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/

19 June 2018
Version 1.292

Title word cross-reference

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

(0, 1) [1050]. (0, s) [2519, 2902]. (a^n - 1)/(a - 1) [914]. (j, c) [727]. (n^2-1) [2472]. (n^4-1) [2473]. (nα) [2472]. (t, m, s) [2031, 2862, 2037, 2336]. (t, s) [2614, 2031, 2327, 2862, 2037]. (X^2 - Y^2)^1/2 [489]. 0.1(0 ÷ 1)0 × 9 [139]. 1 [734, 872, 171, 301, 709, 2937, 2939]. 1, 2, 3 [3448]. 1.13198824... [2496]. 10, 000 [282]. $10.00 [168]. 10^{2857} [2467]. 10^{1035} [2029]. 1200μ [3096]. 128 [3121]. 13 [270]. 16 [270]. 2 [2815, 2106, 926, 3061, 2481, 2795, 2941]. 2, 000 [85]. $24.95 [2074]. 2^{31} - 1 [834, 927]. 2^{15} [2124]. 2^{31} - 1 [3497, 799, 970, 1003, 1191, 1192]. 2^{31} - 69 [3344]. 2^{32} - 1 [1083]. 2^{1468, 2224}. 2^{1311, 1474, 1720}. 2^{2595}. 2^{2k+1} [2595]. 2^{p} [3208]. 2^{p} - 1 [2257]. 3 [1774, 3623]. 32 [3578]. 4 [270]. 48 [245]. 5 [270]. $52.95 [3547]. 64}
\[a = \pm 2^q \pm 2^r\]
0.57 pJ [3221]. 0.57 pJ/bit [3221]. '05 [3874, 3878]. '07 [3884]. '08 [3888].


5.0 [1628]. 5.2 [2732]. 500 [3273, 318]. 51st [3905]. 52 [868]. 52nd [3920]. 5th [3889].

60th [3922]. 61 [1227]. 623-dimensionally [2321]. 64-bit
4


Accumulated [334, 1940]. Accuracy [210, 2596, 1307, 1414, 635, 2499, 3028, 3438, 2399, 2650, 2861, 3097, 3203, 551, 3630, 559, 613, 2145, 2963].
Accurate [2963, 829, 3646, 3027, 585, 3581]. achieving [432].
Acknowledgement [675, 676]. ACM [3812, 3763, 3768, 3774, 3784, 3795, 3804, 3813, 3818, 3845, 3852, 3865, 3874, 3884, 3888, 3898, 3907, 3914, 3921, 3922, 3928, 3897, 3816, 658, 491, 581, 505, 628, 356, 602, 3441, 518].
ACM-SIAM [3812]. ACORN [1441, 1741]. acquisition [2220].
Advanced [1445, 3739, 3903, 3857, 2415, 2490]. Advances [3751, 3769, 3787,
analysis

Analytic

Andersen

Android

Angeles

angenaherten

Angle

animals

Ann

Annealing

Annual

ANSI

Anthanasios

Antithetic

Antonio

ANTS

ANTS-III

any

Aperiodic

APG

apparent

Appearing

Appears

Appendix

Appl

Apple

Applesoft

applicability

Application

Applied

Approximate

Approximately

Approximating

Approximation

Approximations

April

Arbitrary
Archimedean [3253]. Architecture
[2817, 2764, 3333, 2061, 3244, 3504, 3707, 1542]. Architectures
[1445, 3679, 3333, 2061, 3244, 3504, 3707, 1542]. Area
[1445, 3679, 3592]. Areas
[3660, 3029]. areas
[2268, 2359, 2098, 3617, 2713, 717, 3654, 226, 364, 3811, 3478, 3, 1580, 1394, 1217, 1525, 2162, 1823, 1438, 1549]. arithmetical
[293]. arithmetiques
[1374, 3262, 2556, 1360]. Arrays [1472, 912, 3623, 787]. arrival
[3508, 2539, 3466, 3240]. arrivals [2693]. Art
[1702, 1724, 310, 3746]. Artefacts
[1559]. Arthur [3009]. article
[868, 2242]. Artifacts
[3696]. assess [1900]. Assessing [2128, 2398]. Assessment
[1363, 2082, 2756, 2612, 1286, 1443, 2293]. Assignment
[838, 843, 845, 857, 858, 859]. Assoc [1238, 1008]. Associated
[1244, 2731, 3136, 2815, 1002, 21, 253, 419]. Association
[3026, 3367, 3690, 3483, 2825, 3060, 2867, 2342, 3386, 3202]. Attacks
[3885, 3796, 3726, 3814, 3854, 3840, 3849, 3860, 3886, 3739, 3799, 2601]. Austria [3749, 3807, 3843, 3799, 3835]. Authentication
[1968, 3711, 3230, 3231, 3198]. autism [2944]. Autocorrelated
[1603, 982, 1835]. Autocorrelation

Combinations [393, 504, 475, 363, 1758, 1089, 2771, 439, 440, 61]. Combinatorial [618, 3567, 201, 2314, 1517, 2077, 235, 3412, 750].
1281, 2429, 2083, 1855, 1297, 3499, 1131, 2836, 2701, 3513, 759, 2848, 3434, 2721, 2999, 1708, 3684, 1517, 2879, 1959, 1837.


Computing [3758, 3763, 3768, 3774, 3779, 3784, 3795, 3813, 3818, 3827, 3845, 3852, 3865, 3869, 3874, 3884, 3888, 3898, 3907, 3914, 3921, 868, 2963, 2894, 370, 459, 3271, 662, 150, 1757, 1769, 928, 2377, 1258, 935, 3911, 3092, 118, 1012, 1724, 2733, 3882, 3453, 3810, 3464, 3778, 2501, 210, 3156, 2693, 2116, 3909, 3919, 117, 1092, 95, 128, 3299, 2780, 3621, 3808, 3823, 1548, 137, 3777]. con [461].


Conventional [3031]. Convergence
[2189, 1908, 1910, 2173, 1980, 376, 1484, 3354]. Convergent [311].
Conversion [2974]. Converting [3616]. Convex
[832, 2539, 3422, 32, 596, 719]. Convolution [1500, 2256, 3468].
Convolutional [3650]. Convolutions [667, 2548, 1549]. Cooperation [3527].
Cope [2425]. Copenhagen [3775]. Coprocessor [2533, 3575]. copula
[3025]. Copulas [3025]. Copyright [2266]. CORDIC [3581, 3627]. Core
[3055, 2596]. Corfu [3887]. Coprocessor [2533, 3575]. copula
[3025]. Copulas [3025]. Copyright [2266]. CORDIC [3581, 3627]. Core
[3055, 2596]. Corfu [3887]. Coprocessor [2533, 3575]. copula
[3025]. Copulas [3025]. Copyright [2266]. CORDIC [3581, 3627]. Core
[3055, 2596]. Corfu [3887]. Coprocessor [2533, 3575].
Cryptography
[3781, 2269, 878, 1655, 2973, 2907, 888, 2450, 2552, 2929, 3305, 1602, 2484, 2156, 2159, 3882, 2578, 3883, 1633, 2366, 3913, 3885, 2380, 354, 3190, 1683, 1502, 2237, 1927, 2332, 2482, 3327, 2411, 3457, 2580, 3233, 3134, 3879].

Cryptology
[1118, 3761, 3751, 3769, 3770, 3790, 3078, 1150, 3079].

Cryptosystem
[3227, 1335, 3650].

Cryostats
[2388, 1349, 3127].

Crystal
[3846, 53, 3861, 3755, 3802].

Crystallography
[3189].

CSD
[2053].

Cuba
[2838].

Cube
[417, 1541, 784].

Cubic
[1572, 2199, 1818].

CUDA
[3479, 3068, 3195, 3540].

Cumulant
[1657].

Cumulative
[3511, 3512, 2713, 1961, 561].

CURAND
[3479, 3540].

Current
[3078, 1150, 3079].

Current-Mode
[3078, 3079].

curve
[2969, 2779, 3010, 34].

Curves
[3383, 1998, 2840, 2577, 2982, 1585, 1260, 33].

Customer
[2686].

Cusum
[1169].

Cusum-Shewhart
[1169].

Cut
[2526].

Cyber
[1091].

Cycle
[1004, 1807, 1283, 3042, 2608, 2687, 776].

cycles
[222, 2785].

Cyclic
[889, 782, 1681, 3201].

D
[867, 1774, 3061, 3711].

D-PUF
[3711].

D.C
[3876].

d.f
[244].

Daemon
[2597].

Daiguian
[2010].

Dallas
[135].

Dana
[3899].

dangers
[1382].

dans
[2795].

DAP
[1165].

d'apres
[677, 714].

Dark
[3226].

Darling
[2466, 1011].

Data
[918, 919, 569, 2367, 3418, 931, 841, 1785, 934, 1415, 939, 764, 940, 767, 3309, 3310, 816, 986, 947, 1619, 3816, 1440, 3595, 3729, 995, 429, 41, 1771, 3282, 3179, 3286, 3419, 2220, 2452, 2917, 1786, 2128, 773, 1615].

Data-Oriented
[3309, 3310].

Data-Parallel
[1771].

Database
[3804, 1979, 3897].

databases
[1996, 1881].

datasets
[2028].

dbC
[1771].

DC
[3735, 3815, 3547, 3804, 3783, 3767].

DDH
[3337].

Deak
[1707, 1809].

Dear
[2053].

Debian
[3026, 3116].

Decay
[2803, 2811].

December
[3773, 3819, 3832, 3785, 3828, 3867, 3856, 3783, 3842, 3794, 3746, 3861, 3755, 3879, 3802, 3817, 3767].

decentralized
[3709].

Decimal
[290, 1589, 2860, 130, 80, 86, 78].

Decimals
[285, 14, 727].

Deciphering
[937, 1145].

decision
[1179, 3733, 1279, 3242].

Deco
[2080].

Decoding
[2110, 478, 3543].

Decomposition
[1856, 575, 3551, 1965, 949, 2670].

decreasing
[1098, 3454].

DECSYS
[884].

DECSYSTEM-10
[884].

defects
[793, 661, 2997].

defined
[1373, 2940].

Definite
[2387, 1176, 98].

Definition
[520, 521, 382, 553, 1019].

Definitions
[1563].

deformed
[2485].

Degree
[2903, 3301, 3103, 2822, 741, 2760, 3093, 3313].

Degrees
[1682, 1706, 1745, 344].

Del
[3828].

Delay
[963].

Delayed
[808, 3678].

delays
[1936].

delta
[1373].

demands
[750].

Demonstrating
[1382].

Demonstration
[3459, 3460].

Demonstrations
[161].

Deng
[2773].

dénombrable
[781].

dénombrables
[3].

dense
[1843].

d'ensembles
[2795].

denses
[176].

Densities
[1075, 2286, 667, 2499, 2193, 2986].

Density
[2226, 443, 695, 3632, 1456, 2603, 1301, 3272, 1076, 2986, 2643, 1211, 252, 1098, 418, 1961].

denumerable
[781].

Department
[3742].

