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

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

Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

29 September 2023
Version 1.383

Title word cross-reference

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

(0, 1) [1077]. (0, s) [2578, 2978]. \((a^n - 1)/(a - 1)\) [939]. \((j, c)\) [746]. \((n^2\alpha)\) [2529]. \((n^k\alpha)\) [2530]. \((na)\) [2529]. \((t, m, s)\) [2081, 2935, 2087, 2388]. \((t, s)\) [2674, 2081, 2379, 2935, 2087]. \((X, Y)\) [3694]. \((X^2 - Y^2)^{1/2}\) [499].
0.1(0 \times 1)0 \times 9 [141]. 1 [753, 896, 2888, 173, 306, 728, 3013, 3015]. 1, 2, 3 [3549]. 1.13198824 \ldots\ [2553]. 10, 000 [285]. $\textbf{10.00}$ [170]. $10^{2857}$ [2524]. $10^{4355}$ [2078]. $100\mu$ [3178]. 128 [3204]. 13 [273]. 16 [273]. 2
-adic good

\[ \beta > 1, \beta \approx 1509. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta = 32 [1341]. \]

\[ \beta = 28 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]

\[ \beta \approx 32 [1509]. \]

\[ \beta \approx 48 [1509]. \]
0.57pJ [3313]. 0.57pJ/bit [3313]. '05 [4146, 4150]. '07 [4156]. '08 [4161].


Approaches [2738]. Approximate
[898, 2026, 3978, 1627, 2367, 1977, 619, 702, 571, 948, 278, 422, 747, 1776, 2807].
Approximately [509, 1831]. Approximating [2496, 3978, 3526].
Approximation [2240, 2420, 2438, 1447, 1536, 2883, 2556, 1309, 711, 3600].
Approximations [145, 2841, 1073, 484, 1024, 3065, 1249, 3034, 3096].
April [4030, 4000, 4040, 4063, 4178, 4011, 4128, 4013, 4074, 4048, 4049].
Arbitrary [2236, 831, 1561, 3100, 986, 3866, 3896, 3046, 199, 1725, 3555, 3207, 1309, 711, 3600].
Archimedean [3345]. Architecture [2890, 2836, 3905, 3430, 2111, 3336, 3607, 3848, 1580].
Architectures [1479, 4163, 3808, 3702]. arcsine [3930]. Area [241, 1924, 3783, 3106, 2230].
Area-Efficient [3783, 3106]. areas [4157, 4125, 2775]. ARENA [4158].
Argument [684]. arguments [430]. Arisen [1]. Arising [1269, 1550, 3572, 3652].
Arithmetic [2319, 2411, 2148, 766, 3732, 2776, 736, 3775, 228, 369, 4082, 3579, 3, 1619, 1427, 1245, 1563, 2213, 1868, 1472, 1588].
arrangements [59]. Array [1405, 3355, 2615, 1391]. Arrays [1506, 937, 3567, 3332]. ARM7 [3133].
arbitrary [2236, 831, 1561, 3100, 986, 3866, 3896, 3046, 199, 1725, 3555, 3207, 1309, 711, 3600].
Assessment [1394, 2132, 2825, 2672, 1315, 1477, 2344]. Assignment [860, 866, 869, 881, 882, 883].
assumptions [1519]. Astronomical [1429]. Asymmetric [702, 3795].
Asymptotic [577, 102, 3572, 3652]. Asymptotically [2907]. Asymptotics [3064]. asymtotiques [801].
Attacking [3961]. Attacks [3351, 2354, 3092, 3919, 3791, 3954, 3832, 3535, 1460, 166].
Austria [4020, 4078, 4114, 4070, 4106]. Authentication [2015, 3852, 3883, 3322, 3323, 3287].
Autocorrelazioni [987]. Autokorrelation [471]. Autokorrelation [438].


Automata-based [1432]. automated [3847, 1861].

Automates [1580].

Automaton [2887, 3880]. automorphisms [3724].

Automatic [170, 1211, 2830, 2504, 2840, 2521, 786, 163, 2503, 3876, 3965, 137, 176, 3994, 2972, 3048].

Automatically [2411].

Automation [3272, 4185].

Automatically [2411].

Avalanche [3318].

Average [1796, 2153, 2247, 2248, 2671, 2979, 2718, 2154, 2831, 3617, 2441, 3553].

average-case [2154, 3617]. Averages [861].

Averaging [3729, 284]. avoid [1397, 1616].

Avoided [1191]. Avoiding [3675, 2584, 1817].

AVX [3798].

Award [3545]. Awarded [3885]. Aware [1668].

AWC [1907].

AWC/SWB [1907].

AWGN [2656, 3537].

B [399, 2137, 70]. Babington [70]. Babington-Smith [70]. Background [1783, 662].

backpropagation [2920]. backward [3067, 3033, 3440].

bacteriophage [3576].

Bad [2557, 2334, 2904, 4020, 3963, 2278, 2603, 3311, 3971, 3423].

BadRandom [3939]. bag [1728].

Bailey [3664, 3665].

balancing [1356].

ballistic [2327].

Baltimore [4055, 4146].

Banch [822, 686].

Banff [3997].

Baptist [4138].

Barbara [4085, 4159].

Base [1904, 784, 1020, 469, 2387, 3456].

Based [3476, 3584, 3587, 2411, 3893, 2825, 3975, 3953, 2416, 2749, 1698, 3053, 993, 2030, 2670, 635, 2755, 3503, 3959, 3374, 2498, 2680, 2906, 3980, 3729, 2994, 3279, 3157, 2917, 3682, 2438, 3802, 3171, 3686, 3396, 3765, 3005, 3178, 3772, 2088, 925, 3414, 3943, 3849, 3307, 1987, 930, 3309, 2638, 3088, 3202, 3031, 3318, 1778, 3211, 3322, 3323, 1047, 3331, 427, 3223, 3704, 3226, 3367, 3344, 3891, 3229, 3105, 3466, 3467, 102, 2887, 3108, 3921, 3790, 3922, 3582, 3791, 3113, 2892, 3665, 2821, 3116, 2748, 3488, 3238, 3239, 3559, 3362, 3976, 1696, 3494, 3133, 3055, 3722, 3504, 3723, 1064].

based [1224, 2583, 2682, 1065, 2433, 2834, 773, 3268, 1351, 3140, 3378, 3379, 3607, 3270, 1353, 3514, 3518, 3677, 2915, 1432, 3278, 3678, 1622, 3522, 1286, 1439, 3155, 3158, 3906, 3981, 1365, 2279, 2281, 2282, 2697, 2922, 3841, 2580, 2851, 3004, 3287, 3530, 3622, 1841, 3394, 3535, 3806, 3930, 2704, 3293, 3626, 3627, 2191, 2715, 793, 3771, 3297, 1245, 1380, 3407, 3408, 3695, 3984, 2867, 2688, 3017, 3304, 3637, 1651, 3191, 2384, 2539, 2458, 3420, 701, 2631, 2725, 3547, 99, 189, 3085, 1190, 2543, 3550, 3551, 3968, 3434, 1249, 3089, 3201, 1251, 2805, 2640, 2641, 3932, 3559, 3315, 3444, 1472].

based [3208, 3319, 1138, 1663, 2810, 3325, 3450, 3329, 3567, 51, 3785, 3888, 2652, 3334, 2886, 2741, 3988, 3575, 3459, 2958, 3341, 3705, 3043].

basiée [2867].

Bases [2974, 2687, 1143, 581, 1165, 1166, 1013].

Basic [1618, 1232, 921, 1025].

Basics [3372, 3326].

Battery [2069, 2189, 3983, 3971]. Baptin [170].

Bay
[295]. Columbia [4066, 4161]. column [3099]. Combination
[947, 2242, 1107, 1108, 1109, 3079, 2099, 427, 2410, 3268, 2281, 1654, 1248, 2885].
Combinations [398, 515, 484, 368, 1801, 1116, 2843, 447, 448, 62].
Combinatorial [634, 3671, 203, 2366, 1555, 2127, 238, 3510, 770].
Combinatorics [4057, 2762]. Combined
[3271, 3761, 2179, 2443, 2516, 2773, 2731, 1471, 1998, 3568, 3455, 1795, 1929, 1368, 1632, 2181, 2182, 2360, 2446, 2704, 1470, 1661, 2647].
Combiner [2394]. combiner [2394]. combinés [2647]. Combing
[903, 904, 1604, 3256, 2585, 3132, 3728]. Coming [3708]. Comment
[2820, 3117, 1150, 721, 786, 601, 1771]. Commitment [1553, 1645].
Commodore [1144]. Common [1208, 3902, 511, 1287, 1727, 3074, 1751, 1567, 808, 2171, 1119, 3633, 1856, 1085, 750, 3593, 2570, 2240, 1114, 1720, 911, 774, 729, 917, 1362, 2438, 1855, 2082, 940, 1476, 1672]. Commun
[2048, 2170]. Communicating [1310]. Communication
[584, 4154, 1310, 1327, 2491, 2832, 3520]. Communications
[505, 2694, 4150, 4079, 2741]. Comp [2137]. Compact
[2011, 2810, 3038, 3104, 1413, 2509, 3071, 600]. Companion [4198]. Comparative
[1337, 401, 502, 3258, 2112]. Comparing
[1223, 911, 1827, 2178, 3339]. Comparison [669, 578, 1054, 3244, 3837, 3680, 1727, 3164, 2079, 204, 2290, 610, 1081, 700, 2205, 2798, 1672, 1485, 1845, 1493, 591, 592, 1721, 2922, 2519, 3316, 2738, 462, 809]. Comparisons
[1855, 2082, 1476, 1397, 1751, 1856]. compatibility [3662]. Compatible
[1514, 1544, 3611]. Competing [186]. compiled [70]. Complement
[3675, 3922, 681, 4104, 3728, 3784]. Complexity
[2696, 3014, 3013, 3015]. Component-by-Component
[2696, 3014, 3013, 3015]. components [2773]. Component
1907, 1699, 1334, 585, 406, 1417, 2495, 1420, 1503, 1504, 1613, 1614, 1616, 1617, 1709, 1710, 1712, 1713. congruential
[1714, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1915, 1917, 1918, 1919, 1920, 1921, 2034, 2035, 2037, 2154, 2155, 2156, 2248, 2250, 2252, 2328, 2329, 2330, 1217, 1276, 1277, 1339, 1340, 2253, 2334, 2335, 2424, 856, 952, 1219, 1220, 1341, 1811, 765, 2907, 3057, 555, 2684, 1351, 2501, 3058, 3141, 3961, 2590, 775, 864, 3277, 356, 2174, 2175, 2275, 3156, 962, 1173, 1730, 2997, 826, 1367, 2181, 2445, 1174, 2284, 2926, 3393, 2187, 2704, 485, 521, 2371, 2615, 2858, 3076, 3931].


559, 692, 693, 1076, 87, 130, 162, 2628, 528, 1042, 79, 372, 2651, 668, 177, 100.

digraph [3229]. Dimension [3322, 3323, 1027]. Dimensional [270, 196, 201, 3150, 915, 3153, 1842, 1544, 205, 54, 1998, 3574, 714, 1792, 1795, 1331, 2668, 2750, 3371, 221, 222, 2187, 735, 2380, 3016, 188, 3025, 2298, 3030, 3745, 2552, 2121, 2309, 804, 3327]. Dimensionality [2975].


Discrepancies [1874, 2272, 2306, 2400]. Discrepancy [1027, 540].

Discrete [4083, 2009, 1095, 2129, 2564, 2889, 3347, 2240, 3113].

Discrete-Event [1095, 2129, 2564, 2889, 3347, 3327].


discriminatory [3328]. discs [935]. disjoint [1900]. disjunctions [1897].

Disk [1009, 2944]. Diskrepanz [738]. Diskret [3024]. Disney [4088].


distances [3474, 1699, 1700]. Distanz [738]. Distinct [1506, 954].


distribution

Distribution-Free

Distributione

Distributions

disturbance

Divergence

Divergent

Diversity

Diversity-Based

Diverted

Dividing

Divisible

Division

Divisor

divisors

do

Document

Documentation

Does

Doing

Domain

Domains

Domenico

Dominated

Donald

Don’t

Dopant

Dopant-Level

Dorothy

Dose

dot

dot-patterns

double

double-scroll

doubly

Down

Draft

DRAM

drastic

Draw

Drawbacks

Drawing

DRBG

Dress

Drive

Driven

Drives

DRM

DSS

Dual

dual-drive

dual-mode

Duality

Dudewicz

Due

DUHK

d’un

d’une

DUPER

Durbin

Durbin-Watson

durch

Dyadic

Dynamic

dynamic-multithreading

dynamical

Dyson

each

Early

Easily

East

Easy

Easy-to-Use

Eat

Eaton

EC

´ecarts

´echantillon

´echantillonnage

Econometric

Econometrics


Funktionen [246]. Further [2412, 2143, 52, 133, 3780, 420, 289, 3855, 3020].
fused [2655]. Fushimi [2218]. fusion [3236]. Future [3385]. Fuzzy
[350, 3916, 3551].

G [541, 2972, 594, 637, 1956, 1079, 262, 70]. G5
[380, 391, 434, 674, 596, 479, 644, 362, 363, 364, 168, 461, 628].

Galois [2228]. gambler [3161]. Gambling [2481, 2653, 3707].

Game [2869, 3912, 3148]. game-playing [2821].

Gamma [670, 3974, 542, 819, 906, 1272, 766, 867, 919, 2369, 2525, 1375, 3945,
2208, 1044, 534, 887, 888, 1015, 712, 805, 3704, 892, 897, 1261, 1053, 853, 377,
2835, 1032, 1231, 331, 3066, 3844, 785, 3398, 828, 1078, 2086, 565, 617,
701, 880, 747, 1016, 3207, 846, 748, 713, 1018, 761, 683, 3689].

gamma-distributed [331, 683]. Gamma-distribution [761].
gamma-rays [1078].

gammaverteilten [331]. gap [235]. gas [813, 677, 2300].

GASPRNG [3670]. Gate [3145, 2615, 3038]. Gates [3100, 3377]. Gateway
[4132, 4026, 4073].

générateurs [1367, 2647, 2538, 2184]. générateurs [3989]. General
[946, 501, 1930, 1931, 2052, 3803, 3168, 524, 106, 1081, 847, 3222, 2311, 4064,
721, 3763, 385, 968, 1249, 3089, 3555, 3884, 618].

