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/

11 March 2019
Version 1.305

Title word cross-reference

#14 [2267]. #15949 [870]. #4059 [1240]. #8373 [2091].

(0, 1) [1052]. (0, s) [2524, 2908]. (a^n - 1)/(a - 1) [916]. (j, c) [729]. (n^2 \alpha) [2477]. (n^k \alpha) [2478]. (n\alpha) [2477]. (t, m, s) [2035, 2868, 2041, 2340]. (t, s) [2619, 2035, 2331, 2868, 2041]. (X^2 - Y^2)^{1/2} [489]. 0.1(0 \times 1)0 \times 9 [139]. 1 [736, 874, 2821, 171, 711, 2943, 2945]. 1, 2, 3 [3456]. 1.13198824... [2501]. 10, 000 [282]. $10.00 [168]. 10^{2857} [2472]. 10^{1035} [2033]. 1200\mu [3102]. 128 [3128]. 13 [270]. 16 [270]. 2 [2821, 2110, 928, 3067, 2486, 2801, 2947]. 2, 000 [86]. $24.95 [2078]. 2^{-31} - 1 [836, 929]. 2^{15} [2128]. 2^{31} - 1 [3506, 801, 972, 1005, 1193, 1194]. 2^{31} - 69 [3351]. 2^{32} - 1 [1085]. 2^n [1470, 2228]. 2^n [1313, 1476, 1722]. 2^k [2600]. 2^{k-1} [2600]. 2^p [3215]. 2^n - 1 [2260]. 3 [1777, 3633]. 32 [3588]. 4 [270]. 48 [245]. 5 [270]. $52.95 [3556]. 64
\[a = \pm 2^q \pm 2^r\] \[\{ a_n \} \quad \lambda \{ b_n \} \quad \{ a_n(j+\tau)^2 \} \]

\[\phi(\lambda|x^n) \quad \chi^2 \quad D \quad d^2 \quad e \quad f \quad \Gamma \quad j \quad K \quad L \quad \lambda \quad M \quad N \quad \phi(0) \quad P \quad \pi \quad \pi \quad q \quad S \quad \sigma \quad \sqrt{2} \quad \sum a_n/n \quad T \quad U \quad X(1+i) = AX(1+i) \mod 2^3 1 \quad x^2 \mod N \quad X_{n+1} = ax_n + b_n \quad \mod p \quad (a+x) \sin(bx) \mod 1 \quad Z/nZ \quad Z_p \quad [2650].

-g**{adic} \[3306, 445, 444, 2358]. \quad -biased \[1900]. \quad -Bit \[3128, 3736, 245]. \quad -concave \[2555]. \quad -D \[3067]. \quad -deformed \[2490]. \quad -dependent \[1900]. \quad -Detection \[3721]. \quad -digit \[270]. \quad -Dimensional \[267, 194, 199, 893, 1509, 1956, 1756, 786, 203, 1303, 2955]. \quad -discrepancy \[2021]. \quad -distributed \[1315]. \quad -Distribution \[943, 1848, 1037]. \quad -distributions \[1797, 2069]. \quad -
\]

Advanced [1447, 1909, 3769, 3933, 3887, 2420, 2495]. Advances [3781, 3799, 3817, 1066, 3879, 2644, 3838, 2663, 3789, 3791, 3844, 3916, 3802].


Affine [3688, 2491]. Against [2831, 3265, 3710, 1325, 3115, 3555, 3700, 3747].


Air [3764, 1867]. AIS [2542, 2413]. AIX [2738]. Akima [755]. al. [895].


algorithm [1708, 555, 1547, 3868]. algorithmische [555]. algorithmischer [1708].


Approximations [143, 2775, 1048, 1001, 2995, 1223, 2964, 3025]. April [3789, 3760, 3799, 3822, 3933, 3877, 3833, 3807, 3808]. Arbitrary [2189, 812, 1525, 3029, 963, 3732, 2976, 197, 1686, 3462, 1282, 694, 3507].

Archimedean [3260]. Architecture [2823, 2770, 3340, 2065, 3251, 3513, 2964, 3025]. Architectures [1447, 3691, 3602]. Area [2823, 2770, 3340, 2065, 3251, 3513, 3720, 1544]. Area-Efficient [2823, 2770, 3340, 2065, 3251, 3513, 3720, 1544].


automorphisms [3620]. Autonomous [3356]. Autoregressive [1693].
available [3120]. Avalanche [3233]. Average
[1757, 2201, 2202, 2616, 2099, 2661, 2108, 2766, 3522, 2393, 3460].
average-case [2108, 3522]. Averages [841]. Averaging [3624, 281]. avoid
[1368, 1579]. Avoided [1165]. Avoiding [3850, 2530, 1777]. AVX [3682].
award [3452]. Aware [1630]. AWC [1865]. AWC/SWB [1865]. AWGN
[2601, 3444].
Experimental [920, 921, 3157, 3272, 3187, 627, 709, 24, 933, 893, 941, 942, 849, 949, 2742, 3699, 791, 3158, 1890, 1708, 175, 7].
Explaining [2905]. Explicit [2275, 3679, 3062, 1763, 1876, 2869, 3049, 1991, 2110, 2726, 2164].
Exploring [193x586] [3699].
Exploitation [3560, 2863].
Exploration [3699].
Exponent [1684, 1801, 743]. Exponential [563, 1872, 2915, 3068, 2295, 1049, 2560, 304, 769, 2482, 2870, 3112, 953, 2809, 3137, 1364, 1289, 344, 658, 2696, 2113, 2378, 1583, 2769, 3517, 330, 1213, 248, 933, 893, 936, 941, 942, 849, 949, 2742, 3699, 791, 3158, 1890, 1708, 175, 7].
Exponentially [212, 3427, 3129, 312, 3172, 224, 3694].
Exponentiation [2701, 2132, 1617].
exponentiations [1550].
exponents [2783].
Expressing [249].
expression [2014].
Extendable [3661].
Extendable-Output [3661].
Extended [2368, 1136, 1483, 2543, 3653, 1517, 1169, 487, 1236, 3827, 1405, 1789, 3433, 473, 3310, 1215, 2425, 2428].
Extending [1159]. Extends [1788].
Extensible [2452, 2731].
Extension [2247, 3459, 3128, 658].
Extensions [615, 898, 2243, 2125].
extensively [1860, 2305].
extracted [3718].
Extracting [2896, 2155, 1723].
Extraction [3286, 3590, 3545].
Extractor [3679, 2456, 3688, 2593, 2581, 2877, 2428, 3371].
Extrapolation [1338]. Extraterrestrial [2047].
Extreme [1677, 8].
Extremely [472, 723, 584, 585, 3480]. extremely-high-throughput [3480].
Face [3238].
Facilities [1594, 344].
Factored [1292].
Factorial [2242].
Factoring [1012, 1150, 1262, 1821, 1737, 2746].
Factorization [1816, 724, 1332, 683, 1163, 1943, 3548].
Factorizations [1032, 1298, 2607].
failure [2382].
fair [2623, 2460, 2995].
Fairfax [3807].
Fairmont [3815].
Fall [135].
Family [3420, 2546, 2715].
Families [3420, 2546, 2715].
Fat [1554].
fat-tailed [1554].
Feasible [3677, 3393, 3572, 1215].
Fault-tolerant [3572, 1215].
Faulty [3625].
Fauro [2676].
FCRC [3856].
FCSR [2820, 3235].
FCSR[s] [3494, 3180].
FDC [1912].
Features [434, 1547].
February [3929, 3865, 3898, 3774].
Feedback [2517, 1183, 1300, 1037, 1492, 2466, 507, 633, 3693, 635, 848, 3450, 1530, 3552, 2677, 3054, 1683, 2017, 940, 329, 3442, 305, 2023, 2658, 1270, 1351, 3633, 1729, 3742, 3674, 1107].
Feeding [3052].
Feinstein [315].
Feistel [3702].
Feistel-inspired [3702].
Feller [3266, 1376].
Fence [3606].
Fermat [3508].
fermions [3572].
ferromagnetic [720].
Festchrift [3923]. Few [2896, 3058, 3029, 2994, 1276].
Few-body [1276].
Fiar [2691].
Fibonacci [2076, 2178, 3641, 1852, 403, 3420, 1921, 247,
1925, 1926, 2026, 2027, 2028, 2793, 1934, 2409, 1739, 1832, 2501, 2290, 2383, 3838, 1609, 1714, 1815, 2154, 2483.

**Field**

Field-programmable [2561].

**Fields**

[135x634] [2561].

**Finalist**

[2458, 2539].

**Finnish**

[704, 719, 515, 1106, 909, 913].

**First-Order**

[1693, 1325].

First-Order [1693, 1325].

**Fisher**

[920, 921, 933, 936, 941, 942, 949].

**Fishman**

[3923].

**Fitting**

[1825].

**Flaws**

[3266].

**Flies**

[253].

**Flying**

[1072, 1175].

**Floating**

[3072, 1690, 2980, 3431, 2016, 3696, 650, 2166, 1826, 693, 2968].

**Floating-Gate**

[3072, 1690, 2980, 3431, 2016, 3696, 650, 2166, 1826, 693, 2968].

**flashing**

[1072, 1175].

**flaw**

[3573].

**flaws**

[3266].

**flying**

[1072, 1175].

**float**

[3486].

**Floating**

[3072, 1690, 2980, 3431, 2016, 3696, 650, 2166, 1826, 693, 2968].

**Floating-Point**

[2016, 650, 2166, 1826, 693].

**flop**

[160].

**Florida**

[3786, 3864, 3756, 3847, 3776].