Dependence
Efficient

[1287, 2262, 3375, 3256, 3561, 3384, 1072, 2512, 3159, 194, 2437, 2827, 3052, 3496, 2192, 3608, 2612, 2110, 2698, 3637, 2983, 3064, 1419, 3509, 3068, 1401, 3193, 978, 1208, 1338, 2991, 3198, 2854, 1419, 637, 1153, 1512, 1604, 3441, 2558, 2724, 1516, 2330, 1356, 1616, 2947, 2574, 1533, 3451, 2249, 1108, 862, 2955, 1621, 1109, 3660, 2422, 2672, 1112, 1167, 1627, 825, 1022, 1114, 1227, 3363, 3274, 3551, 961, 3029, 3631, 2175, 3560, 3717, 2362, 2687, 1186, 571, 2517, 1579, 3416, 2703, 3437, 3581, 2238, 1436, 3337, 2875, 2956, 1166, 2885, 3498].
efficiently [1856]. EGD [2597]. EICGs [3271].
eighteenth [186].
eight [2597].
Electron [343, 1723].
electron-solids [1723].
electroconvection [2622].
electroencephalogram [3603].
electromagnetic [3483, 3665].
electron [343, 1723].
electronics [2738].
electrophysiology [2220].
elektronnykh [346].
elementary [104, 26, 2040, 1928]. elements [204, 257].
elias [3717].
Eliminating [1852].
Elliptic [3383, 1998, 2840, 2577, 2969, 2982, 1257, 1585, 2779, 1260, 3010].
Elman [3400].
embedded [3895, 2985, 2977, 3055, 2984, 2916, 2266, 2522, 3860, 3214, 3218].
embeddings [2452, 2917]. emergence [512].
Emission [3355].
Emitting [3579]. emphasis [3642]. empirical [244].
Employing [3585]. emulation [2437, 3406, 2761].
emulator [702]. enabled [3320].
encoding [3270]. Encrypted [3310].
encrypting [2128]. Encryption [2680, 773, 3857, 1619, 2415, 2490, 1630, 3362, 3595, 937, 1145, 1590, 903, 1615, 3449, 3450, 3237, 2069, 3358, 3246, 1005].
Encyclopedia [3875, 3900, 3858, 3841, 3912, 3906, 3741, 3754, 3809, 3873, 3913, 3863].
End [3666, 1960, 2395].
End-to-End [3666, 1960]. energy [372, 3657].
Engine [3032].
Engineer [3673]. Engineering [168, 3754, 3809, 3887]. Engineers [626, 274, 1200]. engines [2584].
Enhanced [3636, 2045, 3227, 2195].
Enhancement [3169, 3137, 3269].
Enhancing [1425].
ENIAC [3611, 86].
Enigma [2605].
Enjoy [3025]. Enough [1800]. ensemble [2891].
Enskog [2289].
ENT [3133].
entanglement [3294].
Enthusiasm [2686].
entropies [1584, 2576, 2871].
Entropy [2597, 2086, 3606, 3699, 3669, 968, 1982, 575, 3081, 2229, 3676, 3645, 3580, 2722, 2792, 3685, 3655, 3047, 1038, 3610].
Entropy-Based [968, 1982, 2229, 1038].
Entropy-Uniformity [2086].
Environments [3271, 3156].
EPC [3335].
Equal [648, 215, 1142, 2245].
Equalization [3392].
Equally [624, 1320]. Equation [118].
Equations [2192, 2039, 2265, 1319, 159, 131, 132, 136].
Equidistributed [498, 3702, 217, 1141, 2132, 2394, 2637, 2321].
Equidistribution [3376, 1761, 2105, 2203, 2281, 2198, 2611, 182, 1036].
equilibria [3069].
Exploration [3687].  
Exploring [3916].  
Exponent [1682, 1798, 741].  
Exponential [562, 1869, 2909, 3062, 2292, 1047, 2555, 304, 767, 2477, 2864, 3105, 951, 2803, 3130, 1362, 1287, 344, 657, 2691, 2109, 2374, 1581, 2763, 3508, 330, 1211, 250, 779, 2497, 2947, 260, 452, 2250, 959, 2170].  
Exponentially [212, 3420, 3122, 3165, 224, 3682].  
Exponentiation [2696, 2128, 1615].  
exponentiations [1548].  
exponents [2777].  
Expressing [249].  
expression [2010].  
Extendable [3651].  
Extendable-Output [3651].  
Extended [2364, 1134, 1481, 2538, 3643, 1515, 1167, 487, 1234, 3797, 1403, 1786, 3426, 473, 3303, 691, 2170, 528, 3355, 1233, 921, 751, 1321, 1997, 2706, 2428, 2454, 2988, 979, 1415, 3194, 3084, 3195, 3430, 330, 1595, 332, 1098, 1921, 1928, 2943, 482, 1620, 1946, 2167, 692, 3238, 2587].  
Fastest [3101].  
fat [1552].  
fat-tailed [1552].  
Fault [3665, 3386, 3563, 1213].  
Fault-tolerant [3563, 1213].  
Fauly [3615].  
Faure [2671].  
FCRC [3826].  
FCSR [2814, 3228].  
FCSRs [3485, 3173].  
FDC [1908].  
Features [434, 1545].  
February [3899, 3835, 3868, 3744].  
Feeding [3046].  
Feinstein [315].  
Feller [3259, 1374].  
Fence [3596].  
Fermat [3499].  
fermions [3563].  
ferromagnetic [718].  
Festschrift [3893].  
Few [2890, 3052, 3023, 2988, 1274].  
few-body [1274].  
Fiar [2686].  
Field [2177, 3806, 2803, 1557, 1914, 2556, 1217, 902].  
field-programmable [2556].  
Fields [3301, 1813, 2149, 1743, 313, 3829, 3569, 930, 1148, 2235, 3808, 1607, 1712, 1812, 2150, 2478].  
Fifteenth [3752].  
Fifth [3887, 3812, 3921, 3824].  
Figures [1447].  
File [3148].  
Files [3169].  
filling [186].  
Filter [2998, 3636].
frequencies [64, 73].
Frequency [2001, 2115, 3674, 2869, 1019, 610, 541, 1322, 3202, 2663, 692].
Frequency-Modulated [2869]. frog [2284]. frontiers [3893, 3872].
gamma-distributed [327, 666]. Gamma-distribution [742]. gamma-rays [1051], gammaverteilten [327]. gap [233]. gas [793, 661, 2249].

**generation**

[1165, 958, 147, 2057, 3460, 2167, 2494, 1438, 2958, 3019, 1542, 2495, 1279, 1111, 1280, 824, 3546, 559, 613, 652, 691, 3240, 3024, 2497, 3471, 3548, 2352, 1550, 1225, 2354, 2594, 2676, 3668, 1544, 3238, 1847, 318, 1542, 1466, 976, 606, 866, 740, 1482, 1494, 1495, 1275, 2896, 2972]. **Generations**

[3387, 3428, 3156, 2341].

**Generator**


**generator**


**generator**

[3196, 762, 2014, 2778, 2779, 2851, 2927, 2928, 2464, 1505, 474, 2550, 3431, 3432, 2857, 1797, 2780, 3300, 3433, 3436, 3678, 2135, 2644, 1914, 585, 1595, 633, 3437,
generator

Generatoren [1024, 1026].

Generators [1363, 2259, 2502, 2748, 290, 2072, 2174, 2888, 3253, 1445, 3328, 3329, 3330, 3331, 2048, 3111, 782, 2572, 3113, 1618, 3332, 2049, 3218, 1063, 2408, 2574, 2951, 2163, 555, 2416, 2418, 524, 2582, 2583, 2342, 2806, 1359, 1539, 1735, 1954, 1109, 3347, 558, 2743, 3021, 1624, 1625, 2169, 1832, 2746, 3687, 785, 1282, 2066, 2427, 2593, 422, 1629, 423, 484, 3593, 826, 1633, 2355, 1024, 1116, 1170, 1284, 1286, 1443, 3551, 2595, 1840, 2429, 3028, 3029, 1231, 1369, 1289, 3631, 488, 3552, 2075, 3480, 2077, 1638, 3031, 1640, 2262, 3374, 3555, 3664, 2265, 3481, 3558, 1026, 2964, 3482, 3600, 3256, 3147].

generators

Generatoren [1024, 1026].

Generators [1363, 2259, 2502, 2748, 290, 2072, 2174, 2888, 3253, 1445, 3328, 3329, 3330, 3331, 2048, 3111, 782, 2572, 3113, 1618, 3332, 2049, 3218, 1063, 2408, 2574, 2951, 2163, 555, 2416, 2418, 524, 2582, 2583, 2342, 2806, 1359, 1539, 1735, 1954, 1109, 3347, 558, 2743, 3021, 1624, 1625, 2169, 1832, 2746, 3687, 785, 1282, 2066, 2427, 2593, 422, 1629, 423, 484, 3593, 826, 1633, 2355, 1024, 1116, 1170, 1284, 1286, 1443, 3551, 2595, 1840, 2429, 3028, 3029, 1231, 1369, 1289, 3631, 488, 3552, 2075, 3480, 2077, 1638, 3031, 1640, 2262, 3374, 3555, 3664, 2265, 3481, 3558, 1026, 2964, 3482, 3600, 3256, 3147].
[2489, 2832, 3350]. Man [127]. Management [2363, 3858, 3816, 3141].
Managing [3655]. Manhattan [3577]. MANIAC [1171]. Manipulating
[1244, 193, 3174]. Many [2149, 2638, 1162, 651]. Map
[3269, 3473, 3678, 2042, 3222]. Mapping [3332, 1005, 3422]. Mappings
[3140, 2703]. March
[3725, 3780, 3899, 3760, 3752, 3727, 3810, 3883]. Marginal [2185, 1796].
Marginals [2510]. margins [2250]. Mark [3767]. Markov
[210, 1070, 1173, 2189, 3277, 930, 644, 690, 1743]. marks [2266].
Marotto [3415]. Marriott [3773, 3746, 3861, 3755, 3802]. MARS [2453].
Marsaglia [3251, 2262, 2755, 1308, 1309, 1324, 2020, 2041, 1057, 3687, 3714].
Marshall [2837]. Martuljek [3831]. Maryland [3784, 3874]. mashinakh
[346]. masked [3569]. mass [719, 1550]. Massachusetts [3740]. Massen
[719]. Massy [2893, 3303, 3712]. massively [1890, 3520]. Mat [2948].
Mathematica [3526, 3585, 2050]. Mathematical
[3695, 3731, 3796, 3726, 3745, 3749, 1203, 1204, 95, 3728, 247, 1051, 3652,
2331, 3750, 54, 56, 3737, 3835, 3547, 913, 456, 485, 234, 698, 1190, 2404, 207].
Mathematical-Function [3695]. Mathematicians [2569]. Mathematics
[2357, 3731, 2754, 3726, 3745, 888, 3923, 3892, 3738, 137, 3922, 1701, 3744].
mathématiques [3728]. MathLink [2085]. MATLAB [3072, 2812].
Matrices [2272, 1151, 3018, 1232, 1584, 1099]. Matrix
[1554, 2185, 575, 1253, 1320, 2148, 1284, 1121, 1387, 3186, 3508, 52, 1520,
2035, 2035, 2813, 2874, 3548, 1199]. Matrixgeneratoren [1199, 1320]. max [1424].
Maximal [181, 1573, 1412, 808, 901, 2672, 1669, 2698, 3532, 3228].
Maximal-Length [901, 1412]. Maximally [3702, 2132, 2394]. Maximum
[1243, 1001, 1129, 2211, 2769, 1718, 1855, 2988, 83, 1951, 3024].
Maximum-length [1243, 1951]. Maxwell [3441, 3622]. May
[3758, 3763, 3768, 3774, 3779, 3784, 3795, 3804, 3813, 3818, 3826, 3827, 3845,
3852, 3865, 3874, 3888, 3914, 3729, 3816]. mbedTLS [3715]. MC [2227].
MCNP [1245, 3281]. MCS [3862]. MCV [721, 780]. Mean
[563, 1073, 2769, 586, 2, 528, 1665, 1666, 2693, 1931]. mean-square
[1665, 1666]. meaning [432]. Means [3494, 2922, 3014, 2058, 2531, 3308].
Measure [2176, 2298, 2505, 2836, 2848, 2047, 2586]. measurement
[3161, 3285]. measurements [545, 3466]. Measures
[2887, 2661, 617, 1766, 2221]. measuring [3336]. Mechanical [519].
mechanics [2823]. medians [429]. medical
[23, 46, 72, 113, 114, 169, 170, 3433]. Meeting [3743, 3735, 3864]. Meetings
[3742]. Memorial [3840]. Memory [2356, 2174, 3631, 1700, 1705].
[1447]. Merlin [3009]. Mersenne [2684, 3154, 2686, 2758, 741, 3702, 1682,
889, 2781, 2321, 2932, 2479, 3320, 3114, 3334, 3589, 1734, 2740].
Montgomery [2009, 2128, 2791, 2488]. monthly
Montreal [3813, 3738, 3865, 3822]. Monty [3518, 2317, 2318].
morphological [1665, 1666]. MOSFET [3096]. most [425, 3599, 2128].
mostly [2683, 1880]. mother [1918]. Motion [3407]. mots [740]. mouse
MPPC [3635]. MR [2087, 1238, 1039, 1008, 908, 868]. MR1414863 [2242].
MR2084569 [2948]. MT19937 [2846]. Mulders [3416]. Muller
[267, 699, 747, 2927, 3437, 3581, 638]. Multi
[899, 900, 901, 3277, 1321, 219, 220, 938, 3678, 1880]. multi-access [2678].
[157]. multicomputer [1792]. multicyclic [646]. Multidimensional
[2840, 2221, 3620, 1216, 484, 877, 2757, 2446, 2838]. multidimensionally
Multinomial [1072]. Multiparty [1370, 1640, 2826]. Multiple
[2363, 238, 150, 3052, 3496, 3497, 2370, 971, 2835, 622, 1254, 497, 1397, 3612, 2554, 2818, 2967, 2193, 1148, 2554, 770, 2793, 3315, 3316, 1526, 956].
Multivariant
[221]. Multivariate
[2747, 564, 1746, 2895, 1307, 2527, 1889, 1255, 2226, 2711, 3314, 3211, 3322, 3333, 3125, 2818, 2967, 2193, 1148, 2554, 770, 2793, 3315, 3316, 1526, 956].
Murmur [3456]. musical [3595]. mutual [899, 900]. Mutually [839]. mV
[3273].

