3268]. Co
[168, 2174]. Co-evolving
[2174]. Code
[3166, 2108, 3189, 982, 3324, 2170, 3574, 2697, 971, 3206, 1925, 2057, 3787, 1054]. Coded
[3123, 3723]. Codes
[3291, 2619, 1266, 3914, 270, 3679]. Coding
[2566, 481, 3946, 3950, 3848, 427, 894, 3875]. Coefficient
[335x443]. Coefficients
[3070, 1012, 815, 2601]. Coherent
[1384, 3430, 3484]. Coin
[1756]. Coin-Tossing
[1756]. Coins
[2767, 2469]. Collected
[3798, 1969]. collecting
[138]. collection
[3801, 2215]. Collector
[142]. College
[3792]. Collision
[3513, 2758, 2826]. Collision-Resistant
[3513]. colorectal
[3245]. Coloring
[2255]. Columbia
[3862, 3955]. column
[3040]. Combination
[924, 2202, 1082, 1083, 1084, 3020, 2060, 422, 2370, 3201, 2241, 1621, 1223, 2829]. Combinations
[393, 505, 475, 363, 1766, 1091, 2787, 439, 440, 61]. Combinatorial
[619, 3592, 201, 2326, 1523, 2088, 235, 3435, 752]. Combinatorics
[3853, 2713]. Combined
[3204, 3669, 2140, 2403, 2474, 2724, 2682, 1443, 1962, 3491, 3380, 1761, 1893, 1342, 1599, 2142, 2413, 2320, 2406, 2658, 1442, 1627, 2601]. Combiner
[2354]. combiners
[1712]. combinés
[2601]. Combining
[881, 882, 1571, 3189, 2540, 3072]. Coming
[3623]. Commentary
[2141]. Comments
[2768, 3057, 1125, 704, 768, 587, 1737]. Commitment
[1521, 1612]. Commodore
[1119]. Common
[1183, 3777, 501, 1262, 1693, 3015, 1717, 1535, 790, 2132, 1094, 3554, 1820, 1060, 733, 3516, 2525, 2200, 1089, 1686, 889, 756, 712, 895, 1336, 2398, 1819, 2043, 917, 1448, 1638]. Commun
[2010, 2131]. Communicating
[1285]. Communication
[570, 3949, 1285, 1301, 2451, 2777, 3444]. Communications
[495, 2648, 3945, 3875, 2692]. Comp
[2098]. Compact
[1974, 2759, 2980, 3045, 1386, 2468, 3012, 586]. Companion
[3989]. Comparative
[1311, 396, 492, 3191, 2073]. Comparing
[1198, 889, 1792, 2139, 3268]. Comparison
[654, 565, 1029, 3177, 3734, 3601, 1693, 3103, 202, 2250, 595, 1056, 685, 2166,
ENIAC [3638, 86]. Enigma [2619]. Enjoy [3043]. Enough [1809].
ensemble [2908]. Enskog [2619]. ENT [3153]. entanglement [3316].
Enterprise [2747]. Enthusiasm [2700]. entropies [1590, 2590, 2888].
Entropy [2611, 2097, 3633, 3732, 3701, 970, 1992, 576, 3099, 2239, 3708, 3673,
3606, 2736, 2808, 3717, 3684, 3065, 1040, 3637]. Entropy-Based
Environment [2696, 1976, 2798, 1623]. Environments [3292, 3176]. EPC
[3357]. Equal [649, 215, 1145, 2256]. Equalization [3415]. Equally
[625, 1324]. Equation [118]. Equations [2203, 2050, 2276, 1323, 159, 131, 132, 136, 3768].
Equidistributed [499, 3757, 217, 1144, 2143, 2406, 2651, 2333]. Equidistribution
[3399, 1769, 2116, 2213, 2292, 2208, 2625, 182, 1038]. equilibria [3087].
[2632]. Ergodic [3274, 673, 846, 3122]. Erlang [883]. ERNIE [234, 207].
Erratum [487, 2906, 1195, 2010, 672, 2131, 584, 2253, 910]. Error
[630, 982, 767, 1519, 2, 2827, 2180, 1762, 3074, 3914, 3319, 2945, 610, 2824].
error-correcting [3914]. Errors [2062, 2198, 1683, 2023, 2665, 2806, 2810, 2258].
Erwin [1915]. erzeugte [623, 624]. Erzeugter [430, 463]. Erzeugung
[1026, 616, 1202, 978, 1324, 1472, 326, 1847, 868]. Erzeugungen [607].
Escape [1661]. Escrow [2038]. Española [133]. Especially [3676]. Essays
[2200, 2633, 1043, 94, 630, 1510, 587, 85, 684, 1947, 2827, 529, 1003, 1132,
3207, 1411, 2809, 33, 3721, 3700]. Estimations [2154, 2649, 3026].
Estimators [3099, 1918]. Euclid [104, 26]. Euclidean
[1975, 739, 2372, 2484, 663, 493, 1528, 2972, 2066, 2358, 2359]. Eugene [976].
Euro [2632]. EUROCRYPT [3826, 3836]. Europe [3982]. European
[3810]. Evalua [3048]. Evalua-Test [3048]. Evaluating
[1979, 2729, 1000, 219, 220, 3268]. Evaluation [3577, 1461, 1992, 1005, 750,
751, 498, 242, 842, 1589, 2648, 2551, 327, 3606, 3238, 3690, 2422, 2180, 2081,
3047, 836, 1041, 2863, 2946, 1929, 1938, 1107, 948, 98, 417]. evaluations
[2021]. even [3622, 3496]. even-distribution [3496]. Event
[1070, 2090, 2521, 2833, 3276, 1129, 621, 835, 3407, 542, 1329, 1911]. Events
[766, 2845, 1189]. everyone [3532]. Evidence [2793, 3286, 81, 2716, 2962].
Evolutionary [3943, 2530, 3109, 3562, 3931, 3269, 2545, 2900]. Evolvable
[2606]. Evolved [2940]. evolving [3718, 2174]. Exact
[3517, 539, 1136, 3613, 2267, 1368, 1758, 538, 1099, 2967, 2423, 50, 2082].
exact-approximation [1099]. Exactly [3704]. examination [3933].
Example [567]. Examples [1458, 841, 2673, 2895, 1980]. Exceeding [3199].
Excel [2411, 2664, 2878, 3116, 2665, 2806, 3117]. Exceptionally [1870].
exchange [3692]. Exchangeable [3430, 1123]. Excited [3064, 3428].
exclusive [3249]. Execution [1456]. executive [2962]. exemplary [2084].
Exhaustive [1085, 1480, 1194, 1195, 1315, 2135, 2974, 3485, 3486].

Exist [3676, 3034]. Existence [1780, 850, 2741, 3478, 1234, 1373, 1322].

expanded [1726]. Expanding [3715]. Expansion [669, 405, 433].


Expected [1574, 2421, 3731, 1889, 1326, 1221]. expedient [64].

experience [1564, 2192, 925, 2065]. experiences [409].

Experiment [2770, 3656]. Experimental [920, 921, 3170, 3286, 3200, 626, 709, 24, 933, 893, 936, 941, 942, 849, 949, 2752, 3719, 791, 3171, 1896, 1713, 175, 7].


Explicitly [2917]. Explicitly [2283, 3699, 3074, 1768, 1882, 2580, 1997, 2117, 2735, 2171].

Explicitations [2710, 2139, 1621]. exponentiations [1554]. exponents [2793].

Expressing [249]. expression [2021]. Extendable [3680].

Extendable-Output [3680].

Extended [2376, 1137, 1487, 2552, 3671, 1521, 1170, 487, 1237, 3864, 1408, 1794, 3449, 473, 3325, 1216, 2434, 2437].

Extending [1160]. Extends [1793].


Extracting [2907, 2162, 1728]. Extraction [3301, 3606, 3561]. Extractor [3569, 3759]. Extractions [3699, 2465, 3708, 2602, 2590, 2888, 2437, 3837].

Extrapolation [1340]. Extraterrestrial [2054]. Extreme [1682, 8].

Extremely [472, 723, 584, 585, 3496]. extremely-high-throughput [3496].

Face [3252]. Facilities [1598, 344]. Factored [1294]. Factorial [2250].

Factoring [1012, 1151, 1264, 1827, 1742, 2756]. Factorization [1822, 724, 1334, 683, 1164, 1949, 3564].


Family [872, 1309, 2630, 3712, 1546, 3397, 3512, 1575, 2205, 1260, 993, 3618, 2760].


Fastest [3121]. fat [1558]. fat-tailed [1558]. Fault [3697, 3409, 3588, 1216].