**flow**

[2995, 1741].

**flow-level**

[2995].

**Fly**

[3224].

**Fock**

[2490].

**folding**

[901, 902, 3720, 2889].

**Fonctions**

[4, 281].

**force**

[3764].

**forced**

[3483].

**forests**

[1846].

**Fork**

[1373, 1795].

**Fork-Join**

[1373, 1795].

**form**

[2592].

**formal**

[2594].

**Formal**

[2010].

**formalism**

[2594].

**Formalization**

[2991].

**Format**

[3176].

**Formation**

[197, 469].

**formes**

[2592].

**Forms**

[823, 1178, 1041, 1098, 948].

**formula**

[3429, 2717].

**Formulae**

[167].

**Formulas**

[391].

**Formulation**

[2098, 977, 688].

**Forsythe**

[615].

**Fortran**


**fortune**

[1781].

**Forty**

[3951].

**Forty-fifth**

[3951].

**Forum**

[2691].

**forward**

[2996, 2963].

**Found**

[1751].

**foundation**

[555].

**Foundations**

[3780, 3783, 3786, 3801, 3806, 3812, 3818, 3828, 3851, 3860, 3864, 3885, 3889, 3935, 3950].

**Four**

[1435, 2359, 1682, 2234, 2029, 2030, 2401, 2580, 2669, 3242].

**Four-Bit**

[1435].

**four-dimensional**

[3242].

**Four-Tap**

[2359].

**Fourier**

[2845, 398, 3585, 3308].

**Fourth**

[3895, 3810, 3825, 3879, 3757].

**FPGA**

[3034, 3040, 3158, 2368, 3403, 2442, 2985, 3413, 3190, 3198, 3299, 3737, 3309, 3740, 3331, 3339, 3224, 2580, 2669, 3352, 3354, 3602, 3640, 3671, 2749, 3144, 3250, 3482].

**FPGA-Based**

[2368, 3224, 3034, 3413, 2749, 3482].

**FPGA-Optimised**

[3354].

**FPGAs**
2224, 1205, 2388, 152, 2303, 1899, 2124, 2433, 2459, 3430, 2713, 1259, 1093,
3299, 3199, 1409, 2129, 2130, 2228, 3081, 3082, 3200, 3085, 2462, 981, 1414, 1591,
2852, 584, 585, 245, 763, 1096, 1337, 3301, 2234, 3201, 3302, 985, 3090, 3202

Generators

[3203, 764, 2018, 2784, 2785, 2857, 2933, 2934, 2469, 1507, 474, 2555, 3438, 3439,
2863, 1800, 2786, 3307, 3440, 3443, 3690, 2139, 2649, 1918, 586, 1597, 634, 3444,
3591, 3208, 1511, 1512, 2239, 2650, 3311, 3447, 1925, 3631, 2325, 3448, 774,
446, 811, 2658, 775, 1053, 3314, 899, 813, 3315, 814, 3213, 987, 1219, 3319, 644,
3114, 3596, 3010, 2157, 3219, 1432, 160, 481, 515, 3328, 945, 1615, 3115, 3740,
2336, 2487, 2046, 1273, 782, 603, 2488, 1939, 3331, 605, 362, 3454, 1617, 2952,
2807, 2808, 2954, 1619, 3549, 687, 3670, 2955, 690, 1730, 2341, 3342, 482, 3457].

Generatoren [1026, 1028]. Generators [1365, 2507, 2262, 2754, 290, 2076,
2178, 2894, 3260, 1447, 3562, 3704, 3153, 3038, 2603, 2266, 3040, 2687, 2989,
506, 2086, 3748, 3385, 1561, 2186, 3494, 2090, 878, 1378, 3270, 3612, 2761,
2900, 3045, 2094, 881, 882, 3046, 1180, 2367, 884, 3277, 2369, 1183, 1244, 1300,
3055, 2831, 398, 2520, 1659, 3169, 1464, 1868, 1305, 1662, 1869, 2195, 3058,
3060, 3505, 3506, 3734, 2614, 703, 3509, 1308, 1987, 2105, 2106, 1388, 1309,
1575, 1997, 3410, 2620, 2910, 3511, 746, 801, 972, 1005, 1085, 1476, 1196, 705,
1088, 1772, 1480, 2914, 299, 750, 751, 1775, 2701, 2702, 2841, 3512, 3576].

Generators [3579, 2002, 2005, 2119, 2989, 3070, 3736, 2990, 2219, 2537, 2011,
2846, 842, 3296, 276, 323, 2639, 2306, 2131, 3586, 2542, 547, 2543, 1503, 1210,
1341, 1342, 1694, 2137, 2236, 2311, 2317, 2394, 2395, 2396, 2464, 2465, 2466,
2550, 2645, 2646, 2932, 2998, 3000, 3204, 3436, 3629, 3749, 3686, 1693, 3207,
2647, 2860, 2861, 3097, 3528, 3308, 2318, 1596, 2405, 3590, 353, 3692, 3693,
1152, 1154, 1804, 1806, 2721, 2653, 3102, 1603, 2657, 3593, 1430, 1514, 1516,
1709, 1265, 2150, 2563, 2729, 1812, 2570, 2664, 3540, 719, 849, 595, 639, 776,
777, 3539, 1817, 3662, 3325, 1355, 3012, 1934]. Generators

[1057, 1727, 3666, 414, 1435, 3335, 3336, 3337, 3338, 2052, 3118, 784, 2577, 3120,
1620, 3339, 2053, 3225, 1065, 2413, 2579, 2957, 2167, 556, 2421, 2423, 525, 2587,
2588, 2346, 2812, 1363, 1541, 1738, 1958, 1111, 3354, 559, 2749, 3027, 1626,
1627, 2173, 1835, 2752, 3699, 787, 1284, 2070, 2432, 2598, 422, 1631, 423, 484,
3603, 828, 1635, 2359, 1026, 1118, 1172, 1286, 1288, 1445, 3560, 2600, 1843, 2434,
3034, 3035, 3702, 1233, 1371, 1291, 3641, 488, 3561, 2079, 3488, 2081, 1640, 3037,
1642, 2265, 3381, 3564, 3676, 2268, 3489, 3567, 1028, 2970, 3490, 3610, 3263].

generators [3154, 1971, 3677, 3041, 1646, 1121, 2827, 1029, 2828, 1177, 1973, 1650, 2606,
2689, 2974, 2365, 883, 1459, 1653, 2829, 1179, 701, 3050, 3613, 1860, 3053, 3571,
3402, 1861, 2099, 2190, 535, 2191, 1865, 2100, 2192, 1000, 1866, 3168, 2279, 1304, 1465, 1466, 3170, 1385, 1462, 1463, 3405, 1567, 1663, 2692, 2833, 3059, 3171, 1306, 1386, 618, 2834, 3173, 3174, 1571, 401, 1387, 2695, 2199, 2200, 2446, 1469, 3177, 1389, 1390, 1472, 1671, 1311, 2836, 1880, 1881, 1996, 2112, 2209, 2286, 2287, 2376, 2521, 2522, 1678, 1132, 1770, 836, 928, 929, 1193, 1194, 1313.


generators [2136, 2138, 2232, 2233, 2312, 2314, 2315, 2397, 2398, 2546, 2548, 2642, 2715, 2779, 2855, 2997, 2999, 3305, 1504, 3716, 1097, 2854, 3093, 3205, 2237, 1695, 3094, 1151, 1263, 846, 2558, 3737, 3306, 3002, 3099, 1212, 2141, 2649, 1921, 2023, 3529, 3209, 3531, 439, 440, 476, 511, 1599, 1703, 1922, 1924, 2722, 2652, 3100, 2323, 2561, 2792, 2793, 3532, 3592, 1705, 1927, 2324, 2326, 2724, 2938, 3003, 1706, 1809, 772, 3104, 3005, 3313, 2727, 2798, 1708, 1606, 447, 3595, 3211, 3660, 1711, 594, 3099, 3215, 2151, 640, 1103, 1270, 1522, 2483, 2566, 2633, 1523, 1718].

generators [1719, 3113, 2800, 3320, 3321, 601, 2486, 2802, 2871, 2947, 3324, 1614, 1105, 1272, 1356, 1433, 1721, 1722, 2045, 1357, 2048, 3329, 2948, 1106, 2051, 820, 2337, 1062, 1529, 855, 1063, 2249, 2055, 1535, 1825, 1361, 1438, 1732, 2810, 3601, 2580, 2669, 1733, 2415, 3344, 3723, 260, 2168, 1949, 1734, 3463, 2743, 2424, 3639, 1278, 3465, 2585, 2586, 2425, 3320, 2256, 2591, 2747, 2883, 2962, 2963, 3022, 3349, 3469, 3470, 1623, 1833, 1957, 3023, 3602, 3640, 3355, 2885, 2592, 2428, 2593, 1625, 962, 2750, 2678, 2751, 3359, 1068, 2066, 1069, 3727, 2174, 1836, 3475, 1743, 2597, 2071, 2176].

generators [1962, 454, 3361, 2260, 2967, 3363, 3700, 2683, 3253, 3254, 3673, 3370, 3371, 2273, 3092, 3206, 394, 504]. generators-part [2585]. Generazione [964].

Genetic [2537, 2630, 2631, 628, 672, 2928, 3894, 2812, 2888, 2092, 2830, 2652, 3538, 3906].

