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

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

Tel: +1 801 581 5254
FAX: +1 801 581 4148

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

13 August 2021
Version 1.353

Title word cross-reference

#14 [2300]. #15949 [885]. #4059 [1256]. #8373 [2123].

(0, 1) [1067]. (0, s) [2562, 2959]. (a^n - 1)/(a - 1) [931]. (j, e) [740]. (n^2\alpha) [2513]. (n^k\alpha) [2514]. (n\alpha) [2513]. (t, m, s) [2067, 2917, 2073, 2373]. (t, s) [2657, 2067, 2364, 2917, 2073]. (X, Y) [3662]. (X^2 - Y^2)1/2 [497].

\[ \frac{a}{m} \cdot j, \frac{a}{m} \cdot (j + \tau)^2 \] \mod \{327, \mod 1 \mod 300, 301, 406, 651, 733, 656\}. \mod n
\]

\[ C^\infty [1275]. C \exp(-\lambda|x|^\nu) [1478]. \chi^2 [348, 939, 1097, 1098, 1099, 6, 7]. D [2399, 1824, 3006, 2101]. d^2 [92]. e [80, 1516, 86, 371]. \epsilon [1928]. F_2 [3040, 3049, 3262, 3827]. F_{2w} [2850]. k [1230, 1300]. j [2028]. K [2213, 3844, 1466, 3816, 3846, 1782, 2134, 1052, 1333, 1935, 3703, 3733, 1118, 1370, 1984]. k > 1 [1360]. L^2 [2052, 1980]. L_2 [2152]. L_p [2424]. \lambda [2839]. M [1445, 1214, 1180, 843, 468, 1054, 1024, 445, 249, 1364, 1777, 2359, 2095, 2201, 2203, 2290, 1129, 230]. F_2 [3123, 3484]. F_{2w} [2997]. F_q [3239, 3539]. F_q^\infty [3239, 3539]. GF(2^m) [1574]. \mu [3218]. N [1147, 908, 269, 1321, 1693, 1694, 2247, 721, 3700, 204, 616, 195, 2811, 200, 1532, 3806, 795, 206, 428, 798]. O(3) [1576]. O(n(1 + \log(N/n))) [1945]. P [6, 719, 3863, 3161, 2446, 2194, 3308, 2207, 2391].

\[ \partial^2 u/\partial x^2 + \partial^2 u/\partial y^2 + (K/y)(\partial u/\partial y) = 0 \] [196]. \[ \pi [2883, 80, 1516, 86, 284, 287, 2935]. \pm 1 [659]. \pm 2k^1 \pm 2^j [2293]. \pm 2p^1 \pm 2^{p^2} [2630]. Q [2526]. S [1019, 1886]. \sigma [1576]. X [409, 440]. \sum a_n/n [659]. T [2593, 2867, 1876, 844, 1886, 1319, 3044, 953, 958, 39]. U(0, 1) [2742]. X(1 + I) = AX(I) \mod 2^{317} [776]. X/Z [3662]. x^2 \mod N [2011].

\[ X_{n+1} = a_n X_n + b_n \] (mod p) [1809]. \[ X_t = X_{t-3p} \oplus X_{t-3q} [1500]. Y/Z [3662]. y = [(a + x) \sin(bx)] \mod 1 [2371]. Z [3662]. Z/nZ [1919]. Z_p [1401].

*good* [2689].


/dev/random [2726, 2781, 2872]. /dev/urandom [2781].
0.57pJ [3287]. 0.57pJ/bit [3287]. '05 [4049, 4053]. '07 [4059]. '08 [4063].


5.0 [1655]. 5.2 [2781]. 500 [3339, 321]. 51st [4081]. 52 [885]. 52nd [4096]. 5th [4064].

6 [3653]. 60th [3896]. 61 [1245]. 623-dimensionally [2358]. 64-bit
Advanced [1467, 1937, 3914, 4079, 4032, 2454, 2531]. Advances [3926, 3944, 3962, 1081, 4012, 4024, 2682, 3983, 2703, 3934, 3936, 3989, 4061, 3947].
approaches [2720]. Approximate
Approximately [507, 1818]. Approximating [2481, 3495].
Approximation [2225, 2405, 2423, 1435, 1524, 2865, 2540, 1874, 3114, 1271,
1114, 3733, 1238, 742]. Approximations [144, 2823, 1063, 482, 1016, 3046, 1239, 3015, 3076].
April [3934, 3905, 3944, 3967, 4079, 3915, 614, 696, 567, 940, 277, 421, 741, 1763, 2789].
Arbitrary [2221, 825, 1548, 3080, 978, 3821, 3850, 3027, 198, 1712, 3524, 1299, 705, 3569].
Archimedean [3319]. Architecture [2872, 2818, 3858, 3400, 2097, 3310, 3576, 3805, 1567].
Architectures [1467, 4065, 3770, 3669]. arcsine [3881]. Area [240, 1910, 3746, 3086, 2215].
Area-Efficient [3746, 3086]. areas [4060, 4029, 2757]. Argument [679]. arguments [429].
Arisen [1]. Arising [1259, 1538, 3541, 3621]. Arithmetic [2304, 2396, 2134, 760, 3696, 2758, 730, 3738, 227, 368, 3986, 3548, 3, 1606,
1415, 1235, 1550, 2198, 1854, 1460, 1575]. arithmetical [296]. arithmétique [3]. Arizona [3928, 3969].
Arlington [3987, 4021, 4036, 3930, 3977]. ARM7 [3113]. Arnold [2946]. arranged [21].
arrangements [58]. Array [1394, 3328, 2599, 1380]. Arrays [1494, 929, 3704, 801]. arrival [3581, 2582, 3536, 3306]. arrivals [2738].
Art [1730, 1752, 3742, 346, 3921]. Artefacts [1585]. Art [1446]. article [885, 2278]. Artificial [146, 64, 73]. Ascending [2759].
asHIIP [3417]. ASIC [2814]. Aspects [909, 9337]. Asperger [3001]. ASR [1245].
Assignment [854, 860, 862, 874, 875, 876]. Assoc [1256, 1025]. Associated [1262, 2778, 3199, 2870, 1019, 21, 255, 423].
Asymptotic [573, 101, 3714, 679, 1547, 795, 2288, 1576, 55, 2291, 403, 3224, 2482, 2582, 1767].
Asymptotical [2889]. Asymptotically [295, 3360, 1445, 2362, 661, 3060].
Asymptotics [3045]. asymptotiques [795]. Atari [1446]. ATI [3466].
Attraction [1554, 370, 739]. Attractor [1682]. Auburn [3967]. auctions [3241]. Audio [3461].
Auditorium [4015]. August [4060, 3971, 3900, 3899, 4029, 4015, 4024, 4035, 4061, 3914, 3974, 2644].
Austria [3924, 3982, 4018, 3974, 4010]. Authentication [2001, 3809, 3838, 3296, 3297, 3263].
Autocorrelazioni [979]. Autokorrelation [470]. Autokorrelation [437].
[2849, 1293]. **Bonferroni** [1198, 774]. **BonGCL** [1357]. **bons** [1357]. **Book** [293, 884, 2110, 539, 398, 2472, 318, 2128, 3029, 2953, 169, 590, 1505, 632, 991, 3250, 512, 1519, 1520, 3139, 3653, 2843, 388, 1735, 1069, 1840, 2602, 2853, 3007, 1856, 1294, 3620]. **Boolean** [3787, 3718, 3608]. **Bootstrap** [1956]. **Bootstrapping** [2958]. **borehole** [1570]. **Borrow** [1764, 3808, 1861]. **Borwein** [3896, 3633, 3634]. **both** [1763, 2789]. **Bound** [2074, 2020]. **Boundary** [196, 1929]. **Bounded** [2212, 1126, 933, 2546, 1788, 3524, 3536]. **Bounding** [2304, 3560, 1993]. **Bounds** [1900, 2019, 589, 722, 774, 2275, 2184, 3167, 2280, 1176, 3286, 802, 1788, 3114, 1492, 1699, 1906, 2313, 2314, 1911, 2259, 1430, 1614, 651, 1543, 3066, 2714, 1575]. **Box** [2881, 712, 761, 2984, 3506, 3657, 649]. **BPP** [2416, 1531, 2287]. **Bracket** [2863]. **Braid** [2663, 2589, 1861]. **Branch** [283]. **Branching** [3329, 3681, 3330, 3875, 3832, 2852, 1691, 1418, 2041]. **breakdown** [3505]. **Breaking** [1038, 2667]. **Brilliant** [3764]. **British** [3970, 4063]. **BRL** [117, 128]. **Broadband** [3089]. **Broken** [3083, 3848]. **Brownian** [1596, 3513]. **Browser** [2148]. **Bruitjn** [3206, 2211, 2399, 3850, 515, 3772]. **Brunswick** [4096]. **Bryan** [261]. **BSAFE** [2114, 2299]. **BSDCon** [4043]. **BSTJ** [495]. **BTPEC** [1425]. **Buena** [3992]. **Buffer** [2013]. **buffering** [1649]. **Bug** [3177]. **build** [2912]. **Builder** [3766]. **Building** [1302]. **Built** [3119, 3804, 3072, 1420, 1510, 2359, 3662, 1985]. **Built-In** [3072, 3119, 1420, 1510, 2359, 1985]. **Bulgaria** [4024]. **bulk** [3252]. **Bureau** [90]. **Burlington** [4005]. **Butterfly** [3868]. **butterfly-patterned** [3868].
combiners [1733]. combinés [2630]. Combining
[896, 897, 1591, 3233, 2569, 3112]. Coming [3675]. Comment [294, 1588, 169,
2563, 854, 1056, 948, 1612, 951, 860, 956, 2907, 957, 862, 2613, 964, 876, 869].
Commentary [2166]. Comments [2802, 3097, 1140, 715, 780, 597, 1612, 951, 860,
956, 2907, 957, 862, 2613, 964, 876, 869].
Commitment [1540, 1632]. Commodore [1134]. Common
[1198, 3855, 509, 1277, 1714, 3054, 1738, 1554, 802, 2157, 1109, 3602, 1842,
1075, 744, 3562, 2554, 2225, 1104, 1707, 904, 768, 723, 910, 1352, 2423, 1841,
2068, 932, 1464, 1659]. Commun [2034, 2156]. Communicating
[1300]. Communication [580, 4057, 1300, 1317, 2476, 2814, 3489]. Communications
[503, 2677, 4053, 3983, 2723]. Comp [2123]. Compact
[1997, 2792, 3019, 1402, 2494, 3051, 596]. Companion [4098]. Comparative
[1327, 400, 500, 3235, 2996]. Comparing
[1213, 904, 1814, 2164, 3313]. Comparison [664, 574, 1044, 3221, 3799, 3649,
1714, 3144, 2065, 203, 2275, 605, 1071, 695, 2191, 2780, 1659, 1473, 1671, 1481,
587, 588, 1708, 2904, 2504, 3290, 2720, 461, 803]. Comparisons
[1841, 2068, 1464, 1386, 1738, 1842]. compatibility [3631]. Compatible
[1502, 1532, 3580]. Competing
[185]. compiled [69]. Complement
[1110, 730, 477]. Complete
[1281, 1007, 3929, 927, 2383, 2804, 2804]. Completed
[945]. Completely [507]. Complex
[3644, 676, 4008, 3747]. Complexity
[2797, 2943, 1476, 1778, 3342, 1796, 2895, 3859, 2581, 1827, 1945, 2270, 3149,
3731, 2620, 3917, 1300, 2468, 2119, 1886, 1317, 3796, 3570, 1149, 2891, 2746,
3586, 773, 2903, 3503, 2767, 3056, 1736, 3775, 1542, 2934, 1992, 1868]. complicated
[2534]. Component
[1892, 2679, 2995, 2994, 2996]. Component-by-Component
[2679, 2995, 2994, 2996]. components [2755]. Composite
[3222, 29, 2679, 864, 1561, 2089, 3180, 2132, 1687, 1431, 2088, 1855].
Composite
[3222, 29, 2679, 864, 1561, 2089, 3180, 2132, 1687, 1431, 2088, 1855].
Composited
[3772]. Composition
[1920, 3674, 1228, 840]. Compound
[1260, 2405, 1901, 2025, 2139, 2140, 2232, 2234, 2317, 2929, 3452, 1790, 2024,
2233, 2143, 2144, 2592, 2908, 2605, 79, 2208]. compressed
[2063]. compression
[3961]. Compromise
[3083, 2988]. Compromised
[3685, 3797]. COMPSTAT
[3950]. Comptes
[3902]. Compton
[376]. Comput
[2034, 1056, 2156]. Computability
[4091, 2439, 3274]. Computable
[3789]. Computation
[3897, 3791, 4051, 3980, 2127, 2881, 1686, 848, 29, 141, 4086, 329, 1932, 3997, 3982,
2072, 2075, 3806, 4039, 3204, 933, 3899, 1252, 2398, 1886, 2574, 2492, 2974, 1839,
1744, 1976, 883, 4062]. Computational
[3896, 4070, 2557, 940, 4094, 2438, 2692, 3965, 343, 3866, 4062, 423, 3752, 2878,
1049, 3950, 4045, 1503, 554, 1725, 4099]. Computationally
[3974, 3953]. Computations
[1140, 412, 1158, 3696, 695, 2530, 2119, 2395, 2475, 718, 1418, 1361, 158, 1546].
compute
[2757]. Computer
[572, 665, 978, 1009, 885, 746, 886, 887, 888, 3935, 2731, 1319, 3567, 1144,
3922, 503, 1501, 243, 412, 3915, 3925, 3928, 3931, 3946, 3951, 3957, 3963, 3973,
3996, 4005, 4009, 4030, 4034, 4081, 4096, 1160, 1161, 859, 770, 819, 1523, 723,
corresponding [702, 1125]. Corrigenda [2123].
Corrigendum [2246, 1025, 2512, 1365, 535, 624, 3621]. Corroboration [2731].
Cosmological [3653, 3508]. Cost [3280, 3204, 1000, 3660, 3510, 2445, 3290].
cost-effectiveness [3290].
Cramér [293]. Crash [3876]. CRAY [2406, 1375]. CRAY-System [2406].
Create [2731, 1745]. created [2281]. Creates [2851]. creation [2357].
Criteria [1383, 1465, 2959, 518, 1449, 101, 2347, 2590, 3289]. Criterion [1].
Critical [2731, 1687, 3887, 3028, 1686]. Crofton [2757]. Cross [1773, 3473, 3183, 3184, 3472, 554].
Cross-correlation [1773, 554].
Cryptographically [3207, 3320, 3443, 1014, 1086, 1355, 3388, 3003, 1082, 2724, 3720, 1295, 1878].
Cryptographically-secure [1878]. cryptographiquement [1878].
Cryptography [3956, 2305, 895, 1682, 2649, 3030, 2964, 905, 2490, 2595, 2986, 3372, 1628, 2525, 2192, 2195, 4057, 2621, 4058, 1660, 2403, 4089, 4060, 2417, 4029, 3255, 1711, 1527, 2273, 1959, 2369, 2523, 3394, 2450, 3527, 2623, 3299, 3196, 4054].
Cryptology [1136, 3936, 3926, 3944, 3945, 3965, 1121, 3975, 3934, 3989, 3962, 4061, 3947].
Cryostat [3293, 1355, 3734]. cryostats [2425, 1369, 3189].
Crystal [4021, 53, 4036, 3930, 3977]. crystallography [3254]. CSD [2089].
Discrete