FCSR [2831, 3760, 3249]. FCSRs [3510, 3193, 3758]. FDC [1918]. Features
GASPRNG [3591]. Gate [3084, 2570, 2980]. Gates [3041, 3305]. Gateway
[3928, 3822, 3869]. Gathering [2611]. Gauss [1817]. Gaussian
[3045, 2610, 996, 1379, 659, 1075, 3178, 2451, 3632, 1576, 3190, 294,
345, 2777, 3529, 2229, 3640, 2231, 2470, 3314, 2649, 2794, 2868, 2945, 2946,
3107, 3453, 3543, 3461, 3607, 3674, 3711, 636, 1604, 443, 1014, 3649, 854, 360,
2961, 3354, 3355, 3655, 524, 391, 3035, 3145, 3658, 3691, 1840, 3374, 867, 2901,
GCD [1237, 1792, 1160, 1273, 1953, 1956, 2066, 1843]. GCDs [3111].
GECCO [3943, 3931]. GECCO-2001 [3931]. geeks [2734]. gems
[3976, 3986, 3958]. Gen2 [3175, 3357]. généateurs [3785]. General
[923, 491, 1894, 1895, 2014, 3707, 3107, 514, 1056, 827, 3156, 2271, 3860,
704, 3671, 380, 945, 1224, 3030, 3478, 3765, 603]. General-Purpose
[1056]. Generalised
[2133, 875]. Generalization
[436, 235]. generalizations
[3524]. Generate
[1294, 999, 1071, 1857, 2544, 1496, 3621, 1850, 2370, 754, 2129, 1204, 3765,
1595, 1844, 1637, 1971]. Generated
[3164, 3275, 264, 241, 1044, 598, 368, 3497, 1288, 1752, 568, 738, 1666, 430,
463, 571, 3524, 1392, 1475, 239, 748, 1351, 2999, 623, 1901, 1009, 2235, 2023,
2024, 1149, 3457, 2148, 2328, 680, 779, 1159, 1434, 1525, 2490, 3124, 3557, 904,
817, 1017, 3476, 2828, 231, 2269]. Generating
[995, 2084, 2186, 1645, 3725, 2832, 1563, 1754, 877, 922, 3511, 1074, 1859, 2196,
832, 3631, 3292, 267, 194, 1185, 1186, 1573, 2454, 969, 1248, 3077, 1151, 318,
403, 3433, 3434, 470, 242, 199, 1902, 3640, 153, 2470, 1911, 2021, 759, 1694,
1695, 1095, 984, 1804, 3453, 304, 2029, 3461, 248, 848, 250, 251, 277, 278, 306,
330, 770, 943, 1101, 2329, 2482, 1609, 2038, 773, 3551, 812, 3465, 1268, 1349,
202, 203, 514, 2740, 1529, 1532, 3341, 2418, 1942, 2054, 517, 604, 686, 3237,
2168, 1222, 1066, 452, 2175, 1111, 611, 2261, 2505, 2435, 1285]. Generating
[827, 2076, 1116, 696, 2898, 2978, 1366, 1026, 2518, 660, 1865, 1076, 1078, 749,
1890, 1202, 93, 1491, 1791, 3533, 1502, 938, 1799, 896, 1421, 2565, 3543, 767,
329, 224, 252, 280, 331, 509, 1099, 2330, 2483, 3714, 479, 2336, 3611, 898,
2953, 2341, 602, 647, 339, 1828, 606, 2346, 3686, 1064, 858, 957, 2750, 1544,
730, 191, 165, 1632, 3787, 694, 1447, 2512, 3575, 1847]. Generation
[3389, 3769, 994, 1371, 2368, 3749, 1235, 2765, 3624, 829, 531, 735, 736, 871,
872, 873, 874, 3398, 2275, 2834, 2909, 2912, 2191, 1459, 2280, 2447, 2282, 2102,
3412, 831, 740, 2524, 800, 1075, 1244, 742, 214, 536, 461, 1304, 1988, 1471,
2452, 1077, 1187, 2108, 2702, 3015, 619, 3189, 1035, 1309, 1191, 1998, 3635,
2382, 1081, 2297, 2920, 90, 91, 2631, 1888, 2300, 580, 2301, 2708, 3198, 622,
436, 2302, 2542, 320, 2229, 1689, 1900, 2784, 3534, 3086, 2547, 582, 1331, 2644,
325, 2646, 2133, 2647, 1047, 1333, 3536, 3537, 1912, 1593, 758, 806]. Generation
[1504, 2236, 1423, 2558, 2792, 2942, 3103, 808, 3645, 1150, 3779, 246, 3605, 676,
1602, 1707, 3711, 3546, 2149, 1811, 2800, 2034, 2035, 2949, 443,
2354, 2823, 1365, 1545, 1743, 1964, 1112, 3370, 559, 2759, 3039, 1630,
1631, 2180, 1841, 2762, 3719, 787, 1286, 2077, 2441, 2607, 422, 1635, 423, 484,
3619, 828, 1639, 2367, 1026, 1119, 1173, 1288, 1290, 1449, 3576, 2609, 1849, 2443,
3046, 3047, 3722, 1234, 1373, 1293, 3659, 488, 3577, 2086, 3504, 2088, 1644, 3049,
1646, 2273, 3397, 3580, 3696, 2276, 3705, 3583, 1028, 2982, 3506, 3627, 3277].
generators
[3167, 1977, 3697, 3053, 1650, 1122, 1379, 2838, 1029, 2839, 1178, 1979, 1654,
2615, 2698, 2912, 2986, 2373, 883, 1463, 1657, 2840, 1180, 701, 3062, 3630, 1866,
3065, 3587, 3418, 1867, 2106, 2197, 535, 1000, 1872, 3181, 2287, 1306, 1469, 3187,
1575, 401, 1390, 2704, 2205, 2206, 2455, 1473, 3190, 1392, 1393, 1476, 1676, 1313,
2847, 1886, 1887, 2002, 2119, 2215, 2294, 2295, 2384, 2530, 2531, 1683, 1133, 1775, 836,
928, 929, 1194].
generators
[1195, 1315, 1776, 2005, 3733, 431, 1007, 272, 2299, 839, 974, 2851, 2999, 3734,
1322, 3637, 2853, 3435, 2712, 1687, 1781, 752, 468, 1202, 1257, 1324, 2540, 2638,
2714, 2715, 3080, 3594, 3308, 1489, 3309, 1402, 1873, 1784, 1892, 670, 3439,
3340, 1893, 2015, 2227, 2228, 2307, 2545, 3735, 1403, 2230, 3598, 757, 844, 3310,
3209, 1404, 1904, 3444, 1144, 3601, 1690, 2465, 2466, 2935, 1495, 351, 378, 2132,
2860, 1795, 2135, 2233, 2312, 2313, 3447, 979, 3095, 1414, 2787, 894, 1692,
3101, 2400, 3449, 1696, 2864, 2939, 3008, 807, 1341, 1342, 1422, 1599, 1803].
generators
[2140, 2142, 2143, 2145, 2239, 2240, 2320, 2322, 2323, 2405, 2406, 2555, 2557,
2651, 2724, 2789, 2866, 3009, 3011, 3320, 1508, 3736, 1097, 2865, 3105, 3218,
2244, 1700, 3106, 1132, 1265, 846, 2567, 3759, 3321, 3014, 3112, 1213, 2148, 2658,
1927, 2030, 3545, 3222, 3547, 439, 440, 476, 511, 1603, 1708, 1928, 1930, 2731,
2661, 3113, 2331, 2570, 2802, 2803, 3548, 3608, 1710, 1719, 1933, 2332, 2334, 2733,
2950, 3015, 1711, 1815, 772, 3117, 3017, 3328, 2736, 2808, 1713, 1610, 447, 3611,
3224, 3679, 1716, 594, 3021, 3228, 2158, 640, 1103, 1272, 1526, 2492, 2575, 2672].
generators
[1527, 1723, 1724, 3126, 2810, 3335, 3336, 601, 2495, 2812, 2882,
2959, 3339, 1618, 1105, 1274, 1358, 1436, 1726, 1727, 2052, 1359, 2055, 3344,
2960, 1107, 2058, 820, 2345, 1062, 1532, 855, 1063, 3690, 2257, 2062, 1539,
1831, 1363, 1442, 1737, 2820, 3617, 2589, 2678, 1738, 2424, 3360, 3743, 260,
2175, 1955, 1739, 3479, 2753, 2433, 3657, 1250, 3481, 2594, 2595, 2434, 3244,
2822, 2264, 2600, 2757, 2894, 2974, 2975, 3034, 3365, 3485, 3486, 1627, 1839,
1963, 3035, 3618, 3658, 3371, 2896, 2601, 2437, 2602, 1629, 962, 2760, 2687,
2761, 3375, 1068, 2073, 1069, 3747, 2181, 1842]. generators
[3491, 1748, 2006, 2078, 2183, 1968, 454, 3377, 2268, 2979, 3379, 3720, 2692,
3267, 3268, 3693, 3386, 3387, 2281, 3104, 3219, 394, 504]. generators-part
[2594]. Generazione [964]. Genetic
[2546, 2639, 2640, 628, 672, 2940, 3031, 2823, 2899, 2099, 2841, 2661, 3554, 3943].
Gentle [2968, 2447, 2805]. Genuine [3566, 2828]. Geographic [2281]. Geometric
[3505, 1910, 2157, 2760, 2726, 1716, 2603]. Geometrical
[3256, 2028]. Geometrically [2785, 2713, 2728]. Geometry


Guitar [2700].

Hard-coded [3723]. hard/soft [3235]. hardcore [3627]. hardnesses [2687, 2761]. Hardware [1372, 3584, 3662, 3663, 2280, 3529, 2552, 3104, 3711, 1615, 2164, 3355, 3248, 3145, 3787, 3784, 3295, 2514, 1027, 2536, 3200, 3079, 3213, 3927, 2863, 2794, 2868, 2945, 2946, 3543, 3604, 2874, 3758, 3460, 2661, 2901, 3523, 3219].

Hardware-based [3248, 2794]. Hardware-optimized [3190]. Hardware-optimized [3190].


High [2368, 3390, 2096, 3662, 2617, 3065, 3203, 3204, 3211, 3092, 3706, 3978, 2478, 636, 2033, 3648, 3553, 3340, 1165, 3036, 3038, 100, 3494, 1032, 1302, 2616, 2699, 2622, 2701, 2992, 3075, 3190, 2531, 2777, 3306, 3000, 1691, 1905, 2131, 117, 3102, 3215, 128, 3455, 1924, 3460, 3461, 1931, 774, 2340, 225, 2962, 2887, 2972, 1168, 3656, 3484, 121, 2435, 2509, 3496, 2902]. High-density [2617]. high-dimensional [2622, 2701, 2340, 2972, 3656]. High-entropy [3065]. high-functioning [2962]. high-order [3000]. High-Performance [3092, 3211, 3553, 3455]. high-period [2992]. High-Quality [2096, 2531, 1905, 2131, 1924, 2435, 2509]. High-Speed [2368, 3204, 3706, 3340, 3662, 2478, 1165, 2699, 3190, 1691, 117, 128, 774, 225].


Hyatt [3913, 3987, 3909]. Hybrid [3187, 349, 2508, 3248, 3046, 3173, 546].
hyerbolas [2079, 2361]. Hyperbolic [2746, 875, 996, 1764, 1914, 1947].
Hypercube [3833, 910, 911, 1330]. Hypercubes [3847]. Hypergeometric
[1332, 1146]. hyperplane [2205]. Hyperplanes [2207]. hyperspheres
[3272, 2972]. Hypotheses [173]. Hypothesis [434].
I. [869]. IBM [3795, 704, 795, 662, 1398, 1485, 753, 1513, 482, 454].
IBM-Compatible [1485, 1513]. ibre [1026]. IC
[2699, 3426, 3305, 3306, 2344, 2496, 3369]. ICCMSE [3954]. ICGA [3931].
ICGA-2001 [3931]. ICICTA [3954]. IC ICTA [3977]. Icosahedral
[165]. ideal [795, 662]. identical [931]. Identically [2513, 3312]. Identification
[3926, 3971, 3972, 3987]. If [1460]. IFIP [3970]. II
[3916, 1233, 3282, 1673, 1767, 2216, 1784, 1895, 1206, 251, 1933, 2037, 2410,
638, 1611, 680, 1440, 522, 2595, 866, 2180, 1553, 2082]. II.5 [746]. IIASA
Illustrations [7]. Illustrative [2895]. IMA [3915, 3946]. IMACS [3902].
Image [3425, 3473, 3474, 3258, 3267, 3442, 3454, 1431, 3381]. Images
Impact [3167, 3278, 1105, 2899]. Imperfections [630]. implement [73].
Implementation [1853, 3725, 3052, 1376, 1652, 1181, 1981, 2526, 3067, 1875,
3070, 2706, 3192, 1197, 1484, 1328, 2869, 3605, 1925, 3712, 3874, 2669, 594,
719, 3340, 1435, 2676, 1944, 1945, 3568, 1841, 3162, 1372, 2186, 3585, 3586,
3171, 2374, 3179, 2451, 2622, 466, 2777, 2714, 3200, 3079, 1905, 2131, 3314,
3213, 2240, 3460, 2661, 2164, 1623, 1737, 2589, 2678, 3364].
Implementations [1464, 2377, 2403, 3713, 3730, 2320, 2570]. implemented
[1243, 3419, 1687, 1093, 3604, 1100, 3025]. Implementing
[1298, 799, 3757, 1598, 1812, 1052, 1019, 2722]. implicated [3589].
implications [3193, 544]. implicitly [1377]. imply [3196]. Importance
[2996, 1320, 3450]. important [460]. Impossibility [2949, 1608].
Impossible [2668, 2074]. Improper [626, 1193]. improve [2497]. Improved
[1648, 1766, 1884, 2288, 1134, 2458, 2850, 2391, 3708, 2326, 2807, 3227, 2159,
2959, 879, 1996, 3693]. Improvement [3330, 1938, 1162, 2086, 2658, 3357].
Improvements [3595, 770, 3309, 2173]. improves [3722]. Improving
[737, 3182, 1468, 3072, 3308, 278, 3023, 817, 3480, 3383, 3593, 1457]. incident
[3754]. included [2856, 3558]. including [1134, 2031, 1229]. Incomplete
[2614, 2492, 2671, 1215]. incomputability [3501, 3286]. Increase [3332].
Increasing [1038]. Indefiniteness [3059, 3271]. indentation [3499].
Independence
[173, 3399, 2523, 1773, 1885, 2293, 2625, 2005, 1196, 2563, 780, 1352, 1526, 726].
independences [2036, 2037, 2409]. Independent
[2907, 1378, 1072, 1176, 2103, 3519, 2109, 2921, 841, 3639, 2128, 1419, 1505,
982, 512, 411, 944, 1161, 2165, 516, 1535, 390, 310, 915, 2513, 3769, 2515,