Gentle [2956, 2438, 2795]. Genuine [3550, 2817]. Geographic [2273].


inverted [2040], invertible [3479, 3557], Inverting [319, 2931].
Investigating [409], investigations [1627, 1632, 2097, 1708].
Investing [3657], invitation [3764], Invited [2450, 1596].
Involving [195, 337, 338], Irrational [2440, 449, 2062, 1493].
ISAAC [2433], ISBN [3587, 3556], Ising
[2268, 2099, 1489, 1585, 2250, 2424]. Island [3788, 3786, 3927].
isotropic [530], Isotopic [530]. ISSAC [3852], ISSAC'93 [3835], Issue [3581, 2278].
Issues [3059, 1984], J [870, 1240, 2902, 1041, 1497, 1010, 1054, 910].
J. [168], J3Gen [3594], jaguar [3863]. James [2438, 2795, 2956].
Jansson [504, 394], January [3792, 3874, 2006]. Japan [3821], Japanese [1932, 165].
Java [2758, 2369, 3516, 2787, 3663, 3013]. Java-implemented [3013].
JavaTalk [2308], Jersey [3950]. Jitter [3375, 3376]. JMASM1 [2618], jobs [1795].
jobstreams [958], John [1484, 1496, 1772, 2872, 3761]. Join [1373, 1795].
Joint [324, 3894], Jonathan [3751], Jordan [721], Jordanscher [721].
Jose [3937], Joseph [259], Joy [3031], Jr [168], Julius [2610], July
[3835, 3859, 3775, 3753, 3852, 3873, 3927, 3769, 3894, 3841].
Jump [2989, 3070, 3071], June [3848, 3899, 3914, 3928, 3937, 3951, 3764, 3906, 3868, 3945, 3823, 3779, 3753, 3934, 3762, 3853, 3880, 3927, 3892, 3841, 3854, 3881].
Jungles [2335], Juniper [3733], Justification [2195, 987].
Kakutani [3216], kappa [3604]. KASUMI [2541], Keccak [3496]. KENO
[2050], KENO-Va [2050], kernel [2943]. Kernels [2944, 1954].
Key [3374, 3265, 2722, 3051, 3283, 890, 2455, 2850, 2935, 1604, 2031, 1516, 2489, 1942, 1631, 3043, 3393, 2392, 3314, 1931, 3115].
Key-Stream [3374]. Keys
[3703, 3514, 1604, 3695, 3733, 2880]. keystream [3187, 3458], keystreams
[1769]. Khintchine [2638], Kie [3794, 3835], Kinderman [2813]. kinetic
[3653]. Kingston [3884]. KISS [3311, 3455], Klomov [2826], Kloosterman
[1766], Kloosterman-type [1766]. KMCLib [3653], Known
[1810, 3279, 2286, 783], Knoxville [3796]. Knuth [1700, 679, 716, 3668].
Kochen [3485], Koen [2977], Koksma [2007], Kolmogorov
[63, 399, 71, 1135, 769, 2720, 97, 818, 188, 3461]. Kong [3897], Kongruenz
[1026], Kongruenz-Generatoren [1026], konvexe [32], konvexer [721].
Korea [3907], Körper [32], Kreyszig [1909]. krigen [3500], kriwoi [34].
Kronecker [3499], KY [3919].

L [531, 580, 622], Laboratory [3752, 3754], Lag [595]. Lagged
[2076, 2178, 1921, 2026, 2027, 2028, 1934, 3641, 2206, 1132, 1926, 2793, 1925].
Lagged-Fibonacci \[1921, 2026, 2027, 2028, 3641, 1926, 2793, 1925\].

Lagrange \[1665\]. Lai \[3310\]. Lake \[3847, 3854\]. Lamar \[2928\]. lamp \[2725\].

Landau \[691, 1109\]. language \[3716\]. languages \[3700\]. Laning \[168\].

Lansing \[3768\]. Laplace \[2526, 669, 3008, 3223\]. laptops \[2273\]. Large \[3752, 3269, 3505, 3506, 841, 669, 26, 2860, 2149, 185, 3220, 1531, 2971, 2833, 3059, 3171, 1323, 64, 73, 244, 95, 3737, 1055, 606, 230\]. Large-Order \[3505, 3506\]. Large-Scale \[3752, 185, 2149, 2971, 95, 3737\]. large-size \[73\].

largely \[963\]. Laser \[3222, 3292, 3307, 3468, 3249\]. Lasers \[3108, 3135, 3240\].

Last \[2170\]. Latin \[2332\]. LatMRG \[2135\]. Lattice \[532, 568, 1976, 2901, 2441, 702, 2617, 2837, 2301, 1470, 1767, 1310, 1311, 1133, 2530, 3423, 3424, 2921, 1139, 1140, 2452, 3196, 2228, 674, 710, 2231, 2339, 2397, 2467, 2545, 3304, 2468, 2552, 1918, 850, 2943, 2945, 1062, 3018, 3125, 3462, 2252, 1833, 3742, 392, 455, 3687\].
lattice-based \[3742\]. lattice-bases \[1139\]. lattice-sublattice \[3196\]. lattices \[2100, 2780, 2808\].

Lausanne \[3925\]. lava \[2725\]. LavaRnd \[2572\].

Law \[3401, 3220, 1531, 2175, 3062, 2696, 3183, 15, 197, 2117, 244, 16, 3105, 783, 2339, 3387, 3266, 3076, 2940, 885\].

Laws \[841, 1501, 2736, 562\].

Laxenburg \[3829\]. LC \[2875\]. LCG \[2617\]. LCGs \[2211, 2522, 2234\].

Leading \[2925, 618, 1038\]. leads \[1855\]. leads-to \[1855\]. Leakage \[2430\].

Leap \[3251, 2287\]. leap-frog \[2287\]. learnability \[2177\]. Learning \[3127, 1949\]. Least \[736, 533, 104, 1408\].

Least-Remainder \[104\]. leave \[3733\]. Lecons \[4\]. Lecture \[3587\]. Lectures \[262, 4\]. L’Ecuyer \[1439\]. Lee \[487\].

Left \[3453, 1947, 460\]. Left-Shift \[1947\]. legacy \[3710\]. Legal \[2691\].

Legge \[16\]. legli \[15\]. Lehmer \[1662, 2199, 2200, 748, 3586, 894, 246, 2157, 481, 2059, 231\].


lengths \[2821, 1977\]. Less \[736, 874, 2936\]. Lesson \[1724\]. lessons \[3733\]. Letter \[466, 1204, 1803, 2954, 484\]. letters \[2872\]. leurs \[3\]. Level \[3568, 2480, 1126, 2995, 1790, 3011, 2740\]. Lewis \[743\]. Lexington \[3919\].

Leydold \[2092\]. LFSR \[2275, 3732, 3166, 2398, 3314, 3721, 3251\].

LFSR-Based \[3721\]. Libgcrypt \[3081\]. Liblice \[3762\]. libraries \[2123\].

Library \[3386, 3708, 1035, 1307, 1199, 2550, 2646, 2932, 3000, 2647, 2144, 1441, 1557, 1638, 3384, 3566, 3567, 3609, 2824, 3282, 3181, 3575, 3682, 2844, 2999, 2475, 2476\]. Lie \[1936\]. Life \[2361, 3547\]. light \[3468\]. Lightweight \[3692, 3363\]. Like \[2691, 469, 2031, 3634, 3356\]. Likelihood \[2290, 1003, 1131\].

Limit \[698, 1239, 2444, 1473, 2526, 3587, 3446, 2940, 2158, 2809, 2344, 3476, 562, 63, 2987, 3297, 1701, 3445, 3566, 410, 2728, 1162, 188, 2096\]. limiting \[1708\]. Limits \[618, 85, 38, 2258, 2352\]. Lin \[2779\]. Lindberg \[1376\]. Line \[2101, 2688, 439, 440, 3225\]. linéaire \[1339\]. linéaires \[2486, 2801\]. Linear \[393, 2894, 1377, 2517, 2831, 1980, 924, 3508, 2287, 2288, 1082, 1083, 1084,