Discrete-Event

Discrete-Time

discreteRV
discrets
discriminating
discriminatory
disks
disjoint
disjunctions
Disk
Diskrepanz
Diskret
Disney
Disorder
Dispersion
dissipative
dissociated
dissociation
Distance
Distance-Bounding
distances
distribution
Distribution
Distribution-Free
Distributing
Distribution-Free
Distributing
Extendable [3735]. Extendable-Output [3735]. Extended
[2401, 1152, 1504, 2581, 3726, 1540, 1185, 495, 1252, 3972, 1424, 1816, 3494,
480, 3370, 1231, 2459, 2462]. Extending [1175]. Extends [1815]. Extensible
[2487, 2773]. Extension [2280, 3521, 3182, 668]. Extensions
[625, 913, 2276, 2157], extensively [1888, 2338], extracted [3803].
Extracting [2945, 2187, 1749]. Extraction [3346, 3656, 3609]. Extractor
[3617, 3869]. Extractors [3756, 2491, 3767, 2631, 2169, 2926, 2462, 3432].
Extrapolation [1356]. Extraterrestrial [2079]. Extreme [1703, 8].
Extremely [479, 734, 594, 595, 3542]. extremely-high-throughput [3542].

fabulous [3250]. Face [3297]. Facilities [1618, 348]. Factored [1310].
Factorial [2275]. Factoring [1027, 1166, 1279, 1849, 1763, 2789].
Factorization [1844, 735, 1350, 693, 1179, 1971, 3612]. Factorizations
[1047, 1316, 2645]. fail [3862]. failure [2415]. fair [2661, 2495, 3046]. Fairfax
[3952]. Fairmont [3960]. Family [887, 1325, 2659, 3771, 700, 1565, 3442,
3558, 1595, 2230, 1275, 3700, 1008, 3669, 2793]. Fast
[2638, 1136, 3089, 1042, 3717, 2950, 1678, 1480, 580, 3823, 2145, 2660, 1215,
1415, 675, 1417, 505, 3721, 3124, 3485, 3041, 2254, 2671, 1347, 1818, 2163,
2501, 2904, 3861, 1723, 3828, 1725, 308, 359, 279, 782, 238, 2057, 3055, 1448,
118, 1631, 3603, 2994, 2995, 2996, 734, 3866, 525, 1850, 3175, 1559, 3406, 3710,
3182, 2093, 1765, 3811, 3190, 3299, 704, 2206, 537, 3423, 1251, 938, 765, 1341,
2032, 2751, 2467, 2494, 3045, 996, 1436, 3259, 3143, 3260, 3498, 333, 1621, 335,
[3162]. fat [1578]. fat-tailed [1578]. Fault [3754, 3454, 3636, 1231].
Faulty [3694]. Fault-tolerant [3636, 1231]. Faulty [3694].
Faure [2716]. FCRC [4001]. FCSR [2869, 3830, 3294]. FCSRs [3556, 3237, 3828].
FDC [1940]. Features
[441, 1570]. February [4075, 4010, 4043, 3919]. Feedback
[2555, 1199, 1318, 1052, 1514, 2502, 515, 643, 3772, 645, 863, 3512, 1553, 3616,
2717, 3871, 3106, 1709, 2048, 955, 3880, 332, 3504, 309, 2054, 2698, 1287, 1369,
3704, 1755, 3842, 3750, 1123]. Feeding [3104]. Feinstein [318]. Feistel
[3785]. Feistel-inspired [3785]. Feller [3325, 1394]. Fence [3675]. Fermat
[3570]. fermions [3636]. ferromagnetic [731]. Festschrift [4069]. Few
[2945, 3110, 3080, 3045, 1293]. few-body [1293]. Fiar [2731]. Fibonacci
[3250, 2108, 2210, 3713, 1880, 407, 3481, 1949, 249, 1953, 1954, 2057, 2058,
2059, 2841, 1962, 2442, 1765, 1860, 2537, 230]. Field
[2213, 3981, 2857, 1583, 1946, 2599, 1235, 919]. field-programmable [2599].
Fields [3884, 3653, 3368, 3508, 1844, 2185, 1772, 316, 3821, 4004, 3642, 947,
1166, 2271, 3983, 1633, 1740, 1843, 2186, 2519]. Fifteenth [3927]. Fifth
[4062, 3987, 4097, 3999]. Figures [1469]. File [3211]. Files [3233]. filling
[187]. Filter [3055, 3718]. Filtered [2591, 2869]. Filtering [545, 2963, 3615].
filters [1693, 1694, 1828]. Final [1003, 2434]. Finalist [2531]. Finalists
[2493, 2577]. finalizer [3526]. Finally [1337]. Finance
[3091, 4084, 4076, 3701]. Financial [2380]. Find
Finding
Finely
Fingerprint
Finite
Finite-Difference
Finite-length
FIPS
First
Fishman
fission
Fit
Five
Fix
Fixed
fixing
FPGA
Flash
Flaw
flights
Flip
Flip-flop
Flipper
flipping
Flips
float
Floating
Floating-Gate
Floating-Point
Florida
flow
flow-level
Fly
folding
Flonction
Force
forced
forests
Fork
Fork-Join
Form
Fonction
Foundation
foundations
Four
four-dimensional
Fourier
fractions
Framework
France
Frank
FreeBSD
Freedom
free
French
France
frequencies [64, 73]. Frequency [2036, 2151, 3765, 2924, 1036, 621, 550, 1342, 3267, 2708, 705].
Frustration [3301]. Fukuoka [3966]. Full [3217, 1096, 1021, 3856, 3291, 2790].


General-Purpose [1071].


generating [1010, 2109, 2211, 808, 1666, 3788, 1872, 2395, 766, 2154, 1219, 3839, 1574, 1866, 1658, 1994]. Generating [1010, 2109, 2211, 808, 1666, 3788, 1872, 2395, 766, 2154, 1219, 3839, 1574, 1866, 1658, 1994].


Generation [3075, 3186, 1862, 3189, 3190, 2204, 425, 1130, 1185, 535, 536, 1654, 706, 2464, 1577, 3622, 3784, 3545, 3751, 626, 1248, 430, 2469, 1471, 1774, 3088, 3208, 3752, 1876, 1311, 2946, 3444, 3445, 3629, 3630, 3631, 3678, 1251, 1877, 2116, 3021, 3552, 348, 3092, 979, 2873, 3633, 844, 3849, 2124, 3095, 811, 1045, 1878, 181, 1478, 1399, 938, 898, 1679, 400, 1780, 3793, 401, 2399, 2309, 3027, 2009,
generators
[2320, 2409, 2559, 2560, 1704, 1148, 1797, 850, 943, 944, 1209, 1210, 1331, 1798,
2029, 2324, 274, 2324, 853, 989, 2889, 3038, 3799, 1338, 3689, 2891,
3480, 2743, 1708, 1803, 764, 475, 1217, 1272, 1340, 2569, 2667, 2745, 2746, 3121,
3642, 3553, 1507, 3354, 1418, 1805, 1806, 1914, 1697, 1329,
2885, 1908, 1909, 2026, 2144, 2240, 2319].

generators
[2425, 3494, 1717, 2902, 2978, 3047, 820, 1357, 1358, 1438, 1619,
1825, 2165, 2167, 2168, 2170, 2264, 2345, 2347, 2348, 2430, 2431, 2584,
2586, 2600, 2755, 2827, 2904, 3048, 3050, 3365, 1527, 3801, 1112, 2903, 3146,
3263, 2269, 1721, 3147, 1167, 1280, 861, 2596, 3829, 3366, 3053, 3881, 3153,
1228, 2173, 2687, 1949, 2054, 3593, 3267, 3595, 446, 447, 483, 519, 1623, 1729,
1950, 1952, 2763, 2691, 3154, 3864, 2356, 2599, 2840, 2841, 3596, 3658, 1731,
1955, 2357, 2359, 2765, 2989, 3054, 1732, 1837, 784, 3158, 3056, 3373, 2768,
2846, 1734, 1630, 454, 3832, 3661, 3269].

generators
[2065, 3734, 1737, 604, 3060, 3273, 2183, 650, 1118, 1287, 1545, 2519, 2604, 2703,
1546, 1744, 1745, 3167, 2848, 3350, 3381, 611, 2522, 2850, 2998, 3384, 1638,
1120, 1289, 1374, 1452, 1747, 1748, 2077, 1375, 2080, 3389, 2999, 1122, 2083,
833, 2370, 3836, 1077, 1552, 870, 1078, 3779, 3745, 2282, 2087, 1558, 1853, 1379,
1458, 1758, 2858, 3668, 2618, 2709, 1759, 2449, 3405, 3808, 262, 2200, 1977, 1760,
3525, 2786, 2458, 3710, 1295, 3527, 2623, 2624, 2459, 3289, 2860, 2289, 2629,
2790, 2932, 3013, 3014, 3073, 3410, 3531, 3532, 1648, 1861, 1985, 3074, 3187].

generators
[3669, 3711, 3416, 2934, 2630, 2462, 2631, 1650, 977, 2793, 2718, 2794, 3420, 1083, 2098, 1084, 3812, 3893, 2206, 1864, 3537, 1769, 2635, 2103, 2208, 1991, 461, 3422, 2293, 3018, 3424, 3783, 2723, 3312, 3313, 3749, 3431, 3432, 3206, 3145, 3264, 398, 512].
generators-part
[2623].