[3706]. Naor [3620, 2577]. Nash [3069]. National
[3725, 3846, 3871, 133, 3735, 90]. NATO [3739]. Natural
43

Offord [1907], offs [1640]. Offset [3066]. OMAC [3207]. On-line [3218].
On-the-Fly [3217]. on/off [2693]. One
[1962, 3553, 734, 3382, 2097, 2209, 2383, 3570, 2625, 1585, 1149, 1261, 1594,
439, 440, 475, 2467, 717, 2038, 2156, 1618, 3229, 3473, 1552, 3480, 872, 3287,
1403, 3069, 1406, 186, 2586, 1166, 5, 3247, 3662]. One-chip [3229]. one-class
[3247]. one-dependent [1406]. One-Dimensional [3473, 186]. One-line
[439, 440]. one-shot [3069]. One-Sided [475]. One-Table [1962].
One-Time [3382, 2209, 2156]. One-Way
[3553, 3570, 1594, 2383, 3382, 2097, 2209, 1585, 1149, 1261, 1594, 439, 440,
475, 2467, 717, 2038, 2156, 1618, 3229, 3473, 1552, 3480, 872, 3287, 1403,
3069, 1406, 186, 2586, 1166, 5, 3247, 3662]. Ones
[1353, 2044]. Online
[2574, 3585, 3004]. Only
[2686, 3272, 3283, 3508, 2453]. Ontario
[3854, 3811]. OpenBSD
[2366]. openssl
[3036]. Operating
[2975, 2976, 3168, 2989, 1220]. operation [3031]. Operational [1975, 3734].
Operations
[2268, 3858, 3797, 1688, 1580, 2779, 1110, 3797]. operator
[1965]. operators
[111, 2347]. opinion
[2717]. Optical
[3048, 2610, 3521, 2492, 3470, 3192, 2486]. Optimal
[3691, 1028, 2091, 2361, 1304, 3606, 3699, 1665, 1666, 578, 668, 627, 670, 710,
1265, 3103, 1434, 1361, 1380, 2287, 2531, 2451, 3293, 2010, 3095, 3003, 813,
2804, 1665, 1666]. Optimality
[578, 1087, 1057]. optimisation
[3529]. Optimised
[3210, 3333, 3170, 3719]. Optimizing
[3712, 3243]. Optimum
[644, 610]. Oracle
[3693]. Orbits
[2096, 2891]. Order
[2357, 1657, 1865, 3496, 3497, 2901, 624, 1340, 1691, 2854, 3099, 53, 683, 2590,
1235, 1377, 2827, 3053, 3164, 1034, 2982, 1323, 2628, 45, 3225, 3344, 3462].
Order-Disorder
[53]. Ordered
[2619, 1745, 148, 1854, 1001, 3058, 1129, 40].
ordering
[2539]. Orders
[2382, 1036, 2586, 2879]. ordinal
[429]. ordinateur
[740]. Oregon
[3852, 3838]. organic
[3395]. Oriented
[2609, 3309, 3310, 3114, 1767, 2638, 3432]. Origin
[1769]. origins
[3917]. Orlando
[3856, 3746]. Orleans
[3785]. Orono
[3796]. ors
[3228]. orthogonal
[1232]. Oscillation
[2869]. Oscillator
[3378, 3483, 3405, 3645, 3137, 3360, 3368, 3369, 3665, 2685, 3404, 3181, 3202,
3206, 3352]. Oscillator-Based
[3378, 3368, 3369, 3665, 2685, 3552]. Oscillators
[3521, 3284, 206]. Other
[1445, 2860, 173, 576, 577, 116, 1491, 2463, 2547, 260, 958, 728, 3722, 3247].
Otherwise
[2182]. Ottawa
[3885]. outage
[3311]. Output
[3693, 2689, 3669, 3651, 3587, 3466]. Overview
[2674, 2366, 2849]. Oxford
[3853, 3745].

P [579, 621, 259, 168, 2882, 2883]. P-RnaPredict
[2882, 2883]. P.
[867, 530, 134]. P1363
[2450]. PA
[3747]. PaCAL
[3617]. Package
[3617, 1592, 630, 3089, 3025, 488, 3390, 3604, 1887, 2638, 3432, 636, 595, 600, 1159].
Packing
[2954, 3251, 695, 490, 1142, 1434, 418, 910]. packings
[424]. Pad
[3382, 2209, 2156]. Padé
[1905]. Page
[2450]. pages
[2074]. Pair
[278, 344]. pair-wise
[344]. Pairs
2301, 2389, 2549, 1920, 2563, 3532, 2941, 685, 2741, 3225, 2677, 231, 1228.

Periodic [2891, 179, 727]. periodo [461]. Periods [341, 3228, 1849, 2114, 687, 1565].

Permutation [1118, 1859, 2530, 3525, 3649, 3651, 3024, 3042, 2607, 967, 317, 2014, 1210, 1806, 3314, 1612].

Permutation-Based [3651]. Permutations [3692, 3258, 1675, 3618, 1523, 400, 2080, 435, 1585, 1687, 1342, 308, 257, 1726, 685, 3452, 164, 175].


Perspective [2514, 3582, 3621]. perspectives [3853]. PERT [898].


Phase [3521, 846, 159, 3284, 3285, 3300, 3201, 3236]. phase-dependent [3236].


piecemeal [606]. Piecewise [3511, 3512, 2552, 2958, 3019].

Problem [2089, 3264, 51, 2833, 299, 1422, 383, 3652, 1732, 1560, 2753, 923, 3187, 933, 186].


Procedure [318].

[1072, 1180, 925, 1081, 971, 436, 304, 277, 1721, 1555, 1636, 318, 753, 330, 280, 332, 3529].

Proceedings [3758, 3779, 3804, 3827, 3914, 3921, 3725, 3780, 3761, 3769, 3726, 3793, 3747, 3752, 3766, 3848, 3724, 3788, 3789, 3911, 3822, 3746, 3861, 3862, 3887, 3811, 3742, 3824, 3825, 3868, 3744, 3777, 3738, 3826, 3874, 3884, 3773, 3819, 3764, 3785, 3743, 3759, 3760, 3731, 3805, 3828, 3751, 3829, 3853, 3820, 3745, 3775, 3867, 3787, 3749, 3854, 3798, 3855, 3849, 3856, 3783, 3788, 3842, 3794, 3823, 3843, 3850, 3871, 3739, 3799, 3755, 3757, 3864, 3817, 3844, 3767, 3836, 3812, 3763, 3768, 3774, 3795, 3813, 3818, 3845, 3852, 3865, 3869, 3898, 3907, 3832, 3723, 3729, 3791, 3895, 3915, 3792, 3740].

Proceedings [3815, 3905, 3920, 3860, 3728, 3807, 3897, 3810, 3879, 3816, 3802, 3831, 3835, 3803, 3838, 3814, 3847, 3903, 3889, 3910, 3886, 3772].

Process [2018, 3221, 1663, 517, 956, 3237, 1552].

Process-Voltage-Temperature [3221].


Processing [653, 3398, 3810, 3729, 3560, 1175, 3848, 1325, 2220, 1413, 3084, 3528, 3106, 1936, 1617, 2497].

processor [3257, 1487, 1488, 3578, 3236].

Processors [2370, 3291, 3320, 3334, 3589, 3256, 1378, 1467, 1391, 1581, 1596, 1431, 3363, 3475].

Produce [1086].

Produced [1376, 3641, 546, 1055, 1056, 1377, 2982, 2228, 1520, 2669].

Producing [333, 354, 74, 75, 380, 2875].

Product [2535, 2989, 205, 3119, 874, 1130, 1891, 1211].

Production [167, 327, 174].

Products [2934, 390, 523, 1994, 3426, 2744].

Professor [3853].

Profile [2888, 2759, 2701, 2721, 2999, 1708, 1517, 2879, 1837].

Program [3377, 3558, 2085, 1187, 3670, 223, 3133, 998, 2324, 599, 1352, 1104, 911].

Programmable [2220, 1785, 2556].

Programmed [876, 1650, 2885].

Programmierung [866].

Programming [3695, 2922, 2038, 1611, 3864, 866, 3745, 1190, 2119, 2647, 596, 2164].

Programs [1450, 3263, 3602, 3264, 370, 459, 1000, 689, 1107, 1439, 3573, 897, 1936, 1848].

project [2526].

Projections [3071].

Proof [1963, 2748, 2429, 698, 399].

Proofs [1910, 3525, 3649, 2380, 2047].

Proper [2078, 1316, 2178].

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

Property [179, 3136, 3376, 1120, 3167, 3704, 1266, 783].

property-based [3704].

Pseudo-random
2144, 3706, 1938, 2049, 519, 1535, 1282, 3241, 1283, 2355, 1644, 1378, 2481, 1847, 1071, 1561, 1975, 3563, 755, 2134, 2229, 2638, 3516, 636, 2645, 3304, 2794, 1613, 2042, 1271, 3446, 3223, 2257.

random-pulse [660].