General-Purpose [1081]. Generalised [2172, 897]. Generalization [444, 238]. generalizations
[3601]. Generalized
[3861, 1209, 1328, 1701, 2828, 3258, 1369, 648, 388, 3301, 2734, 1019, 3922,
1894, 3240, 1799, 3718, 1919, 2756, 410, 441, 1351, 3512, 2835, 3727, 1940,
3066, 2062, 3167, 3529, 1850, 1297, 2631, 2725, 2939, 3025, 2731, 1062].

Generate [1320, 1022, 1096, 1893, 2589, 1526, 3706, 1886, 2410, 772, 2168,
1229, 3884, 1587, 1880, 1671, 2008]. Generated
[3230, 3346, 267, 244, 1069, 613, 3775, 373, 3574, 1313, 1786, 581, 755, 1700,
438, 471, 585, 3601, 1419, 1503, 242, 765, 1344, 3057, 638, 1937, 1033, 2275,
2061, 2062, 1174, 3534, 2187, 2368, 695, 797, 1184, 1462, 1557, 2533, 3187,
3636, 926, 836, 1041, 3553, 2884, 233, 2309]. generates [2616, 2944].
générateurs [1367, 2647, 2538, 2184]. Generating
[1018, 2123, 2226, 814, 1679, 3826, 2888, 1596, 1788, 899, 945, 3588, 542, 1099,
1895, 2236, 852, 3717, 3364, 3756, 270, 196, 1210, 1211, 1606, 1798, 2494, 992,
1273, 3138, 153, 323, 408, 3508, 3509, 3923, 478, 245, 201, 1938, 3727, 3728,
155, 2511, 1947, 2059, 777, 1728, 1729, 1120, 1007, 1839, 3529, 309, 2067, 3538,
251, 870, 253, 254, 280, 281, 311, 335, 788, 966, 1126, 2309, 2525, 1642, 2076,
791, 1375, 3630, 831, 3542, 1293, 1376, 204, 205, 524, 2790, 1561, 1564, 3415.
2458, 1978, 2093, 527, 619, 702, 3308, 2207, 1247, 2208, 1091. Generating
[460, 2215, 1136, 626, 2301, 2548, 2475, 1310, 847, 2115, 1141, 713, 2955, 3036, 2393, 1050, 2561, 3751, 675, 1901, 1247, 2208, 1091, 3926, 156, 1778, 3212, 2324, 2425, 426, 2122, 1213, 1704, 1705, 1799, 2244, 3252, 3718, 994, 1153, 1417, 218].

Generation

Generation
[2645, 136, 165, 1778, 3095, 3209, 1876, 3212, 3213, 2219, 426, 1140, 1195, 537, 538, 1667, 712, 2479, 1590, 3653, 3822, 3576, 3788, 631, 1258, 431, 2484, 3859, 1483, 1787, 3108, 3231, 3789, 1890, 1321, 2965, 3474, 3475, 3660, 3661, 3662, 3711, 1261, 1891, 2130, 3040, 3583, 349, 3112, 987, 2891, 3664, 850, 3895, 238, 3115, 817, 1055, 1892, 182, 1490, 1410, 946, 905, 1692, 401, 1417, 3831, 402, 2414, 2324, 3046, 2023, 2326, 468, 1329, 1331, 989, 1605, 2828, 3365, 990, 991, 1024, 1104, 1213, 1704, 1705, 1799, 2244, 3252, 3718, 994, 1153, 1417, 218].

generation
[2038, 2157, 322, 2830, 1421, 2425, 764, 553, 1064, 1280, 1424, 1512, 2981, 555, 185, 1282, 1350, 639, 2834, 3672, 3903, 3379, 3798, 3757, 2990, 2054, 1068, 1823, 2504, 2688, 2769, 1433, 3146, 1032, 202, 1436, 1725, 1523, 1524, 824, 1070, 3927, 118, 1171, 1232, 3156, 1003, 3941, 1444, 779, 1446, 3981, 1006, 1034, 3840, 1957, 2361, 2364, 2847, 3619, 3842, 1837, 129, 3620, 3685, 1452, 3964, 3764, 3807, 1237, 158, 1454, 3766, 2522, 789, 1075, 3689, 1848, 1968, 2448, 2527, 2528, 1849, 160, 130, 1127, 3632, 3813, 561, 562, 1647, 1754, 1755, 1972, 2083].

generation
[2085, 615, 3302, 876, 3696, 418, 3848, 490, 3774, 1080, 1040, 3544, 3850, 3019, 3421, 3020, 1086, 1042, 3023, 3085, 931, 973, 3986, 1190, 878, 2543, 975, 3026, 3744, 2300, 1193, 983, 149, 2107, 3561, 2218, 2551, 1472, 3034, 3096, 3703, 1580, 2552, 1308, 3886, 1139, 1309, 846, 3650, 573, 629, 668, 710, 3332, 3101, 2554, 3572, 3652, 2404, 1589, 1253, 2406, 2654, 2739, 3795, 1582, 3330, 1892, 322, 1580, 1500, 1001, 622, 890, 759, 1517, 1531, 1352, 1304, 2972, 3048].

Generations [3485, 3527, 3242, 2393].
3334, 3221, 1784, 3573, 3224, 3456, 3038, 3225, 3889, 2740, 2886, 3575, 3459, 2958, 3973, 3705, 1256, 1592, 2309, 2959, 1884]. generator

[3497, 3600, 2002, 1215, 459, 461, 3214, 3329]. Generatoren [1050, 1052].

Generators [1394, 2559, 2310, 2815, 293, 3974, 2122, 2225, 2962, 3345, 1479, 3657, 3825, 3232, 3109, 2658, 2314, 3111, 2745, 2966, 578, 2132, 3349, 3989, 3476, 1598, 2233, 3587, 2136, 900, 3862, 3936, 1408, 3356, 3714, 2824, 2969, 3117, 2140, 903, 904, 3118, 1206, 2415, 906, 3363, 2417, 1209, 1270, 3127, 2898, 403, 2574, 1698, 3249, 1496, 1910, 1333, 1701, 1911, 2242, 3130, 3132, 3598, 3599, 3868, 2669, 720, 3602, 3038, 2366, 1633, 2453, 3687, 358, 3809, 3810, 1178, 1180, 1845, 1847, 2780, 2710, 3178, 1640, 2714, 3691, 1461, 1549, 1551, 1748, 1292, 2196, 2617, 2788, 1854, 2624, 2721]. Generators [769, 1815, 2759, 2760, 2908, 3606, 3630, 1976, 3038, 1976, 1092, 1766, 3777, 3816, 419, 1467, 2798, 3424, 3425, 3426, 3427, 2098, 3194, 802, 2632, 3428, 3196, 1657, 3429, 2099, 3310, 1090, 2462, 2634, 3027, 2214, 569, 2470, 2472, 535, 2642, 2643, 2394, 2879, 1392, 1577, 1777, 2000, 1137, 3445, 572, 2810, 3098, 1664, 1665, 2220, 1877, 2813, 3820, 805, 1311, 2116, 2481, 2653, 427, 1669, 428, 494, 3704, 848, 1673, 2407, 1050, 1144, 1198, 1313, 1315, 1477, 3655, 2655, 1885, 2483, 3105, 3106, 3823, 1259, 1400, 1319, 3749, 498, 3656, 2125].

generators [3581, 2127, 1678, 3108, 1680, 2313, 3472, 3659, 3790, 2316, 3582, 3662, 1052, 3040, 3583, 3712, 3348, 3233, 2566, 2014, 3971, 3113, 1684, 1147, 1053, 1406, 2894, 3863, 1054, 2895, 1203, 2016, 1688, 2661, 2747, 2970, 3044, 2413, 905, 1491, 1691, 2896, 1205, 718, 3122, 3716, 1902, 3125, 3897, 3666, 3493, 1903, 2145, 2237, 546, 2288, 1907, 2024, 2146, 2239, 1023, 1908, 3248, 2327, 1332, 1497, 1498, 3250, 1415, 1494, 1495, 3496, 1604, 1702, 2750, 2900, 3131, 3251, 3833, 1344, 1416, 633, 3901, 3253, 3254, 1608, 406, 1417, 2753, 2245, 2246, 2495, 1501, 3257, 1419, 1420, 1504]. generators

[1710, 1339, 2903, 1922, 1923, 2040, 2158, 2255, 2334, 2345, 2424, 2575, 2576, 1717, 1158, 1810, 856, 951, 952, 1219, 1220, 1341, 1811, 2043, 3836, 439, 1030, 275, 2339, 859, 997, 2907, 3057, 3837, 1348, 3724, 2909, 3510, 2761, 1721, 1816, 770, 476, 1227, 1282, 1350, 2585, 2684, 2763, 2764, 3141, 3673, 3380, 1519, 3381, 1430, 1818, 1819, 1928, 685, 3962, 3515, 3516, 1929, 2053, 2267, 2268, 2347, 2590, 3839, 1431, 2270, 3677, 775, 3938, 864, 3382, 3277, 1432, 1940, 3520, 1169, 3680, 1724, 2506, 2507, 2993, 1525, 356, 383, 2171, 2916, 1830].

generators [2174, 2273, 2274, 2352, 3523, 1002, 3156, 1442, 2843, 916, 1720, 3162, 2440, 3525, 1730, 2920, 2997, 3067, 826, 1367, 1368, 1450, 1632, 1838, 2179, 2181, 2182, 2184, 2279, 2280, 2360, 2362, 2363, 2445, 2446, 2600,

Heuristic-Based [2088]. heuristics [3033]. HI [4179]. Hidden [1717, 3889].

hiding [3380]. hierarchical [3149, 3004]. Hierarchy [2188, 3447, 2968, 1603].

High [2408, 3465, 2135, 3753, 2663, 3125, 3270, 3271, 3926, 3279, 3153, 3802, 4186, 2520, 651, 2071, 3737, 3632, 3404, 3414, 1190, 3095, 3097, 101, 3571, 1057, 1326, 2662, 2748, 2668, 2750, 3050, 3135, 3257, 2576, 2832, 3378, 3058, 1725, 1941, 2170, 118, 3163, 3283, 129, 3531, 1960, 3537, 3538, 1967, 792, 2380, 227, 3020, 2944, 3030, 1193, 3745, 3561, 122, 2475, 2552, 3573, 2959].

High-density [2663]. high-dimensional [2668, 2750, 2380, 3030, 3745].

High-entropy [3125]. high-functioning [3020]. high-order [3058].

High-Performance [3153, 3465, 2135, 3753, 2576, 1941, 2170, 118, 3163, 3283, 129, 3531, 1960, 3537, 3538, 1967, 792, 2380, 227, 3020, 2944, 3030, 1193, 3745, 3561, 122, 2475, 2552, 3573, 2959].

High-Quality [2188, 3447, 2968, 1603].

High-Speed [2408, 3271, 3802, 3414, 3753, 2520, 1190, 2748, 3257, 1725, 118, 129, 792, 227].

Higher [2019, 3243, 1698, 2434, 3239, 3521, 1246, 2953].

Higher-Order [1698].


Histogram [3490, 1619]. Histograms [3697, 1308]. Historical [2737].


Hyatt [4117, 4195, 4113]. Hybrid [3254, 3979, 354, 251, 3319, 3105, 3239, 557]. hyperbolas [2118, 2401].

33

[4016, 4011, 4010, 4070]. Integer
[1200, 2494, 2148, 3675, 1529, 3908, 3186, 3913, 2207, 1090, 1879, 1681, 3710, 1342, 3799, 781, 1121, 2931, 2070, 565, 617, 1591]. integer-valued
[1681, 3710, 3799]. Integers
[2976, 3923, 1287, 1403, 2241, 633, 113, 771, 1119, 1289, 3736, 1863, 1085]. Integral
[1887, 819, 1005, 1389, 712, 349, 132, 3551, 713, 3550]. Integrale
[278]. Integrale
[2971, 2254, 996, 2774, 2080, 2205, 2104, 1597, 2232, 901, 4176, 1349, 2911, 1820, 2906, 667, 397, 463, 540, 804, 2867, 540]. integrations
[1080]. integrators
[2277]. integrity
[4071]. Integro
[3355]. Integro-Local
[3355]. Intel
[2046, 3385, 2437]. Intelligent
[4185, 3497]. Intensive
[2921, 4070, 4049]. Inter
[3447]. Inter-domain
[3447]. Interactions
[1764]. interactive
[1793]. interchanges
[1728]. interdependence
[585]. Interface
[4031, 4018, 4023, 4011, 4048, 4049, 2054, 3290, 3966]. Interfaces
[2417]. Interruptions
[1020]. Interpretation
[6, 725, 384, 3361, 2066, 624]. interruptions
[1020]. Interval
[2411, 716, 953, 3960, 3908, 3913, 61, 3302, 2007]. Intervals
[2319, 1798, 953, 1727, 44, 969, 150]. intrainverted
[1722]. Intrinsic
[2233, 1514, 1292, 1761]. Intrinsically
[3625, 3852, 3883]. Introduction
[3858, 2826, 2019, 3243, 2666, 3049, 3159, 1840, 2285, 3170, 262, 1233, 1685, 2235, 2659, 3353, 296, 2326, 1726, 2703]. invalidates
[3418]. Invariance
[579]. Invariant
[1896, 3013]. Invariants
[3176]. Inventor
[3480]. Inverse
[1100, 3978, 2989, 3062, 3168, 187, 4140, 2545, 886, 889, 897, 1019, 3718, 1427, 324, 1068, 3727, 2058, 3529, 3910, 1965, 2863, 876, 1983, 1248, 1249]. Inversen
[1030]. inverses
[3173]. Inversion
[3244, 3004, 3367, 3860, 3046, 3365, 3055, 3607, 2168, 2769, 3529, 3099, 1876, 3889]. Inversion-based
[3004]. Inversions
[1503, 1462, 46]. Inversive
[2086]. invertible
[3572, 3652]. Inverting
[323, 3001]. investigating
[414]. investigation
[2678, 3982]. Investigations
[1665, 1670, 2143, 1747]. investing
[3767]. invitation
[4005]. Invited
[2500, 1633]. Involving
[197, 341, 342]. IoT
[3963, 3940, 3942, 3944]. iris
[3705]. Irrational
38

290, 2519, 2775, 1752, 3641, 2107]. low-dispersion [1377]. Low-Order
[1910, 1409]. Low-overhead [3988]. low-power [3248]. Lower
LPRng [2531, 2095]. LR [1541]. LSI [1156]. LSTMs [3927]. LT [3363].
Luby [2124, 1850, 3186]. Luc [1304]. Lucas [3511, 2403]. luck [3841].
luminescent [3686]. Lüscher [2170, 1941]. LUT [3095, 3702]. LUT-SR
[3702]. LUTs [3445]. LWR [3984]. LWR-based [3984]. LXM [3948].
Lyapunov [2849, 1842]. lying [1314]. LZSS [3359].