Generazione
[979, 488].

Genetic
[2550, 2575, 2668, 2669, 638, 682, 2979, 2760, 4039, 2861, 2937, 2124, 2879, 2691, 3602, 4051].

Gentle
[3007, 2472, 2843].

Genuine
[3614, 2866].

Geographic
[2906].

Geometric
[3551, 760, 1932, 2182, 2793, 2757, 1737, 2632].

Geometrical
[3301, 2052].

Geographically
[2823, 2744, 2759].

Geometry
[2363, 2364, 1049, 3230, 1936].

geophysics
[1570].

George
[4069, 261].

Georgia
[4020, 4007, 3935].

Germain
[2840].

German

Germany
[4079].

Getting
[3300, 2465].

GFSR
[2034, 1388, 1411, 2035, 1731, 1955, 2362, 1296, 1297, 1381, 1860, 1984].

GI
[1942].

GI/G/1
[1942].

Gibbs
[1781, 2014, 2031, 731].

gigahertz
[1470].

Gill
[504].

Giovanni
[3653].

Gitterstruktur
[1041].

Given
[1090, 1201, 1593, 1514, 1, 150, 983, 259, 2286, 1653].

giving
[140].

Glasgow

krivoi [34], Kronecker [3561], FY [4064].

L [539, 590, 632], Laboratory [3897, 3899], Lag [605], Lagged
Lagged-Fibonacci [1949, 2057, 2058, 2059, 3713, 1954, 2841, 1953].
Lagrange [1691], Lai [3370], Lake [3992, 3999], Lamar [2979], lamp [2766].
Landau [2552, 3825, 702, 1125], language [3801, 3883], language-based [3883], languages [3783], Laning [169], Lansing [3913], Laplace [2564, 679, 3059, 3282].
laptops [2306], Large [3897, 3328, 3567, 3568, 855, 679, 26, 2909, 3700, 3863, 2181, 186, 3279, 1554, 3022, 2882, 3111, 3228, 2815, 1341, 73, 246, 95, 3829, 1070, 616, 231].
Large-Order [3567, 3568].
Large-Scale [3897, 186, 2181, 3022, 95, 3829].
large-size [73], largely [978], Laser [3281, 3352, 3886, 3367, 3530, 3308].
Lasers [3162, 3190, 3299], Last [2202], Latin [2365], LatMRG [2167].
lattice-based [3842], lattice-bases [3842], lattice-sublattice [3842].
lattices [2132, 2828, 3863, 2856].
LavaRnd [2610].
Law [3462, 3279, 1554, 2207, 3114, 2736, 3240, 15, 198, 2149, 246, 16, 3881, 3159, 795, 2372, 3448, 3325, 3129, 2991, 2857, 900].
Laws [855, 1524, 2778, 571].
Laxenburg [3974].
LC [2924], LCG [2655], LCGs [2242, 2560, 2266].
Leading [2976, 628, 1053], leads-to [1888], Leakage [2464].
Leap [3876, 3310, 2320], leap-frog [2320], learnability [2209], Learning [3181, 1977].
Least [747, 541, 104, 1427], Least-Remainder [104], leave [3822].
Lecons [4], Lecture [3653].
Lectures [264, 4], L’Ecuyer [1459], Lee [495], Left [3515, 1975, 467], Left-Shift [1975], legacy [3794], Legal [2731].
Legge [16], leggi [15], Lehmann [3250], Lehmer
[1688, 2230, 2231, 759, 3651, 909, 248, 2189, 489, 2091, 232].
Lemma [2625, 2459].
Lemmas [2566], Length [3787, 182, 374, 466, 1257, 240, 1599, 1096, 1021, 823, 1838, 918, 1885, 1261, 216, 469, 1408, 1491, 1697, 1149, 858, 1926, 2491, 1433, 594, 595, 1727, 3167, 654, 1983, 3294, 3539, 3081, 3712].
lengths [2870, 2007].
Less [747, 889, 2987].
Lession [1750], lessons [3822].
Letter [473, 1220, 1831, 3005, 492], letters [2921], leurs [3], Leuven [4065].
Level [3632, 2516, 1142, 3046, 1817, 3062, 2783].
Lewis [754], Lexical [2484].
Lexington [4064], Leydold [2953], LFIB4 [3883], LFSR
[2308, 3821, 3223, 2431, 3374, 3806, 3310].
LFSR-Based [3806], LFSRs [3845, 3850].
Libgcrypt [3759], Liblice [3907], libraries [2155], Library
[3447, 3791, 1050, 1325, 1215, 2588, 2684, 2983, 3051, 2685, 2176, 1461, 1581, 1663, 3445, 3630, 3631, 3678, 2873, 3851, 3341, 3238, 3639, 3761, 2893, 3050, 2511, 2512].
Lie [1964], Life [2394, 3611], light [3530].
Lightweight
low-cost [3600, 3510]. Low-Degree [3368]. low-dimensional [1779, 2107].
Low-Dimensionality [2956]. Low-Discrepancy [2660, 2185, 2363, 1565,
1879, 1233, 1366, 1740, 894, 1673, 2971, 2504, 2757, 1739, 3610, 2093,
2107].

low-dispersion [1366]. Low-Order [1896, 1906, 3066]. Low-Discrepancy
Low-Dimensional [1739, 2107]. Low-Dimensionality [2956]. Low-Discrepancy
LT [3336].
Luby [2110, 1837, 3164]. Lucas [3481, 2388]. luck [3801].
luminescent [3655]. L¨uscher [2156, 1927]. LUT [3075, 3669]. LUT-SR
[3669]. LUTs [3415]. Lyapunov [2831, 1829]. lying [1304]. LZSS [3332].
M [1012, 1941, 69, 3156, 1012, 1941, 3302]. M. [318, 393]. M/M/1 [1941].
M/M/m [1012]. M/PH/1 [3302]. MA [4074, 4035]. Mach [3106].
Manhattan [3651]. MANNIC [1189]. Manipulating [548]. Manipulation
Many [2185, 2081, 1180, 662]. Map [3335, 3543, 3845, 3769, 2078, 3288].
[2595, 3318, 2946, 3216, 861, 3379]. March [3899, 3955, 4075, 3935, 3927,
4086, 3901, 3985, 4058]. Marginal [2221, 1826]. Marginals [2553]. margins [2286].
Marinucci [3653]. Mark [3942]. Markov [2550, 211, 1087, 1191, 2225, 3344,
947, 510, 655, 703, 1987, 1772]. marks [2302]. Marotto [3483]. Marriott [3948,
Marsaglia [3317, 2298, 2806, 1328, 1329, 1344, 2055, 2077, 1074, 3782, 3812].
masking [3642]. Masking [3869]. mass [732, 1576]. Massachusetts [3915].
Massen [732]. Masssey [2948, 3370, 3810]. Massively [3886, 1921, 3593].
[3791]. Mathematica [3599, 3661, 2086]. Mathematical
[3791, 3905, 3971, 3900, 3920, 3924, 1221, 1222, 95, 3653, 3902, 249, 1068, 3736,
2368, 3904, 54, 56, 3911, 4010, 3620, 930, 463, 493, 235, 711, 1208, 2442, 208].
[3905, 2805, 3900, 3920, 905, 4098, 1937, 4068, 3895, 3912, 138, 3896,
1729, 3919]. math´ematiques [3902]. MathLink [2121]. MATLAB
methods [4025, 2517, 4046, 4056, 3165, 488, 1031, 3904, 260, 1179, 1971, 3612, 2444, 873, 967, 972, 975, 289, 1218, 3581, 4024, 1223, 3132, 4066, 953, 2682, 2827, 3725, 3145, 95, 779, 1113, 2433, 1741, 1742, 1957, 3998, 4018].

Metodi [979, 488]. Metric [652, 2706, 3093].

Metropolis [1189, 2470, 2471, 2878, 1781, 1264, 2031, 2246, 2892, 2750]. MHz [2868].


Microscopy [1751]. Microsoft [4028, 2436, 2695, 2696, 2916, 3157, 3158, 1655].


Model-Based [3693]. Modeling [1585, 3847, 2221, 4041, 3765, 3063, 1751, 3674, 1026, 1617, 2499, 2980, 227, 1567]. Modelirovanie [350].


NIST-Recommended [2899]. Nix [3741]. NJ [2110]. \textit{nm} [3339, 3654].


Numbers [2967, 992, 184, 633, 634, 476, 1105, 2486, 3720, 65, 74, 2037, 2250, 2330, 477, 2749, 66, 1219, 993, 1712, 413, 2257, 330, 1516, 20, 1350, 1351, 1024, 2260, 25,
numbers
[2936, 3017, 1866, 69, 2539, 232, 3784, 28, 3430, 3545, 883, 1994, 1870, 1569, 175, 3304, 3562, 2554, 2225, 1104, 1707, 904, 768, 723, 910, 1352, 2423, 1841, 2068, 535, 932, 1464, 1659, 624, 3250]. Numer::
[925].
numerical
[708, 2798, 1197, 3900, 674, 349, 988, 1800, 1606, 4084, 1339, 506, 276, 637, 1218, 1426, 1941, 2437, 3160, 1752, 2191, 490, 1761, 3906, 290, 662, 264, 1575, 3912, 1586, 3338, 3760, 1605, 2893, 2037, 1056, 2751, 2155, 4024, 1515, 22, 1361, 3366, 1113, 1324, 2279, 963, 1857, 2090, 2534, 1566, 1862, 396, 538, 798, 2297, 2214]. Numerics
[3995, 4006, 4011]. nVidia
[3260].
O
[4090, 4032].
Object
[1797, 2681, 3500]. object-oriented
[2681, 3500]. Objectives
[2564].
Oblivious
[3875]. observation
[1581, 1663, 1693, 1694]. Observations
[864, 1081, 348, 22]. Obtain
[3249, 2575]. Obtained
[3680, 545, 1740, 133, 1008]. Obtaining
[695, 66, 962, 1379, 176]. obtenida
[133]. OCCAM
[1451]. Occupancy
[2658]. October
[4021, 3941, 4052, 3931, 3946, 3951, 3957, 3963, 3973, 3996, 4005, 4009, 4034, 4081, 4096, 3913]. octrees
[1908]. odd
[1982]. Odyssey
[4036]. off
[2738]. Offer
[2578]. Office
[3909]. Offord
[1939]. offs
[1667]. Offset
[3125]. Olds
[3913]. OMAC
[3272]. On-line
[3284]. On-the-Fly
[3283]. on/off
[2738]. One
[1995, 3626, 747, 3450, 2133, 2244, 2420, 3643, 2668, 1611, 1167, 1280, 1620, 446, 447, 482, 2508, 730, 2074, 2192, 1644, 3295, 3543, 1578, 3550, 889, 3354, 1424, 3128, 1427, 187, 2629, 1184, 5, 3313, 3749]. One-chip
[3295]. one-class
[3313]. one-dependent
[1427]. One-Dimensional
[3543, 187]. One-line
[446, 447]. one-shot
[3128]. One-Sided
[482]. One-Table
[1995]. One-Time
[3450, 2244, 2192]. One-Way
[3626, 3643, 1620, 2420, 1611, 1167, 1280, 3550, 3354, 1424, 3749]. Ones
[1373, 2080]. Online
[3837, 2617, 3661, 3061]. Only
[2731, 3338, 3350, 3581, 2493]. Ontario
[4029, 3986]. OpenACC
[3883]. OpenCL
[3851]. OpenMP
[3883]. OpenSSL
[3748, 3094]. Operating
[3032, 3033, 3232, 3046, 1238]. operation
[3088].
[321]. Procedure [1089, 1198, 942, 1098, 988, 3855, 443, 308, 279, 1749, 1581, 1663, 321, 767, 333, 282, 335, 3602]. Procedures [2554, 3691, 253, 612, 2616, 1126, 1659, 1671, 578, 319, 2436, 2695, 2916, 3157, 343, 840]. Proceedings [3933, 3954, 3979, 4002, 4097, 3899, 3955, 3936, 3944, 3900, 3968, 3922, 3927, 3941, 4023, 3982, 3963, 3964, 4099, 4087, 3997, 3921, 4036, 4037, 4062, 3986, 3917, 3999, 4000, 4043, 3919, 3952, 3912, 4001, 4049, 4059, 4063, 3948, 3994, 3939, 3960, 3918, 3934, 3935, 3995, 3980, 4003, 3926, 4004, 4028, 3995, 3920, 3950, 4042, 3926, 3924, 4029, 3973, 4030, 4034, 4024, 4031, 3958, 4053, 4017, 3969, 3998, 4018, 4025, 4046, 3914, 3974, 3990, 3931, 3932, 4039, 3992, 4019, 3942, 4011, 3987, 3938, 3943, 3949, 3959, 3970, 3988, 3993, 4020, 4027, 4040, 4044, 4074, 4083, 4007, 3897, 3903, 3966, 4071]. Proceedings [4091, 3967, 3915, 3990, 4081, 4096, 4035, 3902, 3982, 4073, 3985, 4054, 3991, 3977, 4006, 4010, 3978, 4013, 3989, 4022, 4079, 4064, 4086, 4061, 3947].