Linear-Algebra \[1816\]. linear-complexity \[1519\]. linear-size \[3610\]. Linearly \[978\]. linearization \[3674\]. Lineare \[1026\]. linearer \[978\]. linearization \[3674\]. Linearization \[1026\]. linearer \[978\]. linearization \[3674\]. Linearly \[3151, 3261, 3130, 1955\]. Link \[3212\]. linkage \[3774\]. links \[2008\]. Linux \[2917, 3123\]. LISA \[3855\]. List \[654, 1933, 1728\]. list-update \[1933\]. Lists \[922, 877\]. Littlewood \[1911\]. LLL \[2921\]. LLL-spectral \[2921\]. LLRANDOM \[631\]. Lmcgrid \[3148\]. Load \[2210\]. loaded \[2460\]. Loads \[3052\]. Local \[3562, 3269, 715, 590, 1346, 1513, 1602, 1817, 3488, 1328, 3002, 1162\]. Locality \[3562, 3488\]. localization \[1649, 3280\]. Log \[740, 2449, 2344, 1078, 1897, 2453\]. log-concave \[1078, 1897, 2453\]. Log-Normal \[740\]. Logarithm \[2839, 2662, 2175, 3383, 244, 2809\]. Logarithmic \[867, 3603, 990\]. logarithmically \[980\]. logarithms \[1368, 1259\]. logic \[1855, 3290\]. logiciel \[1339\]. Logistic \[3276, 3008, 2046, 3160\]. logspace \[1372, 1642\]. logspace-hard \[1372\]. lois \[783\]. London \[3587\]. Long \[3562, 880, 1864, 1466, 1758, 2374, 3191, 438, 2472, 1810, 1356, 1958, 1285, 3488, 2974, 1304, 2613, 2692, 1390, 1475, 753, 2304, 2643, 1924, 2033, 2947, 687, 2682\]. long-cycle \[2613, 2692\]. Long-Period \[880, 3191, 1958, 2974, 1475, 753, 2947, 687, 2682\]. Long-Range \[2374, 1466, 1758, 1304, 1390\]. Longest \[2472\]. Longest-period \[2472\]. Look \[3165, 3511, 774, 824\]. Look-Up \[3165, 774, 824\]. Lookup \[812\]. Loop \[838\]. loops \[3124\]. Lorentzian \[666\]. Loss \[3681\]. lot \[3258\]. Lottery \[3683\]. Louis \[3818\]. Louisiana \[3815\]. Lovasz \[1998\]. Low \[3562, 1851, 1868, 2905, 2622, 3308, 1217, 1348, 1714, 2153, 2330, 2159, 1542, 1739, 1832, 3148, 3488, 2828, 1379, 879, 1648, 1753, 3168, 2920, 3073, 3302, 985, 1418, 2468, 2717, 2786, 3099, 3594, 3448, 1713, 2246, 3546, 2061, 2075\]. low-cost \[3594, 3448\]. Low-Degree \[3308\]. low-dimensional \[1753, 2075\]. Low-Dimensionality \[2905\]. Low-Discrepancy \[2622, 2153, 2330, 1542, 1851, 1217, 1348, 1714, 879, 1648, 2920, 2468, 2717, 1713, 3546, 2061\]. low-dispersion \[1348\]. Low-Order \[1868, 1379\]. low-power \[3168\]. Lower \[1673, 2281, 1411, 1520, 2674, 1878, 3015\]. Lowness \[3683\]. LP \[2362, 1948\]. LPRng \[2479, 2049\]. LR \[1506\]. LSI \[1130\]. LT \[3277\]. Luby
M [997, 1913, 69, 3102, 997, 1913, 3243]. M. [315, 389]. M/M/1 [1913].
M/M/m [997]. M/PH/1 [3243]. MA [3928, 3890]. Mach [3054]. Machine
[149, 2691, 140, 894, 3685, 816, 164, 3707, 753, 470, 2149, 3334, 190].
Machine-independent [894, 753]. Machinery [3752]. Machines
Made [1477, 1793]. Madland [3667]. Magma [3397].
Mainly [307, 442]. main [3318].
[2367, 3888, 3846, 3148]. Managing [3665]. Manhattan [3586]. MANIAC
[1173]. Manipulating [540]. Manipulation [3649]. mantissa [650, 990].
[2153, 2643, 1164, 652]. Map [3276, 3481, 3690, 2046, 3229]. Maple [1909].
Mapping [3339, 1007, 3429]. Mappings [3147, 2708]. Maps
[2557, 3259, 2897, 3160, 846, 3319]. March
[3754, 3810, 3929, 3790, 3782, 3940, 3756, 3840, 3913]. Marginal [2189, 1799].
Margins [2515]. margins [2253]. Marinucci [3587]. Mark [3797].
Markov [210, 1072, 1175, 2193, 3284, 932, 502, 645, 692, 1746]. marks [2269].
Marotto [3422]. Marriott [3803, 3776, 3891, 3785, 3832]. MARS [2458].
Marsaglia [3258, 2265, 2761, 1310, 1311, 1326, 2024, 2045, 1059, 3699, 3727].
Marshall [2843]. Martuljek [3861]. Maryland [3814, 3904]. mashinakh
[346]. masked [3578]. mass [721, 1552]. Massachusetts [3770]. Massen
Mathematica [3535, 3595, 2054]. Mathematical
[3708, 3760, 3826, 3755, 3775, 3779, 1205, 1206, 95, 3587, 3757, 247, 1053, 3662, 2335, 3759, 54, 56, 3766, 3865, 3556, 915, 456, 485, 234, 700, 1192, 2409, 207].
Mathematical-Function [3708]. Mathematicians [2574]. Mathematics
[2361, 3760, 2760, 3755, 3775, 890, 3952, 1909, 3922, 3767, 137, 3751, 1703, 3774]. mathématiques [3757]. MathLink [2089]. MATLAB [3078, 3106, 2818].
Matrices [2275, 1153, 3024, 1234, 1586, 1101]. Matrix
Maximal [181, 1575, 1414, 810, 903, 2677, 1671, 2703, 3541, 3235].
Maximal-Length [903, 1414]. Maximally [3736, 2136, 2398]. Maximum
[1245, 1003, 1131, 2215, 2775, 1720, 1858, 2994, 83, 1955, 3030].
[3788, 3793, 3798, 3804, 3809, 3814, 3825, 3834, 3843, 3848, 3856, 3857, 3875, 3882, 3895, 3904, 3918, 3944, 3758, 3846]. mbedTLS [3728]. MC [2230].
[3745]. microprocessors [813]. Microscopy [1725]. Microsoft
[3883, 2403, 2655, 2656, 2687, 3103, 3104, 1630]. mid [93]. mid-square [93].
[62, 146, 387, 2576, 166, 1198]. Milwaukee [3851]. MIMD [1433]. MIMO
[3473]. min [1426, 2581, 2877]. min-entropies [2581, 2877]. min-max
minicomputer-based [1112]. Minimal
[2893, 1400, 1388, 2576, 166, 1198]. minimization [3221, 1741].
Minimum [1853, 2624]. Mining [3514]. Minkowski [1117, 1139, 1140].
Minkowski-reduced [1117, 1139]. Minneapolis [3851]. Minnesota
[3846, 3878]. Miscellaneous [701, 800, 639, 696]. Miscellaneous [3750]. Mises
[2067]. Misson [3929]. Missouri [3818]. MISTY [2634, 2541].
MISTY-Type [2541]. misunderstandings [1253]. Mitchell [1631]. mittels
[978, 1841]. Mixed [290, 323, 817, 945]. Mixing [1264, 553, 1679, 1203, 3464].
MIXMAX [3670]. Mixture [1454, 1095, 2077, 1016, 3127].
mixture-of-subsets [3127]. Mixture-plus-Acceptance-Rejection [1095].
[3084, 2574, 3085]. Model [2823, 3624, 184, 53, 2959, 1442, 3148, 792, 2268,
3677, 3388, 1121, 2608, 3646, 2098, 2099, 1489, 2995, 1700, 3592, 3318, 1941,
2250, 2251, 3127, 2424, 1552, 3146, 1554]. Model-Based [3624]. Modeling
[1561, 2189, 3896, 3686, 3012, 1725, 3605, 1011, 1593, 2463, 2929, 226, 1544].
Modelirovanie [346]. modélisation [1544]. modelled [3043]. Modelling
[2741, 3865, 1129, 1188]. Models [495, 1693, 1813, 2077, 3577, 932, 3076,
1789, 2717, 3776, 958, 2253, 2068, 3701, 1964]. Modern
[3374, 3764, 3705, 1128, 2384, 3917, 3609, 3769]. modification [1699, 1563].
Modified [994, 3276, 2110, 414, 2675, 995, 316, 2228, 3694, 191].
Modified-Logistic [3276]. Modular
[2701, 2919, 1157, 2493, 1396, 2132, 3098, 2797]. Modulated [2875].
modulator [3054]. Module [2922, 3157]. Modules [2571, 3750]. moduli
[2365, 2100, 1661, 1306, 1323, 2323, 2792, 3215]. Modulo
[2066, 247, 364, 368, 229, 2079, 928, 1253, 1316, 301, 711, 2642, 2855, 2486,
2947, 1722, 1440, 5, 2940]. Modulus [3506, 801, 972, 1005, 1085, 1476, 2053,
556, 2882, 2600, 1470, 1576, 1580, 1673, 1674, 1762, 1875, 1876, 2109, 2110,
2280, 2281, 1312, 836, 929, 1193, 1194, 1313, 2128, 2228, 764, 3306, 2482, 2870,
1737, 2746, 3350, 3351, 3138, 3139, 3360, 2260]. Molecular [2508, 3714, 1893].
molecular-dynamics [1893]. Moment [1853, 1034, 1569, 2242, 720].
Moment-Generating [1853]. Moments [754, 3420, 3429, 2127, 1220].
Monaco [3892]. Monica [3755]. monitoring [3225]. Monkey [1804, 2045].
Monkeying [2865]. Monographs [3556]. Monotone
[1077, 329, 2864, 2122, 2992, 3522]. Monotonicity [1086]. Monster [2472].
Monite [3764, 176, 2438, 111, 3931, 3897, 1585, 3920, 630, 3926, 3303, 2795,
3853, 3873, 3880, 3901, 3911, 2245, 2050, 98, 187, 2956, 3892, 1828, 1742, 1173,
Number-theoretic numbers.