M/M/m [1020]. M/PH/1 [3328]. MA [4173, 4131]. Mach [3126].
Machine [151, 2749, 142, 916, 3801, 835, 166, 3828, 771, 2195, 3423, 192].
Machine-independent [916, 771]. Machinery [3992]. Machines
MaD0 [3805]. Made [1510, 1833]. Madland [3778]. Magma [3488].
Mahalanobis [135]. Main [3433]. Maine [4067]. mainly [312, 450].
maintenance [3407]. Majorana [3667]. Majority [3917]. Majorizing
[3830, 2546, 2905, 3448]. Man [128]. Management [2415, 4129, 4087, 3227].
Managing [3776]. Manhattan [3682]. MANIAC [1199]. Manipulating
[3362, 3574, 3891, 3922, 3806, 2092, 3314]. Maple [1951]. Mapping
[3429, 1422, 1030, 3521]. Mappings [3226, 2766]. Maps
[2611, 3344, 2965, 3239, 868, 3408, 3968, 3973]. March
[3994, 4051, 4174, 4031, 4023, 4185, 3996, 4081, 4155]. Marginal [2236, 1839].
Marginals [2569]. margins [2301]. Marinucci [3684]. Mario [3807]. Mark
[4038]. Markov
[2566, 212, 1097, 1201, 2240, 3371, 955, 512, 660, 709, 2001, 1785]. marks
[2317]. Marotto [3514]. Marriott [4044, 4017, 4132, 4026, 4073]. MARS
[3343, 2313, 2824, 1338, 1339, 1354, 2069, 2091, 1084, 3820, 3855]. Marshall
[2910]. Martuljek [4102]. Maryland [4055, 4146]. mashinakh [351].
masked [3673]. Masking [3916]. mass [738, 1589]. Massachusetts [4011].
[3829]. Mathematica [3630, 3693, 2100]. Mathematical
[3829, 4000, 4067, 3995, 4016, 4020, 1231, 1232, 96, 3684, 3997, 250, 1078, 3773,
2383, 3999, 55, 57, 4007, 4106, 3651, 938, 464, 495, 236, 717, 1218, 2457, 209].
Mathematical-Function [3829]. Mathematicians [2628]. Mathematics
[2409, 4000, 2823, 3995, 4016, 912, 4198, 1951, 1552, 1853, 4166, 4167, 4008,
139, 4197, 1742, 4015]. mathématiques [3997]. MathLink [2135].
MATLAB [3151, 2709, 3182, 2885]. Matrices
[2323, 1179, 3095, 1260, 1623, 1126]. Matrix [1593, 2236, 590, 1282, 1350,
2198, 1313, 1149, 1419, 3274, 3612, 53, 1558, 2083, 2085, 3572, 3652, 1227.

Matrixgeneratoren [1227, 1350]. matter [3954]. max [1457]. Maximal
[183, 1612, 1445, 829, 925, 2735, 1710, 2761, 3636, 3320]. Maximal-Length
[925, 1445]. Maximally [3872, 2182, 2446]. Maximum
[1271, 1026, 1157, 829, 925, 2735, 1710, 2761, 3636, 3320]. Maximal-length
[3542, 3738]. May
[4029, 4034, 4039, 4045, 4050, 4055, 4066, 4075, 4084, 4089, 4097, 4098, 4116,
4123, 4136, 4146, 4161, 4189, 3998, 4087, 3694]. mbedTLS [3856].
MC
[170]. MCNP [1274, 3375]. MCS [4133]. McShane [506]. MCV
[740, 800]. Mean
[577, 1100, 766, 2841, 601, 2, 539, 1706, 1707, 2756, 1707]. mean-square
[1706, 1707]. meaning [440]. Means [3506, 2998, 3091, 2108, 2590, 3403].
Measure [2227, 2349, 2562, 2909, 2921, 2097, 2646]. measurement
[3248, 3379]. measurements [557, 3567]. Measures
[2961, 3532, 2723, 633, 1809, 2272]. measuring [3434]. Mechanical [530].
mechanics [2896]. Mechanism [3919]. medians [437]. Medical
[24, 299, 47, 73, 114, 115, 171, 172, 3533]. Meeting [4014, 4009, 4005, 4135].
Meetings [1150, 1168]. Mehrfach [638, 639]. mehrfacher [278]. Mellin
[536]. Mellon [4013]. Memorial [4111]. Memory
[2408, 2225, 3749, 3905, 3739, 3912, 3433, 3859, 1741, 1746]. memoryless
[1295]. Mengen
[2747, 3240, 2749, 2828, 760, 3872, 1723, 913, 2853, 2373, 3008, 2536, 3416, 3197, 3431, 3698, 1776, 2807]. Mersenne-Exponent
[1691]. Metaheuristic [3979, 3982]. Metamodels [1727, 3593].
Metastability [3967, 3221, 2930]. Metastability-Based [3211]. Method
[2009, 267, 179, 758, 270, 196, 1210, 1211, 2494, 634, 1274, 2420, 1813, 220,
352, 641, 510, 25, 201, 1824, 1938, 645, 1005, 1120, 2925, 249, 2367, 2067, 601,
281, 335, 337, 359, 2369, 2525, 146, 2375, 2076, 187, 205, 613, 2198, 2202, 658,
19, 741, 527, 619, 702, 970, 4200, 2208, 1659, 2947, 3916, 3448, 1667,
847, 559, 1393, 3706, 630, 941, 1396, 2311, 1261, 1404, 234, 1055, 1792, 195,
1205, 1266, 3046, 320, 989, 948, 1704, 3499, 585, 1214, 2157, 2518, 591, 592,
273, 765, 767, 351, 1000, 1351, 3607, 94, 3515, 1521]. method
[1826, 1937, 67, 76, 3993, 1725, 1070, 2178, 918, 1006, 1034, 1174, 2924, 3003,
2521, 3622, 3537, 385, 828, 1124, 1125, 2370, 2526, 78, 1550, 920, 3001, 2865,
1010, 3879, 695, 797, 1184, 1972, 2083, 2085, 2293, 383, 662, 1084, 99, 189, 566,
877, 4019, 1089, 3699, 1390, 2876, 393, 709, 747, 2733, 1999, 193, 2880, 1876,
1309, 3784, 711, 177, 2223, 1475, 1880, 3972, 2555, 233, 7, 3973, 3787, 2121, 178].
Méthode [178]. Methoden [631, 1747]. Methodology
[3501, 725, 2596, 2462, 4108]. Methods
[576, 670, 4005, 2126, 3111, 2015, 3244, 547, 679, 2243, 1101, 1212, 2036, 2580,
636, 2341, 2757, 4193, 4183, 642, 512, 2172, 1438, 1441, 4171, 827, 788, 1642,
3996, 488, 831, 204, 614, 873, 1756, 2623, 2293, 1081, 4070, 700, 2205, 1865,
841, 4160, 1575, 1993, 2395, 2883, 4049, 464, 495, 651, 986, 1317, 892, 3751,
Modulo

Modulus

Molecular

molecular-dynamics

Moment

Moment-Generating

Moments

Monaco

Monica

monitoring

Monkey

Monkeying

Monographs

Monotone

Monotonicity

Monster

Monte

Monte-Carlo

Monterey

Montgomery

monthly

Montreal

Monty

Mordell

morphological

MOSFET

mostly

mother

Motion

mots

mouse

movement

moyennes

MP

MPI

MPPC

MR

MPR

MR1414863

MR2084569

MT19937

Mulders

Muller

Multi

multi-access

multi-bit

multi-class

multi-dimensional

multi-delays

multi-folding

multi-sequences

multi-stage

multicomputer

multicyclic

Multidimensional

Multigroup

Multiloop

Multimedia

Multinomial

Multiparty

Multicore

Multithreaded

Multithreading

Mulders

Multi-access

multi-bit

multi-class

multi-dimensional

multi-delays

multi-folding

multi-sequences

multi-stage

multicomputer

multicyclic

Multidimensional

Multigroup

Multiloop

Multimedia

Multinomial

Multiparty
2440, 3981, 598, 599, 248, 2920, 2997, 3067, 826, 1365, 3388, 1368, 1632, 1838, 1957, 2179, 2184, 2279, 2280, 2281, 2362, 2363, 2364, 2600, 2602, 2698, 2845, 2847, 2922, 3070, 3592, 3619, 3842. **number**

[3282, 1539, 1174, 3389, 1122, 3163, 3283, 2921, 782, 2849, 2851, 3004, 3166, 2284, 3763, 129, 482, 1734, 3620, 3167, 1542, 483, 868, 3530, 3531, 2612, 3685, 2930, 3766, 3624, 3292, 3293, 3626, 447, 448, 485, 521, 652, 789, 1075, 1179, 1546, 1547, 1636, 1742, 1966, 2287, 2706, 2781, 3399, 2708, 2857, 3176, 3911, 3540, 1848, 1967, 1968, 2448, 2527, 2528, 3627, 3690, 3737, 3628, 2372, 2373, 2783, 3008, 3074, 3180, 3076, 3541, 2786, 2864, 1747, 1643, 792, 454, 455, 830, 3693, 793]. **number**

[3295, 1078, 1127, 3402, 921, 832, 3297, 609, 3632, 3404, 3012, 611, 1010, 655, 1128, 1297, 1647, 1754, 1755, 2083, 2535, 2620, 2720, 3189, 3015, 3302, 3408, 2866, 3409, 3410, 616, 659, 3190, 876, 3696, 3081, 2538, 2868, 2938, 3413, 2203, 3304, 3774, 1463, 1130, 491, 525, 1080, 1299, 1464, 1760, 2091, 968, 1386, 3191, 3880, 2539, 2092, 564, 3544, 2094, 1300, 3418, 800, 3018, 3850, 1131, 618, 2540, 1981, 3421, 260, 1132, 620, 367, 839, 3547, 2215, 2465, 1193, 2639, 2803, 3556, 983, 2804, 2473, 3746, 3948, 3969, 2549, 208, 3090, 3558, 2640, 2641, 3932, 3559, 3315, 3561, 2878, 2304, 2393, 2551, 2730, 2646, 2731, 2733, 2808, 2949, 2950, 2951, 3032, 3033, 3093, 3440, 3441, 3442, 3562, 3563, 3207, 3443, 3444, 1472, 1661, 1875, 1999, 3034, 3094, 3096, 3702, 3747, 2396, 3446, 3321, 167, 2953, 3949, 2476, 1663]. **number**

[1308, 985, 3097, 2811, 3950, 3448, 3450, 1093, 2112, 1094, 3650, 3933, 2553, 3567, 232, 1587, 1878, 3035, 3568, 1754, 2652, 3332, 2117, 2223, 3334, 2005, 462, 2957, 3101, 2554, 3221, 3452, 3572, 3652, 1784, 2406, 2308, 2654, 2739, 3037, 3454, 3224, 3972, 3456, 3038, 3225, 3889, 2740, 2886, 2741, 3338, 3339, 3459, 2958, 3973, 3461, 3705, 1256, 1592, 575, 2959, 3795, 3497, 3600]. **number**

One-chip [3321]. One-class [3339]. One-dependent [1439]. One-Dimensional [3574, 188]. One-line [447, 448]. One-shot [3148]. One-Sided [484].


50


Probabilistic [1813, 922, 3316, 1588, 1900, 1237, 2432, 1724, 1739, 2777, 2931, 454, 1555, 625, 574]. 
Probabilîa [16].
probabilités [3].
Probabilities [950, 1108, 1567, 3828, 3, 3064, 140].
Probability [3858, 1887, 294, 4005, 3827, 2142, 169, 2027, 3138, 82, 305, 1239, 653, 560, 2619, 360, 1129, 1649, 2722, 2627, 2090, 1186, 2204, 526, 262, 207, 4072, 907, 4006, 151, 1331, 1104, 4177, 16, 2163, 381, 1443, 256, 1554, 663, 568, 2649, 3933, 4020, 389, 2618].
Probable [1, 969, 2, 2143, 1796, 1443].
probablistic [564].
Probably [1322].
Problem [2139, 3357, 52, 2906, 304, 1455, 388, 3773, 1774, 1599, 2822, 948, 3512, 958, 3174, 3875, 188, 3889].
procédé [322].
Procedure [1099, 1208, 950, 1108, 996, 3902, 444, 309, 280, 1762, 1594, 1676, 322, 773, 334, 283, 336, 3633].
Procedures [2570, 3726, 254, 565, 617, 2633, 1136, 1672, 1684, 582, 320, 2451, 2712, 2934, 3179, 344, 846].
Proceedings [4029, 4050, 4075, 4098, 4189, 4196, 3994, 4051, 4032, 4040, 3995, 4064, 4018, 4023, 4037, 4119, 3993, 4059, 4060, 4201, 4186, 4093, 4017, 4132, 4133, 4160, 4082, 4013, 4095, 4096, 4139, 4015, 4048, 4008, 4097, 4146, 4156, 4161, 4044, 4090, 4035, 4056, 4014, 4030, 4031, 4000, 4076, 4099, 4022, 4100, 4124, 4091, 4016, 4046, 4138, 4058, 4020, 4125, 4069, 4126, 4130, 4120, 4127, 4054, 4150, 4113, 4065, 4094, 4114, 4121, 4143, 4010, 4070, 4026, 4009, 4028, 4135, 4088, 4115, 4038, 4107, 4083, 4034, 4039, 4045, 4055, 4066, 4084, 4089, 4116, 4123, 4136, 4141, 4173, 4182, 4103, 3992, 3998, 4062, 4170].
Proceedings [4190, 4063, 4011, 4086, 4180, 4195, 4131, 3997, 4078, 4172, 4081, 4151, 4087, 4073, 4102, 4106, 4074, 4109, 4085, 4118, 4178, 4162, 4185, 4159, 4043].
Process [2067, 3313, 1704, 528, 981, 3329, 1591].
Process-Voltage-Temperature [3313].
Processes [170, 300, 350, 1822, 2691, 688, 2439, 97, 102, 1061, 4177, 274, 198, 1520, 3612, 4002, 2598, 3877, 360, 1129, 1649, 2722, 228, 62, 1781, 319, 389, 394].
Processing [669, 3496, 4081, 3998, 3664, 1203, 4119, 1355, 2271, 1446, 3163, 3632, 3189, 1982, 1656, 2554].
processor [3350, 1523, 1524, 3685, 3328].
Processors [2422, 4163, 3385, 3416, 3431, 3698, 3348, 3864, 1410, 1501, 1424, 1620, 1635, 1464, 3461, 3576].
Product [1113, 3978, 3938].
Produced [1408, 3761, 558, 1082, 1083, 1409, 3058, 2278, 1558, 2732].
Producing [337, 359, 75, 76, 385, 2949].
Product [2594, 3065, 207, 3202, 898, 1158, 1936, 1239].
Production [169, 331, 176].
Products [3010, 395, 534, 2042, 3525, 2811].
Profile [2962, 2829, 2764, 2785, 3076, 1749, 1555, 2953, 1882].
Program [3475, 3662, 2133, 1215, 3798, 225, 3218, 1023, 2376, 615, 1383, 1132, 936].
Programmable [2271, 1828, 2615].
Programmed [814, 900, 1690, 2959].
Programmierung [890].
Programming [3829, 3959, 2998, 2088, 1650, 3779, 4135, 890, 4016, 1218, 2169, 2708, 612, 2215, 3701].
Programs [1484, 3356].
3652, 3224, 3456, 2886, 3575, 3338, 3822, 3461, 3462, 438, 471, 639, 362, 3628

Pseudo-aleatoire [1892, 322]. pseudo-aléatoires [759, 284, 1580].