1744, 1838, 3161, 3504, 2839, 879, 1652, 1758, 3181, 2932, 3085, 3317, 985, 1421, 2477, 2726, 2796, 3112, 3610, 3464, 1718, 2254, 3562, 2068, 2082.

Low-cost [3610, 3464]. Low-Degree [3323]. Low-dimensional [1758, 2082]. Low-Dimensionality [2917]. Low-Discrepancy [2631, 2338, 1546, 1857, 1218, 1350, 1719, 879, 1652, 2932, 2477, 2726, 1718, 3562, 2068].


Many [2160, 2652, 1165, 652]. Map [3290, 3497, 3770, 3710, 2053, 3243].


Marsaglia [3272, 2273, 2771, 1312, 1313, 1328, 2031, 2052, 1059, 3719, 3747].


2044, 2046, 3495, 3573, 1202. Matrixgeneratoren [1202, 1324]. max [1429].
Maximal [181, 1579, 1417, 810, 903, 2686, 1676, 2712, 3557, 3249].
May [3825, 3830, 3835, 3841, 3846, 3851, 3862, 3871, 3880, 3885, 3893, 3894, 3912, 3919, 3932, 3941, 3955, 3981, 3983]. mbedTLS [3748].
MC [2237]. MCNP [1249, 3303]. MCS [3929]. MCS [3929].
McShane [496]. MCV [723, 782]. Mean [564, 1075, 2785, 587, 2, 529, 1672, 1673, 2707, 1941].
mean-square [1672, 1673]. meaning [432]. Means [3519, 2940, 3032, 2069, 2545, 3330].
Measure [2187, 2309, 2519, 2853, 2865, 2058, 2600]. measurement [3181, 3307]. measurements [546, 3490].
Mechanical [2840]. mechanics [2840]. mechanics [2840].
Memory [2368, 2185, 3659, 3778, 3650, 3780, 3358, 1707, 1712].
Mellon [3809]. Memorial [3907]. Memory [2368, 2185, 3659, 3778, 3650, 3780, 3358, 1707, 1712].
Metamodels [1693, 3516]. Metastability [3146, 2874].
Multiple-Comparison [1638].
Multiple-Recursive [2159, 2044, 2046]. Multiple-Valued [238]. multiples [2601]. Multiplexed [2637]. Multiplication [2139, 1158, 1557].


NIST-Recommended [2861]. Nix [3686]. NJ [2085]. nm [3294, 3604].
249, 2812, 2882, 3682, 1435, 1105, 481, 515]. **number**
[1055, 1274, 1436, 1726, 2052, 945, 1359, 3128, 3763, 2496, 2053, 553, 3467, 2055,
1275, 3344, 782, 2960, 3742, 1106, 603, 2497, 1945, 3347, 257, 1107, 605, 362,
820, 3470, 2345, 1621, 2962, 1062, 1533, 2964, 1063, 2677, 3026, 1623, 908, 950,
1165, 3565, 687, 2500, 3689, 2967, 690, 607, 2062, 2968, 2349, 1539, 3357, 1831,
482, 3473, 1363, 1442, 1626, 1737, 2063, 2172, 2173, 2820, 3617, 2589, 2678,
1738, 1832, 2259, 2424, 3359, 824, 1833, 3743, 3655, 3478, 2175, 2425, 1168, 2593,
2752, 3479, 960, 2753, 2433, 3657, 2506, 206, 3031, 3481, 2594, 2595, 3482, 3244.
**Number-theoretic** [2249]. **Numbers** [3389, 486, 793, 2903, 2763, 2517,
1643, 2765, 2087, 3579, 2188, 919, 1294, 3398, 2612, 292, 1296, 3508, 922, 2096,
3628, 2614, 236, 181, 740, 2449, 1982, 1183, 214, 2528, 539, 619, 268, 703,
1576, 2379, 1191, 1578, 1582, 1677, 1878, 1995, 2001, 2114, 2207, 2209, 2211,
2918, 2291, 2214, 2296, 2629, 837, 1037, 3302, 48, 318, 403, 841, 3198, 1319,
3433, 3434, 3777, 241, 2394, 2541, 2302, 499, 320, 375, 2544, 2641, 3668, 3208,
1790, 1044, 350, 2644, 324, 2646, 153, 1498, 1797, 3602, 1693, 223, 1695, 1506].
**Numbers** [547, 630, 1509, 2556, 1697, 26, 246, 676, 1926, 1347, 636, 441, 812,
130, 1269, 448, 598, 851, 852, 2416, 2578, 2680, 1615, 3341, 816, 1619,
3234, 2744, 2745, 356, 386, 1943, 3683, 1438, 3469, 517, 3133, 1829, 519, 453,
341, 3032, 613, 368, 1281, 2179, 528, 1116, 1447, 2365, 885, 1026, 1289, 1368,
1560, 3626, 1453, 1975, 1455, 3580, 1295, 3581, 3583, 3727, 176, 3167, 964,
2983, 1563, 1648, 2984, 2697, 313, 3586, 1564, 2192, 1566, 2769, 738, 1462, 103,
396, 492, 3631, 1865, 2618, 212, 213, 742, 3179, 1246, 2773, 57]. **numbers**
[2450, 461, 1465, 1387, 293, 430, 463, 538, 571, 665, 42, 464, 2992, 1472, 112,
216, 1580, 1581, 1583, 1678, 1680, 1767, 1768, 1769, 1770, 1771, 1772, 1773,
1879, 1880, 1881, 1882, 1883, 1884, 1885, 1996, 1997, 1999, 2115, 2116, 2117,
2208, 2210, 2212, 2288, 2289, 2290, 1312, 2213, 2625, 2383, 3756, 317, 151,
2004, 2120, 2386, 2387, 2388, 239, 1776, 182, 747, 748, 1199, 1318, 2390, 2538,
140, 197, 217, 116, 467, 2928, 977, 183, 623]. **numbers**
[624, 469, 1090, 2460, 3665, 65, 74, 2013, 2225, 2305, 470, 2718, 66, 1204, 978,
1691, 409, 2232, 326, 1497, 20, 1334, 1335, 1009, 2235, 25, 30, 31, 21, 2788,
2315, 302, 2317, 3643, 2023, 2242, 2867, 3670, 1801, 984, 985, 2401, 1922, 2027,
2563, 2870, 3543, 508, 2148, 1426, 1602, 1707, 2030, 3461, 307, 442, 2407, 76,
3714, 2735, 679, 716, 479, 2156, 2336, 592, 717, 2571, 2953, 814, 27, 3554,
1717, 1820, 2740, 680, 779, 780, 781, 815, 853, 1015, 1159, 1219, 1351, 1352,
1354, 1434, 1524, 1525, 1821, 1824, 1935]. **numbers**
[2490, 2491, 2576, 2577, 2881, 3124, 338, 3337, 3338, 1530, 413, 2254, 904, 255,
3902, 3870, 3905, 3881, 3914, 3970, 3956, 3977, 3953, 3839. **Process**
[2029, 3242, 1670, 518, 958, 3258, 1558]. **Process-Voltage-Temperature**
[3242]. **Processes**
[2738, 1521, 2415, 639, 598, 815, 851, 852, 1615, 204, 903, 3559, 2342, 3467,
Pseudorandomness

Pseudorandomness
[2904, 2187, 3285, 3515, 706, 2635, 2459, 3535, 2467, 2548, 2643, 2550, 2560, 2147, 3325, 2489, 1612, 2604, 2519, 2094, 2392, 3761, 3040, 2689, 2085].
pseudozufallsvektoren [1324]. Pseudozufallszahlenfolgen [607].
spezdosluchainykh [346].
PSI [1397]. PUB [1825]. Public
[2280, 890, 2464, 1937, 2498, 3207, 2400, 3737]. Public-Key [890, 2464, 2498].
Publications [259, 389]. Publicly [3068]. Published [3603]. PUF [3744].
PUFs [3782]. Pulse [3428, 1793, 661, 3429]. Pulse-Excited [3428].
Pure [3738]. Purpose [1056]. Purposes [2872].
Quadrature [893, 768, 715, 1014, 391, 2461]. Quality
[2096, 3418, 1790, 2644, 3669, 2033, 1065, 3136, 3146, 2899, 3722, 3167, 3278, 1872, 2531, 1901, 1905, 2131, 3102, 3215, 1924, 3460, 1931, 592, 2423, 2424, 2435, 2509, 2900, 2902].
Quantifiers [3183]. Quantis [3569]. Quantitative [3052, 722, 3967, 3648]. quantity [135].
Quantum-Mechanical [520]. Quantumlike [688]. quark [3900]. 'quasi
Quantis [3569]. Quantitative [3052, 722, 3967, 3648]. quantity [135].
Quasi-Monte [3957, 3963, 3910, 3948, 1834, 3299, 2384, 2041, 851, 1722, 2166, 1543, 3656, 2355, 2827, 456, 3968, 3934, 3318, 3890, 3917, 3938, 879, 1785, 2461, 2653, 2561, 2811, 485, 2792, 3103]. Quasi-Monte-Carlo [98].
quasi-white [2231]. quasicrystals [2638]. Quasigroup [3016].
Quasigroups [3434]. Quasirandom [2517, 1298, 2101, 3414, 1197, 2161, 2814, 1739, 3176, 2722, 1345, 1821, 1824, 1835, 2065, 561]. Quaternion
[3374]. QUATRIÈME [3794]. Quick [441]. Quest
[1321, 3395]. questions [84]. Queue [965, 1919, 1920, 997, 2707, 940, 3257].
Queueing [1375, 1216]. Queuing [1456, 605, 784]. Quick [1993]. Quickly
[1890]. Quicksort [2453]. Quinary [903]. Quincunx [3345]. Quintessential
[3345]. quintic [2997]. quotient [1214]. quotients [3524, 1217].
57