Random-Start [3209]. Random-Variate [2873]. random-walk [2248].


randomize [2591]. Randomized [1994, 2617, 3414, 1331, 1789, 2711, 1709, 2146, 2244, 2639, 3296, 682].

randomizer [1471]. Randomly [841, 2037, 648, 2157, 1440, 21, 1791, 3297].

randomly-shifted [3297]. Randomness [3365, 655, 3595, 2890, 996, 126, 3484, 2267, 62, 1851, 3041, 698, 2435, 3269, 1864, 1865, 1868, 2829, 2907, 1392, 1317, 2112, 2529, 3063, 3185, 2766, 2535, 25, 37, 3577, 2770, 2709, 1333, 438, 3580, 2020, 2139, 2646, 2860, 3305, 1344, 1511, 1600, 512, 3683, 119, 1814, 2151, 3211, 3005, 3533, 1817, 282, 2797, 2331, 3326, 3445, 3536, 2573, 3541, 173, 2415, 2490, 1827, 3544, 2880, 2498, 3477, 2750, 3372, 3632, 458, 428, 1647, 211, 3265, 103, 2971, 1297, 3495, 1563, 3163, 41, 80, 1674, 3565, 432, 141, 116, 665, 347, 1323, 3761, 1044, 1900, 22, 3082, 582].

randomness [763, 2996, 3434, 477, 2141, 3705, 1515, 815, 2569, 3109, 1432, 1614, 904, 3327, 2663, 3112, 2800, 2868, 3658, 162, 2739, 49, 3463, 911, 960, 3352, 2064, 3722, 50, 40, 2210, 554, 3547]. randoms [875]. `RANDU' [702].


Rank-1 [2918, 3675]. Rank-based [1323]. Ranking [2086, 2113, 3529].

ranlip [2818]. RANLUX [2212, 2213, 1896, 2120, 2338].


[3673]. RV [1204].

S [3039, 315, 974, 1039, 437, 389, 3579, 2070, 3459]. S-3800 [2070].
Saarbrücken [3762]. SAC [3885, 2530, 2766]. SAC’99 [3854]. Safari [2331].
Safe [2049]. SAC [3885, 2530, 2766]. same [365].
Sample [697, 1073, 3494, 619, 2905, 58, 781, 35].
samplers [1752]. Samples
[1182, 1940, 1947, 8, 828, 64, 73, 17, 39, 134, 33, 230]. Sampling
Samuel [3893]. San [3884, 3907, 3773, 3819, 3899, 3864, 3844, 3868].
Saturday [3876]. Saturday-Wednesday [3876].
Saunders [1530]. Savage [2466]. SC’11 [3911].
Satisfying [518, 453, 1312, 3214, 451, 13].
Scheduling [653]. scheduling [1792, 3311]. schemata [2592].
schemata-based [2592]. Scheme [3262, 1932, 2959, 3303, 773, 1612, 3450].
Schemes [1770, 2475, 723, 1169, 3717, 1401, 2316, 157].
School [2756, 3744, 630]. School-Based [2756].
Scattering [3389, 11].
Sciences [3863]. Scientific
[3735, 2894, 1122, 3734, 1140, 1724, 2489, 3810, 3174, 2717, 3823, 3739].
Scientists [626, 274, 1200]. scores [429]. Scrambled [3209, 3687, 3115].
Scrambling [2614]. scramblings [2727, 3714]. screening [3224, 2586].
scroll [3152, 3181]. SEAC [89]. SEAL [2616]. Search
[3496, 970, 1392, 3614, 812, 908, 909, 2608, 3053, 2517, 927, 2915, 708, 1337, 1795, 1513, 2804, 2584, 3461, 3462]. Searches [2612, 2222, 1415]. Searching
[2847, 2806]. Seattle [3779, 3911]. secant [1756].
Secondary [3723, 3766, 30, 3860, 3005, 861, 3835, 3784, 3852, 3225]. Second-level [3005].
second-order [3225]. Secondary [2882]. Secret [2825, 1276, 2425]. Secure
[3375, 2682, 3258, 1453, 3489, 2110, 2533, 2634, 3077, 3644, 3096, 3015, 1112, 1167, 2679, 3637, 3421, 1401, 2390, 1335, 3091, 3321, 3108, 2946, 2337, 1276, 3546, 2678, 1847]. Securely [3683]. sécuritaire [1847].
Security
[3846, 3378, 3666, 2367, 1868, 2829, 3172, 3502, 2696, 2629, 3878, 2558, 2724, 2566, 3310, 3652, 3586, 1530, 3116, 2955, 2805, 3824, 3844, 3715, 3913,
Services [3113, 3187]. ses [1847]. Session [262]. Set [2600, 928, 2379, 2147, 2808, 1448, 705, 21, 156, 158, 1719, 647, 35]. SETA [3889, 3877]. Sets [2502, 2617, 3080, 3085, 2306, 360, 1540, 2672, 2077, 344, 1750, 41, 2372, 139, 273, 1777, 2293, 3839, 2117, 2540, 719, 1215, 1267, 1711, 1712, 2795, 2940, 601, 945, 2071, 3080]. Setting [3234, 3427].


Tag [3310, 3155, 3440]. Tags [3033, 3321, 3335]. Tail
[925, 1081, 667, 1299, 2988, 3438]. tailed [3384, 1552]. Tails
[2751, 855, 952, 2978]. Taken [8]. Talk [2445]. tandem [3151]. tangent
[1905]. Tap [2355]. taps [2410]. Target [1650]. Targeting [3125, 3665].
Tatzmannsdorf [3749]. Tausworthe [1025, 1753, 1660, 741, 1471, 466, 1036, 1390, 2132, 775, 1013, 1617, 1621, 558, 650]. Tb [3579]. TDIST [2812].
TEA [2824, 2530, 2625, 2626, 2703, 2767, 2654, 2240, 2069]. Teach [2686].
Teaching [3169, 3072]. Technical
[2081, 2007, 1803, 2717, 2048, 3835, 3851, 3643, 236, 319, 403, 400].
Technique [1395, 2008, 808, 3464, 993, 74, 2704, 3707]. Techniques
[3759, 3387, 3392, 3769, 2364, 1863, 269, 2634, 1504, 2717, 637, 3031, 3765, 164, 545, 155, 1545, 3472, 99]. Technology [2270, 3740, 3910, 3892, 3841].
Teil [520, 521]. Telegraphic [1798]. Temperature [3221, 3455]. tempering
[3424, 2847, 2990, 2956, 3342, 3462]. terms [2223, 249, 1162]. termwise
[3228]. Terrain [2043]. TES [1603]. Test
test [1704, 3208, 1101, 1156, 1350, 1429, 3533, 2041, 45, 2799, 2800, 608, 2419, 1951, 2059, 2165, 2167, 2741, 3225, 1278, 1953, 50, 230, 28, 3030, 2839, 1583].
Test-Pattern [725]. tested [1857, 3288, 2302, 3647]. Testing
TESTRAND [1052, 969, 1033, 1305]. Tests
[2744, 1956, 1957, 2064, 2134, 2020, 974]. TESTU01
[2933, 2545, 2641, 2993, 2926, 2994]. Texas [3752, 3844, 3757]. Texture
[790, 930]. Textured [1743]. theatres [1220]. thefts [3564]. Their
Theme [3778]. Theorem [1374, 2633, 105, 3477, 235, 1037, 3415, 3290, 32, 3438, 3646, 410, 2723, 3102, 640, 1160, 2340, 2668, 1237, 2521, 2934, 2803]. theorem-based [3415].


tomorrow [3770]. Too [3606, 3699, 3447, 460]. Tool [3675]. Toolbox [3391].

Toolkit [3479, 2131, 3110]. Tools [2963]. Top [2475]. Top-Level [2475].

topics [906, 948]. Topologies [3349]. topology [2653]. Tosser [3291].


trajectory [3219]. Transactions [3733]. transcendental [1330, 367].


uniform
uniform-Gaussian
uniformement
Uniformity
Uniformization
Uniformly
uniformly-distributed
Uniforms
Unifying
Unimodal
Unique
unit
units
Univariate
Universal
universe
University
UNIX
Unpublished
unreasonable
unrestricted
unsigned
Unsupervised
Untersuchung
Untrusted
UNURAN
Up-and-Down
update
updates
Upper
USA
usable
Usage
Use
Used
useful
Usenet
Use
Uses
using
use
V [2092, 488, 2472, 600, 3723], v. [239]. VA [3812, 3810, 3861, 2046].
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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES

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


REFERENCES


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


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[230] Donald D. Wall. A random number test for large samples. In Anonymous [3729], pages 7–11. LCCN ????


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kolmogorov:1963:TRN


Laughlin:1963:RAR


MacLaren:1963:FPG


Magleby:1963:SNF


Marsaglia:1963:GDR


Marsaglia:1963:RNF


Moses:1963:TRP


Poore:1963:CAR

REFERENCES


REFERENCES


324 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).
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hutchinson:1966:NUP


Jansson:1966:RNG


Loveland:1966:NIM


Marsaglia:1966:GMP


Martin-Lof:1966:CRS


Martin-Lof:1966:DRS


Mckinney:1966:CNG


Miller:1966:BRB

REFERENCES


REFERENCES


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


[405] I. J. Good and T. N. Gover. The generalized serial test and the binary expansion of $\sqrt{2}$. *Journal of the Royal Statistical Society. Series A* (Gen-
REFERENCES


**Gorenstein:1967:TRN**


**Gurland:1967:ISE**


**Hemmerle:1967:SCD**

[409] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3734], pages 64–68. LCCN QA76.5 D55 1965.

**Itzelsberger:1967:SEP**


**Marlow:1967:NLT**


**Mullen:1967:NRT**

REFERENCES


Page:1967:GPR


Ratz:1967:MPN


Sclove:1967:FRE


Serfling:1967:NCR


Sobol:1967:DPC


Solomon:1967:RPD
REFERENCES


REFERENCES

Bell:1968:ANR


Berlekamp:1968:ACT


Bradley:1968:RTR


David:1968:NCM


Dieter:1968:AME


Forsythe:1968:RNG


Gardner:1968:MRS


Good:1968:GST

I. J. Good and T. N. Gover. The generalized serial test and the binary expansion of \(\sqrt{2}\). Journal of the Royal Statistical Society. Series A (General), 131(??):434, ???? 1968. CODEN JSSAEF. ISSN 0035-9238. See [405].
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

[460] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3735], pages 70–111. LCCN QA1 S565 v. 3.


References

Fellen:1969:LEI


Good:1969:HRR


Grosenbaugh:1969:MFR


Gubenko:1969:FPR


Hemmerle:1969:GPN

W. J. Hemmerle. Generating pseudorandom numbers on a two’s complement machine such as the IBM 360. *Communications of the ACM*, 12(7):382–383, July 1969. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).

Knop:1969:RAG


Kruskal:1969:EPR


Lee:1969:ECF

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


[512] P. McShane. \textit{Randomness, statistics and emergence}. University of Notre Dame Press, South Bend, IN, USA, 1970. x + 268 pp. LCCN ????


REFERENCES


REFERENCES


Zaremba:1970:DI


Ashford:1971:BRG


Beyer:1971:LSM


Brown:1971:LRA


Chen:1971:RNN


Cohn:1971:PRB


Craddock:1971:TRM

REFERENCES


REFERENCES


REFERENCES


[554] Claus Peter Schnorr. *Zufälligkeit und Wahrscheinlichkeit: Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*. (German) [Randomness and probability. An algorithmic foundation of probability theory], volume 218 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc.,
REFERENCES


Ahrens:1972:CMS


Alam:1972:AVM


Barr:1972:CMN


Basu:1972:ITF


Behboodian:1972:CNS


Beyer:1972:LSR


Cenacchi:1972:QRS

REFERENCES


REFERENCES

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


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hamming:1973:NMS

Holland:1973:GA

Knop:1973:AAR

Kozlov:1973:EEM

Learmonth:1973:NPS

Levin:1973:NRS

Lewis:1973:GFS
REFERENCES


[639] Frank Neuman, Robert Merrick, and Clyde F. Martin. The correlation structure of several popular pseudorandom number generators. Report
Niederreiter:1973:BEB


Niederreiter:1973:MTD


Overstreet:1973:QCM


Overstreet:1973:RNG


Peskun:1973:OMC


Philipp:1973:EDF


Pohl:1973:MVM

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


REFERENCES


[668] N. Harada. Optimal multipliers for the spectral test of uniform random number generators. Information Processing in Japan, 14(??):120–126, ????. 1974. CODEN ???? ISSN ????