Pseudo-random


Pseudo-random-number

[3386, 2275, 3156, 3281, 1003, 1628, 2919, 248, 1007, 1174, 2441, 2926, 2612, 1841, 3393, 3396, 3292, 3176, 3690, 3737, 2373, 284, 455, 793, 3771, 3011, 1750, 3403, 2289, 695, 797, 799, 794, 798, 1148, 418, 2294, 491, 258, 3417, 662, 800, 663, 3850, 3642, 3022, 878, 3782, 3550, 3551, 2636, 3968, 1193, 345, 570, 3970, 3314, 2217, 2393, 2551, 2730, 165, 193, 3212, 2477, 1094, 3219, 2955, 3036, 1475, 3572, 3652, 3224, 3456, 3575, 3461, 3462, 628, 362].

Pseudo-random-number

[3166, 2864, 2299]. Pseudo-Randomness

[2588, 3142, 2772, 446, 1687, 3534, 1553, 3192]. pseudo-uniform [1023]. Pseudo-Zufallszahlen

[348, 471, 639]. pseudoentropy [3649]. pseudoinverses [1030]. pseudonoise [2915].

Pseudorandom


Pseudorandom

Pseudorandom
[2723, 3639, 1131, 1980, 419, 1467, 2097, 1387, 2632, 3428, 1657, 3197, 881, 882, 
1092, 883, 1991, 2465, 709, 3031, 2474, 2642, 2394, 1306, 1392, 1577, 1663, 1877, 
2113, 3100, 3218, 2116, 2481, 2653, 1141, 494, 2956, 1881, 3226, 3821, 3786, 1673, 
907, 2742, 1050, 1395, 2655, 1885, 1593, 3891, 1259, 1400, 1481, 2011, 498, 2312, 
2127, 2887, 1482, 1401, 1680, 3659, 3790, 2965, 3474, 3582, 3660, 3712, 987, 2014, 
1599, 2894, 3895, 1054, 1055, 1691, 3488, 401, 1793, 3794, 3954, 2664, 3666, 759, 
2827, 1908, 469, 2025, 2327, 1699, 1700, 470, 3955, 471, 3253, 472, 1105, 3601].
pseudorandom
[3977, 2246, 2495, 908, 1419, 1503, 1613, 1614, 1616, 1617, 
1709, 1710, 1712, 1713, 1714, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1915, 
1916, 1917, 1918, 1919, 1920, 2034, 2035, 2037, 2038, 2154, 2155, 2156, 
2248, 2250, 2252, 2328, 2329, 2330, 1338, 1340, 2253, 2333, 2671, 1923, 2040, 
2158, 2255, 2334, 587, 588, 322, 3722, 1811, 2497, 1279, 1224, 1280, 1344, 2338, 
2339, 859, 3837, 1348, 3724, 2909, 555, 379, 2833].
pseudorandom
[771, 185, 639, 3903, 2763, 2501, 2764, 3141, 3673, 3757, 3381, 3962, 3515, 
3516, 2051, 2053, 2265, 2267, 2268, 2345, 478, 2590, 2270, 864, 1432, 1940, 382, 
2507, 2993, 414, 824, 1525, 1941, 2170, 356, 2171, 1286, 2916, 1830, 1361, 2175, 
2176, 2512, 1442, 3907, 1235, 3162, 1445, 2440, 3981, 598, 599, 1365, 2921, 
2063, 2387, 2284, 1177, 1290, 2608, 1542, 483, 868, 3531, 3174, 3736, 3806, 
3910, 3930, 3175, 1372, 1454, 1740, 2068, 1848, 1967, 1968, 2448, 2527, 2528, 
2372, 2374, 2783, 3008, 3074, 1850, 3811, 2785, 3076, 3931, 1550, 3632, 3298, 
1010, 3813, 2197, 655]. pseudorandom
[875, 1039, 1128, 1244, 1245, 1297, 1378, 1379, 1381, 1462, 1556, 1558, 1754, 
1755, 1857, 1971, 2083, 2533, 2534, 2535, 2620, 2621, 2622, 2720, 2937, 3187, 
1758, 3409, 3410, 3412, 616, 3695, 3848, 3774, 1651, 525, 2091, 836, 968, 458, 
1981, 1132, 1654, 1469, 1087, 1565, 1042, 877, 3986, 3644, 2543, 3087, 705, 
2389, 3432, 2211, 2945, 1391, 3435, 3553, 3987, 2946, 624, 983, 3746, 3948, 
3969, 3932, 1775, 1307, 1999, 2953, 1779, 2648, 936, 3649, 3215, 3216, 3451, 
2112, 493, 3933, 710, 2221, 1587, 2117, 2118, 2223]. pseudorandom
pseudorandom-number [2655]. Pseudorandomness [2961, 2227, 3357, 
3592, 3957, 723, 2681, 2500, 3871, 3614, 3904, 2508, 2593, 2689, 2595, 2605, 

Q.R.N.G. [3469]. Qs [3609]. Quadratic [2033, 2037, 2252, 658, 2088, 1650,
Seed
Seeding
Seeds
seeming
Segmentation
Select
Selected
Selection
Selective
Self
self-adaptive
self-assembly
Self-Avoiding
Self-Excited
Self-Similarity
self-test
Self-testing
selfish
Semi
semi-infinite
Semi-Random
Semiconductor
seminar
Seminumerical
Semiparametric
sense
sensitive
Sensitivity
Sensor
sensors
Seoul
September
Sequence
Sequences
Sequential
Serial
Sequencing
Seeding
[4117, 3476, 3792, 2419, 1913, 2902, 3259, 3605, 2759, 2836, 2689, 4150, 2617, 2788, 2625, 3406, 3773, 3695, 1568, 3199, 3031, 2877, 4095, 4115, 3856, 4188, 2134, 2821, 3045, 4057, 3533, 1453, 793, 3298, 3304, 3310, 2946]. Seed
[3825, 2415, 3326, 1149, 2506, 1768, 3448, 3517]. Seeding
[1346, 2375, 3655, 1002, 3418]. Seeding
[135x610]Seeds
[2781, 3849, 1234, 3311]. seeming
[2628]. Segmentation
[1785, 3004]. Select
[1234]. Selection
[1208, 3127, 272, 2978, 3902, 3726, 1461, 2082, 3129, 2362, 2606, 3633, 1010, 2460]. Selecting
[1234]. Selection
[1208, 3127, 272, 2978, 3902, 3726, 1461, 2082, 3129, 2362, 2606, 3633, 1010, 2460]. Selective
[45]. Self
[3124, 2374, 3550, 1999]. Self-Avoiding
[3675, 2584, 1817]. Self-Excited
[3124]. Self-Similarity
[4154]. self-test
[1432, 1522, 2374, 1999]. Self-testing
[3645]. selfish
[3148]. Semi
[1247, 1310, 470]. semi-infinite
[470]. Semi-Random
[1247, 1310]. Semiconductor
[3307, 3213, 3325]. seminar
[3998]. Seminumerical
[2356]. Semiparametric
[1474]. sense
[872, 463]. sensitive
[2224]. Sensitivity
[2327]. Sensor
[2980, 3406, 3764]. sensors
[3559]. Seoul
[4149]. September
[3992, 4014, 4091, 4170, 4098, 4078, 4160, 4102, 4096, 4107, 4008]. Sequence
[1488, 1324, 3592, 3953, 1606, 1708, 1222, 408, 442, 1526, 2694, 384, 386, 3878, 3083, 1083, 3946, 666, 3218, 2407, 907, 1051, 3116, 901, 582, 1693, 1694, 1268, 3126, 37, 470, 551, 586, 3137, 1063, 1224, 2338, 3626, 3267, 3268, 324, 1430, 3838, 2990, 864, 3678, 3520, 306, 2771, 1033, 3156, 3281, 1004, 357, 1365, 3287, 2520, 647, 730, 731, 2187, 1740, 1374, 2374, 452, 453, 1009, 2081, 3695, 3848, 1041, 3420, 1190, 3087, 1769, 1045, 1773, 3314, 50, 2476, 3570, 13, 1253, 3338, 2309]. Sequences
[705, 622, 3198, 2463, 567, 1134, 3699, 345, 803, 1871, 2104, 2107, 1997, 2109, 2216, 2218, 2305, 3320, 1580, 3215, 493, 2553, 574, 1587, 3785, 1475, 807, 1671, 1882, 3575, 41, 809, 4057, 4162, 4149, 694, 733]. Sequential
[1145, 272, 3902, 1927, 558, 781, 1121, 120, 500, 1207]. Serial
[216, 52, 244,
SERPENT [2508, 2593]. server [2663, 2756, 1977]. Service [3468, 3469, 231, 2176, 1184, 1381, 1462, 51].


Ses [3196, 3275]. ses [1892].

Set [265].

SETS [1906, 170, 1732, 3684, 784, 250, 1976, 315, 231, 23, 1130, 20, 1591].

SETA [4162, 4149].

Setting [3326, 3526].

seventeenth [4029].

Seventh [1951, 4115, 4089].

Several [1902, 1827, 2353, 3623, 1499, 655, 1013].

SFQ [3337].

SHA [3772]. SHA-3 [3772].

Shadowing [1718].

Shamir [2893].

Shape [819, 2208, 712, 1053, 852, 3844, 3398, 3207, 713].

Shapes [3671, 2869, 3510].

Shapiro [3878].

Shared [2479, 1793].

Sharing [2076, 1984, 3065, 3328].

Shell [2797].

Shenzhen [4185].

Sheraton [4028].

Sherif [2103].

Sherman [127].

Shewhart [1197].

Shift [2571, 1209, 1328, 1106, 1029, 1062, 2982, 409, 1031, 1526, 2517, 517, 648, 650, 870, 487, 3543, 1566, 2388, 1989, 3647, 1577, 3445, 2735, 3918, 2407, 2410, 1268, 3126, 1508, 723, 1722, 2270, 1004, 3981, 2062, 3929, 333, 3535, 310, 1635, 1741, 2068, 1297, 1380, 1557, 3013, 3740, 1133, 1768, 2101, 3451, 3888, 3973, 3787]. shift-invariant [3013].

Shift-Nets [2388].

Shift-Register [1106, 2982, 650, 487, 1577, 1268, 1508, 2270, 1004].

Shift-Register-Sequence [2407]. shift-remainder [1298]. Shifted [3312, 3391, 3555].

Shifts [2800, 2970, 3044, 161]. shooting [1690]. shootout [3863].

Short [239, 323, 408, 405, 4067, 1159, 1595, 2101].

Shortest [719, 1526, 2874].

Shot [2943, 3148, 3434]. Should [1191].

shown [3707].

Shrinkage [3614, 3904]. Shrinking [1905].

shuffled [2476].

Shuffling [408, 742, 1485]. Shunt [338].

SIAM [4083, 4005, 1066, 4081, 933]. sic [2651].

side-channel [3191].

Sided [484, 3554].

Sieve [4077].

SIGACT [4075, 4172]. SIGACT-SIGMOD-SIGART [4075]. SIGART [4075, 4172].

Sigla [953].

SIGMOD [4075, 4172, 4087]. SIGMOD-SIGACT-SIGART [4172].


signature [1852].

Signed [1595].

significance [1163].

Significant [259, 430, 2914]. significantly [3493]. signing [2178]. silico [3576].

SIMD [3197]. SIMD-Oriented [3197].

Similar [3878].

SIMPL [763].

SIMPL/1 [763].

Simple [1478, 580, 1683, 1202, 1600, 906, 1607, 3758, 1074, 2525, 2374, 2076, 829, 3548, 2636, 2945, 1249, 3462, 2561, 850, 1148, 1795, 1103, 2425, 4104, 1281, 75, 3063, 2181, 2609, 3173, 621, 2473, 3207]. simplest [2063]. simplex [3788].

Simplicial [3819].

Simplicity [2050, 2165]. simplified [3172, 1850].

simplifying [3649]. Simply [2687, 1833]. Simscript [763]. simulate [1518].