random


residues [569, 891, 13]. Resilient [3699]. Resistant [3513, 3288, 3409, 3298].
Resolution [3339, 844]. Resolution-stationary [3339]. resolving
[3446, 3470]. Resonances [3250]. Resort [3923]. Resource
Response [1592, 940, 1826, 958, 2707, 684]. Response-time [958].
restricted [3447, 3485]. restriction [2892]. Restrictions [3528, 3034].
result [372, 722]. Resulting [29]. Results
[1851, 2279, 1299, 103, 2217, 684, 2002, 2015, 376, 132, 3377, 2266, 2632].
retrieval [270]. Retrospective [500]. return [2618].
Reverse [2894]. Reviews [869, 531, 2281, 314]. Revised
[3944, 1142, 1042, 3950, 3952, 2982, 3008]. revision [3743]. Revisited
[3944, 1142, 1042, 3950, 3952, 2982, 3008]. revision [3743]. Revisited
[2910, 2502, 2095]. Revisiting [2272, 3674]. RFC [1877, 2846]. RFID
[3051, 3175, 3192, 3218, 3610, 3464, 3343, 3251, 3252]. Rhode [3825, 3964].
Right [3255, 3542]. Rigorous [3130, 3563]. Ring
[3507, 3466, 3226, 3383, 3697, 3306, 3758, 3222, 3375]. ring-oscillator-based
[3050, 2903, 3333]. risk-based [3333]. RNA [2899, 2900]. RnaPredict
[2899, 2900]. RNG [1650, 3730, 1131, 3099, 2799]. RNGAVXLIB [3702].
RNGs [3776, 2370, 3633, 3732, 3296, 2732, 2351, 2428, 2431].
RNGSSELIB [3400, 3585]. road [1681]. robots [2598]. Robust
[3165, 536, 2995, 3096, 3099, 3715, 1820, 2680, 3097, 1429, 2507].
Robustness [1307, 1668, 3114, 2163, 3383, 2253]. Rockefeller [3856]. rocket [253].
[1753]. Roots [773]. ROP [3784]. Rosenbluth [2854]. Rotation
[1807, 2069]. Round [2843, 2544, 2639, 2643, 2668, 2841].
[768]. RSA [1292, 2973, 3158]. RSA-Based [2973]. RSAEuro [2092].
rstream [2867]. Rudin [3762]. ruin [935, 3100]. rule [239, 2512]. Rules
[2913, 2309, 2936, 2650, 3707, 2725, 1014, 2741, 3029, 3139, 3241, 2476, 3319,
2477, 2561, 2955, 2957, 3030, 3138, 3478]. Rumor [3666]. Run
[1754, 1760, 1887, 2713]. running [3278]. Runs
[428, 494, 3076, 975, 3232, 559, 788, 2832, 465, 1909, 52, 2728, 2875, 58, 55].
Runs-Down [975]. Runs-Up [975]. Russian [2966, 346, 34]. Russians
[3705]. RV [1207].

S [3057, 314, 976, 1041, 437, 389, 3605, 2081, 3483]. S-3800 [2081].
SAFE [3755, 2060]. Salford [1892]. Salt [3891]. Salzburg [3910]. same
[365]. Sample [699, 1075, 3519, 620, 2923, 58, 783, 35]. Sampler [575, 1990].
siamplers [1760]. Samples
[1185, 1950, 1957, 8, 830, 64, 73, 17, 39, 134, 33, 230]. Sampling
[563, 655, 918, 1120, 1972, 3771, 3517, 833, 1247, 1465, 2111, 269, 744, 745,
1086, 1481, 705, 48, 840, 1200, 502, 3639, 24, 3443, 2019, 1332, 1409, 3704, 845,
1923, 2327, 847, 3649, 1, 645, 3764, 859, 860, 861, 611, 161, 1171, 100, 615,
963, 1291, 1369, 3622, 2084, 870, 12, 1566, 237, 149, 42, 2996, 577, 578, 2007,
2221, 116, 65, 73, 74, 2232, 94, 155, 3315, 25, 30, 31, 1338, 3450, 2479, 1704,
1100, 157, 281, 3678, 27, 2739, 2340, 552, 257, 187, 1277, 2507, 2755, 961, 121,
369, 9, 106, 208, 135, 2076, 3042, 69]. sampling [28]. Sampling-Vectorized
[3764]. San [3960]. San [3951, 3974, 3840, 3886, 3966, 3931, 3911, 3935].
Santa [3792, 3881, 3953]. SAR [3934]. Satisfied [407, 544]. Satisfying
[519, 453, 1316, 3235, 451, 13]. Saturday [3943]. Saturday-Wednesday
[3943]. Saunders [3106]. Savage [2480]. SC’11 [3978]. Scalable
[3184, 3219, 3749, 3636, 3591, 2796, 2484, 2485, 2281, 3104]. Scale
[2184, 3789, 769, 185, 10, 2983, 14, 1673, 95, 3759, 1429, 2156, 1055].
Scale-sensitive [2184]. Scaling [2258, 3253]. Scan [3458]. Scan-based
[3458]. Scatter [3196, 2079, 2361]. scattered [372]. Scattering [3412, 11].
Schedules [654]. scheduling [1800, 3333]. schemata [2606].
schemata-based [2606]. Scheme [3283, 1942, 2977, 3325, 775, 1618, 3474].
Schemes [1778, 2489, 725, 1172, 3752, 1406, 2328, 157]. Schnorr [1536].
School [2772, 3811, 631]. School-Based [2772]. Schwinger [2276]. Sci
[1041]. Science
[3814, 3925, 3819, 3807, 3817, 3820, 3823, 3838, 3843, 3849, 3855, 3865, 3888,
397, 3901, 3922, 3926, 3972, 3978, 3979, 3829, 3821, 3876, 3805, 3949, 3954,
3940, 3809, 3844, 3845, 3827, 3920, 3908, 3939, 3808, 3563, 3867]. sciences
[3930]. Scientific
[3801, 2911, 1125, 3800, 1143, 1731, 2503, 3877, 3194, 2731, 3890, 3806].
Scientists [627, 274, 1203]. scores [429]. Scrambled [3230, 3719, 3135].
Scrambling [2628, 3722]. scramblings [2742, 3747]. screening [3245, 2600].
scroll [3172, 3201]. SEAC [89]. SEAL [2630]. Search
[3521, 972, 1397, 3641, 814, 910, 911, 2622, 3071, 2531, 929, 2933, 710, 1341,
1803, 1519, 2820, 2598, 3485, 3486]. Searches [2626, 2233, 1420]. Searching
[2864, 2823]. Seattle [3846, 3978]. secant [1764]. Second
[3789, 3833, 30, 3927, 3023, 863, 3902, 3851, 3919, 3246]. Second-level [3023].
second-order [3246]. Secondary [2899]. Secret [2842, 1280, 2439]. Secure
[3398, 2696, 3279, 1459, 3514, 2121, 2547, 2648, 3095, 3672, 3115, 2747, 3358,
3033, 1115, 1170, 2693, 3665, 3444, 1406, 2311, 1339, 3130, 3343, 3128, 2964,
2349, 1280, 3571, 2692, 3755, 1856]. Securely [3715]. sécuritaire [1856].
Security [3913, 3401, 3698, 2379, 1877, 2846, 3192, 3527, 2710, 2780, 2643,
3945, 2572, 2738, 2580, 3332, 3681, 3612, 1536, 3136, 2973, 2821, 3891, 3911,
3748, 3980, 2095, 2987, 3853, 3456, 1425, 775, 3227, 3233, 3239, 2889]. Seed
[3724, 2375, 3255, 1124, 2465, 1734, 3373, 3441]. Seeding
[1320, 2335, 3576, 979, 3344]. Seeds [2731, 3741, 1209, 3240]. seeming [2583].
Segmentation [1751, 2946]. Select [2525]. Selected
Self-adaptive [3473], self-assembly [3729], Self-Avoiding [3596, 2539, 1782], Self-Excited [3064], Self-Similarity [3949], self-test [1404, 1492, 2334], self-testing [3566], selfish [338], Sensitive [2184], Sensitivity [2287], Sensor [2922, 3332, 3672], sensors [3482], Seoul [3944], September [3789, 3810, 3962, 3887, 3956, 3864, 3833, 3915, 3800, 3874, 3954, 3898, 3892, 3903, 3804].

Sequence [1460, 1298, 3515, 1573, 1674, 1197, 403, 434, 1496, 2648, 379, 381, 3762, 3024, 1058, 651, 3153, 2367, 885, 1027, 3056, 879, 1659, 1660, 1243, 3066, 36, 462, 540, 572, 3076, 1038, 1199, 2298, 3195, 3200, 3201, 319, 1402, 2932, 844, 3599, 3444, 301, 2722, 1009, 3095, 3213, 981, 352, 1339, 3218, 2478, 632, 713, 714, 2148, 1706, 1348, 2334, 444, 445, 986, 2042, 3612, 3740, 1017, 3346, 1165, 3028, 1735, 1021, 1739, 3243, 49, 2436, 3493, 13, 1228, 3627, 2269].


sequences [785, 1835, 2065, 2068, 1961, 2070, 2176, 2178, 2265, 3249, 1548, 3150, 483, 2510, 561, 1554, 1447, 789, 1637, 1846, 3498, 40, 791, 3853, 3956, 3944, 679, 716].


Simulation-Based [2398]. Simulations

tests
[2760, 1966, 1967, 2075, 2145, 2031, 976]. TESTU01
[2951, 2559, 2655, 3011, 2944, 3012]. Texas [3819, 3911, 3824]. Texture
[792, 932]. Textured [1751]. theatres [1223]. thefts [3589]. Their
[502, 2648, 2473, 2566, 2415, 1026, 3, 3524, 1878, 1586, 3734, 3956, 3944, 2230,
3209, 439, 440, 1613, 2492, 3028, 365, 147, 3481, 2692]. Theme [3845].