Oscillator-Based

Oscillators

Other

Otherwise

Ottawa

Output

Overview

Oxford

P

P-RnaPredict

P. PA

Package

Packings

Pad

Pages

Pair

Pair-wise

Pairs

Pairwise

Palace

Palasti

Palo

Paper

Papers

Papoulis

Paragon

Parallel

Parameter

Parametric

Paris

Park

Patching

Passage

Passau

Passive

Password

Patchwork

Partitioning

Partitions

parts

PASCAL

Pass [2651]

Passau [3933]

Passive [3039, 3594]

Password [1819, 1422]

past [3303]

Patchwork

Patchwork-Verwerfung

path
prime-power [2482]. Primes [2102, 916]. Primitive
[2078, 3952]. Principle [3645, 3414]. Principles
[3834, 178, 797, 1302, 2611, 2979, 835, 2311, 3927, 3867, 2573, 1484, 1496, 1497].
Primes [2102, 916]. Primitive
[2078, 3952]. Principle [3645, 3414]. Principles
[3834, 178, 797, 1302, 2611, 2979, 835, 2311, 3927, 3867, 2573, 1484, 1496, 1497].
[1604, 2087]. Prize [2778]. PRNG [3681, 2772, 3594, 2660]. PRNGlib [2144].
Probabilistic [1773, 900, 3231, 1551, 1858, 1299, 2384, 1685, 1700, 2864, 446, 555, 2594, 3779, 384, 2564].
Probabilities [927, 1083, 1531, 3707, 3, 2994, 138].
Probability [3730, 1845, 291, 3764, 3706, 2096, 167, 1983, 3065, 81, 300, 1213, 638, 549, 2565, 355, 1104, 1612, 2665, 2573, 2044, 1160, 2158, 516, 259, 205, 3831, 885, 3765, 149, 1303, 1079, 3932, 15, 2117, 376, 1412, 253, 1518, 648, 555, 2594, 3779, 384, 2564].
Probable [1, 946, 2, 2097, 1757, 1412]. probabilistic [553]. Probably [1294].
Problem [2093, 3271, 51, 2839, 299, 1424, 383, 3662, 1735, 1562, 2759, 925, 3194, 935, 186].
180, 3306, 3309, 1597, 3208, 3100, 3592, 3631, 2325, 281, 3448, 2727, 2798, 447, 775, 3660, 2941, 1711, 3315, 2241, 680, 779, 780, 781, 1158, 3319, 1526, 413, 2246, 481, 255, 1055, 328, 3115, 3116, 647, 782, 648, 3722, 3331, 3547.

pseudo [947, 2952, 856, 690, 607, 3457, 3458, 2581, 2251, 1167, 341, 557, 3229, 2170, 2345, 2499, 2672, 163, 2348, 191, 1544, 3355, 3134, 2428, 3672, 3357, 1069, 3141, 2887, 2966, 1443, 3479, 3557, 3145, 3365, 2819, 3482, 3253, 3701, 3370, 3371, 430, 463, 624, 357, 613].

test-aleatoire [1121].


Pseudo-random [2859, 2558, 1800, 3306, 3309, 3208, 3100, 3592, 3631, 2325, 281, 447, 775, 3660, 2941, 1711, 3315, 2241, 680, 779, 780, 781, 1158, 413, 2246, 481, 255, 1055, 328, 3115, 3116, 647, 782, 648, 3722, 3547, 2952, 856, 3457, 3458, 2581, 1167, 341, 557, 3229, 2170, 2345, 2499, 2672, 163, 191, 3134, 2428, 1069, 3141, 2887, 2966, 1443, 3479, 3557, 3145, 3365, 3482, 3370, 3371, 613, 357].


Pseudorandom

pseudorandom

pseudorandom

pseudorandom-number

pseudorandomness

pseudosuchainykh [346].  PSI [1394].  PUB [1819].  Public


random

random-access [3075].
Random-Bit [1381, 535].
Random-dierence [19].
Random-Number

Random-Start [3216].
Random-Variate [2879].
random-walk [2251].
randomised [1846].
Randomized [1998, 2622, 3421, 1333, 1792, 2716, 1711, 2150, 2247, 2644, 3303, 684].
randomizer [1473].
Randomly [843, 2041, 649, 2161, 1442, 21, 1794, 3304].
randomly-shifted [3304].
Randomness

RANEXP [1890].
RANF [1093].
Range [2374, 8, 399, 1304, 1466, 1758, 1390, 2291, 1356].
RANGEN [2618].
ranges [2417].
Rank [998, 1325, 2924, 3687, 2943, 2945, 3017].
rank- [2943, 2945].
Rank-1 [2924, 3687].
Rank-based [1325].
Ranking [2090, 3743, 2117, 3538].
Sequences

\[ \{3372, 2893, 2080, 3151, 3261, 829, 264, 1456, 999, 1071, 179, 1378, 1851, 880, 2096, 181, 370, 459, 570, 3278, 537, 2445, 1573, 1081, 2524, 2908, 1088, 838, 2912, 2628, 141, 404, 499, 242, 324, 3651, 3077, 223, 3091, 438, 3693, 509, 510, 848, 589, 2477, 2478, 794, 1513, 1602, 1264, 810, 2329, 49, 2427, 3477, 13, 1227, 3253, 2261 \}\]

sequences \[ \{1754, 2366, 3049, 1245, 1566, 1756, 1865, 1658, 215, 181, 370, 459, 570, 3278, 537, 2445, 1573, 1081, 2524, 2908, 1088, 838, 2912, 2628, 141, 404, 499, 242, 324, 3651, 3077, 223, 3091, 438, 3693, 509, 510, 848, 589, 2477, 2478, 794, 1513, 1602, 1264, 810, 2329, 49, 2427, 3477, 13, 1227, 3253, 2261 \}\]

Sequential \[ \{2061, 1955, 2063, 2169, 2171, 2257, 3235, 1544, 3137, 483, 2501, 561, 1550, 1443, 269, 3743, 1885, 547, 763, 1096, 119, 490, 1554 \}\]

Serial \[ \{214, 51, 241, 2645, 852, 538, 1774, 116, 172, 405, 433, 1325, 2130, 1158, 1352, 1431, 50 \}\]

Series \[ \{1864, 168, 1693, 3587, 766, 247, 1934, 311, 229, 22, 1105, 19, 1554 \}\]

Serpent \[ \{2458, 2539 \}\]

Server \[ \{2608, 2698, 1935 \}\]

Serpent-\[ \{2605, 930, 2383, 2151, 2814, 1450, 707, 21, 156, 158, 1721, 648, 35 \}\]

SETA \[ \{3919, 3907 \}\]

Sets \[ \{2507, 2622, 3086, 3091, 2310, 360, 1542, 2679, 2081, 344, 1753, 41, 2376, 139, 273, 1780, 2296, 3869, 2121, 2545, 2468, 2552, 721, 1217, 1269, 1713, 1714, 2801, 2946, 602, 947, 2075, 3086 \}\]

Setting \[ \{3241, 3434 \}\]

seventeenth \[ \{3788 \}\]

Seventh \[ \{1909, 3874, 3848 \}\]

Several \[ \{1860, 1787, 2305, 3528, 1467, 640, 990 \}\]

SFQ \[ \{3252 \}\]

SHA \[ \{3661 \}\]

SHA-3 \[ \{3661 \}\]

Shadowing \[ \{1679 \}\]

Shamir \[ \{2826 \}\]

Shape \[ \{800, 695, 832, 696 \}\]

Shapes \[ \{3576, 2803, 3419 \}\]

Shapiro \[ \{3739 \}\]

Shared \[ \{2430, 1754 \}\]

Sharing \[ \{2031, 1942, 2995, 3243 \}\]

Shell \[ \{2737 \}\]

Shenzhen \[ \{3940 \}\]

Sheraton \[ \{3787 \}\]

Sherif \[ \{2057 \}\]

Sherman \[ \{126 \}\]

Shewhart \[ \{1171 \}\]

Shift \[ \{2517, 1183, 1300, 1081, 1006, 1037, 2912, 404, 1008, 1492, 2466, 507, 633, 635, 848, 478, 3450, 1530, 2340, 1947, 3552, 1541, 3354, 2677, 2359, 2362, 1242, 3054, 1475, 706, 1683, 2223, 981, 2017, 329, 3442, 305, 1598, 1702, 2023, 1270, 1351, 1521, 1271, 2943, 3633, 1107, 1729, 2055, 3360, 3742, 3674 \}\]

Shift-invariant \[ \{2943 \}\]

Shift-Nets \[ \{2340 \}\]

Shift-Register \[ \{1081, 2912, 635, 478, 1541, 1242, 1475, 2223, 981 \}\]

Shift-Register-Sequence \[ \{2359 \}\]

shift-remainder \[ \{1271 \}\]

Shifted \[ \{3227, 3304, 3462 \}\]

Shifts \[ \{2739, 2974, 159 \}\]

shooting \[ \{1652 \}\]

Short
Small-bias [3189]. smaller [2128]. Smart [3692, 3102, 2690, 3933].
Small-World [3189]. small-deviation [3198].
Software/hardware [3527]. SOI [3588]. Sojourn [1955, 2063, 2171, 2169].
Source [1072, 3679, 3195, 3688, 635, 2163, 3750, 1175, 2690, 217, 3426, 3582, 2880]. Sources [1231, 2806, 29, 3286, 3697, 1221, 1283, 1299, 1508, 1802, 3718, 2730, 2254, 3359].
Specker [3485]. Spectral [1659, 750, 751, 1141, 842, 1042, 443, 3215, 2807, 2954, 3250, 2375, 670, 2921, 2300, 2227, 2233, 2674, 2747, 3232, 1280].
Spectrum [2845, 3308, 3667]. Speed [2360, 3191, 3686, 636, 3325, 3222, 100, 3478, 3250, 3644, 2690, 3063, 3177, 2767, 3291, 1686, 117, 2132, 128, 2469, 774, 225, 552, 1164, 2876, 121].
Symposium [374, 3226]. synchronized [1636, 3259, 1940]. Syndrome [2104].
Symmetry [133]. Systematic [2226, 3110, 2800, 910, 911, 2810, 2250].

Systolic [2092, 1236].