Simulated [2570, 1776, 2807, 1901, 1223, 3025]. Simulating [2814, 3935, 1411, 758, 1215, 1266, 552, 2865, 1383, 1084].
Sophie-Germain [2858]. Sorrento [4091]. sort [1246]. Sorted [945, 899].
sound [2352, 3774]. Source
[1097, 3793, 3276, 3804, 650, 2210, 3991, 1201, 2748, 219, 3518, 3677, 3966, 2948].
Sources [1257, 1316, 2964, 30, 3373, 3814, 1247, 1310, 1327, 1543, 1843, 3845, 2790, 2302, 3886, 3450]. sous [801]. Southeast [4063, 4074]. Sowey
[931, 973]. SP [3045, 3814, 3428]. SP800 [2912, 3637]. SP800-22
[2912, 3637]. Spa [4127, 2055]. Space
[3144, 3075, 1680, 3371, 822, 686, 1559, 1757, 188, 2542]. space-bounded
[1559, 1757]. Spaces [3935, 3903, 1554, 3013, 3030]. Spacings
[366, 1945, 2282, 2600]. Spanish [134]. sparing
[1138]. Sparre
[238]. Sparse
[1516, 2700]. sparsest
[3681]. sparsity
[3724]. Spatial
[2515, 3047, 3683, 928, 3314]. Special
[2986, 3676, 3734, 3221]. Species [186]. Specific
[3720, 4163, 1007, 2008]. Specification [3905]. Specifications
[2505]. Specified
[2569, 1839, 2367, 3308]. Specker [3578]. Spectral
[3935, 1698, 768, 769, 1167, 862, 1067, 3928, 3911, 451, 3299, 2873, 3024, 3335, 2423, 685, 2991, 2348, 2274, 2280, 2508, 3317, 1307]. spectrally
[3699]. Spectrum
[2912, 3395, 3818, 3778]. Speed
[2408, 3271, 3802, 651, 3414, 3307, 101, 3571, 3335, 3753, 2748, 3135, 3257, 2832, 3378, 1725, 118, 2178, 129, 2520, 792, 227, 563, 1190, 2944, 122]. Speedy
[1662]. Sphere
[196, 201, 3684, 3539, 602, 845, 1579, 1139, 429]. Spheres
[205, 1170, 3327, 270]. Spherical
[341, 342]. Spherically
[169]. Spin
[3723, 3155, 735]. spintronics
[3723]. spirals
[1314]. Splittable
[3666, 3782, 3746, 3948]. Splitter
[2670]. splitters
[3315]. Splitting
[1631, 2158, 2223, 2554]. sponge
[3589]. spongy
[3741]. sponsored
[4005, 4016]. Spontaneous
[3453]. Spooler
[2095]. Spreading
[3758, 3274]. spreadsheet
[2862]. Spritz
[3741]. SPRNG
[2321, 2527, 2528]. sprout
[3311]. Square
[823, 44, 390, 3405, 1706, 1707, 2584, 94, 1627, 3166, 88, 14]. squared
[1352, 1172]. Squarefree
[2976]. Squares
[3878, 1439, 161]. squaring
[1308]. Squeeze
[880, 980, 828, 1089]. SR
[3702]. SRAM
[3976, 3276]. SRS
[1945]. SRU
[609]. SSE2
[3475]. St
[4059]. Stability
[319, 1813, 688, 394, 2230, 2598]. Stable
[758, 3519, 2507, 2993, 2439, 3945, 1266, 3252, 1383]. Stack
[2871]. STACS
[4033]. Stage
[1099, 3501, 159]. staircase
[1749, 1882]. Standard
[1492, 3506, 1418, 2505, 1861, 3772, 3644, 813, 677, 3958, 1947, 1629, 1654, 3881, 3061, 4128, 2469, 2547]. Standards
[91, 2541, 167]. Stanford
[4111]. Star
[2974, 2994, 3088, 3202, 3312, 3089, 3555]. Start
[584, 3301]. Start-Up
[584]. STATCOM
[3124]. State
[4017]. State-transition
[3095]. States
[3374, 2194, 3912, 3630, 3693, 3434]. stationarity
[817]. Stationary
[350, 688, 784, 3065, 2598, 3189, 3413]. Statist
[1266, 1066, 1034, 692, 693]. Statistical
[3934, 2816, 896, 3039, 2565, 3349, 815, 716, 851, 1698, 947, 2242, 1025, 585, 2242, 1025, 585.


time-dependent
[3536, 3822]. time-space [1680]. time-tested [3767]. Times
[2524, 941, 1620, 1982, 891]. Timestamp [2479]. timing [2479].
Tina [3477]. tiny [2119, 2743, 3460]. Tippett [43, 49, 28, 29]. TLP [902, 1033]. TLS
[3939, 3963]. TODAES [3545]. today [4041]. Together [3895]. Token
[2479]. Top [2532]. Top-Level [2532]. topics [931, 973]. Topologies [3447].
topology [2715]. Toss [3826, 1790]. Touted [2524]. tracing [1922].
Tract [70]. Traffic [505, 2756, 147, 3328]. Training [584]. trajectory
[590]. Transform [1887, 2323, 3871, 2912, 3186, 848, 1696, 3680, 3308, 3703]. Transformation
[654, 3301, 889, 3704, 1691, 718, 43, 923, 924, 1983, 2543, 2392, 1016].
Transformation-Based [3704]. Transformations
[296, 2269, 2172, 2595, 791, 3582, 1261, 194, 2028, 1718, 3277, 1249].
Transformed [2337, 1938, 805, 1826, 3062, 2703]. Transforming [2825].
transportation [3275]. transpositions [992]. Trapdoor [1094, 1049].
trapezoidal [3521]. Treatment [2669, 1850, 87]. tree [1278, 1308]. Trees
[1774, 1679, 1787, 1899, 1912, 1112, 1430, 1834]. Trends [3103, 1647]. Trial
[1183]. Trials [643, 687, 147, 393]. Triangle [4053]. triangles [2167].
Triangular [1405, 3355, 3636]. Trident [3408]. Trier [4068]. trigamma
[1705]. Trinomials [1723, 2191, 1997]. triple [2821, 2917]. triples
[2037, 2250, 2329]. trivariate [3970]. trivial [770]. TRNG
[3893, 3765, 3985, 3988]. TRNGs [3912, 3458]. Trojans [3663]. True
[2818, 3110, 2745, 3584, 3490, 3975, 3595, 3053, 3133, 2755, 3139, 2581, 3669, 1347, 3276, 3145, 3383, 2566, 3802, 3865, 3394, 3846, 3081, 3414, 3943, 3640, 3309, 2634, 3029, 3313, 3437, 3560, 3092, 3211, 2810, 3333, 3335, 3106, 3466, 3467, 3791, 3115, 3116, 3236, 3237, 3238, 3267, 3268, 3270, 3278, 2520, 3530, 3536, 3293, 3555, 3443, 3450, 3566, 3452, 3450, 3038, 3214, 3329]. Truly
[3241, 3503, 857, 2682, 3379, 3666, 1979, 537, 538, 3113, 3861, 2748, 3723, 2583, 600, 3630, 3693, 573, 629, 668]. Truncated [2898, 1537, 417, 1474, 853, 1342].
true [2346]. trustless [3850]. Trustworthy [3843]. trx [3843]. Tsallis
[3025]. Tucson [4024]. Tunable [3269, 2841]. Tuning [2809, 2882]. Tunnel
[3975]. tuples [2441]. Turán [2052, 656]. Turbo [3647, 1608, 1364].
[1398, 1154, 1615, 1711, 1451, 1086]. Tweedie [3789]. Twelfth [4075].
twentieth

twenty-eighth

twenty-second

twenty-fourth

twenty-sixth

Twin

twisters

twisting

Two-bit

Two-Dimensional

Two-Queue

Two-Sided

two-term

UHF

UHF-RFID

UK

Ultimate

ultracomputers

Ultrahigh-Speed

Ultrahigh

Unavoidable

Unbiased

uncertain

Unconditional

Unconstrained

Understanding

uniform

Uniform

Uniform-Gaussian

uniformément

uniform-distributed

uniforms

uniclone

Ultimate

Unique

units

unity

Univariate
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


This paper introduces the Klein–Nishina distribution of random numbers.


REFERENCES


REFERENCES


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


REFERENCES


Dixon:1944:FCP


Levene:1944:CMR


Onsager:1944:CST


Rice:1944:MAR


Wolfowitz:1944:ADR


Rice:1945:MAR


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Cameron:1952:RST


Goodman:1952:EPSa


Ore:1952:GCR


Tippett:1952:RSN


Anonymous:1953:RDa


Anonymous:1953:RDb


Anonymous:1953:RDc


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


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


REFERENCES

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


REFERENCES


REFERENCES


REFERENCES


[232] Donald D. Wall. A random number test for large samples. In Anonymous [3998], pages 7–11. LCCN ????


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Scheuer:1962:GNR


Shanks:1962:CD


Sibuya:1962:FCN


Spanier:1962:UAM


Todd:1962:SNA


Walsh:1962:HNS


Allard:1963:MCR


Anonymous:1963:BRBd

REFERENCES


Barnes:1963:CEG


Bolshev:1963:APT


DeMatteis:1963:SAP


Firestone:1963:CNU


Fisher:1963:STB


Franklin:1963:DSR


Gabai:1963:DCSa

REFERENCES


REFERENCES


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


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


REFERENCES

Tocher:1964:AS


Barker:1965:MCC


Barnett:1965:RNE


Franklin:1965:NSS


Golenko:1965:MSA


Greenberger:1965:MR


Hampton:1965:EUP


Hampton:1965:HAD

REFERENCES


REFERENCES

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

Pike:1965:ARN


Pike:1965:CAGb


Potter:1965:CNS


Pyke:1965:S


Reeves:1965:AUR


Rosenberg:1965:CNN


Scheinok:1965:DFR


Seshadri:1965:RVW

[370] V. Seshadri. On random variables which have the same distribution as their reciprocals. *Canadian mathematical bulletin = Bulletin canadien
de mathématiques, 8(??):819–824, ???? 1965. CODEN CMBUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[414] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [4004], pages 64–68. LCCN QA76.5 D55 1965.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

141

CODEN BRMIAC. ISSN 0005-7878. URL http://www.springerlink.com/content/16q4517x00r56955/.


[468] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [4005], pages 70–111. LCCN QA1 S565 v. 3.


REFERENCES


REFERENCES


Anonymous:1970:EWC


Anonymous:1970:FVP


Blaisdell:1970:RSP


Butler:1970:AAG

REFERENCES

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

[Cenacchi:1970:PRN]


[Dixon:1970:NSE]


[Downham:1970:SAA]


[Fuchs:1970:EDR]


[Good:1970:RPM]


[Haber:1970:NEM]

REFERENCES


REFERENCES

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


McShane:1970:RSE


Murry:1970:GAG


Payne:1970:FTP


Prasad:1970:PDA


Rader:1970:FMG


Reader:1970:RDM


Schaffer:1970:AAG

REFERENCES

49, January 1970. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES

153


Vincent:1970:CGT


Vincent:1970:GTR


White:1970:FDC


Zaremba:1970:DII


Ashford:1971:BRG


Berman:1971:GGD


Beyer:1971:LSM

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


Sowey:1972:CCB


Sullins:1972:CAP


Vincent:1972:CPA


Ahrens:1973:EFM


Ahrens:1973:NME


Burford:1973:BAC

REFERENCES


[646] G. P. Learmonth and P. A. W. Lewis. Naval Postgraduate School random number generator package LLRANDOM. Report NP555LW73061A, Naval Postgraduate School, Monterey, CA, USA, 1973. The shuffling algorithm proposed in this report does *not* lengthen the period, and only marginally reduces the lattice structure of linear congruential generators,
despite the apparently tiny difference with the [754] algorithm: see [1485] for a comparison, both mathematical, and graphical.


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


REFERENCES


1973. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).

Tsuda:1973:NIF


Vincent:1973:RGT


Adam:1974:CLS


Ahrens:1974:CMS


Alam:1974:SNT


Beasley:1974:CSR


Block:1974:CBE

REFERENCES


Brent:1974:AAG


Chen:1974:GRV


Cohn:1974:CRP


Coldwell:1974:CDS


Collins:1974:CTE


Dahlquist:1974:NM


Dieter:1974:URN

REFERENCES


REFERENCES


[694] Michel Mendès France. Suites de nombres au hasard (d’après Knuth). (French) [Sequences of random numbers (according to Knuth)]. *Sémin Théorie des Nombres*, 6(??):??, ???. 1974–1975. CODEN ???. ISSN ???


References


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES


REFERENCES


REFERENCES


[756] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [4013], pages 321–355. ISBN 0-12-697540-X. LCCN QA76.6 .SD195 1976. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.7959. The complexity of the binary Euclidean algorithm for the greatest common denominator is shown to be $O(0.705 \lg N)$ for large $N = \max(|u|, |v|)$. See [2488] for an update, and a repair to an incorrect conjecture in this paper. See also [2412], where the worst case
complexity is shown to be $O(\lg N)$, and the number of right shifts at most $2\lg(N)$.


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


ISSN 0010-485X (print), 1436-5057 (electronic). See [670].

0035-9254 (print), 1467-9876 (electronic).

[894] A. C. Atkinson. A family of switching algorithms for the computer gen-
CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL

[895] A. C. Atkinson. Recent developments in the computer generation of
CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic).

AS 134: The generation of beta random variables with one parameter
greater than and one parameter less than 1. Applied Statistics, 28(1):90–
93, March 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-9876

Gaussian, generalised hyperbolic, gamma, and related random variables.
Research reports — Department of Theoretical Statistics, University of
Aarhus; no. 52. Department of Theoretical Statistics, Institute of Math-
ematics, University of Aarhus, Arhus, Denmark, 1979. 48 (various) pp.
LCCN QA273.6 .A84.

[898] Niels Bache. Approximate percentage points for the distribution of a
product of independent positive random variables. Applied Statistics, 28
(2):158–162, 1979. CODEN APSTAG. ISSN 0035-9254 (print), 1467-
9876 (electronic).


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Pangratz:1979:PRN


Pavlov:1979:PNG


Reeds:1979:CMC


Ripley:1979:TRS


Roberts:1979:ITN


Rubin:1979:SCB


Sahai:1979:SSB

REFERENCES


REFERENCES


REFERENCES


Sahai:1980:SSB


Sampson:1980:NCD


Schmeiser:1980:ARM


Schmeiser:1980:BVG


Schmeiser:1980:GVD


Schmeiser:1980:RVGa


Schmeiser:1980:RVGb

REFERENCES


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


REFERENCES

Dudewicz:1981:HRN


Fishman:1981:SCM


Friedman:1981:NPP


Gentle:1981:PCR


Grafton:1981:SAA


Green:1981:BRBa


Greenwood:1981:PFA


REFERENCES


REFERENCES

[1014] B. W. Schmeiser and V. Kachitvichyanukul. Poisson random variate generation. Research Memorandum 81-4, School of Industrial Engineering, Purdue University, West Lafayette, IN, USA, 1981.