Theorem [1378, 2647, 105, 3501, 235, 1039, 3438, 3312, 32, 3461, 3674, 410,
2737, 3122, 641, 1163, 2352, 2682, 1240, 2535, 2952, 2819]. theorem-based
[3438]. Theorems [1973, 3283, 2103, 71, 350, 3603, 3462, 590, 2165, 2675,
683, 566, 1477, 63, 642, 188, 3492]. theoretic [2249]. Theoretical
[757, 3829, 945, 2975, 1749, 3377, 2142, 2254, 647]. Theme [243, 4, 3804].

Time [3405, 663, 2200, 1574, 2219, 2711, 3311, 712, 1698, 1923,
2167, 1646, 1647, 566, 2697, 3053, 2618, 2707, 1889, 754, 1422, 940, 3459, 3675,
986, 2040, 3226, 3127, 1105, 958, 3484, 1961, 2070, 2176, 2177, 1746, 3490,
3261, 19, 1558, 3384, 3721, 1587]. time-dependent [3459, 3721].
time-space [1646]. time-tested [3675]. Times [2481, 918, 1587, 1946, 869].

Tight [1889]. Tile [3729, 2638]. tilings [1007]. Tillich [3129]. Tilted
[3443, 3185]. Time [3405, 663, 2200, 1574, 2219, 2711, 3311, 712, 1698, 1923,
2167, 1646, 1647, 566, 2697, 3053, 2618, 2707, 1889, 754, 1422, 940, 3459, 3675,
986, 2040, 3226, 3127, 1105, 958, 3484, 1961, 2070, 2176, 2177, 1746, 3490,
3261, 19, 1558, 3384, 3721, 1587]. time-dependent [3459, 3721].
time-space [1646]. time-tested [3675]. Times [2481, 918, 1587, 1946, 869].

Threshold [2527, 3609, 3105, 3328]. throughput [3172, 3496]. Tied [2700].

Too [2527, 3609, 3105, 3328]. throughput [3172, 3496]. Tied [2700].

Too [2527, 3609, 3105, 3328]. throughput [3172, 3496]. Tied [2700].

Too [2527, 3609, 3105, 3328]. throughput [3172, 3496]. Tied [2700].

Too [2527, 3609, 3105, 3328]. throughput [3172, 3496]. Tied [2700].


V [2103, 488, 2486, 601, 3798]. v. [239]. VA [3879, 3877, 3928, 2057].
Vacuum [3302, 3359]. Valentin [2103]. valeurs [2145]. Validating [2727].
Validation [1693, 3170, 3171, 3200, 3149]. Valuable [2549, 3622]. Value [564, 395, 3059, 195, 3271, 2039, 1941, 3373].
Values [393, 291, 735, 736, 737, 2522, 3403, 567, 1458, 2279, 2371, 1378, 3283, 314, 1859, 741, 800, 3417, 3517, 3519, 238, 924, 1573, 1248, 2109, 2380, 3077, 2919, 1082, 1083, 1084, 2921, 294, 3430, 2537, 495, 2633, 841, 2222, 668, 436, 625, 545, 669, 3667, 581, 1898, 1902, 582, 2645, 2785, 505, 1048, 1798, 758, 806, 1504, 1419, 1505, 3644, 1506, 1095, 1049, 897, 2569, 2727, 2327, 304, 96, 251, 277, 278, 279, 330, 332, 354, 512, 770, 943, 1428, 1604, 2329, 2482, 2800, 590, 384, 549, 3465, 1268, 1349].


Zufallsvektoren \[1202\]. Zufallszahlen \[978, 1847, 868, 174, 1028, 430, 463, 2390, 624, 326\]. Zufallszahlengeneratoren \[1713\]. zur \[1026, 616, 1202, 1324, 1713, 275, 978, 650\].

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


Karl Pearson. On a new method of determining “goodness of fit”. *Biometrika*, 26(4):425–442, December 1934. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL http://www.jstor.org/stable/2331988. According to [369, page 36], this paper introduced the $P_n(\lambda)$ test for “determining whether a sample of size $n$, supposed to have been drawn at random from a parent population having a known probability integral has probably been drawn at random.” See [27] for its first use on random numbers from a uniform distribution.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Anonymous:1954:RDb


Anonymous:1954:RDc


Anonymous:1954:RDd


Bartholomew:1954:NUS


Hammersley:1954:PMM


Lehmer:1954:DRN


Meyer:1954:GTR


Moshman:1954:GPR

REFERENCES


REFERENCES


[162] Alan Stuart. The efficiencies of tests of randomness, distribution-free methods vs. normal alternatives. Journal of the American Statistical...
REFERENCES


REFERENCES


REFERENCES


Bolshev:1959:TRV


Cashwell:1959:PMM


Cook:1959:RRP


Ehrlich:1959:MCS

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

Golenko:1959:DCS


Golenko:1959:FRN


Green:1959:ETA

REFERENCES


REFERENCES


Halton:1960:ECQ


Hammersley:1960:MCM


Hunter:1960:NTR


Kleinrock:1960:PTS


Marsaglia:1960:GED


Pakov:1960:GRC


Postnikov:1960:AMR


[230] Donald D. Wall. A random number test for large samples. In Anonymous [3795], pages 7–11. LCCN ????


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

January 1963. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Hoeffding:1963:PIS


Jagerman:1963:AFS


Kolmogorov:1963:TRN


Laughlin:1963:RAR


MacLaren:1963:FPG


Magleby:1963:SNF


Marsaglia:1963:GDR


Marsaglia:1963:RNF

REFERENCES


REFERENCES


[323] David L. Jagerman. The autocorrelation and joint distribution functions of the sequences \( \left\{ \frac{a}{m}j^2 \right\} \), \( \left\{ \frac{a}{m}(j+\tau)^2 \right\} \). *Mathematics of Computation*, 18
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Mckinney:1966:CNG


Miller:1966:BRB


Murthy:1966:NER


Pike:1966:RAG


RAND:1966:MRD


Shreider:1966:MCM


Spitzer:1966:RPP

REFERENCES


129

REFERENCES


REFERENCES


[409] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3800], pages 64–68. LCCN QA76.5 D55 1965.

REFERENCES


REFERENCES


REFERENCES


[430] Ulrich Dieter. Autokorrelation multiplikativ erzeugter Pseudo-Zufallszahlen (German) [Autocorrelation generated multiplicative pseudo-random
REFERENCES

numbers]. Operations Research-Verfahren, 6(??):69–85, ????. 1968. CODEN ORVEAI. ISSN 0078-5318.


REFERENCES


Meijer:1968:DASa


Meijer:1968:DASb


Millenson:1968:HRN


Miller:1968:ACP


Muller:1968:RN


Pillai:1968:NEI

REFERENCES


REFERENCES


[460] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3801], pages 70–111. LCCN QA1 S565 v. 3.


REFERENCES

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

[464] T. Donnelly. Some techniques for using pseudorandom numbers in com-
1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (elec-
tronic).

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

[466] Bryna M. Fellen. Letter to the Editor: an implementation of the Taus-
CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See
[454].

[467] I. J. Good. How random are random numbers? The American Statis-
tician, 23(4):42–45, October 1969. CODEN ASTAAJ. ISSN 0003-1305
2681742.

[468] L. R. Grosenbaugh. More on Fortran random number generators. Com-
CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES


REFERENCES


REFERENCES


Butler:1970:AAG


Cenacchi:1970:PRN


Dixon:1970:NSE


Downham:1970:SAA


Fuchs:1970:EDR


Good:1970:RPM


Gustavson:1970:FRN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[555] 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


REFERENCES


REFERENCES


REFERENCES


Niederreiter:1972:MED


Norman:1972:CPG


Overstreet:1972:FVP


Phillips:1972:PGG


Proll:1972:RAA


Ramberg:1972:AMG

160


Sowey:1972:CCB


Sullins:1972:CAP


Vincent:1972:CPA


Ahrens:1973:EFM


Ahrens:1973:NME


Burford:1973:BAC


Diaconis:1973:LMI

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


[625] Shanti S. Gupta, Klaus Nagel, and S. Panchapakesan. On the order statistics from equally correlated normal random variables. Biometrika,
REFERENCES


Hader:1973:IMR

Hamming:1973:NMS

Holland:1973:GAO

Knop:1973:AAR

Kozlov:1973:EEM

Learmonth:1973:NPS
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[679] 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


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

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

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[739] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3809], pages 321–355. ISBN 0-12-697540-X. LCCN QA76.6 .S9195 1976. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.7959. The complexity of the binary Euclidean algorithm for the greatest common denominator is shown to be $O(0.705 \log N)$ for large $N = \max(|u|,|v|)$. See [2448] for an update, and a repair to an incorrect conjecture in this paper. See also [2372], where the worst case complexity is shown to be $O(\log N)$, and the number of right shifts at most $2 \log(N)$.


---

**Atkinson:1976:SAG**

**Bays:1976:IPR**

**Blood:1976:CPR**

**Brent:1976:ABE**

**Chamayou:1976:DAG**

**Chambers:1976:MSS**
REFERENCES


REFERENCES

Golder:1976:BMM

Golder:1976:SAA

Golder:1976:SAR

Greenwood:1976:DTC

Greenwood:1976:FMI

Greenwood:1976:MTG
J. Arthur Greenwood. Moments of the time to generate random variables by rejection. *Annals of the Institute of Statistical Mathematics (Tokyo)*,
REFERENCES


[761] Donald E. Knuth and Andrew C. Yao. The complexity of nonuniform random number generation. In Traub [3809], pages 357–428. ISBN 0-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[804] Rudy A. Gideon and John Gurland. Some alternative expansions for the distribution function of a noncentral chi-square random variable. SIAM
REFERENCES


Mitchell:1977:TLM


Mueller:1977:RNG


Musyck:1977:SPG


Niederreiter:1977:PRN


Payne:1977:NRN


Peskun:1977:IAR


Pettitt:1977:KSG

REFERENCES


REFERENCES


REFERENCES


REFERENCES


1979. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (electronic).

Niederreiter:1978:QMC

Niederreiter:1978:STLa

Niederreiter:1978:STLb

Padgett:1978:CCI

Romankevich:1978:MCN

Sakasegawa:1978:GNP

Schmeiser:1978:GVD
Management, Southern Methodist University, Dallas, TX 75275, USA, 1978. ?? pp.


REFERENCES


REFERENCES


REFERENCES

Carnegie-Mellon University, Pittsburgh, PA, USA, March 1979. Published in [922].