T-Concave [2012].
Tabla [133]. Table [1966, 3165, 812, 824, 78, 3671, 1289, 674, 508, 774, 44].
Table-free [1289].
Table-Hadamard [3671]. Table-Lookup [812]. Tables [313, 6, 435, 20, 31, 2397, 2398, 17, 308, 2035, 2484, 134, 189, 68, 49, 69, 23, 46, 72, 113, 114, 169, 170, 1324, 302, 2309, 7, 869, 133].
Tabular [3164].
Tag [3317, 3162, 3448]. Tags [3039, 3328, 3342]. Tail [927, 1083, 669, 1301, 2994, 3445].
tailed [3391, 1554]. Tails [2757, 857, 954, 2984]. Taken [8]. Talk [2450]. tandem [3158].
tangent [1908]. Tap [2359]. taps [2415]. Target [1652]. Targeting [3132, 3677].
Tatzmannsdorf [3779]. Tausworthe [1027, 1756, 1662, 743, 1473, 466, 1038, 1392, 2136, 777, 1015, 515, 1619, 1023, 559, 651]. Tb [3589]. TDIST [2818].
TEA [2830, 2535, 2630, 2631, 2708, 2773, 2659, 2243, 2073]. Teach [2691].
Teaching [3176, 3078]. Technical [2085, 2011, 1806, 2722, 2052, 3865, 3881, 3653, 236, 319, 403, 400].

Twin-floating [3486]. Twist [2588]. Twisted [1705, 1927].

twister [2325, 2691, 2787, 2938, 3327, 3121, 3341, 3599].

twisters [3503].

twisting [1705, 1927].


Two-Sided [3461]. Two-Source [3679, 3688].

Two-Stage [3825].

two-term [3825].

two-sh [2458].

type [176, 199, 2541, 769, 2873, 864, 2173, 3149, 399, 1766, 1135, 351, 684, 3134, 3479, 3557].

types [3528, 562].


Unavoidable [1036]. Unbiased [1072, 1299, 1175, 572]. Unbounded [2909, 2766, 2992]. uncertain [3186]. uncertainty [3896, 1192, 3213].

Unconditional [3099]. Unconstrained [2042]. Uncorrelated [1454, 294].

Uncovering [2409]. Underlying [843]. Understanding [2925, 3665].

unequal [138]. unicorn [3717].


uniform [1226, 2964, 3025, 3602, 913, 5, 1838, 2681, 3281, 2991, 2930, 420, 1277].

uniform-Gaussian [2224]. uniformément [176]. Uniformity [2090, 970, 841, 2645, 484, 2911, 2559, 2147, 1103, 1829].

Uniformly [267, 194, 199, 1690, 1693, 549, 203, 1110, 785, 176, 1467, 2377, 1201, 469, 301, 1258, 2864, 1168, 693, 1443]. uniformly-distributed [176]. Uniforms [1896, 2126, 1629, 1364, 1895, 2127, 2470, 1540].

Unifying [3591]. Unimodal [1077, 2197, 1100]. Unique [3287, 1338, 3143]. unit [424].

units [3264, 3569, 3090, 95, 3537, 3405]. Univariate [1047, 503, 1902, 2555].

Variables

Variance

Variations

Various

Varying

Varyable

Variation

Variational

Variations

Vector

Vectorial

Vectorized

Vectors

Vegas

Verifiable

Verification

Verified

Vermont

Versatile

Verschlusselungsabbildungen

Version

Versions

VAX

VAX-11

Vector

Vector [3494, 1179, 1357]

Vectorized [3741, 1179, 1475, 1357]

Vectors [532, 2189, 2515, 702, 2284, 506, 284, 1020, 3345, 1286, 2362, 568, 2091, 3614, 1756, 2285, 1133, 1201, 1255, 1322, 2231, 1522, 2481, 2808, 608, 1948, 2674]

Vegas [3848, 3889, 3935, 3853]

Verifiable [3678, 3056]

Verification [2770]

Verified [2363, 3728]

Vermont [3860]

Versatile [509]

Verschlusselungsabbildungen [1007]

Version [3561, 998, 1092, 2606, 3000, 3635]
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.


[3] Émile Borel. Les probabilités dénombrables et leurs applications arithmétiques. (French) [Countable probabilities and their arithmetic ap-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kendall:1941:TR

Kolmogoroff:1941:CLU

Nair:1941:DSC

Young:1941:ROS

Dodd:1942:CTR

Dodd:1942:TTR

Mann:1942:CNC

Peatman:1942:TRN


REFERENCES


REFERENCES


[61] S. M. Ulam and John von Neumann. On combinations of stochastic and deterministic processes. Bulletin of the American Mathematical Society, 53(11):1120, November 1947. CODEN BAMOAD. ISSN 0002-9904 (print), 1936-881X (electronic). URL http://www.jstor.org/stable/2236265. The abstract notes “... starting with almost every $x_1$ (in the sense of Lebesgue measure) and iterating the function $f(x) = 4 \cdot (1 - x)$ one obtains a sequence of numbers on $(0, 1)$ with a computable algebraic distribution. By playing suitable games with numbers ‘drawn’ in this fashion, one can obtain various other distributions, either given explicitly or satisfying given differential or integral equations.”.


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


REFERENCES


REFERENCES


REFERENCES

Richtmyer:1951:EDI


vonNeumann:1951:VTU


Votaw:1951:HSS


Anderson:1952:ATC


Anonymous:1952:RD


Cameron:1952:RST


Goodman:1952:EPSa


REFERENCES


REFERENCES

on the development and practice of science and engineering in the 20th Century.” See [2436, 2437], and the Hasting–Metropolis generalization in [502]. See also [343, 645, 2710].


REFERENCES


[133] Jose Royo and Sebastian Ferrer. Tabla de numeros aleatorios obtenida de los numeros de la Loteria Nacional Española. (spanish) [Tables of random numbers obtained from numbers in the Spanish National Lottery].


[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 × 1)0 × 9*, volume 26 of *Tracts for computers*. Cambridge University Press, Cambridge, UK, 1955. 60 pp. LCCN QA47 .T7 no.26. Compiled from Herman Wold’s Table of random normal deviates (Tract no. XXV) by E. C. Fieller, T. Lewis, and E. S. Pearson: *Random normal deviates.*

REFERENCES


REFERENCES


REFERENCES


REFERENCES


vonHoerner:1957:HZR


Walsh:1957:EMO


Bass:1958:MMC


Bauer:1958:MCM


Bendat:1958:PAR


Bofinger:1958:PPP


Box:1958:NGR

REFERENCES


REFERENCES


REFERENCES

[195] Louis W. Ehrlich. Monte Carlo solutions of boundary value problems involving the difference analogue of $\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{1}{(K/y)} \frac{\partial u}{\partial y} = 0$. *Journal of the ACM*, 6(2):204–218, April 1959. CODEN JACOAH. ISSN 0004-5411 (print), 1557-735X (electronic).


REFERENCES

Bureau of Standards (1934), 64B(??):211–215, ???? 1960. CODEN ????
ISSN 0091-0635.

Butcher:1960:SR

????, ?????, 1960. LCCN ???? URL ????.

Clark:1960:EDR

distributed random numbers. Published for Operations Research Office,
Johns Hopkins University by Johns Hopkins Press, Baltimore, MD, USA,

Clark:1960:USR

Research, 8(2):185–195, March/April 1960. CODEN OPREAI. ISSN

Coveyou:1960:SCG

COAH. ISSN 0004-5411 (print), 1557-735X (electronic).

DeMatteis:1960:PRS

length. Report 88, Comitato AND Nazionale per l’Energia Nucleare,
Bologna, Italy, 1960.

Edmonds:1960:GPR

[216] A. R. Edmonds. The generation of pseudo-random numbers on
1460-2067 (electronic). URL http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/020181.sgm.abs.html; http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/tiff/181.tif; http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/tiff/182.tif; http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/tiff/183.tif; http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/tiff/184.tif; http://www3.oup.co.uk/computer_journ-
al/hdb/Volume_02/Issue_04/tiff/185.tif.


REFERENCES


[230] Donald D. Wall. A random number test for large samples. In Anonymous [3758], pages 7–11. LCCN ????

REFERENCES


REFERENCES


REFERENCES


REFERENCES


Hlawk:1962:ABM


Hull:1962:RNG


Marsaglia:1962:FPG


Marsaglia:1962:IPM


Marsaglia:1962:RVC


Marsaglia:1962:SPG


MendesFrance:1962:CMF

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


Kronmal:1964:EPN


Liu:1964:MFS


MacLaren:1964:FPG


Marsaglia:1964:CMG


Marsaglia:1964:FPG


Marsaglia:1964:MPR


Marsaglia:1964:RDA

REFERENCES


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


REFERENCES


[409] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3763], pages 64–68. LCCN QA76.5 D55 1965.


REFERENCES


[433] 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].


the hyperplane problem that linear congruential generators suffer from, although careful choice of multipliers can minimize its importance: see [398, 2200, 2199, 2446].


REFERENCES


REFERENCES

1436-5081 (electronic). URL http://www.springerlink.com/content/j48m46451580607q/.

Zarem:1968:MBM


Beasley:1969:DTS


Bell:1969:DFT


Chaitin:1969:LPC


Coveyou:1969:RNG

[460] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3764], pages 70–111. LCCN QA1 S565 v. 3.

Cunsolo:1969:CNP

[461] D. Cunsolo. Costruzione di numeri pseudorandom con periodo superiore alla base m. (Italian) [generation of pseudorandom numbers with period greater than the base m]. Calcolo: a quarterly on numerical analysis and theory of computation, 6(1):69–85, March 1969. CODEN
REFERENCES

CALOBK. ISSN 0008-0624 (print), 1126-5434 (electronic). URL http://www.springerlink.com/content/60u464k30851uj27/.