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

75t-47.

Jack P. C. Kleijnen. Antithetic variates, Common Random Numbers and
optimal computer time allocation in simulation. Management Science,
21(10):1176–1185, June 1975. CODEN MSCIAM. ISSN 0025-1909 (print),
1526-5501 (electronic).

M. B. Levin. On the uniform distribution of the sequence αλ. Mat. Sb.
(N.S.), 98(??):??, ???. 1975. CODEN ???? ISSN ????

Michael A. Malcolm and R. Bruce Simpson. Local versus global strategies
for adaptive quadrature. ACM Transactions on Mathematical Software,
1(2):129–146, June 1975. CODEN ACMSCU. ISSN 0098-3500 (print),
1557-7295 (electronic).

Michel Mendès France. Suites de nombres au hasard, d’après Knuth.
(French) [Sequences of random numbers]. Technical report, Lab. Théorie
des Nombres, Centre Nat. Recherche Sci., Talence, France, 1975. 11
Talence), Exp. No. 6.

O. Miyatake, H. Inoue, and Y. Yoshizawa. Generation of physical random
numbers. Mathematica Japonica, 20(??):207–217, ???. 1975. CODEN
MAJAA9. ISSN 0025-5513.

James L. Monroe. Correlation inequalities for two-dimensional vector
spin systems. Journal of Mathematical Physics, 16(9):1809–1812,
September 1975. CODEN JMAPAQ. ISSN 0022-2488 (print), 1089-
7658 (electronic), 1527-2427. URL http://jmp.aip.org/resource/1/
jmapaq/v16/i9/p1809_s1.
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[737] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3742], pages 321–355. ISBN 0-12-697540-X. LCCN QA76.6 .S9195 1976. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.7959. The complexity of the binary Euclidean algorithm for the greatest common denominator is shown to be $O(0.705 \log N)$ for large $N = \max(|u|, |v|)$. See [2434] for an update, and a repair to an incorrect conjecture in this paper. See also [2360], where the worst case complexity is shown to be $O(\log N)$, and the number of right shifts at most $2 \log(N)$.


REFERENCES


Golder:1976:SAR


Greenwood:1976:DTC


Greenwood:1976:FMI


Greenwood:1976:MTG


Guerra:1976:RNG


Heikes:1976:UCR

REFERENCES


REFERENCES

Marsaglia:1976:RNG


McArdle:1976:ETM


Michael:1976:GRV


Miklich:1976:HSN


Mitchell:1976:EAD


Neuman:1976:APC


Neuman:1976:AST

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES

[845] Colin L. Mallows. Pseudorandom number assignment in statistically
designed simulation and distribution sampling experiments: Comment.
Journal of the American Statistical Association, 73(363):520, September
1978. CODEN JSTNAL. ISSN 0162-1459 (print), 1537-274X (electronic).

[846] D. G. Maritsas, A. C. Arvillias, and A. C. Bounas. Phase-shift anal-
ysis of linear feedback shift register structures generating pseudoran-
dom sequences. IEEE Transactions on Computers, C-27(7):660–669,
July 1978. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (elec-
arnumber=1675166.

[847] Richard E. Nance and Claude Overstreet, Jr. Some experimental obser-
vations on the behavior of composite random number generators. Op-
erations Research, 26(5):915–935, September/October 1978. CODEN
OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic). URL http://

[848] Harald Niederreiter. Existence of good lattice points in the sense of
1979. CODEN MNMTA2. ISSN 0026-9255 (print), 1436-5081 (elec-
tronic).

[849] Harald Niederreiter. Quasi-Monte Carlo methods and pseudo-random
1041, November 1978. CODEN BAMOAD. ISSN 0002-9904 (print),

[850] Harald Niederreiter. The serial test for linear congruential pseudo-
random numbers. Bulletin of the American Mathematical Society, 84
(2):273–274, 1978. CODEN BAMOAD. ISSN 0002-9904 (print),
1936-881X (electronic).


[857] Lee W. Schruben and Barry H. Margolin. Pseudorandom number assignment in statistically designed simulation and distribution sampling experiments. *Journal of the American Statistical Association*, 73
REFERENCES


REFERENCES


REFERENCES


198

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


M. S. Petkovic. A representation of random variables by the probable intervals. Freiburger Intervall-Ber. 80/10, Universitat Freiburg, Freiburg, Germany, 1980. 12–20 pp.


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


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


REFERENCES


Battaglia:1981:RDA


Calo:1981:DAT


Deak:1981:EMR


Devroye:1981:CGP


Devroye:1981:CGR


Diaconis:1981:GRP


REFERENCES


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


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

Bartels:1982:RVN


Blum:1982:HGC


Crigler:1982:RCP


Devroye:1982:NAR


DiDonato:1982:FSP


Dykstra:1982:MLE

REFERENCES


REFERENCES


[1014] Arthur V. Peterson, Jr. and Richard A. Kronmal. On mixture methods for the computer generation of random variables. The American Statis-
REFERENCES

Plumstead:1982:ISG


Rizzi:1982:GPB


Roberts:1982:ITN


Schmeiser:1982:BGR


Shen:1982:FAD


Tracht:1982:RAN


Vahle:1982:BPR


REFERENCES

Borosh:1983:OMP


Bratley:1983:GS


Brillhart:1983:FHP


Chen:1983:SSR


Devroye:1983:MIR


Dudewicz:1983:TRN


Erber:1983:SRP

REFERENCES


REFERENCES


REFERENCES


[1083] 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


REFERENCES


REFERENCES


REFERENCES


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


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


REFERENCES


REFERENCES


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

239


Monahan:1985:ARN


Montgomery:1985:MMT


Niederreiter:1985:STP


Norton:1985:EBG


Percus:1985:PBS


Pierchala:1985:IMU


Reichert:1985:LLT

REFERENCES


REFERENCES


Vitter:1985:RSR


Yashchin:1985:ADC


Afferbach:1986:SLS


Anderson:1986:MCC


Anon:1986:IRN


Blum:1986:IUC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Nicola:1986:QAF


Niederreiter:1986:DFS


Niederreiter:1986:LDP


Niederreiter:1986:MNI


Niederreiter:1986:PVG


Panny:1986:NHM


Santha:1986:GQR

REFERENCES

Shore:1986:AID


Shore:1986:SGA


Sowey:1986:TCB


Stephens:1986:TBE


Stephens:1986:TUD


Wolfram:1986:RSG


Wolfram:1986:TAC

Zeisel:1986:SAR


Zielinski:1986:QRN


Agnew:1987:RSC


Aldridge:1987:CRR


Allender:1987:SCE


Anderson:1987:GRO


Barbu:1987:NFM

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

1613-9798 (electronic). URL http://www.springerlink.com/content/q7885421202m6656/.


[1292] Pierre Beauchemin, Gilles Brassard, Claude Crépeau, Claude Goutier, and Carl Pomerance. The generation of random numbers that are probably prime. *Journal of Cryptology: the journal of the International
REFERENCES


REFERENCES


REFERENCES

Durst:1988:TPR


Edwards:1988:CAM


Eichenauer:1988:MLTb


Eichenauer:1988:MLTc


Eichenauer:1988:NCP


Fishman:1988:MCR


Frieze:1988:RTI

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


[Fushimi:1988:DUR]


[Fushimi:1988:STP]


[Giord:1988:NRN]


[Gleason:1988:IPS]


[Goldreich:1988:EPG]


[Greiner:1988:NIS]

REFERENCES


REFERENCES


REFERENCES


[1344] M. Matsumoto and Y. Kurita. The fixed point of an \( m \)-sequence and local non-randomness. Report 88-027, Department of Information Science, University of Tokyo, Tokyo, Japan, 1988.

Niederreiter:1988:LDL


Niederreiter:1988:RNC


Niederreiter:1988:SIN


Niederreiter:1988:SNC


Niederreiter:1988:STD


Ore:1988:NTH


Panton:1988:PPS


Park:1988:RNG


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES

Luby:1989:SPS


Maclaren:1989:GMI


Manas:1989:PCI


Marsaglia:1989:RVS


Martin:1989:AMM


McIntosh:1989:RAE


Meer:1989:SIP


Meier:1989:FCA

REFERENCES


Mertsch:1989:PAS


Niederreiter:1989:STC


Paul:1989:IRN


Percus:1989:RNG


Pickover:1989:PRG


Reber:1989:PNG


Rhee:1989:OPiA

[1434] Wansoo T. Rhee and Michel Talagrand. Optimal bin packing with items of random sizes. II. SIAM Journal on Computing, 18(1):139–151, Febru-
REFERENCES

ary 1989. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic).


REFERENCES


REFERENCES


REFERENCES

Dagpunar:1990:SMD


Deak:1990:RNG


Deak:1990:URN


DeArman:1990:IRN


DeMatteis:1990:CPR


DeMatteis:1990:LRC


Deng:1990:GUV


Doring:1990:ENZ

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


REFERENCES


Goldreich:1990:NCI


Goldreich:1990:SPD


Golland:1990:BRB


Haastad:1990:PRG


Hildebrand:1990:RCS


Hormann:1990:AMG


Hortensius:1990:CAC

REFERENCES


Koutras:1990:TCN


Krawczyk:1990:HPC


Lagarias:1990:PNG


L’Ecuyer:1990:RNS


L’Ecuyer:1990:UVW


Levitan:1990:PNG


Lutz:1990:PSB


REFERENCES


REFERENCES

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


REFERENCES


Computer Science Institute, Berkeley, CA, August 1990.


[1545] V. A. Velizhanin, I. G. Dyadkin, F. Kh. Enikeeva, B. K. Zhuravlyov,
B. E. Lukhminsky, and R. T. Khanatdinov. Monte Carlo simulation in
nuclear geophysics — I. Features of Monte Carlo algorithmic techniques
for solving problems in borehole nuclear geophysics. Nuclear Geophysics,


[1547] Y. H. Wang. Dependent random variables with independent subsets. II.
Canadian mathematical bulletin = Bulletin canadien de mathématiques,
33(??):24–28, ???? 1990. CODEN CMBUA3. ISSN 0008-4395 (print),
1496-4287 (electronic).

[1548] C. C. Wang and D. Pei. A VLSI design for computing exponentia-
tions in GF(2^m) and its application to generate pseudorandom
1990. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (elec-
arnumber=45211.

CODEN LIARE4. ISSN 0888-613x (print), 1873-4731 (electronic).


Compagner:1991:DR


Compagner:1991:HCR


Deng:1991:CRN


Deng:1991:RDR


Devroye:1991:AGD


Devroye:1991:ETA


Dohmann:1991:RNG

REFERENCES


REFERENCES


REFERENCES


REFERENCES

[1616] Terry Ritter. The efficient generation of cryptographic confusion sequences. *Cryptologia*, 15(2):81–139, April 1991. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://fizz.sys.uea.ac.uk/~rs/ritter.html; http://www.ciphersbyritter.com/ARTS/CRNG2ART.HTM; http://www.informaworld.com/smpp/content~content=a741902748~db=all~order=page. cryptographic confusion sequences; pseudo-random sequence; random number generators; cryptographic applications; random sequences; incompleteness theorem; deterministic implementation; external analysis; RNG comparison; chaos; Čebyshev mixing; cellular automata; linear congruential; linear feedback shift register; nonlinear shift register; generalized feedback shift register; additive types; isolator mechanisms; one-way functions; combined sequences; random permutations; primitive mod 2 polynomials; empirical state-trajectory approach; RNG design analysis; GFSR.