Process [2053, 3287, 1691, 526, 973, 3303, 1578].


Processing [664, 3466, 3985, 3903, 3633, 1193, 4023, 1345, 2256, 1434, 3143, 3601, 3167, 1968, 1643, 2538].

Processors [2407, 4065, 3358, 3387, 3401, 3666, 3322, 1399, 1489, 1412, 1607, 1622, 1452, 3431, 3545].

Produced [1397, 3724, 555, 1072, 1073, 1398, 3039, 2263, 1545, 2714]. Producing [336, 358, 74, 75, 384, 2930].

Product [2578, 3046, 206, 3180, 891, 1148, 1922, 1229]. Production [168, 330, 175].

Products [2991, 394, 532, 2028, 3494, 2793]. Professor [4028]. Profile [2943, 2811, 2746, 2767, 3056, 1736, 1542, 2934, 1868]. Program [3445, 3631, 2121, 1205, 3761, 224, 3195, 1015, 2361, 610, 1372, 1122, 928]. Programmable [2256, 1815, 2599].

Producing [808, 893, 1677, 2940].

Programmierung [883].

Programming [3791, 2979, 2074, 1637, 3742, 4039, 883, 3920, 1208, 2155, 2691, 607, 2200].

Programs [1472, 3329, 3681, 3330, 374, 466, 1017, 3875, 702, 1125, 1461, 3646, 914, 1968, 1879].

progressive [3841]. project [2569].

Projections [5130].


Property [180, 3199, 3444, 1138, 3231, 3801, 1285, 797]. property-based [3801].


Propriétés [795].

Prospective [508]. protection [2302].


Proton [347].

Proton-Electron [347]. Provable [3012, 1871]. Provably
pseudorandom


Pseudorandomness


Pseudozufallsvektoren [1340]. Pseudozufallszahlenfolgen [617].

Pseudoluchainykh [350]. PSI [1413]. PUB [1847].


62

[2937, 2938]. RnaPredict [2937, 2938]. RNG
[1671, 3794, 1146, 3140, 2837, 3890]. RNGAVXLIB [3761]. RNG> [3885].
RNGs [3854, 2395, 3685, 3797, 3341, 2764, 2376, 2453, 2456]. RNGSSELIB
[3445, 3631]. road [1702]. robots [2627]. Robust
[3208, 1445, 2534]. Robustness
[3208, 1323, 1689, 3155, 2188, 3428, 2278]. Rockefeller
[3964]. rocket [255].
[1774]. Roots [785]. ROP [3872]. Rosenbluth [2892]. Rotation
[1829, 2094]. Round [2881, 2573, 2668, 2672, 2699, 2879]. Rounding
[2223, 2047]. Rounds [2669]. Route [3687]. Routine [1302]. Routines
[780]. RSA [1308, 3012, 3201]. RSA-Based [3012]. RSAEuro [2117].
rstream [2905]. Rudin [3833]. ruin [950, 3141]. rule [241, 2539].
rule [241, 2539]. Ruins-Down [990]. Ruins-Up [990]. Russian
[3005, 350, 34]. Russians [3764].
RV [3764].

S [3097, 318, 991, 1056, 444, 393, 3655, 2106, 3529]. S-3800 [2106].
SAFE [3823, 2085]. Salford [1914]. Salt [3999]. Salzburg [4018]. same
[369]. Sample [710, 1090, 3565, 630, 760, 2962, 58, 795, 35]. Sampler
[585, 2014]. samplers [1781]. Samples
[1200, 1972, 1979, 8, 430, 844, 64, 73, 17, 39, 134, 33, 231]. Sampling
[572, 665, 933, 1135, 1995, 3846, 3563, 847, 1262, 1481, 2136, 271, 755, 756,
1101, 1498, 716, 48, 854, 1215, 510, 3691, 24, 3488, 2043, 1348, 1425, 3763,
860, 1945, 2352, 862, 3702, 1, 3889, 655, 3837, 874, 875, 876, 621, 162, 1186,
100, 625, 978, 1307, 1385, 3674, 2109, 885, 12, 1586, 239, 150, 42, 3035, 3825,
587, 588, 2031, 2246, 116, 65, 73, 74, 2257, 94, 156, 3360, 25, 30, 31, 1354,
3495, 2506, 1725, 1155, 158, 283, 3733, 27, 2771, 2365, 560, 259, 188, 1292,
2534, 2788, 976, 121, 373, 9, 106, 209, 136, 2101]. sampling [3081, 69, 28].
Sampling-Vectorized [3837]. Samuel [4069]. San
[4059, 4083, 3948, 3994, 4075, 4039, 4019, 4043]. Santa [3900, 3989, 4061].
SAR [4042]. Satisfied [411, 552]. Satisfying [527, 460, 1332, 3280, 458, 13].
Saturday [4051]. Saturday-Wednesday [4051]. Saunders [3147, 2780].
Savage [2507]. Saving [3825]. SC’11 [4087]. Scalable
[3228, 3264, 3814, 3688, 3639, 2834, 2511, 2512, 2306, 3145]. Scale
[2209, 3897, 781, 186, 10, 3022, 14, 1694, 3886, 95, 3829, 1445, 2181, 1070].
Scale-sensitive [2209]. Scaling [2283, 3298]. Scan [3504]. Scan-based
Schedules [664]. scheduling [1822, 3378]. schemata [2635].
schemata-based [2635]. Scheme [3328, 1964, 3016, 3370, 787, 1638, 3520].
Schemes [1800, 2516, 736, 1187, 3817, 1422, 2353, 158]. Schnorr [1555].
Sequences [3433, 2942, 2112, 3207, 3320, 843, 266, 1476, 112, 1086, 180, 236, 1397, 1879, 895, 2128, 182, 374, 466, 580, 3337, 545, 2479, 1597, 1096, 2562, 2959, 1103, 852, 2963, 2666, 142, 408, 507, 244, 327, 3724, 3130, 224, 3144, 445, 3501, 2760, 3772, 517, 518, 863, 599, 2513, 2514, 2842, 1536, 1626, 1281, 823, 2362, 3833, 2185, 2363, 2364, 2917, 3275, 2073, 2279, 918, 2190, 2706, 2707, 3608, 1072, 2191, 2852, 1642, 1237, 1082, 1564, 1860, 1984, 2716, 2382, 1300, 2207, 1302, 1867, 743, 3543, 210, 1773, 2211, 1390, 2870, 177, 2395, 1477, 234, 1398].


Sieve [3981]. SIGACT [3979, 4073]. SIGACT-SIGMOD-SIGART [3979]. SIGART [3979, 4073]. Sigla [945]. SIGMOD [3979, 4073, 3991].
Similar [3833]. Similarity [2308, 4057]. SIMPL [757]. SIMPL/1 [757].
Simple [1466, 576, 1670, 1192, 1158, 899, 1594, 3721, 1064, 2509, 2359, 2062, 823, 3517, 2619, 2926, 1239, 3432, 2545, 844, 1138, 1782, 1093, 2410, 4008, 1271, 74, 3044, 2167, 2593, 3152, 616, 2458]. simplest [2049].
simulation [2642, 3326, 3452, 212, 1889, 1482, 471, 1051, 273, 1271, 1105, 3645, 3908, 2489, 1511, 2257, 1160, 1274, 3045, 1933, 1434, 2905, 2051, 3500, 3602, 1738, 1957, 256, 2849, 1120, 615, 1377, 2086, 1645, 973, 373, 1570, 570, 742, 3542, 3202, 3921, 3974, 1735, 1840. Simulation-Based [2423].
Sixteenth [3935]. Sixth [3985, 4039, 3988, 3900]. Size [3787, 710, 2136, 3444, 3679, 64, 73, 1929]. sizes [2430, 1456]. sketch [3065].
small-deviation [380]. Small-World [3246]. smaller [2100]. Smart [3771, 3156, 2730, 4079]. Smart-Card [3156]. Smirnov
Strela [191]. strength [3704]. strength- [3704]. Strengthen [3600].


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.
REFERENCES


Student:1908:PEM


Borel:1909:PDL


Borel:1914:LTF


Weyl:1916:GZM


Fisher:1922:ICT


Yule:1922:AMA


Tippett:1925:EIR

Tippett:1927:RSN


Yule:1927:RS


Klein:1929:SSD


Baker:1930:RSN


Ward:1931:DRS


Champernowne:1933:CDN


Glivenko:1933:SDE


Karl Pearson. On a new method of determining “goodness of fit”. *Biometrika*, 26(4):425–442, December 1934. CODEN BIOKAX. ISSN 0006-3444 (print), 1464-3510 (electronic). URL http://www.jstor.org/stable/2331988. According to [373, page 36], this paper introduced the $P_n(\lambda)$ test for “determining whether a sample of size $n$, supposed to have been drawn at random from a parent population having a known probability integral has probably been drawn at random.” See [27] for its first use on random numbers from a uniform distribution.


[29] E. Dietze and W. D. Goodale, Jr. The computation of the composite noise resulting from random variable sources. *The Bell Sys-
REFERENCES


Kendall:1939:SPR


Kendall:1939:TRS


Mahler:1939:UKK


Smirnov:1939:EDB


Smirnov:1939:OUE


Vickery:1939:DRS


REFERENCES


REFERENCES


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


Fisher:1949:STB


Hamaker:1949:RSF


Hamaker:1949:STP


Horton:1949:DMP


Mauchly:1949:PRN


Metropolis:1949:MCM


Stevens:1949:TRD


Walsh:1949:CCR

REFERENCES


REFERENCES


REFERENCES


Anonymous:1954:RDb


Anonymous:1954:RDc


Anonymous:1954:RDd


Bartholomew:1954:NUS


Hammersley:1954:PMM


Lehmer:1954:DRN


Meyer:1954:GTR


Moshman:1954:GPR

REFERENCES


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


[Stuart:1956:ETR]


[Taussky:1956:GTP]

C. B. TOMPKINS. Machine attacks on problems whose variables are permutations. In *Curtiss [500]*, pages 195–212. LCCN ????.

[Tompkins:1956:MAP]


[Tompkins:1956:RJS]


[Tompkins:1956:RMR]


[Cook:1957:RFP]


[Davis:1957:CJH]
REFERENCES


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


Bauer:1958:MCM


Bendat:1958:PAR


Bofinger:1958:PPP


Box:1958:NGR


Certaine:1958:SPR


Franklin:1958:EPR


Gross:1958:AGP


Leslie:1958:PSM
REFERENCES


Muller:1958:IMG


Renyi:1958:ODP


Richtmyer:1958:NRS


Schmid:1958:KSL


Sengupta:1958:TRN


Sobol:1958:PRN


Thomson:1958:MCM

REFERENCES


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


REFERENCES

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


REFERENCES


REFERENCES


[231] Donald D. Wall. A random number test for large samples. In Anonymous [3903], pages 7–11. LCCN ????


REFERENCES


REFERENCES


Pinkham:1961:DFS


Rao:1961:GRP


Richtmyer:1961:MCM


Riffenburgh:1961:RPI


Sibuya:1961:EOR


Solomon:1961:SIA

REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


Magleby:1963:SNF


Marsaglia:1963:GDR


Marsaglia:1963:RNF


Moses:1963:TRP


Poore:1963:CAR


Tucker:1963:QCS


Ahsanullah:1964:RVE


Alanen:1964:TFF

Bekessy:1964:RBD


Brillinger:1964:BRI


Chow:1964:RNG


Durstenfeld:1964:ARP


Esmenjaud-Bonnardel:1964:PGN


Gebhardt:1964:GND


Halton:1964:ARI


Hammer:1964:GRN

REFERENCES


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


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES

CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See certification [623] and remarks [379, 390].