Blum:1982:HGC


Crigler:1982:RCP


Devroye:1982:NAR


DiDonato:1982:FSP


Dykstra:1982:MLE


Faure:1982:DSA

REFERENCES


REFERENCES


REFERENCES


Afflerbach:1983:LKG


Barel:1983:FHR


Barel:1983:UGG


Best:1983:NGV


Blum:1983:CTP

[1054] Lenore Blum, Manuel Blum, and Michael Shub. Comparison of two pseudorandom number generators. In Chaum et al. [4022], pages 61–
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Schmeiser:1983:RAG


Shamir:1983:GCS


VanEs:1983:RNG


Vazirani:1983:TPR


Banks:1984:DES


Blum:1984:HGC

REFERENCES


REFERENCES


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

Fishman:1984:SDD


Frederickson:1984:PRT


Frieze:1984:LCG


Gal:1984:OEC


Guinier:1984:RNS


Hamedani:1984:NLC


Heth:1984:PVP

REFERENCES

Kalle:1984:PRN

Kannan:1984:SPA

Kronmal:1984:ACA

Kuo:1984:SRI

Landauer:1984:ERN

Lugannani:1984:DRQ


REFERENCES


Thesen:1984:SER


Tolleth:1984:SSM


Ulrich:1984:CGD


Vazirani:1984:ESP


Whitney:1984:GTP


Wichmann:1984:SAC


Afflerbach:1985:CMR

REFERENCES


REFERENCES


REFERENCES


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


Gordon:1985:SSB


Griffiths:1985:ASA


Helfrich:1985:ACMa


Helfrich:1985:ACMb


Hill:1985:SAR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES

Kleijnen:1986:SRN


Ko:1986:NIP


LEcuyer:1986:EPB


Loukas:1986:CGB


Luby:1986:PRP


Malik:1986:PDF


Marsaglia:1986:IFC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Chiu:1987:SRS


Chung:1987:RWA


Collings:1987:CRN


Compagner:1987:MLS


Dagpunar:1987:NMS


Diaconis:1987:SAG

REFERENCES


 REFERENCES


REFERENCES


REFERENCES


REFERENCES


Salvat:1987:ARS


Schmidt:1987:VGF


Steele:1987:BRB


Stern:1987:SLC


Tezuka:1987:DGP


Tsang:1987:DTA


Ulrich:1987:MCG


Vaziranni:1987:SCC


Warnock:1987:RNG


Wichmann:1987:BRN


Afflerbach:1988:LSP


Afflerbach:1988:NRN


REFERENCES


Dudewicz:1988:TVF

[1335] Edward J. Dudewicz and Zaven A. Karian. TESTRAND for the VAX-
11 family of computers: a random-number generation and testing li-
ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic). URL http://

Durst:1988:TPR

[1336] Mark J. Durst. Testing parallel random number generators. In Weg-
man et al. [4048], pages 228–231. URL http://www.dtic.mil/dtic/
tr/fulltext/u2/a208838.pdf.

Edwards:1988:CAM

random number generators. In Wegman et al. [4048], pages 618–623.

Eichenauer:1988:MLTb

[1338] Jürgen Eichenauer and Harald Niederreiter. On Marsaglia’s lattice test
1988. CODEN MSMHB2. ISSN 0025-2611 (print), 1432-1785 (elec-
tronic).

Eichenauer:1988:MLTc

[1339] Jürgen Eichenauer, Holger Grothe, and Jürgen Lehn. Marsaglia’s lat-
tice test and non-linear congruential pseudo-random number generators.
1435-926X (electronic).

Eichenauer:1988:NCP

[1340] Jürgen Eichenauer, Jürgen Lehn, and Alev Topuzoğlu. A nonlinear con-
gruential pseudorandom number generator with power of two modulus.
MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL http://

Fishman:1988:MCR

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


[1348] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. In IEEE [4047], pages 12–24. CODEN ASF-
REFERENCES


REFERENCES

Heidelberger:1988:DES


Hong:1988:LGA


Izumi:1988:FGW


Kachitvichyanukul:1988:AHS


Kachitvichyanukul:1988:BRV


Kannan:1988:PFN

REFERENCES


[1367] Pierre L’Ecuyer and François Blouin. BonGCL, un logiciel pour la recherche de bons générateurs à congruence linéaire. (French) [BonGCL,

LEcuyer:1988:EPC


LEcuyer:1988:GLC


LEcuyer:1988:LCG


Levitan:1988:QSN


Luby:1988:HCP


Mactutus:1988:CSN

Matsumoto:1988:FPS


Minh:1988:GGV


Monahan:1988:CAG


Niederreiter:1988:LDL


Niederreiter:1988:RNC


Niederreiter:1988:SIN


Niederreiter:1988:SNC

Niederreiter:1988:STD


Ore:1988:NTH


Panton:1988:PPS


Park:1988:RNG


Percus:1988:LRC


Petersen:1988:SVR


Reif:1988:EPP

REFERENCES


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


Ahrens:1989:AMS


Ahrens:1989:HAL


Ahrens:1989:NUR


Ahrens:1989:NUR


Aiello:1989:HIG


Allender:1989:SCE

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kharitonov:1989:LBP


Kim:1989:PRP


Kleijnen:1989:PNG


Komo:1989:MLP


Koniges:1989:PPR


Korolev:1989:ANA

REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kinderman:1990:CCG


Korolev:1990:ADR


Koutras:1990:TCN


Krawczyk:1990:HPC


Lagarias:1990:PNG


LEcuyer:1990:RNS


REFERENCES


REFERENCES

Norton:1990:AAE


Oommen:1990:GRP


Oyanagi:1990:SPR


Palmore:1990:CAC


Parrish:1990:GRD


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


Silvio Micali 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


[1655] Terry Ritter. The efficient generation of cryptographic confusion sequences. *Cryptologia*, 15(2):81–139, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://fizz.sys.uea.ac.uk/~rs/ritter.html; http://www.ciphersbyritter.com/ARTS/CRNG2ART.HTM; http://www.informaworld.com/smpp/content~content=a741902748~db=all~order=page. cryptographic confusion sequences; pseudo-random sequence; random number generators; cryptographic applications; random sequences; incompleteness theorem; deterministic implementation; external analysis; RNG comparison; chaos; 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


REFERENCES


REFERENCES

Bays:1992:IRN


Bellido:1992:SBR


Berdnikov:1992:RNG


Binder:1992:MCS


Bratley:1992:ITL


Brenner:1992:PRL


REFERENCES


Canfield:1992:RARb


Carroll:1992:CCE


Collins:1992:RNG


Dai:1992:BSD


DalleMolle:1992:HOC


REFERENCES


Dougherty:1992:OMS


Dougherty:1992:OMSb


Ehrenfeucht:1992:PSH


Eichenauer-Herrmann:1992:ASI


Eichenauer-Herrmann:1992:CIC


Eichenauer-Herrmann:1992:ICP

Eichenauer-Herrmann:1992:LBD


Eichenauer-Herrmann:1992:NIC


Eichenauer-Herrmann:1992:RDQ


Engel:1992:RRP


Faure:1992:GPE


Ferrenberg:1992:MCS


Louchard:1992:DAD


Maclaren:1992:LUL


Makino:1992:GSR


Marsaglia:1992:MRN


Mason:1992:ACA


Matsumoto:1992:TGG


Maurer:1992:UST


Ressler:1992:RLP


Savir:1992:MSL


Schneier:1992:PRS


Sedgewick:1992:AC


Sezgin:1992:SCC


Sharp:1992:RPR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Chen:1993:PGH

Couture:1993:DDV

Damgaard:1993:ACE

DeMatteis:1993:LRC

Devroye:1993:GRI

Devroye:1993:RVG
REFERENCES

Dobkin:1993:CD


Dufour:1993:IEB


Eichenauer-Herrmann:1993:DIC


Eichenauer-Herrmann:1993:EIC


Eichenauer-Herrmann:1993:EPN


Eichenauer-Herrmann:1993:ICP


Eichenauer-Herrmann:1993:KTS

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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Lee:1993:GRB


Li:1993:IKC


Lin:1993:NCP


Loparo:1993:LER


Makino:1993:SPR


Marsaglia:1993:LHR

REFERENCES


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.


REFERENCES

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

[Niederreiter:1993:FPS]


[Niederreiter:1993:LRP]


[Niederreiter:1993:PNQ]


[NIST:1993:FPS]


[Park:1993:ATR]

[1862] Stephen K. Park, Keith W. Miller, and Paul K. Stockmeyer. Another test for randomness: Response. *Communications of the ACM*, 36(7):108–110, July 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [1384, 1492, 1847, 1872]. The authors report that they would now recommend the MCG \( x_{n+1} = 48 \, 271 \, x_n \mod (2^{31} - 1) \) over their original \( x_{n+1} = 16 \, 807 \, x_n \mod (2^{31} - 1) \).

[Pollard:1993:FCI]

Rajasekaran:1993:FAG


Saarinen:1993:RNT


Schrift:1993:UTN


Selke:1993:CFM


Sharp:1993:PRN


Sherif:1993:DTN


Sloan:1993:BRB

REFERENCES

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


REFERENCES


REFERENCES


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.


Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic randomness from air turbulence in disk drives. In Desmedt [4085], pages
REFERENCES


DeArmon:1994:RLO


Deng:1994:DIR


Devroye:1994:NHS


Eastlake:1994:RRR


Eichenauer-Herrmann:1994:BES


Eichenauer-Herrmann:1994:CNC


REFERENCES


Hartel:1994:CRN

Hellekalek:1994:GDEa

Hellekalek:1994:GDEb

Hennecke:1994:RER

Hildebrand:1994:RWS

Hill:1994:CMR


REFERENCES


[1941] F. James. RANLUX: a Fortran implementation of the high-quality pseudorandom number generator of Lüscher. Computer Physics Communications-


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/mtnvin1.html. This article describes the Maple-language random-number generator, a multiplicative congruential generator \((x_{\text{new}} = (A \times x + C) \mod P)\) 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.


Luscher:1994:PHQ


Ma:1994:IMC


MacLaren:1994:CPN


Makino:1994:LFR


Marsaglia:1994:MAR


Marsaglia:1994:REI


Marsaglia:1994:SPV

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

Mascagni:1994:FHQ


Mascagni:1994:PPN


Matsumoto:1994:TGG


McGrath:1994:SAB


Niederreiter:1994:NCP


Niederreiter:1994:PVG


Odlyzko:1994:PKC

REFERENCES


REFERENCES


REFERENCES

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

Rivest:1994:DBI


Schneier:1994:AAd


Shallit:1994:ALS


Shukhman:1994:GQR


Sitharam:1994:PGL


Sorenson:1994:TFG


Spanier:1994:QRM

REFERENCES


REFERENCES


REFERENCES

Barnes:1995:APE

Baum:1995:CCP

Bellare:1995:XMN

Bowman:1995:EPR

Carrasco:1995:RRT

Chen:1995:IDP

Childs:1995:CIH
[2020] Wun-Seng Chou and Harald Niederreiter. On the lattice test for inversive
congruential pseudorandom numbers. In Niederreiter and Shiue [4094],
1995.

1036 (print), 1730-6264 (electronic).

[2022] Chee-Seng Chow and Amir Herzberg. Network randomization protocol:
a proactive pseudo-random generator. In USENIX [4095], pages 55–64 (or

*Physical Review E (Statistical physics, plasmas, fluids, and related
interdisciplinary topics)*, 52(5):5634–5645, November 1995. CO-
DEN PLEEE8. ISSN 1539-3755 (print), 1550-2376 (electronic). URL

[2024] Raymond Couture and Pierre L’Ecuyer. Linear recurrences with
carry as random number generators. In Alexopoulos et al. [4090],
pages 263–267. CODEN WSCPDK. ISBN 0-7803-3018-8, 0-7803-
3017-X. ISSN 0275-0708, 0743-1902. LCCN QA76.9.C65 W56
jsp?punumber=3475. IEEE Catalog No. 95CB35865.

[2025] T. W. Cusick. Properties of the $x^2 \bmod N$ pseudorandom number gener-
1995. CODEN IETTAW. ISSN 0018-9448 (print), 1557-9654 (electronic).


REFERENCES


REFERENCES

Hormann:1995:RTS


Kaliski:1995:MIA


Kessler:1995:GOC


Koc:1995:RCS


Kubota:1995:DRE


Kurita:1995:DWD


Lee:1995:CSS


Pattanaik:1995:AER


Penrice:1995:AEP


Percus:1995:TAM


Phatak:1995:LMP


Pickover:1995:GET


Pickover:1995:RNG

REFERENCES


Takashima:1995:STT


Tezuka:1995:URN


Varhol:1995:ANS


Vattulainen:1995:CSS


Vattulainen:1995:MIF


Vattulainen:1995:PMT

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


Ogawa:1996:RRP


Paplinski:1996:HIL


Petrov:1996:LTP


Radovic:1996:QMC


Rubin:1996:OTP


Sanchis:1996:PAC

REFERENCES


Sipper:1996:CEP


Sipper:1996:GPR


Takashima:1996:HWT


Takashima:1996:LVT


Takashima:1996:STT


Ugrin-Sparac:1996:NAG


Ugrin-Sparac:1996:PET

[2220] G. Ugrin-Šparac and D. Ugrin-Šparac. On a possible error of type II in statistical evaluation of pseudo-random number genera-
Wallace:1996:FPG


Wang:1996:LIL


Wegenkittl:1996:RSP


Alon:1997:SSD


Aluru:1997:LFR

REFERENCES

Annexstein:1997:GBS


Arvind:1997:RBM


Athanasiu:1997:SGP


Baker:1997:NPU


Balakrishnan:1997:ASW


Bellare:1997:PRN

REFERENCES

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


REFERENCES

Eichenauer-Herrmann:1997:CCC


Eichenauer-Herrmann:1997:ICP


Eichenauer-Herrmann:1997:PSN


Eichenauer-Herrmann:1997:QCP


Emmerich:1997:EPQ


[2266] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [4106], page ?? ISBN 3-901608-11-7. LCCN ???
REFERENCES


\[
\begin{align*}
\text{#define } & \text{znew } ((z=36969*(z\&65535)+(z\&\sim16))\sim16) \\
\text{#define } & \text{wnew } ((w=18000*(w\&65535)+(w\&\sim16))\&65535) \\
\text{#define } & \text{IUNI } (znew+wnew) \\
\text{#define } & \text{UNI } (znew+wnew)*4.656613e-10 \\
\text{static unsigned } & \text{long } z=362436069, w=521288629; \\
\text{void setseed(} & \text{unsigned long i1,unsigned long i2)} \\
\text{z=}&i1; \text{w=}&i2; \text{Whenever you need random integers or random reals in your C program, just insert those six lines at (near?) the beginning of the program. In every expression where you want a random real in [0, 1) use UNI, or use IUNI for a random 32-bit integer. No need to mess with ranf() or ranf(lastI), etc, with their requisite overheads. Choices for replacing the two multipliers 36969 and 18000 are given below. Thus you can tailor your own in-line multiply-with-carry random number generator.”.
\end{align*}
\]


REFERENCES


REFERENCES

Woodward:1997:ECD

Wu:1997:MCR

Zubkov:1997:PTD

Aiello:1998:DPP

Andreev:1998:NGD

Antoch:1998:RPN
REFERENCES


REFERENCES


REFERENCES

Couture:1998:GEI


DSouza:1998:SBD


Eichenauer-Herrmann:1998:IUB


Eichenauer-Herrmann:1998:LBD


Eichenauer-Herrmann:1998:SQI


Ellison:1998:CRN


Emmerich:1998:EPC

REFERENCES


[2338] A. Fuster-Sabater and L. J. Garcia-Villalba. Likelihood that a pseudorandom sequence generator has optimal properties. Electronics Let-


REFERENCES


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


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

Kolmogorov:1998:TRN


Larcher:1998:DPS


LEcuyer:1998:GPI


LEcuyer:1998:RNGa


LEcuyer:1998:RNGb


LEcuyer:1998:RNGb


REFERENCES

(3):1–8, 1998. CODEN JSSOBK. ISSN 1548-7660. URL http://www.jstatsoft.org/v03/i03; http://www.jstatsoft.org/v03/i03/GERMGAM.PDF; http://www.jstatsoft.org/v03/i03/GERMGAM.PS; http://www.jstatsoft.org/v03/i03/updates.