Deo:1969:APN


Dieter:1969:AME


Donnelly:1969:STU


Downham:1969:RT


Fellen:1969:LEI


Good:1969:HRR

REFERENCES


Formation of pseudo-random uniformly distributed numbers from noise-like signals. 

[470] W. J. Hemmerle. Generating pseudorandom numbers on a two’s complement machine such as the IBM 360. 


REFERENCES


REFERENCES


REFERENCES

Gustavson:1970:FRN


Haber:1970:NEM


Haber:1970:SNA


Halton:1970:RPS


Harris:1970:AFG


Hastings:1970:MCS


Johnson:1970:CUD

REFERENCES


REFERENCES


REFERENCES


Good:1971:SRS


Han:1971:DR


Jackson:1971:PCC


Kozlov:1971:DRN


Marsaglia:1971:RVI

REFERENCES


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


REFERENCES


REFERENCES


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


Kral:1972:NAP


Maddocks:1972:CAG


Majithia:1972:CFD


Marsaglia:1972:CPS


Marsaglia:1972:SLC


Mason:1972:LTN


Mihram:1972:SV


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


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


REFERENCES


REFERENCES


REFERENCES


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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

[714] 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.


[739] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3772], 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 [2439] for an update, and a repair to an incorrect conjecture in this paper. See also [2364], 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


Marsaglia:1976:IFM


Marsaglia:1976:RNG


McArdle:1976:ETM


Michael:1976:GRV


Miklich:1976:HSN


Mitchell:1976:EAD


Neuman:1976:APC


[783] Alain Rouault. Propriétés asymptotiques d’un n-échantillon d’une variable aléatoire dénombrable connues sous le nom de lois de Zipf. (French) [asymptotic properties of an n-sample of a denumerable random variable known under the name of Zipf’s law]. *Comptes Rendus Hebdomadaires

Rudolph:1976:RNG


Sobol:1976:UDS


vanDooren:1976:AAN


Wallace:1976:TRG


Wedderburn:1976:SAR


Williams:1976:PRS


Witsenhausen:1976:VBC

[790] H. S. Witsenhausen. Values and bounds for the common information of two discrete random variables. SIAM Journal on Applied Mathematics,

Zakharov:1976:ECS


Zucker:1976:TMT


Ahrens:1977:URN


Akchurin:1977:RNG


Amadori:1977:CDS


Beasley:1977:SAA


Bendat:1977:PAR

Bohrer:1977:SSR


Camp:1977:IPN


Cheng:1977:MGG


Fishman:1977:ETM


Gait:1977:NNP


Garling:1977:SBS


Gideon:1977:SAE

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES

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

Schmeiser:1978:SMG


Schruben:1978:PNAa


Schruben:1978:PNAb


Simon:1978:PNA


Singh:1978:CPP


Sowey:1978:SCB

REFERENCES


REFERENCES

Atkinson:1979:CGP

Atkinson:1979:FSA

Atkinson:1979:RDC

Atkinson:1979:SAA

Atkinson:1979:SGI

Bache:1979:APP

Bentley:1979:AGS
J. L. Bentley and J. B. Saxe. Algorithm: Generating sorted lists of randoms. Report CMU-CS-79-113, Department of Computer Science,
REFERENCES

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


REFERENCES


REFERENCES

Monahan:1979:ENM


Moore:1979:RNG


Nadas:1979:PP


Niki:1979:CMF


Niki:1979:MFN


Pangratz:1979:PRN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

???? 1980. CODEN OPREAI. ISSN 0030-364X (print), 1526-5463 (electronic).


REFERENCES


Diaconis:1981:GRP


Dudewicz:1981:EBT


Dudewicz:1981:HRN


Fishman:1981:SCM


Friedman:1981:NPP


Gentle:1981:PCR

REFERENCES


REFERENCES


Rubinstein:1981:RNG

Schatte:1981:RVL

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

Tadikamalla:1981:CGG

Tadikamalla:1981:FDO

Ahrens:1982:CGP

Ahrens:1982:GGV


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES


REFERENCES


REFERENCES


Hora:1983:EIF


Inoue:1983:RNG


Jennergren:1983:AMR


Kac:1983:WR


Kachitvichyanukul:1983:DUR


Keefer:1983:TPA


Lawrance:1983:SDP

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Fishman:1984:EAM]


[Fishman:1984:SDD]


[Frederickson:1984:PRT]


[Frieze:1984:LCG]


[Guinier:1984:RNS]


REFERENCES


REFERENCES


REFERENCES


Ahrens:1985:SRS


Akl:1985:FPR


Berry:1985:RPD


Blom:1985:SPE


Bounas:1985:DDS


Burks:1985:CEM

[1124] Arthur W. Burks, Alston S. Householder, N. Metropolis, and S. M. Ulam. Comments on early Monte Carlo computations and scien-
REFERENCES


Clark:1985:PNG


Dowdy:1985:AUM


Dudewicz:1985:RNG


Dudewicz:1985:TMD


Dyadkin:1985:AMN


Fairfield:1985:LRN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1201] H. Grothe. Matrixgeneratoren zur Erzeugung gleichverteilter Zufallsvektoren. (German) [Matrix generators for generating uniformly distributed


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


Chiu:1987:SRS


Chung:1987:RWA


Collings:1987:CRN


Compagner:1987:MLS


Dagpunar:1987:NMS


Doolen:1987:MCW


REFERENCES


REFERENCES


REFERENCES

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


REFERENCES


Binder:1988:MCS


Bratley:1988:AIS


Brickell:1988:CSR


Brillhart:1988:FHP


Chor:1988:UBS


Collings:1988:AIG

REFERENCES


REFERENCES

Durst:1988:TPR

Edwards:1988:CAM

Eichenauer:1988:MLTb

Eichenauer:1988:MLTc

Eichenauer:1988:NCP

Fishman:1988:MCR

Frieze:1988:RTI
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]


[Gifford:1988:NRN]


[Gleason:1988:IPS]


[Gleck:1988:QTR]


[Goldreich:1988:EPG]


[Greiner:1988:NIS]

REFERENCES

Grothe:1988:MEG


Guinier:1988:FPU


Haberman:1988:WUC


Hallin:1988:RBT


Harmon:1988:AIM


Heidelberger:1988:DES

REFERENCES

Hong:1988:LGA


Izumi:1988:FGW


Kachitvichyanukul:1988:AHS


Kachitvichyanukul:1988:BRV


Kannan:1988:PFN


Karloff:1988:RAP

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Impagliazzo:1989:ECS


Impagliazzo:1989:HRR


Impagliazzo:1989:PRG


Kachitvichyanukul:1989:ABS


Kahaner:1989:NMS


Kamps:1989:CPL

[1408] U. Kamps. Chebyshev polynomials and least squares estimation based on one-dependent random variables. Linear Algebra and its Applications,
Kao:1989:RNG


Kelton:1989:RIM


Kharitonov:1989:LBP


Kim:1989:PRP


Kleijnen:1989:PNG


Komo:1989:MLP

REFERENCES


REFERENCES

Association for Cryptologic Research, 1(3):159–176, ????. 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Mertsch:1989:Pas


Niederreiter:1989:Stc


Paul:1989:Irn


Percus:1989:Rng


Pickover:1989:Prg


Reber:1989:PNG

REFERENCES


REFERENCES


REFERENCES


REFERENCES

August 1990. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).


January 1990. CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic). URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/76379.html. See criticism and errata [1732], and further criticism in [1820]. The latter point out that Carta’s implementation does not correspond to their proposal.


[1467] Lih-Yuan Deng and E. Olusegun George. Generation of uniform variates from several nearly uniformly distributed variables. Communications
REFERENCES


Doring:1990:ENZ


Eddy:1990:RNG


Eichenauer-Herrmann:1990:LSN


Eichenauer-Herrmann:1990:PLC


Eichenauer-Herrmann:1990:UBB


REFERENCES


REFERENCES


[1493] Bruce R. Johnson and David J. Leeming. A study of the digits of \( \pi \), \( e \), and certain other irrational numbers. *Sankhyā (Indian Journal of*
REFERENCES


Korolev:1990:ADR


Koutras:1990:TCN


Krawczyk:1990:HPC


Lagarias:1990:PNG


LEcuyer:1990:RNS


LEcuyer:1990:UVW


REFERENCES


REFERENCES


REFERENCES


[1531] L. V. Rozovskii. Probabilities of large deviations of sums of independent random variables with common distribution function in the domain of

Rueppel:1990:SSP


Sarno:1990:GDR


Schmeiser:1990:NCI


Schnorr:1990:EPR


Sezgin:1990:FPU


Sezgin:1990:RNG

REFERENCES

Sherif:1990:DNC


Sobol:1990:QMC


Stadlober:1990:RUA


Tezuka:1990:LSP


Tezuka:1990:NFL


Tichy:1990:RPC


Tindo:1990:ACA

[1544] G. Tindo. *Automates cellulaires: applications à la modélisation de certains 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]. Dis-
sertation (thesis), Université de Nantes, Nantes, France, 1990.

Computer Science Institute, Berkeley, CA, August 1990.

[1546] A. van der Steen. Portable parallel generation of random numbers. Su-
percomputer, 7(1):18–20, January 1990. CODEN SPCOEL. ISSN 0168-
7875.

[1547] 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 — 1. Features of Monte Carlo algorithmic techniques
for solving problems in borehole nuclear geophysics. Nuclear Geophysics,
4(B12):425–435, 2376, ???? 1990. ISSN 0969-8086 (print), 1878-6383
(electronic).

and Engineering, 5(2):82–88, April 1990. CODEN CSSEEI. ISSN 0267-
6192.