Pike:1965:ARN


Pike:1965:CAGb


Potter:1965:CNS


Pyke:1965:S


Reeves:1965:AUR


Rosenberg:1965:CNN


Scheinok:1965:DFR


Seshadri:1965:RVW

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

127

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


REFERENCES


Fleiss:1966:NER


Gorenstein:1966:APN


Hansson:1966:RAG


Heyde:1966:SRS


Hutchinson:1966:NUP


Jansson:1966:RNG


Loveland:1966:NIM

REFERENCES


REFERENCES


REFERENCES


Behboodian:1967:EAV


Canavos:1967:CAT


Chambers:1967:RNG


Coveyou:1967:FAU


Csorgo:1967:NPS


deBalbine:1967:NRP


Downham:1967:MCP

REFERENCES


REFERENCES


[413] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3908], pages 64–68. LCCN QA76.5 D55 1965.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


[Muller:1968:RN]


[Pillai:1968:NEI]


REFERENCES


[467] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3909], pages 70–111. LCCN QA1 S565 v. 3.


Fellen:1969:LEI


Good:1969:HRR


Grosenbaugh:1969:MFR


Gubenko:1969:FPR


Hemmerle:1969:GPN


Knop:1969:RAG


Kruskal:1969:EPR


REFERENCES


REFERENCES


Anonymous:1970:EWC


Anonymous:1970:FVP


Behboodian:1970:ERV


Blaisdell:1970:RSP


Butler:1970:AAG


Cenacchi:1970:PRN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[549] I. G. Dyadkin. An analogue of von Neumann’s algorithm for simulating a normal distribution. In *Monte Carlo methods and applications*
REFERENCES


Friedman:1971:REG


Gibbons:1971:NSI


Good:1971:SRS


Han:1971:DRV


Jackson:1971:PCC


REFERENCES


REFERENCES

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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). See erratum [682].


[645] D. G. Maritsas. The autocorrelation function of the two feedback shift-register pseudorandom source. *IEEE Transactions on Computers*, C-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

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


REFERENCES


REFERENCES


REFERENCES


for a comparison, both mathematical, and graphical, of the two algorithms. Reference [3] for IBM Report GC20-8011-0 is incorrectly given year 1969; the correct year is 1959.


[750] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3917], pages 321–355. ISBN 0-12-697540-X. LCCN QA76.6 .S9195 1976. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.7959. The complexity of the binary Euclidean algorithm for the greatest common denominator is shown to be $O(0.705 \lg N)$ for large $N = \max(|u|, |v|)$. See [2473] for an update, and a repair to an incorrect conjecture in this paper. See also [2397], where the worst case complexity is shown to be $O(\lg N)$, and the number of right shifts at most $2 \lg(N)$.


REFERENCES


REFERENCES


REFERENCES


[773] Donald E. Knuth and Andrew C. Yao. The complexity of nonuniform random number generation. In Traub [3917], pages 357–428. ISBN 0-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[830] P. Peskun. Improving the apparent randomness of pseudorandom numbers generated by the mixed congruential method. In D. Hogben and
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hollander:1978:TDU


Holmlid:1978:UCP


Kemp:1978:CGB


Kiefer:1978:PNA


Li:1978:EMN


Mallows:1978:PNA

REFERENCES


REFERENCES

1978. CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-5163.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES

Landauer:1981:RNF


Menzefricke:1981:BAC


Nekrutkin:1981:JSM


Preece:1981:DFD


Rubinstein:1981:RNG


Schatte:1981:RVL

REFERENCES

[1006] 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


Reprinted in [1154, pages 238–242]. See also the extended 32-bit generator in [3017].


REFERENCES


[1052] Masanori Fushimi and Shu Tezuka. The $k$-distribution of Generalized Feedback Shift Register pseudorandom numbers. *Communications of the
REFERENCES


REFERENCES


Miyatake:1983:MAR

Muller:1983:BRB

Pearson:1983:APR

Peterson:1983:ACT

Plumstead:1983:ISPa

Plumstead:1983:ISPb

Pokhodzei:1983:OMM
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kalle:1984:PRN


Kannan:1984:SPA


Kronmal:1984:ACA


Kuo:1984:SRI


Landauer:1984:ERN


Lugannani:1984:DRQ


Marsaglia:1984:EAM

References

236

Marsaglia:1984:FEI

Marsaglia:1984:GCM

Modianos:1984:RNG

Niederreiter:1984:PSP

Papoulis:1984:PRV

Paulsen:1984:IRN

Porter:1984:CNS
REFERENCES

237


Rasmussen:1984:FPS


Ronse:1984:FSR


Scholtz:1984:GS


Schorr:1984:PLV


Smith:1984:EMC


Thesen:1984:SER

REFERENCES


REFERENCES


REFERENCES

April/June 1985. CODEN AHCOE5. ISSN 0164-1239. URL http://
dlib.computer.org/an/books/an1985/pdf/a2141.pdf; http://

252–255, November 1985. CODEN SIMUA2. ISSN 0037-5497 (print),
1741-3133 (electronic). See criticism and response [1220].

[1142] Lawrence W. Dowdy and Manvinder S. Chopra. On the applicability of
using multiprogramming level distributions. *ACM SIGMETRICS Per-
ISSN 0163-5999 (print), 1557-9484 (electronic).

generation on microcomputers. In ????, editor, *Modeling and Simulation
San Diego, CA, USA, 1985. ISBN ????. LCCN ????

and Analysis of Discrete-Event Computer Simulations*. IEEE Computer
Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
USA, 1985. ISBN 0-8186-0597-9 (paperback), 0-8186-4597-0. ix + 475

*U.S.S.R. Computational Mathematics and Mathematical Physics*, 25
(4):91–93, ???? 1985. CODEN CMMPA9. ISSN 0041-5553, 0502-
004155538590148X. English translation of Russian original published in

number generator (RNG). In Blakley and Chaum [3936], pages
0302-9743 (print), 1611-3349 (electronic). LCCN QA76.9.A25 C791
REFERENCES


Feltz:1985:MLE


Figiel:1985:NLP


Fincke:1985:IMC


Gibbons:1985:NSI


Gleser:1985:EPG


Goldreich:1985:CAR


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Collings:1986:IGF


Deak:1986:EMG


Devroye:1986:AMG


Devroye:1986:GMS


Devroye:1986:NUR


Dyadkin:1986:EAM

REFERENCES


REFERENCES


[1217] H. Grothe. Matrixgeneratoren zur Erzeugung gleichverteilter Zufallsvektoren. (German) [Matrix generators for generating uniformly distributed


Kleijnen:1986:SRN


Ko:1986:NIP


LEcuyer:1986:EPB


Loukas:1986:CGB


Luby:1986:PRP


Malik:1986:PDF


Marsaglia:1986:IFC

REFERENCES


REFERENCES


REFERENCES


Bojanczyk:1987:SAE


Bonclet:1987:ACO


Bratley:1987:GS


Burton:1987:CLT


Chambers:1987:CMS


Chin:1987:TLP


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Dudewicz:1988:TVF


Durst:1988:TPR


Edwards:1988:CAM


Eichenauer:1988:MLTb


Eichenauer:1988:MLTc


Eichenauer:1988:NCP


Fishman:1988:MCR

[1331] G. S. Fishman. Multiplicative congruential random number generators with modulus $2^\beta$: An exhaustive analysis for $\beta = 32$ and a partial anal-


[1338] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. In IEEE [3951], pages 12–24. CODEN ASF-


REFERENCES

Heidelberger:1988:DES


Hong:1988:LGA


Izumi:1988:FGW


Kachitvichyanukul:1988:AHS


Kachitvichyanukul:1988:BRV


Kannan:1988:PFN

REFERENCES


[1357] Pierre L’Ecuyer and François Blouin. BonGCL, un logiciel pour la recherche de bons générateurs à congruence linéaire. (French) [BonGCL,


REFERENCES


REFERENCES


Ahrens:1989:AMS


Ahrens:1989:HAL


Ahrens:1989:NUR


Aiello:1989:HIG


Allender:1989:SCE


Babai:1989:MPL

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kachitvichyanukul:1989:ABS


Kahaner:1989:NMS


Kamps:1989:CPL


Kao:1989:RNG


Kelton:1989:RIM


Kharitonov:1989:LBP

REFERENCES


REFERENCES

generators. In MacNair et al. [3958], pages 467–476. ISBN 0-911801-58-

5823. IEEE order number 89CH2778-9.

[1440] David J. Lilja. Efficient generation of Poisson distributed random vari-
able. Technical Report CSRD 900, University of Illinois at Urbana-
Champaign, Center for Supercomputing Research and Development, Urb-
ana, IL 61801, USA, July 31, 1989. 15 pp.

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

[1442] N. M. Maclaren. The generation of multiple independent sequences of
DEN APSTAG. ISSN 0035-9254 (print), 1467-9876 (electronic). URL

(print), 1095-7200 (electronic).


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

McIntosh:1989:RAE


Meer:1989:SIP


Meier:1989:FCA


Mertsch:1989:PAS


Niederreiter:1989:STC


Paul:1989:IRN


Percus:1989:RNG

[1452] Ora E. Percus and Malvin H. Kalos. Random number generators for MIMD parallel processors. Journal of Parallel and Distributed Com-


REFERENCES


REFERENCES


[1472] François Baccelli and Zhen Liu. On the execution of parallel programs on multiprocessor systems — a queuing theory approach. *Journal of the


REFERENCES

Bralic:1990:AGR

Burford:1990:RNG

Carta:1990:TFI

Dagpunar:1990:SMD

Deak:1990:RNG

Deak:1990:URN

DeArman:1990:IRN


REFERENCES


[1497] George S. Fishman. Multiplicative congruential random number generators with modulus $2^\beta$: An exhaustive analysis for $\beta \approx 32$ and a partial


[1504] Oded Goldreich and Hugo Krawczyk. Sparse pseudorandom distributions (extended abstract). Lecture Notes in Computer Science, 435:113–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


[1561] Y. S. Sherif and R. G. Dear. Development of a new composite pseudo-
random number generator. *Microelectronics and Reliability*, 30(??):545–
553, ???? 1990. CODEN MCRLAS. ISSN 0026-2714 (print), 1872-941X
(electronic).

24(??):55–61, ???? 1990. CODEN PNENDE. ISSN 0149-1970 (print),
1878-4224 (electronic).

[1563] Ernst Stadlober. The ratio of uniforms approach for generating dis-
crete random variates. *Journal of Computational and Applied Mathemat-
science/article/pii/0377042790903495.

[1564] Shu Tezuka. Lattice structure of pseudorandom sequences from shift-
register generators. In Balci et al. [3960], pages 266–269. ISBN 0-911801-
72-3. LCCN QA76.5.W56 1990.

IBM Research, Tokyo Research Laboratory, Tokyo, Japan, January 1990.

[1566] Robert F. Tichy. Random points in the cube and on the sphere with
applications to numerical analysis. *Journal of Computational and Ap-

[1567] G. Tindo. *Automates cellulaires: applications à la modélisation de cer-
tains systèmes discrets et à la conception d’une architecture parallèle pour
la génération de suites pseudo-aléatoires.* (French) [Cellular automata:
applications to the modeling of certain discrete systems and toward the
design of a parallel architecture for generation of random sequences]. Disses-
tation (thesis), Université de Nantes, Nantes, France, 1990.


REFERENCES


[1588] Alan T. Clementson. A comment on a random-number generator for microcomputers. OR: the journal of the Operational Research Society,
REFERENCES


Compagner:1991:DR


Compagner:1991:HCR


Deng:1991:CRN


Deng:1991:RDR


Devroye:1991:AGD


Devroye:1991:ETA


Dohmann:1991:RNG

REFERENCES


Eichenauer-Herrmann:1991:ICPa


Eichenauer-Herrmann:1991:ICPb


Eichenauer-Herrmann:1991:NIC


Geers:1991:HEB


Gerasimov:1991:NOH


Gupta:1991:PAT


Hultquist:1991:GRN

REFERENCES


Maier:1991:FPR

Makino:1991:GSR

Marsaglia:1991:NCR

Marsaglia:1991:NGR

Matus:1991:AFD

Maurer:1991:LRP

Maurer:1991:UST


REFERENCES


[1641] Timothy E. Revello. A combination of exponentiation ciphers and the data encryption standard as a pseudorandom number generator. The-
sis (M.S.), Rensselaer Polytechnic Institute at The Hartford Graduate Center, Troy, NY, USA, 1991. viii + 68 pp.