REFERENCES


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


REFERENCES


Schatte:1998:BLV


Schmid:1998:SNN


Schneier:1998:YSP


Shchur:1998:RGR


Soto:1998:STR


Sugita:1998:LTS

REFERENCES


vanHameren:1998:GLD


Wegenkittl:1998:THS


Wheeler:1998:CX


Williams:1998:ELP


Williamson:1998:CNR


Wolf:1998:RWP


REFERENCES


Entacher:1999:QMC


Falk:1999:SAG


Fernandez:1999:AER


Fernandez:1999:ANRa


Fernandez:1999:ANRb


Gartner:1999:PCP


Gartner:1999:RCZ

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


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


REFERENCES


REFERENCES

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


REFERENCES


[2482] Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, Accumulate, Add, and Count) is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.


REFERENCES


REFERENCES


Hormann:2000:ARV


IEEE:2000:IPH


Impagliazzo:2000:EPR


Indyk:2000:SDP


Iwata:2000:PAF


Mansharamani:2000:RTG


Marsaglia:2000:ADS


Marsaglia:2000:MRN

[2524] George Marsaglia. The monster, a random number generator with period over $10^{2857}$ times as long as the previously touted longest-period one. Technical report ????, Florida State University, Tallahassee, FL, USA, ????. 2000.

Marsaglia:2000:SMG


Marsaglia:2000:ZMG


Mascagni:2000:ASS

REFERENCES

DEN ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL http://doi.acm.org/10.1145/358407.358427. See correction [2528].

Mascagni:2000:CAS


Mauduit:2000:FPBa


Mauduit:2000:FPBb


Miles:2000:L


Moriai:2000:PTL


Niederreiter:2000:DPN

Niederreiter:2000:ESD


Niederreiter:2000:IES


Nishimura:2000:TBM


NIST:2000:RNG


Panneton:2000:GNA


Petrie:2000:NBI


Proykova:2000:HIR

REFERENCES


Stefanescu:2000:GUR


Stefanov:2000:OQR


Sugita:2000:RWS


Takashima:2000:HPR


Tomassini:2000:GHQ


Viswanath:2000:RFS


REFERENCES


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

[Battaglia:2001:GAP]


[Batu:2001:TRV]


[Chamayou:2001:PRN]


[Chen:2001:ING]


[Chick:2001:NPS]


[Chowdhury:2001:ESI]

REFERENCES


REFERENCES


[2584] Richard J. Gonsalves. Pivot algorithm for self-avoiding walks on a square lattice. Fortran program, 2001. URL http://www.physics.buffalo.edu/gonsalves/phy411-506_spring01/files/Chapter12/saw.f. The program contains code (near the end) for the portable rannyu() generator. It is a linear congruential generator with multiplier $A = 3167285 = 0x1d9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.


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


REFERENCES


REFERENCES


LEcuyer:2001:RN


LEcuyer:2001:RNG


LEcuyer:2001:SUR


LEcuyer:2001:TSL


Lee:2001:PBG


Lemieux:2001:SCL

REFERENCES


REFERENCES


RAND:2001:MRD


Raqab:2001:ELS


Rukhin:2001:STS


Rukhin:2001:TRS


Schindler:2001:EOT


Stojanovski:2001:CBRb


Sudan:2001:PGX


Swartz:2001:NTR


Talim:2001:CRW


Tan:2001:PPR


Tang:2001:SAS

Touzin:2001:GRM

[2647] Renée Touzin. Des générateurs récursifs multiples combinés rapides avec des coefficients de la forme $\pm 2^{p_1} \pm 2^{p_2}$. (French) [Fast combined multiple recursive generators of the form $\pm 2^{p_1} \pm 2^{p_2}$]. Thèse (M.Sc.), Département d’informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2001. xiii + 128 pp. Mémoire présenté à la faculté des études supérieures en vue de l’obtention du grade de Maître ès sciences (M.Sc.) en informatique option recherche opérationnelle.

Trevisan:2001:EPG


Tu:2001:NFG


Vadhan:2001:OP


Vanura:2001:ARC


Watkins:2001:ERN


Wegenkittl:2001:GTP


REFERENCES


Brent:2002:SUN


Brillhart:2002:FHP


Cameron:2002:HDM


Choe:2002:FRT


Churchhouse:2002:CCJ


Delfs:2002:ICP


REFERENCES


REFERENCES


Janke:2002:PRN

Jeruchim:2002:FRV

Jeruchim:2002:MCS

Jones:2002:KTP

Karras:2002:SPB


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

Marsaglia:2002:SDP


Martin:2002:ARN


Martinez:2002:CSH


Matsumoto:2002:NTW


Maurer:2002:IRS

REFERENCES


[2717] Mark R. V. Murray. An implementation of the Yarrow PRNG for FreeBSD. In USENIX [4139], pages 47–53. ISBN 1-880446-02-


REFERENCES


Umans:2002:PRG

Wang:2002:HOL

Wang:2002:NCT

Wu:2002:BPR

Yaguchi:2002:CLP

Yao:2002:CBR
REFERENCES


[2744] Anonymous. /dev/random. Web site., June 8, 2003. From the site: “Thus, in 1994 noted Linux kernel hacker Theodore Ts’o wrote a driver for Linux, which takes information about hard to predict events like keyboard and mouse use, packet and disk drive timings, and so on, and uses it to seed a cryptographically secure random number generator. A process can then open up the ‘file’ /dev/random (usually a character device), and read out random bytes. The driver keeps an estimate of how much entropy remains in the pool — if it goes below 0 then any reads will block until more entropy is added.” Also this: “the actual driver is implemented in drivers/char/random.c in the Linux source tree.”.


REFERENCES


[2749] Diane Crawford, Simone Santini, Ralph Castain, William F. Dowling, John Cook, Simon Dobson, Peter J. Denning, Robert Dunham, Jef Raskin, and Dennis Tsichritzis. Forum: When is a computer more like a guitar than a washing machine?; corroboration the only way to determine Web accuracy; how to teach critical thinking about Web content; create a random number service based on the Mersenne Twister; make fair uses a legal requirement in DRM systems; “The Missing Customer” redux; enthusiasm, drive, wisdom, patience not tied to age. Communications of the ACM, 46(7):11–13, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


REFERENCES


[2759] Oded Goldreich and Vered Rosen. On the security of modular exponentiation with application to the construction of pseudorandom genera-
Gonnet:2003:RTT


Goresky:2003:EMC


Grabner:2003:CGD


Guimond:2003:SPI


Gutierrez:2003:LNC


Hellekalek:2003:EEC

Hernandez:2003:FED


Hill:2003:UPO


Hitchcock:2003:HMH


Hormann:2003:CRV


Intel:2003:IRN


Joe:2003:RAI

REFERENCES


REFERENCES


REFERENCES


Anonymous:2004:RNG


Anonymous:2004:TRR


Bauke:2004:PRC


Beebe:2004:CJR


Bellare:2004:CBG


Blacher:2004:SCA


Borwein:2004:MEP

REFERENCES


REFERENCES


REFERENCES


[2841] Daniel R. Jeske and Todd Blessinger. Tunable approximations for the mean and variance of the maximum of heterogeneous geometrically dis-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Banks:2005:DES

Barak:2005:MAP

Beliakov:2005:CLR

Beliakov:2005:UNR

Benony:2005:CPC

Blackburn:2005:PNP

Bogdanov:2005:PGL


Calvayrac:2005:RNG


Castro:2005:NRG


Contini:2005:SAA


Damgaard:2005:CRM

[2899] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. Lecture Notes in Computer
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2948] Janusz Stoklosa and Jaroslaw Bubicz. Compound inversive congruential generator as a source of keys for stream ciphers. In Hamid R. Arab-
REFERENCES


REFERENCES

Wichmann:2005:GGP


Wiese:2005:IPN


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ

REFERENCES


REFERENCES


REFERENCES

535


REFERENCES


[3003] Dong-U Lee, John D. Villasenor, Wayne Luk, and Philip H. W. Leong. A hardware Gaussian noise generator using the Box–Muller method and


REFERENCES


REFERENCES


REFERENCES


Brown:2007:SAN


Cheung:2007:HGA


Chiu:2007:CKC


Cowles:2007:BRB


Delfs:2007:ICP

REFERENCES


Edgington:2007:RT


Gerlovina:2007:LBS


Gutierrez:2007:ISP


Haramoto:2007:EJA


Hars:2007:PRS

Hasan:2007:FSU


Hormann:2007:ITD


Hormann:2007:SGD


Juneja:2007:AFS


Kang:2007:PFS


Kundu:2007:CWG

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Alimohammad:2008:CAG


Alimohammad:2008:EAH


Alioto:2008:APE


Alvarez:2008:ETR


Attya:2008:ROC

REFERENCES

Bader:2008:DFP


Balachandran:2008:TRN


Banks:2008:FIP


Basu:2008:CCE


Beirami:2008:PMD


Bello:2008:OPR

REFERENCES


Collins:2008:TSI


Cordero:2008:DPV


Das:2008:ASS


Deng:2008:DIE


Deng:2008:ICS


Deng:2008:IRN


Drutarovsky:2008:CSC

M. Drutarovsky and M. Varchola. Cryptographic system on a chip based on Actel ARM7 soft-core with embedded true random number genera-


REFERENCES


[3150] Stephen Joe and Frances Y. Kuo. Constructing Sobol’ sequences with better two-dimensional projections. *SIAM Journal on Scientific Com-


REFERENCES


Katz:2008:RRNa


Katz:2008:RRNb


Kiessler:2008:BRBe


Killmann:2008:DPR


Kim:2008:TRG

Kolokotronis:2008:CPN


Langdon:2008:FHQ


LEcuyer:2008:CPS


Lee:2008:HAS


Lee:2008:PRN


Leiva:2008:RNG

REFERENCES


REFERENCES


McCullough:2008:MEW


Miller:2008:OSB


Moler:2008:NCM


Murdoch:2008:VRV


Murphy:2008:CLW


Nandakumar:2008:EET


Nguyen:2008:ODD


REFERENCES


REFERENCES


Tokunaga:2008:TRN


Toyama:2008:GPR


Uchida:2008:FPR


Udawatta:2008:TVN


Varbanets:2008:ESS


Varbanets:2008:ICGa

REFERENCES


REFERENCES

Wold:2008:AER


Xiang:2008:NPR


Xu:2008:SMS


Yaguchi:2008:NNP


Yang:2008:LLM


Yang:2008:NTR

REFERENCES


Alhakim:2009:MSG


Anyanwu:2009:DCS


Awerbuch:2009:RRN


Aycock:2009:COU


Bastos-Filho:2009:IQR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Holcomb:2009:PSS


Hornfeck:2009:MCG


Hu:2009:TRN


Jun:2009:HPP


Kanter:2009:OUR


Katti:2009:EHI


McCullough:2009:AES


Mitchum:2009:DPR


Mustafa:2009:DPR


Nakura:2009:ROB


Nandi:2009:ISA


Nekrutkin:2009:STS


Qiu:2009:CMW


Reidler:2009:USR


Ridout:2009:GRN


Santoro:2009:FEF


Santoro:2009:LMR


Sindhikara:2009:BSS

REFERENCES


Srinivasan:2009:BPV


Sun:2009:CPR


Svozil:2009:TCQ


Tafazzoli:2009:PCE


Tang:2009:FPS

REFERENCES


[3323] Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authentication protocol based on infinite dimension pseudo random number
REFERENCES


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


Wold:2009:OST


Xiao-chen:2009:URN


Yamanashi:2009:SRN


Youssef:2009:IEU


Yu:2009:ESC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3373] Ariel Gabizon. Deterministic Extraction from Weak Random Sources. Monographs in theoretical computer science. Springer-Verlag, Berlin,
REFERENCES


Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei. Truly random number generation based on measurement of phase noise of a laser. *Physical Re-
view E (Statistical physics, plasmas, fluids, and related interdisciplinary
topics), 81(5):051137, May 2010. CODEN PLEEE8. ISSN 1539-3755
1103/PhysRevE.81.051137.

[3380] C. Guyeux, Qianxue Wang, and J. M. Bahi. Improving random number
generators by chaotic iterations application in data hiding. In 2010 In-
ternational Conference on Computer Application and System Modeling
(ICCASM), volume 13, pages V13–643–V13–647. IEEE Computer So-
ciety Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
USA, 2010. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?
tp=&arnumber=5622199.