REFERENCES


REFERENCES

Monahan:1979:ENM

Moore:1979:RNG

Nadas:1979:PP

Niki:1979:CMF

Niki:1979:MFN

Pangratz:1979:PRN
REFERENCES


REFERENCES


REFERENCES


Atkinson:1980:TPR


Basu:1980:RAEa


Basu:1980:RAEb


Bentley:1980:GSL


Brown:1980:GFG


Davies:1980:SAA


Dempster:1980:CEA

REFERENCES


REFERENCES


Lam:1980:RTD


Lane:1980:RAE


Lindley:1980:RAE


Marsaglia:1980:GRV


O'Brien:1980:PIR


Peskun:1980:TTC


Petkovic:1980:RRV


REFERENCES


REFERENCES


REFERENCES


Rubinstein:1981:RNG


Schatte:1981:RVL


Schmeiser:1981:PRV

[991] B. W. Schmeiser and V. Kachitvichyanukul. Poisson random variate generation. Research Memorandum 81-4, School of Industrial Engineering, Purdue University, West Lafayette, IN, USA, 1981.

Tadikamalla:1981:CGG


Tadikamalla:1981:FDO


Ahrens:1982:CGP


Ahrens:1982:GGV

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

DEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). See [426].


References


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


See [823, 927, 924, 1083].

Fishman:1984:EAM


Fishman:1984:SDD


Frederickson:1984:PRT


Frieze:1984:LCG


Gal:1984:OEC


Guinier:1984:RNS

REFERENCES


References


REFERENCES


REFERENCES


Bounas:1985:DDS


Burks:1985:CEM


Clark:1985:PNG


Dowdy:1985:AUM


Dudewicz:1985:RNG


Dudewicz:1985:TMD


Dyadkin:1985:AMN

REFERENCES 237


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1194] George S. Fishman and Louis R. Moore III. An exhaustive analysis of multiplicative congruential random number generators with modulus


Goldreich:1986:HCR

Grothe:1986:MEG

Hamming:1986:NMS

Hosack:1986:UCM

Hultquist:1986:LST

Inoue:1986:MAR
REFERENCES


REFERENCES


Marsaglia:1986:IFC


Nicola:1986:QAF


Niederreiter:1986:DFS


Niederreiter:1986:LDP


Niederreiter:1986:MNI


Niederreiter:1986:PVG

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Chin:1987:TLP

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

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1348] 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.


REFERENCES


Ahrens:1989:AMS


Ahrens:1989:HAL


Ahrens:1989:NUR


Aiello:1989:HIG


Allender:1989:SCE


Babai:1989:MPL

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

punumber=5823. IEEE order number 89CH2778-9.

5823. IEEE order number 89CH2778-9.

[1424] David J. Lilja. Efficient generation of Poisson distributed random vari-
ables. Technical Report CSRD 900, University of Illinois at Urbana-
Champaign, Center for Supercomputing Research and Development, Urb-
ana, IL 61801, USA, July 31, 1989. 15 pp.

of Cryptology: the journal of the International Association for Crypt-
ologic Research, 1(3):151–158, ???. 1989. CODEN JOCREQ. ISSN
0933-2790 (print), 1432-1378 (electronic).

[1426] N. M. Maclaren. The generation of multiple independent sequences of
DEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL

(print), 1095-7200 (electronic).


robust $M$-estimates of scale for positive random variables. Journal of the
References


McIntosh:1989:RAE


Meer:1989:SIP


Meier:1989:FCA


Mertsch:1989:PAS


Niederreiter:1989:STC


Paul:1989:IRN


Percus:1989:RNG

[1436] Ora E. Percus and Malvin H. Kalos. Random number generators for MIMD parallel processors. Journal of Parallel and Distributed Com-
REFERENCES

Pickover:1989:PRG


Reber:1989:PNG


Rhee:1989:OPIa


Richards:1989:GRP


Sezgin:1989:EPC


Tezuka:1989:ALC


REFERENCES


[1456] François Baccelli and Zhen Liu. On the execution of parallel programs on multiprocessor systems — a queuing theory approach. Journal of the
REFERENCES


Bays:1990:CIR


Behboodian:1990:EUD


Bernstein:1990:SRN


Beth:1990:CPR


Bhavsar:1990:EDL

REFERENCES


Bralic:1990:AGR


Burford:1990:RNG


Carta:1990:TFI


Dagpunar:1990:SMD


Deak:1990:RNG


Deak:1990:URN


REFERENCES


REFERENCES


REFERENCES

Kemp:1990:NAG


Kemp:1990:PRA


Kinderman:1990:CCG


Korolev:1990:ADR


Koutras:1990:TCN


Krawczyk:1990:HPC

REFERENCES


REFERENCES

Marsaglia:1990:TUR

Maurer:1990:PLR

Micali:1990:EPR

Mitchell:1990:EEA

Mitchell:1990:NKG

Naor:1990:BCU


Norton:1990:AAE


Oommen:1990:GRP


Oyanagi:1990:SPR

Yoshio Oyanagi, Eiichi Goto, and N. Yoshida. Supercomputing pseudo random numbers: proposals on hardware and software. Technical report 90-012, University of Tokyo, Faculty of Science, Dept. of Information Science, Tokyo, Japan, April 1990. 6 pp.

Palmore:1990:CAC


Parrish:1990:GRD


REFERENCES


REFERENCES


REFERENCES


304

Deng:1991:RDR

[1572] L. Y. Deng and C. Rousseau. Recent development in random number
????

Devroye:1991:AGD

[1573] Luc Devroye. Algorithms for generating discrete random variables with
a given generating function or a given moment sequence. SIAM Journal
CODEN SIJCD4. ISSN 0196-5204.

Devroye:1991:ETA

[1574] Luc Devroye. Expected time analysis of a simple recursive Poisson ran-
don variate generator. Computing: Archiv für Informatik und Numerik,
1436-5057 (electronic).

Dohmann:1991:RNG

& Data Analysis, 12(1):129–132, August 1991. CODEN CSDADW. ISSN
sciencedirect.com/science/article/pii/016794739190108E.

Dunweg:1991:BDS

[1576] Burkhard Düngweg and Wolfgang Paul. Brownian dynamics sim-
ulations without Gaussian random numbers. International Journal
of Modern Physics C [Physics and Computers], 2(3):817–827,
September 1991. CODEN IJMPEO. ISSN 0129-1831 (print), 1793-
6586 (electronic). URL http://www.worldscinet.com/ijmpc/02/
0203/S0129183191001037.html.

Eichenauer-Herrmann:1991:ASI

congruential pseudorandom number sequences. Technical Report 1384,
Technische Hochschule Darmstadt, FB Mathematik, Darmstadt, Ger-


REFERENCES

Kao:1991:CRN


Kemp:1991:PRV


Koen:1991:ACB


Komo:1991:DPR


Lai:1991:PNB


Law:1991:SMA


[1998, 1839] 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


Micalli:1991:EPP

[1610] Silvio Micalli and Claus-Peter Schnorr. Efficient, perfect polynomial random number generators. *Journal of Cryptology: the journal of the Inter-
REFERENCES


Mulmuley:1991:FPP


Naor:1991:BCU


Niederreiter:1991:FFT


Niederreiter:1991:RTR


Oyanagi:1991:SPR


Papoulis:1991:PRV


Pardalos:1991:CTP

REFERENCES


[1622] Terry Ritter. The efficient generation of cryptographic confusion sequences. *Cryptologia*, 15(2):81–139, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://fizz.sys.uea.ac.uk/~rs/ritter.html; http://www.ciphersbyritter.com/ARTS/CRNG2ART.HTM; http://www.informaworld.com/smpp/content~content=a741902748"db=all"order=page. cryptographic confusion sequences; pseudo-random sequence; random number generators; cryptographic applications; random sequences; incompleteness theorem; deterministic implementation; external analysis; RNG comparison; chaos; Čebyšev mixing; cellular automata; linear congruential; linear feedback shift register; nonlinear shift register; generalized feedback shift register; additive types; isolator mechanisms; one-way functions; combined sequences; random permutations; primitive mod 2 polynomials; empirical state-trajectory approach; RNG design analysis; GFSR.


REFERENCES


Tyurin:1991:TRN


Ugrin-Sparac:1991:SIP


Vose:1991:LAG


Wakefield:1991:EGR


Walsh:1991:MFR


Wheeler:1991:PMN

REFERENCES

Wheeler:1991:SIC


Yamamoto:1991:NEM


Yang:1991:UCR


Zeng:1991:PBG


Agrawal:1992:PAS


Aluru:1992:RNG

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Collins:1992:RNG


Dai:1992:BSD


DalleMolle:1992:HOC


DeMatteis:1992:CCD


DeMatteis:1992:CDP


REFERENCES


REFERENCES


[1700] J. Lehn. Pseudorandom number generators. In Gritzmann et al. [3864],

*ACM Transactions on Mathematical Software*, 18(4):454–455, December

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

[1703] Sheelagh Lloyd. Counting binary functions with certain cryptographic
properties. *Journal of Cryptology: the journal of the International As-
JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).


[1705] G. Louchard, B. Randrianarimanana, and R. Schott. Dynamic algo-
ISSN 0304-3975 (print), 1879-2294 (electronic).

[1706] N. M. Maclaren. A limit on the usable length of a pseudorandom
REFERENCES

Makino:1992:GSR


Marsaglia:1992:MRN


Mason:1992:ACA


Matsumoto:1992:TGG


Maurer:1992:UST


Meier:1992:CPC


Mertsch:1992:MBB

[1713] Michael Mertsch. *Methoden zur Bestimmung und Begrenzung des Einflusses algorithmischer Zufallszahlengeneratoren auf simulative Untersuchungen*. (German) [Methods for determining and limiting the influence of algorithmic random number generators on experimental investigations], volume 199 of *Fortschritt-Berichte VDI: Reihe 10*. VDI-Verlag,
REFERENCES


[Fisher:1993:OOR]


[Flahive:1993:ICG]


[Galway:1993:ESCb]


[Ganzha:1993:PSM]


[Gokhale:1993:DBC]


[Goldreich:1993:EPG]

Grassberger:1993:CGR


Grassberger:1993:MCS


Hamilton:1993:PNGa


Hamilton:1993:PNGb


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

[1793] Christoph Kalkuhl. Pulse/data channel extends programmable pulse generator applications. *Hewlett-Packard Journal: technical information*
REFERENCES


REFERENCES


REFERENCES


[1826] 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 [1357, 1464, 1812, 1836]. 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


REFERENCES


Annan:1994:RAA


Anonymous:1994:IPR


Bailey:1994:PGR


Barcucci:1994:RGD


Boucher:1994:GPA


Bratley:1994:APG

REFERENCES


REFERENCES


REFERENCES

function; component series; cryptanalysis; multiloop system; computationally secure; personal computers; Spectra Publishing; Power Basic; BASIC.

Couture:1994:LSC


Cuccaro:1994:TTQ


Davis:1994:CRA


DeArmon:1994:RLO


Deng:1994:DIR


Devroye:1994:NHS

November 11, 1994. CODEN IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).