[1642] 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

Vose:1991:LAG


Wakefield:1991:EGR


Walsh:1991:MFR


Wheeler:1991:PMN


Wheeler:1991:SIC


Yamamoto:1991:NEM

REFERENCES


REFERENCES


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

Dai:1992:BSD


DalleMolle:1992:HOC


DeMatteis:1992:CCD


DeMatteis:1992:CDP


Deng:1992:GLT


Deng:1992:RSN


[1702] Eduardo Engel. *A road to randomness in physical systems*, volume 71 of *Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidel-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Grassberger:1993:CGR


Grassberger:1993:MCS


Hamilton:1993:PNGa


Hamilton:1993:PNGb


Hansen:1993:GPC


Hayes:1993:WF


Hildebrand:1993:RPF

Hormann:1993:GBR


Hormann:1993:PRN


Hormann:1993:QNU


Hormann:1993:TRM


Jebelean:1993:CSG


Kalkuhl:1993:PDC

[1815] Christoph Kalkuhl. Pulse/data channel extends programmable pulse generator applications. *Hewlett-Packard Journal: technical information*
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1848] 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 [1373, 1480, 1834, 1858]. The authors report that they would now recommend the MCG $x_{n+1} = 48271x_n \mod (2^{31} - 1)$ over their original $x_{n+1} = 16807x_n \mod (2^{31} - 1)$.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

Couture:1994:LSC

[1893] Raymond Couture and Pierre L’Ecuyer. On the lattice structure of

Cuccaro:1994:TTQ

[1894] Steven A. Cuccaro, Michael Mascagni, and Daniel V. Pryor. Tech-
niques for testing the quality of parallel pseudorandom number gener-
ators. Technical report SRC-TR-94-128, Supercomputing Research Cen-

Davis:1994:CRA

[1895] Don Davis, Ross Ihaka, and Philip Fenstermacher. Cryptographic ran-
domness from air turbulence in disk drives. In Desmedt [3989], pages
114–120. CODEN LNCSDE. ISBN 3-540-58333-5 (Berlin), 0-387-58333-
5 (New York). ISSN 0302-9743 (print), 1611-3349 (electronic). LCCN
service/series/0558/bibs/0839/08390114.htm; http://link.springer-

DeArmon:1994:RLO

[1896] James S. DeArmon. Randomness of low-order bits in random number
sagepub.com/content/62/6/373.abstract.

Deng:1994:DIR

of random number generators for multiprocessor systems. *International
IMSIEK. ISSN 0228-6203 (print), 1925-7082 (electronic). URL http://

Devroye:1994:NHS

[1898] Luc Devroye and Paul Kruszewski. A note on the Horton–Strahler num-
ber for random trees. *Information Processing Letters*, 52(3):155–159,
REFERENCES

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


REFERENCES


Eichenauer-Herrmann:1994:GIC


Eichenauer-Herrmann:1994:ILB


Eichenauer-Herrmann:1994:SIN


Endl:1994:CRG


Entacher:1994:CNP


Gaines:1994:RGS


Hormann:1994:TRM


Hormann:1994:UGD


Huber:1994:PLG


James:1994:RFI


Jimbo:1994:RBB


Jimbo:1994:RBD


Johnson:1994:CUD


REFERENCES


Makino:1994:LFR


Marsaglia:1994:MAR


Marsaglia:1994:REI


Marsaglia:1994:SPV


Mascagni:1994:FHQ


Mascagni:1994:PPN


Matsumoto:1994:TGG

REFERENCES


[Rarity:1994:QRN]


[Riesel:1994:PNC]


[Ritter:1994:EPR]


[Rivest:1994:DBI]


[Schneier:1994:AAd]


[Shallit:1994:ALS]

Shukhman:1994:GQR


Sitharam:1994:PGL


Sorenson:1994:TFG


Spanier:1994:QRM


Strauch:1994:D


Swan:1994:AAa


Szwarcfiter:1994:EKD

REFERENCES

Takashima:1994:STT

ISSN 0915-2350 (print), 1881-1337 (electronic).

Tezuka:1994:DDC


Tezuka:1994:MDC


Tezuka:1994:UVL


Tierney:1994:MCE


vanderMeer:1994:RBG


Vattulainen:1994:NTR

Institute for Theoretical Physics, University of Helsinki, Helsinki, Finland.


REFERENCES


Carrasco:1995:RRT


Chen:1995:IDP


Childs:1995:CIH


Chou:1995:LTI


Chou:1995:PLI


Chow:1995:NRP


Compagner:1995:OCR

[2009] A. Compagner. Operational conditions for random-number generation. Physical Review E (Statistical physics, plasmas, fluids, and re-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Koc:1995:RCS


Kubota:1995:DRE


Kurita:1995:DWD


Lee:1995:CSS


Leeb:1995:DT


Leeb:1995:RNC


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Vattulainen:1995:CSS


Vattulainen:1995:MIF


Vattulainen:1995:PMT


Walker:1995:GRV


Wegenkittl:1995:ETPa


Wegenkittl:1995:ETPb


Wegenkittl:1995:THS

[2104] Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inversive congruential pseudorandom numbers? Journal of Computational


REFERENCES


REFERENCES

Barron:1996:RTR


Barry:1996:RTU


Beaver:1996:CPC


Bellare:1996:PFR


Berdnikov:1996:NMP


Bernhofen:1996:RBR

REFERENCES


REFERENCES


[2134] Martin Dietzfelbinger. Universal hashing and k-wise independent random variables via integer arithmetic without primes. Lecture Notes in
REFERENCES


Dodge:1996:NRN


Dorfman:1996:PSR


Dwyer:1996:TRNa


Dwyer:1996:TRNb


Eichenauer-Herrmann:1996:ABC


Eichenauer-Herrmann:1996:CIC


Eichenauer-Herrmann:1996:EPI

REFERENCES


Eichenauer-Herrmann:1996:MEI


Emmerich:1996:PVG


Entacher:1996:RSP


Fernandez:1996:FAR


Fischer:1996:EPR


Fishman:1996:MCC


REFERENCES


[2160] Chiang Kao and J. Y. Wong. An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus

**Kato:1996:NCP**


**Kato:1996:STN**


**Kemp:1996:CFP**


**Koc:1996:ACM**

REFERENCES


Luby:1996:PCA


Luo:1996:TDS


Marini:1996:CHR


Marsaglia:1996:DBT


Masuda:1996:PPR


Matsumoto:1996:SDR


Matthews:1996:SRN

REFERENCES


REFERENCES


[2191] Igor Radović, Ilya M. Sobol, and Robert F. Tichy. Quasi-Monte Carlo methods for numerical integration: Comparison of different low discrep-

[Rubin:1996:OTP]


[Sanchis:1996:PAC]


[Schervish:1996:VWT]


[Schneier:1996:ACP]


[Sethumadhavan:1996:NPE]


[Sezgin:1996:RNG]


REFERENCES


Ugrin-Sparac:1996:PET


Wallace:1996:FPG


Wang:1996:LIL


Wegenkittl:1996:RSP


Alon:1997:SSD

REFERENCES


REFERENCES


Bellare:1997:PRN


Berblinger:1997:MCI


Berg:1997:CNF


Binder:1997:AMC


Binder:1997:MCS


Cario:1997:MGR

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


Eichenauer-Herrmann:1997:AEP


Eichenauer-Herrmann:1997:CCC


Eichenauer-Herrmann:1997:ICP


Eichenauer-Herrmann:1997:PSN


Eichenauer-Herrmann:1997:QCP


REFERENCES


[2250] P. Hellekalek. On correlation analysis of pseudorandom numbers. In H. Niederreiter, P. Hellekalek, G. Larcher, and P. Zinterhof, editors,
REFERENCES


[2251] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [4010], page ?? ISBN 3-901608-11-7. LCCN ????


REFERENCES


[2269] Hannes Leeb and Stefan Wegenkittl. Inversive and linear congruential pseudorandom number generators in empirical tests. *ACM Transactions*


#define znew ((z=36969*(z&65535)+(z¿¿16))¡¡16) 
#define wnew ((w=18000*(w&65535)+(w¿¿16))&65535) 
#define IUNI (znew+wnew) 
#define UNI (znew+wnew)*4.656613e-10 
static unsigned long z=362436069, w=521288629; void setseed(unsigned long i1,unsigned long i2)z=i1; w=i2; Whenever you need random integers or random reals in your C program, just insert those six lines at (near?) the beginning of the program. In every expression where you want a random real in [0, 1) use UNI, or use IUNI for a random 32-bit integer. No need to mess with ranf() or ranf(lastI), etc, with their requisite overheads. Choices for replacing the two multipliers 36969 and 18000 are given below. Thus you can tailor your own in-line multiply-with-carry random number generator.”.


REFERENCES


REFERENCES


vanHameren:1997:GLD


Woodward:1997:ECD


Wu:1997:MCR


Zubkov:1997:PTD


Aiello:1998:DPP


Andreev:1998:NGD

Antoch:1998:RPN


Bach:1998:EPM


Baldwin:1998:PAB


Baldwin:1998:PPR


Ballesteros:1998:TRN


Barni:1998:CPD

REFERENCES


REFERENCES

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

Coddington:1998:RNG


Couture:1998:GEI


DSouza:1998:SBD


Eichenauer-Herrmann:1998:IUB


Eichenauer-Herrmann:1998:LBD


Eichenauer-Herrmann:1998:SQI

REFERENCES

loc.gov/catdir/enhancements/fy0815/97034133-d.html;  http://www.loc.gov/catdir/enhancements/fy0815/97034133-t.html.

Ellison:1998:CRN


Emmerich:1998:EPC


Emmerich:1998:SIP


Entacher:1998:BSW


Entacher:1998:LCG


Entacher:1998:LIP


REFERENCES


REFERENCES


[Hickernell:1998:LRH]

[Hoffman:1998:RNG]

[Jakobsson:1998:PSP]

[Kao:1998:RNG]

[Kao:1998:SET]

John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. Lecture Notes in
Knudsen:1998:JHH


Knuth:1998:SA


Kolmogorov:1998:TRN


Larcher:1998:DPS


LEcuyer:1998:DPS


LEcuyer:1998:GPI


Philip M. Lurie and Matthew S. Goldberg. An approximate method for sampling correlated random variables from partially-specified distri-


[2358] Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number genera-
REFERENCES


REFERENCES


REFERENCES


Pong P. Chu and Robert E. Jones. Design techniques of FPGA-based random number generator (extended abstract). In ?????, editor, *MAPLD 99 Proceedings: Military and Aerospace Applications*


REFERENCES


REFERENCES


[2419] Frances Griffin, Harald Niederreiter, and Igor Shparlinski. On the distribution of nonlinear recursive congruential pseudorandom numbers of


REFERENCES


Sobol:1999:PRN


Soto:1999:EST


Soto:1999:RTA


Soto:1999:STRa


Soto:1999:STRb


Soto:1999:STRc

Stauffer:1999:IMT


Sudan:1999:PGX


Tomassini:1999:GHQ


Tretiakov:1999:EMC


Trevisan:1999:CEU


Vattulainen:1999:FTR

I. Vattulainen. Framework for testing random numbers in parallel calculations. *Physical Review E (Statistical physics, plasmas, fluids, and


[2467] 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


Fukuyama:2000:PFA


Gennaro:2000:IPR


Gentleman:2000:LSS


Goldreich:2000:ITP


Gutierrez:2000:MDI

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2508] George Marsaglia. The monster, a random number generator with period over $10^{2857}$ times as long as the previously touted longest-period one. Technical report ????., Florida State University, Tallahassee, FL, USA, ???? 2000.