[3381] Iftach Haitner, Omer Reingold, and Salil Vadhan. Efficiency improve-
ments in constructing pseudorandom generators from one-way func-
tions. In ACM [4173], pages 437–446. ISBN 1-60558-817-2. LCCN
63314455x..

[3382] Kenta Hongo, Ryo Maezono, and Kenichi Miura. Random number gen-
erators tested on quantum Monte Carlo simulations. Journal of Compu-
tational Chemistry, 31(11):2186–2194, August 2010. CODEN JCCHDD.
ISSN 0192-8651 (print), 1096-987X (electronic).

testing of true random number generators through dynamic reconfigu-
ration. In 2010 13th Euromicro Conference on Digital System Design:
Architectures, Methods and Tools (DSD), pages 247–250. IEEE Com-
puter Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
jsp?tp=&arnumber=5615649.

rem for sums of independent identically distributed random variables.
Journal of Mathematical Physics, 51(1):015208, January 2010. CODEN
JMAPAQ. ISSN 0022-2488 (print), 1089-7658 (electronic), 1527-2427.
URL http://jmp.aip.org/resource/1/jmapaq/v51/i1/p015208_s1.


REFERENCES


[3396] Lan Luan. The pseudo-random code generator design based on FPGA. In *2010 International Conference on System Science, Engineering Design and Manufacturing Informatization (ICSEM)*, volume 2, pages 282–284. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver
REFERENCES

605


Luo:2010:PAE


Maaref:2010:GVR


Marsaglia:2010:SKR


Marton:2010:RDC


Meka:2010:PGP


Moghadam:2010:DRN


Ostafe:2010:DGS


Ostafe:2010:MPP


Ostafe:2010:PNH


Ostafe:2010:PNM


Panneton:2010:RSR


Pareschi:2010:ITH

[3414] F. Pareschi, G. Setti, and R. Rovatti. Implementation and testing of high-speed CMOS true random number generators based on chaotic systems.
Pashley:2010:GRN


Passerat-Palmbach:2010:RIG


Peris-Lopez:2010:CSP


Plesser:2010:RSI


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3471] Araneus Information Systems Oy. Araneus Alea I. Web site, 2011. URL http://www.araneus.fi/products-alea-eng.html. From the Web site: “The Alea I uses a reverse biased semiconductor junction to generate wide-band Gaussian white noise. This noise is amplified and digitized using an analog-to-digital converter. The raw output bits from the A/D converter are then further processed by an embedded microprocessor to combine the entropy from multiple samples into each final
random bit and remove any bias caused by imperfections in the noise source and A/D converter.”.

[Bahi:2011:DFC]


[Bahi:2011:ECS]


[Barash:2011:ADD]


[Barash:2011:RPL]


[Baudet:2011:SOB]


REFERENCES


REFERENCES


Hwang:2011:SID


Jian:2011:TBQ


Kao:2011:EAT


Kleimo:2011:RNG


Koucky:2011:PGG


LEcuyer:2011:AZV

REFERENCES


REFERENCES


[3544] Carolyn L. Phillips, Joshua A. Anderson, and Sharon C. Glotzer. Pseudorandom number generation for Brownian Dynamics and Dissipative Par-


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. [4186], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????

REFERENCES


Seyedzadeh:2011:IES


Shaolan:2011:EDE


Shparlinski:2011:ADP


Simard:2011:CTS


Sinescu:2011:ECS


Soucarros:2011:ITT

generators. In 2011 IEEE International Symposium on Hardware-
Oriented Security and Trust (HOST), pages 24–27. IEEE Computer
Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
USA, 2011. URL http://ieeexplore.ieee.org/stamp/stamp.jsp?
.tp=&arnumber=5954990.

64-bit finalizer. Blog on “Twiddling the Bits”, September 28,
2011. URL http://zimbry.blogspot.com/2011/09/better-bit-
mixing-improving-on.html.

[3558] M. Stipcevic. Quantum random number generators and their use in
cryptography. In 2011 Proceedings of the 34th International Convention
MIPRO, pages 1474–1479. IEEE Computer Society Press, 1109 Spring
Street, Suite 300, Silver Spring, MD 20910, USA, 2011. URL http://
ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967293.

[3559] A. Suciu, D. Lebu, and K. Marton. Unpredictable random number gen-
erator based on mobile sensors. In 2011 IEEE International Conference
on Intelligent Computer Communication and Processing (ICCP), pages
445–448. IEEE Computer Society Press, 1109 Spring Street, Suite 300,
org/stamp/stamp.jsp?tp=&arnumber=6047913.

Gbit/s generation of superconductive true random number generator.
2011. CODEN ITASE9. ISSN 1051-8223 (print), 1558-2515 (elec-
arnumber=5674104.

[3561] T. Symul, S. M. Assad, and P. K. Lam. Real time demonstration of
high bitrate quantum random number generation with coherent laser
APPLAB. ISSN 0003-6951 (print), 1077-3118 (electronic), 1520-8842.
URL http://apl.aip.org/resource/1/applab/v98/i23.


REFERENCES

Wang:2011:CRN

Wang:2011:LTA

Wang:2011:MPF

Wei:2011:HSB

Wikramaratna:2011:CIM

Wu:2011:TEH


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Horstmann:2012:JEC


Horvath:2012:ARM


Horvath:2012:EGP


Impagliazzo:2012:PS


Kaczynski:2012:BNR


Kaczynski:2012:NRV

[3616] W. Kaczynski, L. Leemis, N. Loehr, and J. McQueston. Nonparametric random variate generation using a piecewise-linear cumulative distribu-


[3622] Y. Li, P. Chow, J. Jiang, M. Zhang, and S. Wei. Software/hardware framework for generating parallel Gaussian random numbers based on

Li:2012:TST

[3623] Liang Li. Testing several types of random number generators. MS thesis, Department of Computer Science, Florida State University, Tallahassee, FL, USA, Fall 2012. vi + 91 pp. URL http://search.proquest.com/pqdtglobal/docview/1287745850/.

Manssen:2012:RNG


Marandi:2012:AOQ


Marquardt:2012:PNG


Mascagni:2012:PRN

REFERENCES

Masse:2012:RNS


Miles:2012:SPN


Miszczak:2012:GUT


Molina-Gil:2012:PGS


Nandapalan:2012:HPP


Nazzal:2012:UGA

REFERENCES


REFERENCES


[3663] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL http://people.umass.edu/gbecker/BeckerChes13.pdf.
REFERENCES

[Beliakov:2013:EIBa]

[Beliakov:2013:EIBb]

[Claessen:2013:SPN]

[Deng:2013:FTQ]

[Ducklin:2013:ARN]
REFERENCES


REFERENCES


REFERENCES


Mukhopadhyay:2013:RBI


Ozkaynak:2013:SPP


Pae:2013:EOR


Sainudiin:2013:PER


Saito:2013:VMT


Schretter:2013:DIM

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

Sezgin:2013:FBP


Stroustrup:2013:CPL


Thomas:2013:LSF


Thomas:2013:PGG


Xi:2013:LTB


Zhu:2013:NIC


REFERENCES


Baron:2014:LSP


Blacher:2014:PRN


Braverman:2014:PGR


Brown:2014:DRN


Chen:2014:EES


Cheng:2014:GBR


REFERENCES


Gomez-Perez:2014:AEA


Haigh:2014:ABE


Healey:2014:SPS


Hormann:2014:GGI


Hosseini:2014:GPR


Hu:2014:MBA

[3729] Jiaqiao Hu, Enlu Zhou, and Qi Fan. Model-based annealing random search with stochastic averaging. ACM Transactions on Modeling and
Kawai:2014:ADT


Koo:2014:CRB


Korzen:2014:PPP


Langr:2014:APP


LEcuyer:2014:LSS


Ling:2014:MDN

Liu:2014:LFP


Mascagni:2014:HPC


Mohamed:2014:MCS


Mortari:2014:MAV


Raaphorst:2014:CSC


REFERENCES

Beznosko:2015:HSH


Beznosko:2015:PPF


Carlet:2015:EBF


Claessen:2015:GCR


Guyeux:2015:ECS


Haeupler:2015:SFD


REFERENCES

Lubicz:2015:TOB


Malik:2015:RCL


Malkiel:2015:RWW


Miles:2015:CCP


Miles:2015:SPN


Mortari:2015:VAS


REFERENCES

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


REFERENCES


REFERENCES

Balkova:2016:APN


Bayon:2016:FME


Chang-Fong:2016:CSC


Chattopadhyay:2016:ETS


Chen:2016:PEP


deanRade:2016:RNG

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


Lao:2016:BFD


Lecuyer:2016:ALB


Li:2016:ITS


Li:2016:MUN


Liu:2016:PBG


Losego:2016:SMW


Malik:2016:GRN

REFERENCES

Mandal:2016:DIW


Mandal:2016:FRI


McFarland:2016:MZA


Miller:2016:RPS


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA

REFERENCES


[3824] 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 [3832] for details of the attack.


[3827] George Barmpalias, Douglas Cenzer, and Christopher P. Porter. The probability of a computable output from a random oracle. *ACM Trans-


REFERENCES

Kuhl:2017:HRV


Lampropoulos:2017:BLI


LeCuyer:2017:HRN


Lenstra:2017:TPR


Liu:2017:ESG


Monroe:2017:NPR


Nordrum:2017:TRN

REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

SoltaniPanah:2019:CDG


Steele:2019:UBP


Ueno:2019:TBP


Viola:2019:CEP


Xu:2019:NPF


Zhang:2019:REU


Anonymous:2020:X

xorshift+, xoshiro, and xoroshiro, with comments about which common test suites they pass or fail. Lua 5.4 changed from the previous default of C’s rand() or random() to a new one based on xoshiro256** (256-bit state, 32- or 64-bit result). The period of xoshiro256** is \(2^{256} - 1\) (about \(10^{77}\)). See [3862, 3863].


REFERENCES


Stpiczynski:2020:ALB


Vigna:2020:POR


AlmarazLuengo:2021:RSR


Arroyo:2021:ARI


Blackman:2021:SLP

REFERENCES


[3943] Adriaan Peetermans, Vladimir Rozić, and Ingrid Verbauwhede. Design and analysis of configurable ring oscillators for true random number
REFERENCES


[3950] Ikram Ullah, Naveed Ahmed Azam, and Umar Hayat. Efficient and secure substitution box and random number generators over Mordell el-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Zheng:2022:BCS

AlmarazLuengo:2023:GPR

Chatterjee:2023:FFT

Cicek:2023:NRW

Dupin:2023:AIR

Giles:2023:AIC


REFERENCES


[3991] 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.


REFERENCES


Anonymous:1969:CPP


Bose:1970:EPS


Rice:1971:MS


Zaremba:1972:ANT


Schaffner:1974:PPB


Patil:1975:MCS


[4016] M. A. H. Dempster, editor. Stochastic programming: proceedings of an international conference sponsored by the Institute of Mathematics and
REFERENCES


Oren:1980:SDM


Eddy:1981:CSS


Rubinstein:1981:SMC


Grossmann:1982:PSI


IEEE:1982:ASF


Chaum:1983:ACP


REFERENCES

710


REFERENCES

www.acm.org/pubs/contents/proceedings/simulation/318242/.

[4039] ACM, editor. Proceedings of the nineteenth annual ACM Symposium on
LCCN QA 76.6 A13 1987. ACM order number 508870.

EUROCRYPT ’87: Workshop on the Theory and Application of Cryp-
tographic Techniques, Amsterdam, The Netherlands, April 13–15, 1987:
Proceedings, volume 304 of Lecture Notes in Computer Science. Spring-
er-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,

Cryptology yesterday, today, and tomorrow. The Artech House communi-
cation and electronic defense library. Artech House Inc., Norwood, MA,
US$60.00. First volume of selected papers from issues of Cryptologia.

[4042] IEEE, editor. 28th annual Symposium on Foundations of Computer Sci-
ence, October 12–14, 1987, Los Angeles, California. IEEE Computer
Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
USA, 1987. CODEN ASFPDV. ISBN 0-8186-0807-2, 0-8186-4807-4 (mi-
crofiche), 0-8186-8807-6 (casebound). ISSN 0272-5428. LCCN QA 76
S979 1987. IEEE Catalog no. 87CH2471-1. Computer Society order num-
ber 807.

proceedings, volume 263 of Lecture Notes in Computer Science. Spring-
er-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,
0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791
Conference held at the University of California, Santa Barbara, Aug. 11–15, 1986.


REFERENCES


ACM:1989:PTF

Anonymous:1989:PFC

Beker:1989:CC

IEEE:1989:ASF

MacNair:1989:WSC


REFERENCES


[Pomerance:1990:CCNb]


[Day:1991:PAA]


[Dorninger:1991:CGA]


REFERENCES


[4071] Gustavus J. Simmons, editor. Contemporary Cryptology: the science of information integrity. IEEE Computer Society Press, 1109 Spring Street,
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


IEEE:1996:ASF


IEEE:1996:ASF


IEEE:1996:ASF


IEEE:1996:ASF


REFERENCES


REFERENCES

Anonymous:1999:NIS


Fossorier:1999:AAA


Heath:1999:APP


Iliev:1999:RAN


Niederreiter:1999:MCQ

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Helleseth:2005:STA


Meadows:2005:CPA


Smart:2005:CCI


Henderson:2006:S


Niederreiter:2006:MCQ

REFERENCES


REFERENCES


[4164] Alexander Keller, Stefan Heinrich, and Harald Niederreiter, editors. Monte Carlo and Quasi-Monte Carlo methods 2006. Springer-Ver-
REFERENCES


Christophe Clavier and Kris Gaj, editors. *Cryptographic Hardware and Embedded Systems — CHES 2009: 11th International Workshop*


REFERENCES

2), 0-08-044897-6 (vol. 3), 0-08-044898-4 (vol. 4), 0-08-044899-2 (vol. 5), 0-08-044900-X (vol. 6), 0-08-044901-8 (vol. 7), 0-08-044902-6 (vol. 8). Cannot read pp. LCCN LB15 .I569 2010. URL http://sfx.metabib.ch/sfx\_locater?sid=ALEPH:DSV01\%26isbn=0-08-044894-1. Eight volumes.


REFERENCES


[Hwu:2012:GCG]

[IEEE:2012:PIA]

[ACM:2013:SPF]

[Bailey:2013:CAM]

[Higham:2015:PCA]
REFERENCES