REFERENCES


REFERENCES


REFERENCES


Aluru:1992:RNG


Anastasio:1992:OCL


Anderson:1992:CRN


Arno:1992:PSC


Atkinson:1992:GBT


Babai:1992:MPP

REFERENCES


Brenner:1992:PRL


Brent:1992:URN


Brickell:1992:CSR


Brightwell:1992:TSP


Burgess:1992:FLC


Burton:1992:DRN

REFERENCES


REFERENCES


[1671] Jürgen Eichenauer-Herrmann and Harald Niederreiter. Lower bounds for
the discrepancy of inversive congruential pseudorandom numbers with
power of two modulus. *Mathematics of Computation*, 58(198):775–779,
April 1992. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842
.pdf.

[1672] Jürgen Eichenauer-Herrmann and Holger Grothe. A new inversive con-
gruential pseudorandom number generator with power of two modulus.
*ACM Transactions on Modeling and Computer Simulation*, 2(1):1–11,
January 1992. CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195
(electronic).

[1673] Jürgen Eichenauer-Herrmann. A remark on the discrepancy of quadratic
congruential pseudorandom numbers. *Journal of Computational and Ap-
sciencedirect.com/science/article/pii/037704279290023Q.

[1674] Eduardo Engel. *A road to randomness in physical systems*, volume 71 of
*Lecture notes in statistics*. Springer-Verlag, Berlin, Germany / Heidel-
York), 3-540-97740-6 (Berlin). viii + 155 pp. LCCN QC20.7.P7 E54

0022-314X (print), 1096-1658 (electronic).

simulations: Hidden errors from ‘good’ random number generators. *Physical
ISSN 0031-9007 (print), 1079-7114 (electronic), 1092-0145.
URL http://prl.aps.org/abstract/PRL/v69/i23/p3382_1. See also
[1773].
REFERENCES


Ishikawa:1992:MHS


Kleijnen:1992:PNG


Kleijnen:1992:RMS


Ko:1992:GPB


Kolonko:1992:GUD


Krawczyk:1992:HPC


Lagarias:1992:PN

REFERENCES


REFERENCES


REFERENCES


Szyszkwicz:1992:GRP


Tang:1992:SDA


Tezuka:1992:AAC


Tezuka:1992:FGL


Traub:1992:MCA


Tsai:1992:AFT

vonHanxleden:1992:CDP

Warford:1992:GPR

Wikramaratna:1992:TBA

Wollan:1992:PRN

Won:1992:USN

Anderson:1993:CCB

Atkinson:1993:UGR
REFERENCES

Belisle:1993:HRA


Brickell:1993:SRI


Browne:1993:CTC


Bshouty:1993:CFR


Bundschuh:1993:MEC


Cerecedo:1993:NIG


Chen:1993:PGH

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Nelson:1993:RMC


Niederreiter:1993:FFP


Niederreiter:1993:FPS


Niederreiter:1993:LRP


Niederreiter:1993:PNQ


NIST:1993:FPS

[1817] Stephen K. Park, Keith W. Miller, and Paul K. Stockmeyer. Another test for randomness: Response. *Communications of the ACM*, 36(7):108–110, July 1993. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). See [1353, 1458, 1803, 1827]. The authors report that they would now recommend the MCG \( x_{n+1} = 48271x_n \mod (2^{31} - 1) \) over their original \( x_{n+1} = 16807x_n \mod (2^{31} - 1) \).


Sherif:1993:DTN


Sloan:1993:BRB


Sobol:1993:RQS


Sullivan:1993:ATR


Swain:1993:AA


Tezuka:1993:CFP


Tezuka:1993:LSA


[Toral:1993:GGD]


[Vattulainen:1993:IIP]


[Wang:1993:URP]


[Weber:1993:AIG]


[Willemain:1993:MGA]


[Winkler:1993:SRP]


REFERENCES

Anonymous:1994:IPR


Bailey:1994:PGR


Barcucci:1994:RGD


Boucher:1994:GPA


Bratley:1994:APG


Brent:1994:PGF


Cain:1994:MGF


[1861] William J. Corcoran. A multiloop Vigenère cipher with exceptionally long component series. *Cryptologia*, 18(4):356–371, October 1994. CODEN CRYPE6. ISSN 0161-1194 (print), 1558-1586 (electronic). URL http://www.informaworld.com/smpp/content-content=a748639272\&db=all\&order=page. multiloop Vigenère cipher; exceptionally long component series; computer generation; polyalphabetic cryptographic system; character set; linear congruential generating function; component series; cryptanalysis; multiloop system; computationally secure; personal computers; Spectra Publishing; Power Basic; BASIC.

REFERENCES


[Cuccaro:1994:TTQ]


[Davis:1994:CRA]


[DeArmon:1994:RLO]


[Deng:1994:DIR]


[Devroye:1994:NHS]


[Eastlake:1994:RRR]

REFERENCES


REFERENCES

Hildebrand:1994:RWS


Hill:1994:CMR


Holian:1994:PNG


Hoogland:1994:GPR


Hormann:1994:NQR


Hormann:1994:TRM


Hormann:1994:UGD

REFERENCES


REFERENCES

Kenan:1994:SAG


Kari:1994:GNS


Karian:1994:RNG

[1903] Zaven A. Karian and Rohit Goyal. Random number generation and testing. *Maple Technical Newsletter*, 1(1):32–37, Spring 1994. CODEN ????? ISSN 1061-5733. URL http://www.can.nl/Systems_and_Packages/Per_Purpose/General/Maple/mtn/mtnv1n1.html. This article describes the Maple-language random-number generator, a multiplicative congruential generator (xnew = (Ax+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.

Karloff:1994:CWI


Kenney:1994:HTI


REFERENCES


REFERENCES


REFERENCES 359


Ritter:1994:EPR


Rivest:1994:DBI


Schneier:1994:AAd


Shallit:1994:ALS


Shukhman:1994:GQR


Sitharam:1994:PGL

360
REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


Eichenauer-Herrmann:1995:IUB


Eichenauer-Herrmann:1995:NPE


Eichenauer-Herrmann:1995:PNG


Eichenauer-Herrmann:1995:QCP


Eichenauer-Herrmann:1995:RCM


Eichenauer-Herrmann:1995:UAA


REFERENCES


Hennecke:1995:FIR


Hermanns:1995:FCI


Herring:1995:TCR


Hormann:1995:RTS


Kaliski:1995:MIA


Kaliski:1995:MIA
Kessler:1995:GOC


Koc:1995:RCS


Kubota:1995:DRE


Kurita:1995:DWD


Lee:1995:CSS


Leeb:1995:DT

REFERENCES


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


Mascagni:1995:PPNa


Mascagni:1995:PPNb


Matus:1995:CIAa


Matus:1995:CIAb


Micali:1995:SMG


Miller:1995:RAC

REFERENCES


REFERENCES


id_volume=20&id_journal=8.


REFERENCES


REFERENCES


Sorenson:1995:ALE


Storn:1995:CO


Struckmeier:1995:FGL


Sugita:1995:PRN


Takashima:1995:STT


Tezuka:1995:URN


Varhol:1995:ANS

Vattulainen:1995:CSS

Vattulainen:1995:MIF

Vattulainen:1995:PMT

Walker:1995:GRV

Wegenkittl:1995:ETPa

Wegenkittl:1995:ETPb

Wegenkittl:1995:THS
Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inverse congruential pseudorandom numbers? *Journal of Computational...*
REFERENCES


Wheeler:1995:TTE


Wong:1995:EHS


Zhu:1995:MEC


Aluru:1996:PAL


Anderson:1996:GPR


Anonymous:1996:BRPe

REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


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


REFERENCES


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


distributions of the congruent sums of random values. *Doklady Akademii
Nauk SSSR*, 347(1):23–26, ???. 1996. CODEN DANKAS. ISSN 0002-
3264.

under multiple access. *Theory of Probability and its Applications*, 40
(4):679–689, ???. 1996. CODEN TPRBAU. ISSN 0040-585X (print),

[2145] Alexander I. Mikov. Large-scale addition of machine real numbers: Acc-
05, 1996. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (elec-
tronic). URL http://www.elsevier.com/cgi-bin/cas/tree/store/
tcs/cas_sub/browse/browse.cgi?year=1996&volume=162&issue=1&
aid=2194.

[2146] Ketan Mulmuley. Randomized geometric algorithms and pseudorandom
ISSN 0178-4617 (print), 1432-0541 (electronic).

[2147] S. Nemnyugin and A. Larionov. Set of random walk tests for pseudo-
random generators. In Peter Borcherds, Marian Bubak, and Andrzej
Maksymowicz, editors, *Proceedings of the 8th Joint EPS-APS Interna-
tional Conference on Physics Computing: PC ’96: September 17–
CYFRONET, Kraków, Poland, 1996. ISBN 83-902363-3-8. LCCN QC20
.I45 1996.

[2148] Harald Niederreiter. Improved bounds in the multiple-recursive matrix
method for pseudorandom number and vector generation. *Finite Fields
REFERENCES


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

Rubin:1996:OTP


Sanchis:1996:PAC


Schervish:1996:VWT


Schneier:1996:ACP


Sethumadhavan:1996:NPE


Sezgin:1996:RNG

REFERENCES


REFERENCES


Wallace:1996:FPG


Wang:1996:LIL


Wegenkittl:1996:RSP


Alon:1997:SSD


REFERENCES


Berblinger:1997:MCI


Berg:1997:CNF


Binder:1997:AMC


Binder:1997:MCS


Cario:1997:MGR

REFERENCES

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

Coddington:1997:RNG


Compagner:1997:RER


Couture:1997:DPM


Dai:1997:RCD


Dai:1997:RRW


Deng:1997:SJC


REFERENCES


REFERENCES


Foster:1997:DOT


Gell-Mann:1997:ETZ


Grabner:1997:MSR


Hamilton:1997:AR


Hamilton:1997:ARP


Hellekalek:1997:CAP

REFERENCES


Hellekalek:1997:GRN

[2215] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [3835], page ?? ISBN 3-901608-11-7. LCCN ???

Hellekalek:1997:NPNa


Hellekalek:1997:NPNb


Herendi:1997:FGR


Heuer:1997:CCS


Imperiale:1997:PUG

REFERENCES


REFERENCES


REFERENCES


[2236] George Marsaglia. A random number generator for C. Posted to the sci.math.num-analysis news group, September 29, 1997. URL http://mathforum.org/kb/thread.jspa?messageID=1607565. From the posting: “Keep the following six lines of code somewhere in your files. #define znew ((z=36969*(z&65535)+(z>>16))<<16) #define wnew ((w=18000*(w&65535)+(w>>16))&65535) #define IUNI (znew+wnew) #define UNI (znew+wnew)*4.656613e-10 static unsigned long z=362436069, w=521288629; void setseed(unsigned long i1,unsigned long i2)z=i1; w=i2; Whenever you need random integers or random reals in your C program, just insert those six lines at (near?) the beginning of the program. In every expression where you want a random real in [0,1) use UNI, or use IUNI for a random 32-bit integer. No need to mess with ranf() or ranf(lastI), etc, with their requisite overheads. Choices for replacing the two multipliers 36969 and 18000 are given below. Thus you can tailor your own in-line multiply-with-carry random number generator.”.