REFERENCES


Mascagni:2000:ASS


Mascagni:2000:CAS


Mauduit:2000:FPBa


Mauduit:2000:FPBb


Miles:2000:L


Moriai:2000:PTL


REFERENCES


Viswanath:2000:RFS


Wikramaratna:2000:PRN


Yaguchi:2000:RHR


Zhukov:2000:ANA


Ackermann:2001:PRN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Gerosa:2001:FIB


Gonsalves:2001:PAS

[2568] Richard J. Gonsalves. Pivot algorithm for self-avoiding walks on a square lattice. Fortran program, 2001. URL http://www.physics.buffalo.edu/gonsalves/phy411-506_spring01/Files/Chapter12/saw.f. The program contains code (near the end) for the portable rannyu() generator. It is a linear congruential generator with multiplier $A = 31\, 167\, 285 = 0x1d9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.

Guimond:2001:CRN


Gutierrez:2001:IMP


Gutmann:2001:RNG


REFERENCES


[2582] Lei Kuang and Armand M. Makowski. Convex stability and asymptotic convex ordering for non-stationary arrival processes. *ACM SIGMET-
REFERENCES


tions in honor of the seventieth birthday of Masanobu Shinozuka on December 23, 2000.

Li:2001:SPD


Liang:2001:NET


Liang:2001:TMU


Litvak:2001:SPE


Mascagni:2001:PIC

REFERENCES


[2606] Harald Niederreiter and Igor E. Shparlinski. On the distribution of
inversive congruential pseudorandom numbers in parts of the period.
*Mathematics of Computation*, 70(236):1569–1574, October 2001. CO-
DEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (electronic). URL
http://www.ams.org/journal-getitem?pii=S0025-5718-00-01273-
4; http://www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-
4/S0025-5718-00-01273-4.dvi; http://www.ams.org/mcom/2001-
70-236/S0025-5718-00-01273-4/S0025-5718-00-01273-4.pdf; http:
//www.ams.org/mcom/2001-70-236/S0025-5718-00-01273-4/S0025-
5718-00-01273-4.ps; http://www.ams.org/mcom/2001-70-236/S0025-

[2607] Harald Niederreiter and Arne Winterhof. On a new class of inversive
pseudorandom numbers for parallelized simulation methods. *Periodica
0031-5303 (print), 1588-2829 (electronic).

[2608] NIST. *Batteries of Statistical Tests for Random Number Generators.*
National Institute for Standards and Technology, Gaithersburg, MD,
Wide Web site.

[2609] NIST. Security requirements for cryptographic modules. Federal In-
formation Processing Standards Publication FIPS PUB 140-2, National
Institute for Standards and Technology, Gaithersburg, MD, USA, May

[2610] Landon Curt Noll, Simon Cooper, and Mel Pleasant. How good is
test.html.

[2611] Peyton Z. Peebles. *Probability, random variables, and random
signal principles.* McGraw-Hill series in electrical and computer
engineering. McGraw-Hill, New York, NY, USA, fourth edition,
REFERENCES


REFERENCES


[2630] 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.

Touzin:2001:GRM


Trevisan:2001:EPG


Tu:2001:NFG


Vadhan:2001:OP


Vanura:2001:ARC


Watkins:2001:ERN


REFERENCES


REFERENCES


[2654] Frank Emmerich. Average equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the


REFERENCES


REFERENCES


REFERENCES


[2682] Pierre L’Ecuyer and Christiane Lemieux. Recent advances in randomized
quasi-Monte Carlo methods. In Dror et al. [4041], pages 419–474. ISBN
gov/catdir/enhancements/fy0820/2001050485-d.html; http://
www.loc.gov/catdir/enhancements/fy0820/2001050485-t.html.

tests of uniformity for random number generators. SIAM Journal on
siam.org/sam-bin/dbq/article/34903.

[2684] Pierre L’Ecuyer and Richard Simard. TestU01: a software library in
ANSI C for empirical testing of random number generators: Software
user’s guide. Web report, Département d’Informatique et de Recherche
Opérationnelle, Université de Montréal, Montréal, Québec, Canada,
http://www.iro.umontreal.ca/~simardr/testu01/tu01.html.

[2685] J. Leydold and W. Hörmann. UNURAN — a library for universal non-
uniform random number generators. Web software archive., 2002. URL
http://statistik.wu-wien.ac.at/unuran.

rejection and correlation introduction. In Fang et al. [4042], pages 345–
http://www.loc.gov/catdir/enhancements/fy0817/2002283816-d.
html.

[2687] Ping Luo. A combined generator based on linear congruential generators
and its structural improvement. Journal on Numerical Methods and

[2688] Hosam Mahmoud and Tatsuie Tsukiji. On the internal structure of ran-
dom recursive circuits. Journal of Computational and Applied Mathe-
matics, 142(1):155–171, May 1, 2002. CODEN JCAMDI. ISSN 0377-0427

[Marsaglia:2002:RGB]


[Marsaglia:2002:SDP]


[Martin:2002:ARN]


[Martinez:2002:CSH]


[Matsumoto:2002:NTW]

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2726] 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.”.


[2731] Diane Crawford, Simone Santini, Ralph Castain, William F. Dowling, John Cook, Simon Dobson, Peter J. Denning, Robert Dunham, Jef Raskin, and Dennis Tsichritzis. Forum: When is a computer more like a guitar than a washing machine?; corroboration the only way to determine Web accuracy; how to teach critical thinking about Web content; create a random number service based on the Mersenne Twister; make fiar uses a legal requirement in DRM systems; “The Missing Customer” redux; enthusiasm, drive, wisdom, patience not tied to age. *Communications of the ACM*, 46(7):11–13, July 2003. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

[2806] Richard P. Brent. Note on Marsaglia’s xorshift random number genera-
ISSN 1548-7660. URL http://www.jstatsoft.org/counter.php?id=
101&url=v11/105/v11i05.pdf&ct=1. See [2764, 2920, 3782]. This arti-
cle shows the equivalence of xorshift generators and the well-understood
linear feedback shift register generators.

[2807] Timothy C. Brown. Transforming a random variable to a prescribed dis-
tribution: An application to school-based assessment. Journal of Applied
3215980.

[2808] James Antonio Bucklew. Introduction to Rare Event Simulation, vol-
ume ?? of Springer Series in Statistics. Springer-Verlag, Berlin, Ger-
many / Heidelberg, Germany / London, UK / etc., 2004. CODEN ????
ISBN 0-387-20078-9, 1-4419-1893-0, 1-4757-4078-6 (e-book). ISSN 0172-

[2809] Alessandro Conflitti and Igor E. Shparlinski. On the multidimen-
tional distribution of the subset sum generator of pseudorandom
numbers. Mathematics of Computation, 73(246):1005–1011,
April 2004. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-
S0025-5718-03-01563-1/home.html; http://www.ams.org/mcom/
2004-73-246/S0025-5718-03-01563-1/S0025-5718-03-01563-1-dvi;
http://www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-
5718-03-01563-1-1.pdf; http://www.ams.org/mcom/2004-73-
246/S0025-5718-03-01563-1/S0025-5718-03-01563-1-1.ps; http:
//www.ams.org/mcom/2004-73-246/S0025-5718-03-01563-1/S0025-
5718-03-01563-1.tex; http://www.jstor.org/stable/pdfplus/
4099816.pdf.

[2810] Lih-Yuan Deng. Generalized Mersenne prime number and its applica-
www.loc.gov/catdir/enhancements/fy0817/2004041328-d.html.


REFERENCES


[2823] Daniel R. Jeske and Todd Blessinger. Tunable approximations for the mean and variance of the maximum of heterogeneous geometrically dis-


REFERENCES


Ossola:2004:SED


Panneton:2004:CEP


Panneton:2004:RNG


Peitgen:2004:CGH


Rasulov:2004:QSB

REFERENCES


REFERENCES


REFERENCES


[2881] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. Lecture Notes in Computer

Deng:2005:EPM


Dodge:2005:RNG


Eastlake:2005:RRR


Elsner:2005:IRN


Entacher:2005:BLP


Falcioni:2005:PMC


Gennaro:2005:IPR


Gerlovina:2005:ABL


Gonnet:2005:MRG


Gonzalez:2005:SCM


Gubernatis:2005:MRM


Hahn:2005:CLM

REFERENCES


REFERENCES


REFERENCES


Tang:2005:EER


Tang:2005:MLC


Tang:2005:RMR


Terpstra:2005:SIC


Topuzoglu:2005:LCP


Tu:2005:SRD

REFERENCES

Wichmann:2005:GGP


Wiese:2005:IPN


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ


REFERENCES

Barker:2006:RRN


BenAtti:2006:BMA


Berkovitz:2006:EHR


Brent:2006:FRR


Brent:2006:SLP


Cools:2006:CEL


Creutzig:2006:BRW

REFERENCES


Devroye:2006:NRV


Dick:2006:WSD


Dickinson:2006:EEL


El-Mahassni:2006:DNC


Evans:2006:DOS


Faure:2006:SCR

REFERENCES


REFERENCES


REFERENCES

springerlink.com/content/c60q42qt2m035685/.

gov/catdir/toc/ecip0611/2006010073.html.

article/pii/S0927050706130030.


arnumber=1628955.

REFERENCES


Mueller:2006:SMG


Nau:2006:RN


Nuyens:2006:FAC


Nuyens:2006:FCCa


Nuyens:2006:FCCb


Panneton:2006:IDH


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Drutarovsky:2007:RCB


Dupuis:2007:ISS


Echeverria:2007:FGR


Edgington:2007:RT


Gerlovina:2007:LBS


REFERENCES


REFERENCES


REFERENCES


[3081] Sastra Wijaya, Syn Kiat Tan, and Sheng-Uei Guan. Permutation and sampling with maximum length CA or pseudorandom number genera-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

556


[3122] Johan Håstad and Mats Näslund. Practical construction and analysis of pseudo-randomness primitives. *Journal of Cryptology: the jour-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3150] Wei Li, Kangshun Li, Wensheng Zhang, Chao Wang, and Ying Huang. A random number generator based on particle dynamical evolutionary algorithm. In 2008. ICNC ’08. Fourth International Conference on
REFERENCES

Li:2008:SAD


Liu:2008:CMI


Lovett:2008:UPG


Martin:2008:IPR


Masaro:2008:RODb


Matsumoto:2008:MPR


Nandakumar:2008:EET


Nguyen:2008:ODD


Niederreiter:2008:CPN


Niederreiter:2008:ESN


Niuda:2008:BFL


Ozdemir:2008:RNG


[3181] Manas Somaiya, Christopher Jermaine, and Sanjay Ranka. Learning correlations using the mixture-of-subsets model. ACM Transactions on


David B. Thomas and Wayne Luk. Resource efficient generators for the floating-point uniform and exponential distributions. In IEEE [4065],
REFERENCES

cites

Tokunaga:2008:TRN


Toyama:2008:GPR


Uchida:2008:FPR


Udawatta:2008:TVN


Varbanets:2008:ESS


Varbanets:2008:ICGa

Varbanets:2008:ICGb


Walker:2008:EPN


Wang:2008:DCP


Ware:2008:RIE


Wikramaratna:2008:ACR


Willink:2008:UPN

Wold:2008:AER


Xiang:2008:NPR


Xu:2008:SMS


Yaguchi:2008:NNP


Yang:2008:LLM


Yang:2008:NTR

REFERENCES

on Information Science and Engineering, volume 2, pages 236–238. IEEE
Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
.jsp?tp=&arnumber=4732384.

[3206] Abbas Alhakim and Mufutau Akinwande. A multiple stream gener-
ator based on de Bruijn digraph homomorphisms. Journal of Sta-
CODEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic).
1563-5163. URL http://www.tandfonline.com/doi/abs/10.1080/
00949650802322129.

of cryptographically strong generator by linearly generated sequences.
International Journal of Computer Science and Security (IJCSS), 3(3):
186–200, June 2009. CODEN ???? ISSN 1985-1553. URL http:/
/www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/
Issue3/IJCSS-78.pdf.

[3208] Baruch Awerbuch and Christian Scheideler. Robust random number
generation for peer-to-peer systems. Theoretical Computer Science, 410
(6–7):453–466, February 28, 2009. CODEN TCSCDI. ISSN 0304-3975
(print), 1879-2294 (electronic).

using pseudo-random number generators. In 2009. CSE ’09. Interna-
tional Conference on Computational Science and Engineering, volume 3,
pages 418–423. IEEE Computer Society Press, 1109 Spring Street, Suite
300, Silver Spring, MD 20910, USA, 2009. URL http://ieeexplore.
ieee.org/stamp/stamp.jsp?tp=&arnumber=5283236.