REFERENCES

Eichenauer-Herrmann:1994:GIC


Eichenauer-Herrmann:1994:ILB


Eichenauer-Herrmann:1994:SIN


Endl:1994:CRG


Entacher:1994:CNP


Gaines:1994:RGS


REFERENCES


Hennecke:1994:RER


Hildebrand:1994:RWS


Hill:1994:CMR


Holian:1994:PNG


Hoogland:1994:GPR


Hormann:1994:NQR

REFERENCES

355

Hormann:1994:TRM

Hormann:1994:UGD

Huber:1994:PLG

James:1994:RFI

Jimbo:1994:RBB

Jimbo:1994:RBD

Johnson:1994:CUD


[1912] 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 \((x_{\text{new}} = (A \times + C) \mod P)\) 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


Dwyer:1995:QPR


Edgington:1995:RT


Eichenauer-Herrmann:1995:DBN


Eichenauer-Herrmann:1995:IUB


Eichenauer-Herrmann:1995:NPE


Eichenauer-Herrmann:1995:PNG


Eichenauer-Herrmann:1995:QCP


REFERENCES


REFERENCES


REFERENCES

Schmid:1995:EMC


Sezgin:1995:SRN


Sherif:1995:UWF


Sobol:1995:IQS


Sorenson:1995:ALE


Storn:1995:CO


Struckmeier:1995:FGL

REFERENCES


Sugita:1995:PRN


Takashima:1995:STT


Tezuka:1995:URN


Varhol:1995:ANS


Vattulainen:1995:CSS


Vattulainen:1995:MIF


REFERENCES


REFERENCES


Boppana:1996:BCP


Bromley:1996:QNG


Brunner:1996:PCO


Bryc:1996:BRB


Burthe:1996:FIS


Chandwani:1996:FAP


REFERENCES


REFERENCES


See [2137] for a treatment of the discrepancy of the inversive congruential generator, [2235] for an analysis of lattice structure of inverse congruential generators.

Kato:1996:STN


Kemp:1996:CFP


Koc:1996:ACM


LEcuyer:1996:CMR


LEcuyer:1996:CSA

REFERENCES


[2148] Ping Luo. The two-dimensional structure of the sequence of random numbers generated by multiplicative congruential generators. Journal
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Devroye:1997:RVG


Dyadkin:1997:FEL


Dyadkin:1997:SBM


Eichenauer-Herrmann:1997:ADH


Eichenauer-Herrmann:1997:AEP


Entacher:1997:CSP

Entacher:1997:PPL

Entacher:1997:PPP

Fishman:1997:MCC

Foster:1997:DOT

Gell-Mann:1997:ETZ

Gilks:1997:CAR


[2226] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [3902], page ?? ISBN 3-901608-11-7. LCCN ????


[226] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of mathematics and its applications*. Cambridge Univer-
REFERENCES


[2247] 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.”.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Emmerich:1998:SIP


Entacher:1998:BSW


Entacher:1998:LIP


Entacher:1998:LCG


Evans:1998:RVG


Fuster-Sabater:1998:LPS

REFERENCES


REFERENCES


REFERENCES


REFERENCES

423


LEcuyer:1998:URNa


LEcuyer:1998:URNb


Lu:1998:IPG


Lurie:1998:AMS


Malov:1998:RVG


Marsaglia:1998:MPMa


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Wegenkittl:1998:THS


Wheeler:1998:CX


Williams:1998:ELP


Williamson:1998:CNR


Wolf:1998:RWP


Woodcock:1998:ACR


REFERENCES


Durrant:1999:RND


Eichelsbacher:1999:CPA


Entacher:1999:CSR


Entacher:1999:PRN


Entacher:1999:PSL


Entacher:1999:QMC


REFERENCES


[2397] Benjamin Jun and Paul Kocher. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Re-
REFERENCES


McCullough:1999:ARS


McCullough:1999:ASP


McCullough:1999:NRE


MRaihi:1999:CAR


Muller:1999:CRV


Naor:1999:STA

REFERENCES


REFERENCES

Soto:1999:RTA


Soto:1999:STRa


Soto:1999:STRb


Soto:1999:STRc


Stauffer:1999:IMT


Sudan:1999:PGX

REFERENCES


REFERENCES


[2442] 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


REFERENCES


Goldreich:2000:ITP


Gutierrez:2000:MDI


Hickernell:2000:ELS


Hormann:2000:AAG


Hormann:2000:ARV

IEEE:2000:IPH


Impagliazzo:2000:EPR


Indyk:2000:SDP


Iwata:2000:PAF


Jennewein:2000:FCQ


Juels:2000:HTL


REFERENCES

448


[2481] 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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Coffman:2001:TPS


Crandall:2001:PNC


Cryan:2001:PGN


Entacher:2001:ORN


Entacher:2001:EOR


Entacher:2001:PQ

REFERENCES


REFERENCES


[2539] 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 ranlux() generator. It is a linear congruential generator with multiplier $A = 31 167 285 = 0x1db_9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.


REFERENCES


Lemieux:2001:SCL


Lenczewski:2001:FRV


Levin:2001:SIC


Leydold:2001:SUG


Leydold:2001:UAA

REFERENCES

Li:2001:SPD


Liang:2001:NET


Liang:2001:TMU


Litvak:2001:SPE


Mascagni:2001:PIC


REFERENCES


REFERENCES


[2601] Renée Touzin. Des générateurs récursifs multiples combinés rapides avec des coefficients de la forme $\pm2^p_1 \pm 2^p_2$. (French) [Fast combined multiple recursive generators of the form $\pm2^p_1 \pm 2^p_2$]. 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 Maîtres sciences (M.Sc.) en informatique option recherche opérationnelle.


REFERENCES


REFERENCES


REFERENCES


[2625] Frank Emmerich. Average equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the
REFERENCES


REFERENCES

Fluhrer:2002:CSP


Friedel:2002:FGR


Futschik:2002:EFE


Gangnon:2002:MDE


Gennaro:2002:CPG


Gilbert:2002:NRP

Gleeson:2002:TRN


Golic:2002:SWM


Guimond:2002:PDP


Hernandez:2002:AGA


Hernandez:2002:GCT


Hertling:2002:SNN

Hormann:2002:FGO


Iwata:2002:RSS


Janke:2002:PRN


Jeruchim:2002:FRV


Jeruchim:2002:MCS

REFERENCES


REFERENCES


LEcuyer:2002:RAR


LEcuyer:2002:SST


LEcuyer:2002:TSL


Leydold:2002:ULU


Leydold:2002:VTD


Luo:2002:CGB

[2659] George Marsaglia. Re: *good* 64-bit random-number generator. Posting to the sci.crypt.random-numbers news group, September 3,
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2695] 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’ \texttt{/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 \texttt{drivers/char/random.c} in the Linux source tree.”.


[2700] 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 fiar uses a legal requirement in DRM systems; “The Missing Customer” redux; enthusiasm, drive, wisdom, patience not tied to age. \textit{Communications of the ACM}, 46(12):59–61, December 2003.

Deng:2003:SHD


Devroye:2003:NUR


Dichtl:2003:HPO


Dwyer:2003:PRN


Engel:2003:BLE


Epstein:2003:DIT

REFERENCES


REFERENCES


Myers:2003:EAS


Neal:2003:SS


Neuenschwander:2003:GRN


Niederreiter:2003:EGE


Owen:2003:VAS


Papadimitrioul:2003:FSS


PeytonJones:2003:RNa

REFERENCES


Soubusta:2003:ERQ


13th Polish-Czech-Slovak Conference on Wave and Quantum Aspects of Contemporary Optics.

Srinivasan:2003:TPR


Stipcevic:2003:NDR


Sugita:2003:DRW


Tang:2003:SDA


Tang:2003:SPM

Tsang:2003:TCT


Tsoi:2003:CFB


Tu:2003:GRI


Umans:2003:PRG


Vavriv:2003:RNG


Al-Subaihi:2004:SCM

496


REFERENCES


REFERENCES

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/an4492lnlaa5bf0g/.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Arnault:2005:DPN


Balakirsky:2005:GFA


Banks:2005:DES


Barak:2005:MAP


Beliakov:2005:CLR


Beliakov:2005:UNR

REFERENCES


[2841] Julio César Hernández Castro and Pedro Isasi Viñuela. New results on the genetic cryptanalysis of TEA and reduced-round versions of
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2896] Alev Topuzoglu and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hechenleitner:2006:PSG


Hong:2006:DRN


Indyk:2006:SDP


Joe:2006:CGR


Kossovsky:2006:TBU


Kuipers:2006:UDS


[2945] Dong-U Lee, John D. Villasenor, Wayne Luk, and Philip H. W. Leong. A hardware Gaussian noise generator using the Box–Muller method and


McCullough:2006:RT


Miller:2006:MCL


Mueller:2006:SMG


Nau:2006:RN


Nuyens:2006:FAC


Nuyens:2006:FCCa

REFERENCES


REFERENCES


REFERENCES


Atman:2007:ATA


Barker:2007:RRN


Bauke:2007:RNL


Becher:2007:TUA


Bhatnagar:2007:ANB


Brent:2007:SLP

REFERENCES


REFERENCES


Hasan:2007:FSU


Hormann:2007:ITD


Hormann:2007:SGD


Juneja:2007:AFS


Kang:2007:PFS


Kung:2007:RFB


REFERENCES


Matsumoto:2007:FSC


Meidl:2007:LCP


Mislove:2007:DRV


Morgenstern:2007:URR


Nadarajah:2007:LCL


Nekrutkin:2007:AAO

REFERENCES

Panditaratne:2007:TRN


Pareschi:2007:SLN


Pazo-Robles:2007:MPS


Perez:2007:RJI


Rusu:2007:PRN


Santhanam:2007:CLB

REFERENCES


[3033] B. Sunar, W. J. Martin, and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. IEEE
REFERENCES


REFERENCES


Alimohammad:2008:EAH


Alioto:2008:APE


Alvarez:2008:ETR


Attya:2008:ROC


Bader:2008:DFP


REFERENCES


REFERENCES


REFERENCES


Howes:2008:U


Inaltekin:2008:ANE


Jang:2008:CDH


Joe:2008:CSS


Jovanovic-Dolecek:2008:UMT


Kalos:2008:MCM


Kang:2008:HPP

REFERENCES


REFERENCES


Kiessler:2008:BRB


Killmann:2008:DPR


Kim:2008:TRG


Kolokotronis:2008:CPN


Langdon:2008:FHQ


LEcuyer:2008:CPS

[3103] Pierre L’Ecuyer. Comparison of point sets and sequences for Quasi-Monte Carlo and for random number generation. In Golomb et al. [3956], pages


REFERENCES


[3115] M. Matsumoto, S. Yasuda, R. Ohba, K. Ikegami, T. Tanamoto, and S. Fujita. 1200µ m² physical random-number generators based on SiN