[2238] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In IEEE [3834], pages 458–467. CODEN ASF-
REFERENCES

Naveau:1997:CBC


Needham:1997:TE


Novak:1997:DRS


Ogawa:1997:EAR


Pages:1997:SLD


Woodward:1997:ECD


Wu:1997:MCR


Zubkov:1997:PTD


Aiello:1998:DPP


Andreev:1998:NGD


Antoch:1998:RPN

REFERENCES


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


REFERENCES


Hellekalek:1998:ARQ


Hellekalek:1998:CAP


Hellekalek:1998:DTP


Hellekalek:1998:GRN


Hellekalek:1998:WST


Hickernell:1998:LRH


REFERENCES


REFERENCES

Marsaglia:1998:MPMb


Mascagni:1998:PLC


Matsumoto:1998:DCP


Matsumoto:1998:MTD


Mende:1998:MSP

REFERENCES


REFERENCES


[2342] H. Tanaka, T. Ohishi, and T. Kaneko. An optimised linear attack on pseudorandom generators using a non linear combiner. Lecture Notes in


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Durrant:1999:RND


Eichelsbacher:1999:CPA


Entacher:1999:CSR


Entacher:1999:PRN


Entacher:1999:PSL


Entacher:1999:QMC

Karl Entacher, Peter Hellekalek, and Pierre L’Ecuyer. Quasi-Monte Carlo node sets from linear congruential generators. In Niederreiter and Spanier [3850], pages 188–198. ISBN 3-540-66176-X (soft-


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


Kleinman:1999:SBO


Koldobsky:1999:PDD


Koshiba:1999:UPN


Larcher:1999:ADS


LEcuyer:1999:BLC


REFERENCES

2163 (electronic). URL http://journals.cambridge.org/action/displayIssue?jid=CPC&volumeId=8&issueId=03.

Mccullough:1999:ARS


Mccullough:1999:ASP


Mccullough:1999:NRE


Mrahi:1999:CAR


Muller:1999:CRV


Niederreiter:1999:DLS

REFERENCES


REFERENCES

Siu:1999:PNG


Sobol:1999:DRR


Sobol:1999:PRN


Soto:1999:EST


Soto:1999:RTA


Soto:1999:STRa


Soto:1999:STRb

REFERENCES

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


[2428] Bob Jenkins, Jr. ISAAC: a fast cryptographic random number generator. Web site, 19xx. URL http://burtleburtle.net/bob/rand/isaacafa.html. ISAAC (Indirection, Shift, Accumulate, Add, and Count) is based on cryptographic principles, and generates 32-bit random numbers. ISAAC-64 is similar, but requires 64-bit arithmetic, and generates 64-bit results.
REFERENCES


REFERENCES


REFERENCES

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


Iwata:2000:PAF


Jennewein:2000:FCQ


Juels:2000:HTL


Kabal:2000:GGP


Kelsey:2000:YND


[2467] 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


Agrawal:2001:CDF

REFERENCES


REFERENCES


REFERENCES


[2520] Julio F. Fern{a}ndez and Carlos Criado. Reply to “Comment on ‘Algorithm for normal random numbers’”. *Physical Review E (Statistical physics,
REFERENCES


The program contains code (near the end) for the portable `rannyu()` generator. It is a linear congruential generator with multiplier $A = 31\,167\,285 = 0x1db\,9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.


Hernandez:2001:FNO


Hernandez:2001:GAC


Howgrave-Graham:2001:PRN


Iwata:2001:PAF


Johnson:2001:CCO


Kang:2001:PMT

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


REFERENCES


REFERENCES

Lenczewski:2001:FRV


Levin:2001:SIC


Leydold:2001:SUG


Leydold:2001:UAA


Li:2001:SPD


Liang:2001:NET


REFERENCES


REFERENCES

NIST:2001:BST


NIST:2001:SRC


Noll:2001:HGL


Peebles:2001:PRV


Peterson:2001:PMM


Probert:2001:CAN


RAND:2001:MRD


REFERENCES


[2587] Renée Touzin. Des générateurs récursifs multiples combinés rapides avec des coefficients de la forme ±2^p_1 ± 2^p_2. (French) [Fast combined multiple recursive generators of the form ±2^p_1 ± 2^p_2]. Thèse (M.Sc.), Département d’informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2001. xiii + 128 pp. Mémoire présenté à la faculté des études supérieures en vue de l’obtention du grade de Maître ès sciences (M.Sc.) en informatique option recherche opérationnelle.


REFERENCES


REFERENCES


Entacher:2002:ELA


Fahoome:2002:JRF


Faure:2002:ARS


Figotin:2002:ONT


Fluhrer:2002:CSP


Friedel:2002:FGR


REFERENCES


REFERENCES


REFERENCES

link.springer.de/link/service/series/0558/papers/2557/25570615.pdf.


REFERENCES


REFERENCES


REFERENCES


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


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


[2681] Anonymous. /dev/random. Web site., June 8, 2003. From the site: “Thus, in 1994 noted Linux kernel hacker Theodore Ts’o wrote a driver for Linux, which takes information about hard to predict events like keyboard and mouse use, packet and disk drive timings, and so on, and uses it to seed a cryptographically secure random number generator. A process can then open up the ‘file’ /dev/random (usually a character device), and read out random bytes. The driver keeps an estimate of how much entropy remains in the pool — if it goes below 0 then any reads will block until more entropy is added.” Also this: “the actual driver is implemented in drivers/char/random.c in the Linux source tree.”.
Barak:2003:TRN


Beebe:2003:PRN


Brent:2003:RNG


Bucci:2003:HSO


Crawford:2003:FWC

[2686] Diane Crawford, Simone Santini, Ralph Castain, William F. Dowling, John Cook, Simon Dobson, Peter J. Denning, Robert Dunham, Jef Raskin, and Dennis Tsichritzis. Forum: When is a computer more like a guitar than a washing machine?: corroboration the only way to determine Web accuracy; how to teach critical thinking about Web content; create a random number service based on the Mersenne Twister; make 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).

Deng:2003:SHD

REFERENCES


REFERENCES


REFERENCES


Intel:2003:IRN


Joe:2003:RAI


Kocarev:2003:CPR


LEcuyer:2003:CGC


Lemieux:2003:RPL


Li:2003:ULD


xorshift generators and the well-understood linear feedback shift register generators. See also [3448, 3540, 3629] for the failure of Marsaglia’s xorwow() generator from this paper. See [2865, 3687] for detailed analysis.


REFERENCES


REFERENCES


Stipcevic:2003:NDR


Sugita:2003:DR


Tang:2003:SDA


Tang:2003:SPM


Tsang:2003:TCT


Tsoi:2003:CFB

REFERENCES


 REFERENCES


REFERENCES


REFERENCES


Luk:2004:DMT


Maigne:2004:PMC


Marsaglia:2004:BURA


Marsaglia:2004:FGD


Martin:2004:ICF


Mascagni:2004:PLC

REFERENCES

Mascagni:2004:PPM


Mauduit:2004:CPB


McCullough:2004:BRB


McCullough:2004:FSE


McIvor:2004:IIM


Mertens:2004:EPR

REFERENCES


REFERENCES

Rasulov:2004:QSB

Ryabko:2004:BSN

Ryabko:2004:NTR

Rybakov:2004:SPL

Rybakov:2004:SVL

Schmuland:2004:CLT

Sezgin:2004:MSS
Sugita:2004:SPR


Tang:2004:SGM


Tirler:2004:EKR


Tonon:2004:URS


Tsang:2004:TCT

REFERENCES


REFERENCES


REFERENCES

Bogdanov:2005:PGL

Calvayrac:2005:RNG

Castro:2005:NRG

Contini:2005:SAA

Damgaard:2005:CRM
Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. Lecture Notes in Computer
REFERENCES


Deng:2005:EPM


Dodge:2005:RNG


Eastlake:2005:RRR


Elsner:2005:IRN


Entacher:2005:BLP


Falcioni:2005:PMC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Wichmann:2005:GGP


Wiese:2005:IPN


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ

Aistleitner:2006:NZG


Alon:2006:MPF


Aly:2006:LCP


Anonymous:2006:E


Barak:2006:ERU


Barash:2006:POE

REFERENCES


REFERENCES

517


REFERENCES

Jerusalem and University of Haifa, Jerusalem and Haifa, Israel, March 6, 2006. 18 pp. URL http://www.pinkas.net/PAPERS/gpr06.pdf.


LCCN
LEcuyer:2006:ISB


LEcuyer:2006:TSL


Lee:2006:HGN


Lee:2006:IBH


Maffre:2006:WKT

REFERENCES


REFERENCES


REFERENCES


Purczynski:2006:FGF


Rinehart:2006:PRN


Ripley:2006:SS


Rose:2006:CSP


Rubin:2006:EGE


Rybakov:2006:LES


Schanze:2006:EDT

REFERENCES


Schmidt:2006:BRJ


Schroeder:2006:RNG


Sezgin:2006:DLP


Simka:2006:MTR


Skoge:2006:PHH

REFERENCES


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


REFERENCES


REFERENCES


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


REFERENCES

Hars:2007:PRS

Hasan:2007:FSU

Hormann:2007:ITD

Hormann:2007:SGD

Juneja:2007:AFS

Kang:2007:PFS


References


Nekrutkin:2007:AAO


Panditaratne:2007:TRN


Pareschi:2007:SLN


Pazo-Robles:2007:MPS


Perez:2007:RJI

Rusu:2007:PRN


Santhanam:2007:CLB


Sathyanarayana:2007:GPS


Sinescu:2007:GIR


Sinescu:2007:GLR


Stipcevic:2007:QRN


Tsoi:2007:HPP

physical random number generator. IET Computers & Digital Techniques,
punumber=4117424; http://link.aip.org/link/?CDT/1/349/1.

Turiel:2007:QRB

Statistician, 61(3):255–259, August 2007. CODEN ASTAAJ. ISSN 0003-
1305 (print), 1537-2731 (electronic).

Vadhan:2007:UTP


Viola:2007:PBC

[3023] Emanuele Viola. Pseudorandom bits for constant-depth circuits with few
arbitrary symmetric gates. SIAM Journal on Computing, 36(5):1387–
1403, ????? 2007. CODEN SMJCAT. ISSN 0097-5397 (print), 1095-7111
(electronic).

Wijaya:2007:PSM

[3024] Sastra Wijaya, Syn Kiat Tan, and Sheng-Uei Guan. Permutation and
sampling with maximum length CA or pseudorandom number genera-
1, 2007. CODEN AMHCBQ. ISSN 0096-3003 (print), 1873-5649 (elec-
tronic).

Yan:2007:EJC

1548-7660. URL http://www.jstatsoft.org/v21/i04.

Ahmad:2008:ATT

[3026] David Ahmad. Attack trends: Two years of broken crypto: Debian’s
dress rehearsal for a global PKI compromise. IEEE Security & Privacy,
6(5):70–73, September/October 2008. CODEN ????? ISSN 1540-7993
(print), 1558-4046 (electronic).