Impact of the quality of random numbers generators on the perform-
ance of particle swarm optimization. In IEEE International Conference on
Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD
.jsp?tp=&arnumber=5346366.
Blacher:2009:FRN


Blacher:2009:PRN


Blaszczyk:2009:EVT


Blaszczyk:2009:HIP


Cao:2009:DSB


Cecen:2009:NHN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3264] JunKyu Lee, Yu Bi, Gregory D. Peterson, Robert J. Hinde, and Robert J. Harrison. HASPRNG: Hardware Accelerated Scalable Parallel Ran-
REFERENCES


Lemieux:2009:PNG


Marchi:2009:PPR


Markenos:2009:FIA


McCullough:2009:AES


Mitchum:2009:DPR

REFERENCES


Orlov:2009:ORN


Paindaveine:2009:MRT


Pareschi:2009:PAC


Petrov:2009:SLL


Qiu:2009:CMW


Reidler:2009:USR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Wang:2009:NPR


Wayne:2009:PAT


Wei:2009:BFT


Wei:2009:QRN


Wold:2009:OST


Xiao-chen:2009:URN


Abbott:2010:QRN


Agapie:2010:RPH


Akhshani:2010:PRN


Anashin:2010:NAE


Anyanwu:2010:DCS


Banks:2010:DES

REFERENCES


[3328] A. A. Borovkov. Integro-local and local theorems on normal and large deviations of the sums of nonidentically distributed random variables in


REFERENCES


REFERENCES

2618–2626, December 2010. CODEN JSSODM. ISSN 0164-1212 (print), 1873-1228 (electronic).


Hongo:2010:RNG


Hotoleanu:2010:RTT


Jaksic:2010:QCL


Jones:2010:IMD


Kang:2010:FIG


Kawai:2010:AOA

REFERENCES


REFERENCES

Meka:2010:PGP


Moghadam:2010:DRN


Murguia:2010:IAP


Navin:2010:CSR


Navin:2010:ETU


REFERENCES


Panneton:2010:RSR


Pareschi:2010:ITH


Pashley:2010:GRN


Passerat-Palmbach:2010:RIG


Peris-Lopez:2010:CSP


Plesser:2010:RSI


Prochan:2010:BQQ


Qi:2010:DFR


Quantis:2010:RNG


Quantis:2010:RTR


REFERENCES


Stankovski:2010:GDN


Suciu:2010:PIN


Tang:2010:BHA


Tang:2010:BLC


Tang:2010:OMR


REFERENCES


REFERENCES


REFERENCES


Zafar:2010:GRN


Zhmurov:2010:EPR


Zimand:2010:SEC


Abbott:2011:NNS


Abbott:2011:QRN


Al-Abiachi:2011:CDN


[3441] 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.


Demchik:2011:PRN


deOliveira:2011:DRP


desai:2011:PRN


Devroye:2011:DCM


Duan:2011:POR


Ergun:2011:IPS


REFERENCES


Harase:2011:FLR


Heam:2011:SEU


Hedayatpour:2011:HFB


Hofert:2011:SET


Hung:2011:DRD


REFERENCES


REFERENCES


REFERENCES


Marinucci:2011:RFS


Marton:2011:PUR


Merhi:2011:SPR


Mohamed:2011:EAG


Mukherjee:2011:RGU


Phillips:2011:PRN


[3518] 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. [4087], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????

Seyedzadeh:2011:IES


Shaolan:2011:EDE


Shparlinski:2011:ADP


Simard:2011:CTS


Sinescu:2011:ECS


Soucarros:2011:ITT


REFERENCES


REFERENCES


REFERENCES

Anonymous:2012:CTC

Applebaum:2012:PGL

Barash:2012:GSP

Barker:2012:RRN

Bayon:2012:CEA

Becher:2012:TNN

Beisbart:2012:WMC
[3555] Claus Beisbart and John D. Norton. Why Monte Carlo simulations are inferences and not experiments. International Studies in the Philosophy


REFERENCES

Chen:2012:ECR


Chi:2012:ESN


Chiu:2012:MTR


Cohen:2012:SMI


Colbeck:2012:FRC


Deng:2012:ECS

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

[3592] Liang Li. Testing several types of random number generators. MS thesis, Department of Computer Science, Florida State University, Tallahassee, FL, USA, Fall 2012. vi + 91 pp. URL http://search.proquest.com/pqdtglobal/docview/1287745850/.


REFERENCES


[3604] NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Insti-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3632] 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.


Claessen:2013:SPN


Deng:2013:FTQ


Ducklin:2013:ARN


Frauchiger:2013:TRR


Gao:2013:GGA


Gopalan:2013:PGC


REFERENCES


Liberty:2013:THR


Liu:2013:ITT


Ma:2013:PQR


Malik:2013:UCB


Mascagni:2013:PPR

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Devroye:2014:RVG


Dodis:2014:HEY


Doty-Humphrey:2014:STP


England:2014:ERG


Fukushima:2014:SDS


Gomez-Perez:2014:AEA

Domingo Gómez-Pérez, Alina Ostafe, and Igor Shparlinski. Algebraic entropy, automorphisms and sparsity of algebraic dynamical sys-


REFERENCES


REFERENCES


REFERENCES


Andersen:2015:MEL


Astor:2015:ADI


Berman:2015:NAA


Beznosko:2015:HSH


Beznosko:2015:PPF


Carlet:2015:EBF

Claessen:2015:GCR


Guyeux:2015:ECS


Haeupler:2015:SFD


Hare:2015:MDR


Hill:2015:PRN


Jessa:2015:QRS

REFERENCES


REFERENCES


[3743] Santanu Sarkar. Further non-randomness in RC4, RC4A and VMPC. 
CODEN ???. ISSN 1936-2447 (print), 1936-2455 (electronic). URL 
http://link.springer.com/accesspage/article/10.1007/s12095- 
014-0119-0.

[3744] Konstantin G. Savvidy. The MIXMAX random number genera-
pii/S0010465515002489.

[3745] Hans Georg Schaathun. Evaluation of splittable pseudo-random gener-
CODEN JFPRES. ISSN 0956-7968 (print), 1469-7653 (electronic). URL https:// 
www.cambridge.org/core/journals/journal-of-functional-programming/article/evaluation-of-splittable-pseudorandom-generators/3EBAA9F14939C5BB5560E32D1A13 
2F

Gaussian random number generator. *ACM Transactions on Reconfig-
CODEN ???. ISSN 1936-7406 (print), 1936-7414 (electronic).

[3747] Ryo Urano and Yuko Okamoto. Deterministic replica-exchange method 
without pseudo random numbers for simulations of complex sys-
pii/S0010465515003069.

[3748] Yongge Wang and Tony Nicol. On statistical distance based test-
pii/S0167404815000693.


REFERENCES


REFERENCES


Miller:2016:RPS


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA


Raitza:2016:RRN


Savvidy:2016:ACS


Savvidy:2016:SEC

Konstantin Savvidy and George Savvidy. Spectrum and entropy of C-systems MIXMAX random number generator. *Chaos, Solitons & Frac-
REFERENCES


VanBever:2016:SBT


Vigna:2016:EEM


Yamakami:2016:PGA


Yu:2016:GPR


Aljahdali:2017:FIS


Anonymous:2017:DAD

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 [3794] for details of the attack.


[3792] Riccardo Bernardini and Roberto Rinaldo. Making random permutations from physically unclonable constants. *International Journal of In-
REFERENCES


Chalk:2017:CIR


Cohney:2017:PSR


Deng:2017:DPR


Devroye:2017:EBC


Dodis:2017:HEY


Fog:2017:PRN

Ghersi:2017:CQR


Herrero-Collantes:2017:QRN


Lampropoulos:2017:BLL


Lenstra:2017:TPR


Monroe:2017:NPR


Nordrum:2017:TRN


REFERENCES


Blackman:2018:SLP


Blackman:2018:XXG


Cai:2018:VHA


Chang:2018:CSL


Checkoway:2018:WDL


Deng:2018:SFE


REFERENCES


Wang:2018:LBA


Xu:2018:SCM


Achiha:2019:GKW


Alhadawi:2019:DPB


Arnas:2019:RSU


Bernard:2019:PSM

REFERENCES


REFERENCES


Kim:2019:GBA


Kissel:2019:KRC


Lemire:2019:FRI


Lemire:2019:XXX


Liu:2019:LFP


Martirosyan:2019:STM


Zhang:2019:REU


Anonymous:2020:X

[3873] Anonymous. Xorshift. Web site., 2020. URL https://en.wikipedia.org/wiki/Xorshift. This article discusses Marsaglia’s Xorshift family of generators, including 32-bit, 64-bit, and 128-bit variants, plus xorwow, xorshift+, xoshiro, and xoroshiro, with comments about which common test suites they pass or fail. Lua 5.4 changed from the previous default of C’s rand() or random() to a new one based on xoshiro256** (256-bit state, 32- or 64-bit result). The period of xoshiro256** is 2**256 - 1 (about 10**77). See [3818, 3819].

Goualard:2020:GRF


Gurjar:2020:PBO


Hurley-Smith:2020:QLC


James:2020:RHQ

REFERENCES


[3894] David Wagner. Writings on randomness; source code for generating randomness; source code for testing randomness; hardware for generating randomness; source code to other useful crypto modules; miscellaneous. World-Wide Web site., 20xx. URL http://www.cs.berkeley.edu/~daw/rnd/.

[3895] Yvan Saint-Aubin and Christiane Rousseau, editors. Mathematics and Technology. Springer Undergraduate Texts in Mathematics and Technol-


REFERENCES


REFERENCES


REFERENCES


[3919] Peter C. C. Wang, editor. Information linkage between applied mathematics and industry: Proceedings of the First Annual Workshop on the
REFERENCES


Dempster:1980:SPP


Oren:1980:SDM


Eddy:1981:CSS


Rubinstein:1981:SMC


Grossmann:1982:PSI


IEEE:1982:ASF

REFERENCES


REFERENCES


REFERENCES


Mehlhorn:1985:SAS


ACM:1986:PEA


Arkin:1986:SOP


DAgostino:1986:GFT


Heath:1986:HMP

Wilson:1986:WSC


ACM:1987:PNA


Chaum:1987:ACE


Deavours:1987:CYT


IEEE:1987:ASF


Odlyzko:1987:ACC


REFERENCES


REFERENCES


IEEE:1990:PSN


Pomerance:1990:CCNb


Anonymous:1991:PIS


Day:1991:PAA


Dorninger:1991:CGA


Nelson:1991:WSC

REFERENCES


[3975] Gustavus J. Simmons, editor. Contemporary Cryptology: the science of information integrity. IEEE Computer Society Press, 1109 Spring Street,
REFERENCES


Steele:1992:PA


Swain:1992:PWS


Vouk:1992:PAS


ACM:1993:PPT


Bronstein:1993:IPI


Lenstra:1993:DNF

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


IEEE:1996:ASF


IEEE:1996:ASF


Trobec:1996:PIW


Andradottir:1997:PWS


Gell-Mann:1997:QJA
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Schueller:2001:MCS


Smelser:2001:IES


Spector:2001:GPG


ACM:2002:PTF


Dror:2002:MUE

REFERENCES

713


Fang:2002:MCQ


USENIX:2002:PBF


ACM:2004:PAA


Gentle:2004:HCS


Niederreiter:2004:MCQ

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[4068] Christiane Rousseau and Yvan Saint-Aubin, editors. Mathematics and Technology. Springer Undergraduate Texts in Mathematics and Technol-
REFERENCES


REFERENCES


[4079] Dieter Gollmann, Jean-Louis Lanet, and Julien Iguchi-Cartigny, editors. *Smart card research and advanced application: 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14–16, 2010: proceedings*, volume 6035 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / Lon-
REFERENCES

IEEE:2010:ISV


IEEE:2010:PIA


Peterson:2010:IEE


ACM:2011:PAI


Gilli:2011:NMO

REFERENCES


REFERENCES

Cooper:2012:HWC


Dunn:2012:EMC


Dyson:2012:TCO


Gentle:2012:HCS


Hwu:2012:GCG


IEEE:2012:PIA

REFERENCES

ACM:2013:SPF


Higham:2015:PCA


Krizhizhanovskaya:2020:CSI