McCullough:2008:ASP


McCullough:2008:MEW


Moler:2008:NCM


Murdoch:2008:VRV


Murphy:2008:CLW


REFERENCES


[3140] Manas Somaiya, Christopher Jermaine, and Sanjay Ranka. Learning correlations using the mixture-of-subsets model. ACM Transactions on
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3188] Leo Dorrendorf, Zvi Gutterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. ACM
REFERENCES


Dryver:2009:CSE


Edrees:2009:HOZ


Faure:2009:GHS


Feldhofer:2009:HIS


Fischer:2009:SRF

REFERENCES


Galassi:2009:GSL


Gao:2009:MPL


Gauvrit:2009:SRI


Gelenbe:2009:ASN


Gentle:2009:GRN


Guha:2009:EEC


Guinee:2009:EVH

REFERENCES


REFERENCES


REFERENCES


Kanter:2009:OUR


Katti:2009:EHI


Ladd:2009:FRN


Langdon:2009:FHQ


Laracy:2009:RVG

Lee:2009:ERA


Lee:2009:HHA


Lemieux:2009:PNG


Marchi:2009:PPR


Markenos:2009:FIA

REFERENCES

McCullough:2009:AES


Mitchum:2009:DPR


Mustafa:2009:DPR


Nakura:2009:ROB


Nandi:2009:ISA


Nekrutkin:2009:STS

REFERENCES


REFERENCES


Srinivasan:2009:BPV


Sun:2009:CPR


Svozil:2009:TCQ


Tafazzoli:2009:PCE


Tang:2009:FPS

REFERENCES


[3252] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number
References

Tzeng:2009:RNG


Uchida:2009:FPR


Umlauft:2009:GNS


vanMeel:2009:GFS


Verloop:2009:HTA

I. M. Verloop, U. Ayesta, and R. Núñez-Queija. Heavy-traffic analysis of the M/PH/1 discriminatory processor sharing queue with phase-
REFERENCES


REFERENCES

Wold:2009:OST


Xiao-chen:2009:URN


Yamanashi:2009:SRN


Youssef:2009:IEU


Yu:2009:ESC


Yuhua:2009:EDR


Zhu:2009:WFB


Abbott:2010:QRN


Agapie:2010:RPH


Akhshani:2010:PRN
REFERENCES


[3280] Arno Berger and Theodore P. Hill. Fundamental flaws in Feller’s classical
derivation of Benford’s Law. ArXiv e-prints, May 2010. CODEN ????.

[3281] K. (Kurt) Binder and Dieter W. Heermann. Monte Carlo simulation in
statistical physics: an introduction. Graduate texts in physics. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,

[3282] R. Blacher. A perfect random number generator. II. Rapport de recherche
LJK, Université de Grenoble, Grenoble, France, 2010. URL http://hal.archives-ouvertes.fr/hal-00443576/fr/.

[3283] A. A. Borovkov. Integro-local and local theorems on normal and large
deviations of the sums of nonidentically distributed random variables in
the triangular array scheme. Theory of Probability and its Applications,
54(4):571–587, ???? 2010. CODEN TPRBAU. ISSN 0040-585X (print),
1095-7219 (electronic).

[3284] Mark Braverman, Anup Rao, Ran Raz, and Amir Yehudayoff. Pseudo-
random generators for regular branching programs. In IEEE [3972], pages
year=2010&volume=00&catalog=4244&acronym=focs. IEEE Computer Society order number P4244.

[3285] Joshua Brody and Elad Verbin. The coin problem and pseudo-
randomness for branching programs. In IEEE [3972], pages 30–39.
year=2010&volume=00&catalog=4244&acronym=focs. IEEE Computer Society order number P4244.
REFERENCES


REFERENCES


Chi:2010:GPR


Derflinger:2010:RVG


DeRoover:2010:MPR


deSchryver:2010:NHE

REFERENCES


[3301] Ariel Gabizon. Deterministic Extraction from Weak Random Sources. Monographs in theoretical computer science. Springer-Verlag, Berlin,


Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei. Truly random number generation based on measurement of phase noise of a laser. *Physical Re-

Guyeux:2010:IRN


Haitner:2010:EIC


Hongo:2010:RNG


Hotoleanu:2010:RTT


Jaksic:2010:QCL

Jones:2010:IMD


Kang:2010:FIG


Kawai:2010:AOA


Kwon:2010:QRN


Lan:2010:RNG


LEcuyer:2010:CPR

REFERENCES


REFERENCES


[3341] P. J. Pashley and A. Amodeo. Generating random numbers. In Peterson et al. [3973], pages 184–189. ISBN 0-08-044894-1 (e-book), 0-08-044893-3 (set), 0-08-044895-X (vol. 1), 0-08-044896-8 (vol. 2), 0-08-044897-6 (vol. 3), 0-08-044898-4 (vol. 4), 0-08-044899-2 (vol. 5), 0-08-044900-X (vol. 6), 0-08-044901-8 (vol. 7), 0-08-044902-6 (vol. 8). LCCN LB15 .1569

Passerat-Palmbach:2010:RIG


Peris-Lopez:2010:CSP


Plesser:2010:RSI


Proschman:2010:BQQ


Qi:2010:DFR


Saiprasert:2010:MMM


Saiprasert:2010:OHA


Saito:2010:VMT


Segui:2010:AIP


Seznec:2010:PCM


Shen:2010:PQR

REFERENCES


REFERENCES

13(6):593–600, December 2010. CODEN ???? ISSN 0972-0529.


REFERENCES


REFERENCES


[3388] Alastair A. Abbott and Cristian S. Calude. Von Neumann normalisation and symptoms of randomness: An application to sequences of

Abbott:2011:QRN


Al-Abiachi:2011:CDN


Amaki:2011:JAO


Amaki:2011:OBT


Anonymous:2011:QRB

REFERENCES


[3396] 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.”.


Barash:2011:RPL


Baudet:2011:SOB


Bauke:2011:TRN


Becker:2011:BLC


Behnia:2011:NDM


Bellovin:2011:FMI


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3472] 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. [3978], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????.


Symul:2011:RTD


Tang:2011:ESG


Tang:2011:PES


Taylor:2011:DR


Veillette:2011:TCP


Versolatto:2011:MPR


REFERENCES


Becher:2012:TNN


Beisbart:2012:WMC


Berger:2012:CPR


Bergman:2012:GRV


Bertoni:2012:KSF


Boldyreva:2012:NPG


REFERENCES


Deng:2012:ECS


Deng:2012:LOM


deSchryver:2012:HER


Du:2012:LCP


Dunn:2012:PNG


REFERENCES

Horstmann:2012:JEC


Horvath:2012:ARM


Horvath:2012:EGP


Impagliazzo:2012:PS


Kaczynski:2012:BNR


Kaczynski:2012:NRV


Karakostas:2012:DAC

REFERENCES


[3544] 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/.


Miszczak:2012:GUT


Molina-Gil:2012:PGS


Nandapalan:2012:HPP


Nazzal:2012:UGA


Neves:2012:FSN


NIST:2012:RRN

NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Insti-
tute for Standards and Technology, Gaithersburg, MD, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.


REFERENCES


REFERENCES


[3584] 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


REFERENCES


Anawis:2014:ARR


Anonymous:2014:CEF


Anonymous:2014:RNG


Barabesi:2014:NUR


Barash:2014:PGA


Baron:2014:LSP

REFERENCES


[Bracher:2014:PRN]


[Braverman:2014:PGR]


[Chen:2014:EES]


[Cheng:2014:GBR]


[Devroye:2014:RVG]


[Dodis:2014:HEY]
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Carlet:2015:EBF


Guyeux:2015:ECS


Haeupler:2015:SFD


Hare:2015:MDR


Hill:2015:PRN


Jessa:2015:QRS


REFERENCES


Mandal:2016:FRI


McFarland:2016:MZA


Miller:2016:RPS


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA


Vigna:2016:EEM

REFERENCES

657


Yamakami:2016:PGA


Yu:2016:GPR


Aljahdali:2017:FIS


Anonymous:2017:DAD

[3723] 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 [3730] for details of the attack.

Artemenko:2017:PGO

REFERENCES


[3737] Arjen K. Lenstra and Benjamin Wesolowski. Trustworthy public randomness with sloth, unicorn, and trx. *International Journal of*
REFERENCES


ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://
cacm.acm.org/magazines/2017/1/211100/fulltext.


ISSN 1084-4309 (print), 1557-7309 (electronic).

ISSN 1862-2976 (print), 1862-2984 (electronic).


REFERENCES


Ermakov:2018:RRQ


Harase:2018:IBM


Lin:2018:FCB


Lin:2018:RNG


Liu:2018:SFS


Meral:2018:PAS


REFERENCES


Quaglia:2019:RCR


Ueno:2019:TBP


Xu:2019:NPF


Zhang:2019:REU


Basuyaux:20xx:RNG


LEcuyer:20xx:PNG

REFERENCES

[3787] 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


[3811] Peter C. C. Wang, editor. Information linkage between applied mathematics and industry: Proceedings of the First Annual Workshop on the
REFERENCES


REFERENCES


REFERENCES


Mehlhorn:1985:SAS


ACM:1986:PEA


Arkin:1986:SOP


DAgostino:1986:GFT


Heath:1986:HMP


REFERENCES


REFERENCES


ACM:1990:PTS


Balci:1990:WSC


Capocelli:1990:SCC


Goldwasser:1990:ACC


IEEE:1990:PAS

REFERENCES  


REFERENCES

ACM:1992:PTF


Burr:1992:UEN


Gritzmann:1992:ORE


IEEE:1992:ASF


Pflug:1992:SOP


Simmons:1992:CCS

REFERENCES


REFERENCES


Miola:1993:DIS


Mullen:1993:FFC


Ralston:1993:ECS


Sincovec:1993:PSS


Swartzlander:1993:PSC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Cohen:1996:FFA


IEEE:1996:ASF


Trobec:1996:PIW


Andradottir:1997:PWS


Gell-Mann:1997:QJA


REFERENCES


REFERENCES

NIST:2000:TAE


Gass:2001:EOR


IEEE:2001:ISF


Koc:2001:CHEa


Peters:2001:WPW

REFERENCES


Schueller:2001:MCS


Smelser:2001:IES


Spector:2001:GPG


ACM:2002:PTF


Dror:2002:MUE

REFERENCES


Fang:2002:MCQ


USENIX:2002:PBF


ACM:2004:PAA


Gentle:2004:HCS


Niederreiter:2004:MCQ


REFERENCES


REFERENCES


REFERENCES


[3960] Christos Alexopoulos, David Goldsman, and James R. Wilson, editors. Advancing the frontiers of simulation: a Festschrift in honor of George

[Belsley:2009:HCE]


[Clavier:2009:CHE]


[LEcuyer:2009:MCQ]


[Paredaens:2009:PTE]


[ACM:2010:PAI]

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3989] Nicholas J. Higham, Mark R. Dennis, Paul Glendinning, Paul A. Martin, Fadil Santosa, and Jared Tanner, editors. The Princeton Companion to