REFERENCES

Bader:2008:DFP


Balachandran:2008:TRN


Banks:2008:FIP


Beirami:2008:PMD


Bello:2008:OPR


Blaszczyk:2008:NMT

REFERENCES


Blaszczyk:2008:TRB


Brent:2008:SCC


Bucci:2008:FDR


Calude:2008:QRV


Cesmelioglu:2008:CSP


Chen:2008:FBS

REFERENCES


Chen:2008:GFT


Chen:2008:RKD


Chen:2008:SCS


Chindris:2008:HER


Christen:2008:OPR


Collins:2008:TSI

REFERENCES


REFERENCES


REFERENCES


Howes:2008:U


Inaltekin:2008:ANE


Jang:2008:CDH


Joe:2008:CSS


Jovanovic-Dolecek:2008:UMT


Kalos:2008:MCM

Kang:2008:HPP


Kato:2008:QSC


Katsoprinakis:2008:QRN


Katti:2008:SPR


Katz:2008:RRNa

REFERENCES


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


McCullough:2008:ASP


McCullough:2008:MEW


Miller:2008:OSB


Murdoch:2008:VRV


Murphy:2008:CLW


Nandakumar:2008:EET


Nguyen:2008:ODD


REFERENCES


REFERENCES


REFERENCES


Uchida:2008:FPR


Udawatta:2008:TVN


Varbanets:2008:ESS


Varbanets:2008:ICGa


Varbanets:2008:ICGb


Walker:2008:EPN


Wang:2008:DCP


REFERENCES

Cao:2009:DSB

Cecen:2009:NHN

Chen:2009:FPM

Chen:2009:MTR

Chi:2009:PQN


REFERENCES


Edrees:2009:HOZ


Faure:2009:GHS


Feldhofer:2009:HIS


Fischer:2009:SRF


Galassi:2009:GSL


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

Guo:2009:RNG


Gyorfi:2009:HPT


Hai-Wei:2009:HSL


Haramoto:2009:AST


Hashim:2009:RMS

REFERENCES


REFERENCES


Lee:2009:HHA


Lemieux:2009:PNG


Marchi:2009:PPR


Markenos:2009:FIA


McCullough:2009:AES


Mitchum:2009:DPR

REFERENCES


Paindaveine:2009:MR


Pareschi:2009:PA


Petrov:2009:SLL


Qiu:2009:CMW


Reidler:2009:USR


Ridout:2009:GRN

REFERENCES


2219, ????, 2009. CODEN CSFOEH. ISSN 0960-0779 (print), 1873-2887 (electronic).


REFERENCES


Wayne:2009:PA


Wei:2009:BFT


Wei:2009:QRN


Wold:2009:OST


Xiao-chen:2009:URN

REFERENCES


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

search Report CDMTCS-396, Centre for Discrete Mathematics and
Theoretical Computer Science, The University of Auckland, Auckland,
researchreports/396cris.pdf.

[3251] Stefan C. Agapie and Paula A. Whitlock. Random packing of hy-
perspheres and Marsaglia’s parking lot test. *Monte Carlo Methods
and Applications*, 16(3–4):197–209, December 2010. CODEN MC-
MAC6. ISSN 0929-9629 (print), 1569-3961 (electronic). URL http://

[3252] Afshin Akhshani, Sohrab Behnia, Amir Akhavan, Siew-Choo Lim, and
Zainuriah Hassan. Pseudo random number generator based on syn-
chronized chaotic maps. *International Journal of Modern Physics C
[Physics and Computers]*, 21(2):275–290, February 2010. CODEN LIM-
PEO. ISSN 0129-1831 (print), 1793-6586 (electronic). URL http://

[3253] Vladimir Anashin. Non-Archimedean ergodic theory and pseudorandom
CMPJA6. ISSN 0010-4620 (print), 1460-2067 (electronic). URL http://
comjnl.oxfordjournals.org/cgi/content/abstract/53/4/370;

of cryptographically strong generator by linearly generated sequences.
Report ??, The University of Memphis, Memphis, TN 38152, USA,
Mathew-security-paper.pdf.

*Discrete-Event System Simulation*. Prentice-Hall, Upper Saddle River,
REFERENCES


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


REFERENCES


REFERENCES


[3300] Yu Liu, Wenzhuo Tang, and Hong Guo. True random number generator based on the phase noise of laser. In 2010 Conference on Lasers and Electro-Optics (CLEO) and Quantum Electronics and Laser Science Conference (QELS), pages 1–2. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver Spring, MD 20910,
REFERENCES


Lovett:2010:PGC


Luan:2010:PR


Luo:2010:PAE


Marsaglia:2010:SKR


Marton:2010:RDC


Meka:2010:PGP

REFERENCES


Orue:2010:TNP


Ostafe:2010:DGS


Ostafe:2010:MPP


Ostafe:2010:PNH


Ostafe:2010:PNM


Panneton:2010:RSR

Pareschi:2010:ITH


Pashley:2010:GRN


Passerat-Palmbach:2010:RIG


Peris-Lopez:2010:CSP


Plesser:2010:RSI

REFERENCES


REFERENCES


Thomas:2010:FOU


Tirdad:2010:HNN


Tomasik:2010:AAG


Urivskiy:2010:MMS


Vakhania:2010:QGR


Valtchanov:2010:CRS

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


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


REFERENCES


REFERENCES


[3373] 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.”.


[3375] Jacques M. Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of


REFERENCES

Bustard:2011:QRB


Cai:2011:ADB


Carter:2011:TQS


Chan:2011:TRN


Chen:2011:ARN


Chevallier:2011:LSB


REFERENCES


[3412] Parikshit Gopalan, Raghu Meka, Omer Reingold, and David Zuckerman. Pseudorandom generators for combinatorial shapes. In ACM [3907],
Griffiths:2011:FFL


Haitner:2011:PRI


Han:2011:MTB


Harase:2011:ELR


Harase:2011:FLR


Kao:2011:EAT


Kleimo:2011:RNG


Koucky:2011:PGG


LEcuyer:2011:AZV


LEcuyer:2011:NUR


LEcuyer:2011:URN


Leydold:2011:GGI

REFERENCES


Malik:2011:EHI


Malik:2011:GHT


Marton:2011:PUR


Merhi:2011:SPR


Mohamed:2011:EAG


[3448] John K. Salmon, Mark A. Moraes, Ron O. Dror, and David E. Shaw. Parallel random numbers: as easy as 1, 2, 3. In Lathrop et al. [3911], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????


REFERENCES


Wahl:2011:UQR


Wang:2011:CRN


Wang:2011:LTA


Wang:2011:MPF


Wei:2011:HSB


REFERENCES


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


Becher:2012:TNN


Berger:2012:CPR


Bergman:2012:GRV


Bertoni:2012:KSF


Boldyreva:2012:NPG


Boureanu:2012:PF

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3514] Ping Koy Lam, Thomas Symul, and Syed Assad. Quantum random number generator. Web site, April 2012. URL http:
Random numbers are generated from quantum vacuum noise. See [3460] for details.


[3519] 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


REFERENCES


REFERENCES


Zhang:2012:RAG


Afshar:2013:ESR


Anonymous:2013:ERN


Applebaum:2013:PGL


AragonArtacho:2013:WRN


Bailey:2013:NNP

REFERENCES


[3559] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL http://people.umass.edu/gbecker/BeckerChes13.pdf.


REFERENCES


REFERENCES

Hu:2013:PSG


IBM:2013:IPC


Imai:2013:CRN


Khoshkenar:2013:NTR


Liberty:2013:THR


Liu:2013:ITT


REFERENCES


REFERENCES


[3604] Ching-Wei Cheng, Ying-Chao Hung, and Narayanawswamy Balakrishnan. Generating beta random numbers and Dirichlet random vectors
REFERENCES


Devroye:2014:RVG


Dodis:2014:HEY


Doty-Humphrey:2014:STP


England:2014:ERG


Fukushima:2014:SDS

REFERENCES


REFERENCES

Koo:2014:CRB


Korzen:2014:PPP


Langr:2014:APP


LECuyer:2014:LSS


Ling:2014:MDN


Mascagni:2014:HPC

REFERENCES


REFERENCES

Sobol:2014:QMC


Steele:2014:FSP


Thomas:2014:FGR


Andersen:2015:MEL


Astor:2015:ADI


Berman:2015:NAA


Hill:2015:PRN


Jessa:2015:QRS


LeCuyer:2015:RNP


Leetmaa:2015:KER


LoRe:2015:SRN


Lubicz:2015:TOB

REFERENCES


REFERENCES


REFERENCES


Nekrutkin:2016:CBF


NIST:2016:SDR


Ohsaka:2016:DIA


Vigna:2016:EEM


Yamakami:2016:PGA


Yu:2016:GPR

Anonymous:2017:DAD

[3690] 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 [3697] for details of the attack.

Artemenko:2017:PGO


Bacher:2017:GRP


Barmpalias:2017:PCO


Barmpalias:2017:RNP


Beebe:2017:MFC

REFERENCES


REFERENCES


REFERENCES

Pomeranz:2017:CSL


Popov:2017:DTP


Sibidanov:2017:RSB


Sutar:2017:DP1


Sys:2017:AON


Thorup:2017:FPH


Vigna:2017:FSM

[3714] Sebastiano Vigna. Further scramblings of Marsaglia’s xorshift generators. *Journal of Computational and Applied Mathematics*, 315(??):175–181, May 1, 2017. CODEN JCAMDI. ISSN 0377-0427 (print), 1879-
REFERENCES


Ye:2017:VCS


Aletti:2018:GDR


Bernardin:2018:GES


Lin:2018:RNG


Petrica:2018:FOC

REFERENCES


[3722] David Wagner. Writings on randomness; source code for generating randomness; source code for testing randomness; hardware for generating randomness; source code to other useful crypto modules; miscellaneous. World-Wide Web site., 20xx. URL http://www.cs.berkeley.edu/~daw/rnd/.


REFERENCES

Meyer:1956:SMC


Macphail:1959:PFC


Anonymous:1960:PFI


Ralston:1960:MMD


Birkhoff:1961:NRT


Taub:1963:JNCa


Kozesnik:1964:TTP

REFERENCES


REFERENCES


REFERENCES


[IEEE:1983:ASF]


REFERENCES


[3762] Kurt Mehlhorn, editor. STACS 85: 2nd Annual Symposium on Theoretical Aspects of Computer Science, Saarbrücken, January 3–5, 1985, vol-
ACM:1986:PEA


Arkin:1986:SOP


DAgostino:1986:GFT


Heath:1986:HMP


Wilson:1986:WSC

REFERENCES

ACM:1987:PNA


Chaum:1987:ACE


Deavours:1987:CYT


IEEE:1987:ASF


Odlyzko:1987:ACC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Pomerance:1990:CCNb


Anonymous:1991:PIS


Day:1991:PA


Dorninger:1991:CGA


Nelson:1991:WSC

REFERENCES


REFERENCES


REFERENCES


ACM-SIAM:1994:ASD


ACM:1994:PTS


Desmedt:1994:ACC


IEEE:1994:PSW


Snodgrass:1994:PAS
REFERENCES


REFERENCES


REFERENCES


IEEE:1996:ASF


IEEE:1996:ASF

Trobec:1996:PIW


Trobec:1996:PIW

Andradottir:1997:PWS


Andradottir:1997:PWS

Gell-Mann:1997:QJA


Gell-Mann:1997:QJA
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Meadows:2005:CPA


Smart:2005:CCI


Henderson:S


Niederreiter:2006:MCQ


Schroeder:2006:NTS

REFERENCES


Ytrehus:2006:CCI


ACM:2007:SPA


Adams:2007:SAC


Menezes:2007:ACC


Simos:2007:CMS


[3893] Christos Alexopoulos, David Goldsman, and James R. Wilson, editors. *Advancing the frontiers of simulation: a Festschrift in honor of George


REFERENCES


IEEE:2010:PIA


Peterson:2010:IEE


ACM:2011:PAI


Gilli:2011:NMO


Hwu:2011:GCG


IEEE:2011:ICI


REFERENCES


Dyson:2012:TCO


Gentle:2012:HCS


Hwu:2012:GCG


IEEE:2012:PIA


ACM:2013:SPF


Bailey:2013:CAM

[3922] David H. Bailey, Heinz H. Bauschke, Peter Borwein, Frank Garvan, Michel Théra, Jon D. Vanderwerff, and Henry Wolkowicz, editors. *Com-
REFERENCES