[1549] 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).

[1550] C. C. Wang and D. Pei. A VLSI design for computing exponentia-
tions in GF(2^m) and its application to generate pseudorandom num-
ber sequences. IEEE Transactions on Computers, 39(2):258–262, Febru-
ary 1990. CODEN ITCOB4. ISSN 0018-9340 (print), 1557-9956 (elec-

methods for calculating convolutions and dependency bounds. Inter-
REFERENCES

Wolff:1990:AFM


Wong:1990:RNG


Yeh:1990:ODT


Zielinski:1990:APN


Akopov:1991:MGP


Anastasio:1991:OCL

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Papoulis:1991:PRV


Pardalos:1991:CTP


Patarin:1991:NRP


Peterson:1991:NRN


Pickover:1991:PRG


Revello:1991:CEC
REFERENCES

[1618] 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


Walsh:1991:MFR


Wheeler:1991:PMN


Wheeler:1991:SIC


Yamamoto:1991:NEM


Yang:1991:UCR


Zeng:1991:PBG


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1713] H. Niederreiter. Constructions of low-discrepancy point sets and sequences. In *Colloquia Mathematica Societatis János Bolyai, 60. Sets,


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Chen:1993:PGH


Couture:1993:DDV


Damgaard:1993:ACE


DeMatteis:1993:LRC


Devroye:1993:RVG


Dobkin:1993:CD

REFERENCES


REFERENCES


Eichenauer-Herrmann:1993:SIN


Erdmann:1993:CMT


Fisher:1993:OOR


Flahive:1993:ICG


Galway:1993:ESCb


Ganzha:1993:PSM

REFERENCES


REFERENCES


Lin:1993:NCP


Loparo:1993:LER


Makino:1993:SPR


Marsaglia:1993:LHR


Marsaglia:1993:MTR


Marsaglia:1993:RNG


Marsaglia:1993:TCR

REFERENCES


REFERENCES


REFERENCES


[1820] 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 [1355, 1460, 1806, 1830]. The authors report that they would now recommend the MCG \( x_{n+1} = 48 \cdot 271x_n \mod (2^{31} - 1) \) over their original \( x_{n+1} = 16 \cdot 807x_n \mod (2^{31} - 1) \).


REFERENCES


Tezuka:1993:LSA


Toral:1993:GGD


Vattulainen:1993:IIP


Wang:1993:URP


Weber:1993:AIG


Willemain:1993:MGA

REFERENCES


REFERENCES


REFERENCES


REFERENCES


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

Couture:1994:LSC


Cuccaro:1994:TTQ


Davis:1994:CRA


DeArmon:1994:RLO


Deng:1994:DIR


Devroye:1994:NHS

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

REFERENCES

Gemmell:1994:TBE


Gray:1994:QGB


Gupta:1994:RSD


Hamilton:1994:PNG


Hartel:1994:CRN


Hellekalek:1994:GDEa


Hellekalek:1994:GDEb


Hennecke:1994:RER


Hildebrand:1994:RWS


Hill:1994:CMR


Holian:1994:PNG


Hoogland:1994:GPR


Hormann:1994:NQR

REFERENCES

Hormann:1994:TRM


Hormann:1994:UGD


Huber:1994:PLG


James:1994:RFI


Jimbo:1994:RBB


Jimbo:1994:RBD


Johnson:1994:CUD

REFERENCES 354


Kaigh:1994:SRS


Kanatani:1994:SAG


Kari:1994:GNS


Karian:1994:RNG

[1906] 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/mtnvini.html. This article describes the Maple-language random-number generator, a multiplicative congruential generator (xnew = (A x + C) mod P) with A = 427,419,669,081, C = 0, P = 1012 – 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

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Takashima:1994:STT

Tezuka:1994:DDC

Tezuka:1994:MDC

Tezuka:1994:UVL

VanderMeer:1994:RBG

Vattulainen:1994:NTR

Vattulainen:1994:PTR

Weingartner:1994:NCP


Wolfram:1994:CA


Zhang:1994:PEE


Zijp:1994:UTC


Ahrens:1995:OTM


Al-Hussaini:1995:UPT


REFERENCES


Cusic:1995:PPN


Damien:1995:ARV


Dan:1995:CDA


Dellaportas:1995:RVT


DeMatteis:1995:CCP


Dudewicz:1995:EBR

REFERENCES


REFERENCES


[2006] P. Hellekalek. Correlations between pseudorandom numbers: theory and numerical practice. In P. Hellekalek, G. Larcher, and P. Zinterhof, edi-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Penrice:1995:AEP


Percus:1995:TAM


Phatak:1995:LMP


Pickover:1995:GET


Pickover:1995:RNG


Powell:1995:LEP


Ramon:1995:PKV

REFERENCES


REFERENCES

Sherif:1995:UWF

Sobol:1995:IQS

Sorenson:1995:ALE

Storn:1995:CO

Struckmeier:1995:FGL

Sugita:1995:PRN

Takashima:1995:STT


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Devroye:1996:RVG


Dietzfelbinger:1996:UHW


Dodge:1996:NRN


Dorfman:1996:PSR


Dwyer:1996:TRNa


Dwyer:1996:TRNb


Eichenauer-Herrmann:1996:ABC

REFERENCES

FFTAFM. ISSN 1071-5797 (print), 1090-2465 (electronic). URL http://

[2108] Jürgen Eichenauer-Herrmann and Frank Emmerich. Compound in-
versive congruential pseudorandom numbers: an average-case anal-
CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (elec-
110&arg1=S0025-5718-96-00675-8&u=/mcom/1996-65-213/; http:/

[2109] Jürgen Eichenauer-Herrmann. Equidistribution properties of inver-
sive congruential pseudorandom numbers with power of two modulus.
44(3):199–205, 1996. CODEN MTRKA8. ISSN 0026-1335 (print), 1435-
926X (electronic).

[2110] Jürgen Eichenauer-Herrmann. Modified explicit inversive congruential
pseudorandom numbers with power of 2 modulus. Statistics and Compu-
ting, 6(1):31–36, March 1996. CODEN STACE3. ISSN 0960-3174 (print),
1007/BF00161571.

[2111] Frank Emmerich. Pseudorandom vector generation by the compound in-
versive method. Mathematics of Computation, 65(214):749–760, April
1996. CODEN MCMPAF. ISSN 0025-5718 (print), 1088-6842 (elec-
110&arg1=S0025-5718-96-00706-5&u=/mcom/1996-65-214/; http:/

[2112] Karl Entacher and Stefan Wegenkittl. On the relevance of splitting prop-
erties and the compound method in parallel applications of pseudoran-
dom number generators. In Trobec et al. [3861], pages 64–74. ISBN
86-80023-25-6. LCCN ????

with exponential and normal distributions. Computers in Physics, 10
See [2378] for a proof of the algorithm proposed here for exponential random numbers.


Heinrich:1996:EA


Hofmeister:1996:ISG


Hormann:1996:RIG


Horstmann:1996:CCL


James:1996:ERF


Johnson:1996:RES

REFERENCES


REFERENCES


Masuda:1996:PPR


Matsumoto:1996:SDR


Matthews:1996:SRN


Mikhailov:1996:ENU


Mikhailov:1996:RSR


Mikov:1996:LSA


Mulmuley:1996:RGA

[2151] S. Nemnyugin and A. Larionov. Set of random walk tests for pseudo-
random generators. In Peter Borchers, Marian Bubak, and Andrzej
Maksymowicz, editors, Proceedings of the 8th Joint EPS-APS Inter-
national Conference on Physics Computing: PC ’96: September 17–
CYFRONET, Kraków, Poland, 1996. ISBN 83-902363-3-8. LCCN QC20
J45 1996.

[2152] Harald Niederreiter. Improved bounds in the multiple-recursive matrix
method for pseudorandom number and vector generation. Finite Fields

[2153] H. Niederreiter and C. Xing. Low-discrepancy sequences and global func-
tion fields with many rational places. Finite Fields and their Applications,
2(3):241–273, ???? 1996. CODEN FFTAFM. ISSN 1071-5797 (print),
1090-2465 (electronic).

[2154] H. Niederreiter and C. Xing. Quasirandom points and global function
fields. In Cohen and Niederreiter [3859], pages 269–296. ISBN 0-521-

Homer and Jin-Yi Cai, editors, Proceedings of the 11th Annual IEEE
Conference on Computational Complexity, 24–27 May 1996, pages 44–
58. IEEE Computer Society Press, 1109 Spring Street, Suite 300, Silver
Spring, MD 20910, USA, 1996. ISBN 0-8186-7386-9, 0-8186-7387-7 (case-

[2156] Shigeyoshi Ogawa. On a robustness of the random particle method.
CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961 (elec-
issue-3/mcma.1996.2.3.175/mcma.1996.2.3.175.xml; http://www.
math.utah.edu/pub/tex/bib/prng.bib. See erratum [2245].
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Baker:1997:NPU


Balakrishnan:1997:ASW


Bellare:1997:PRN


Berblinger:1997:MCI


Berg:1997:CNF

REFERENCES


REFERENCES


Eichenauer-Herrmann:1997:ICP


Eichenauer-Herrmann:1997:PSN


Eichenauer-Herrmann:1997:QCP


Emmeric:1997:EPQ


Entacher:1997:ASP


Entacher:1997:CSP


REFERENCES


Hellekalek:1997:CAP


Hellekalek:1997:GRN

[2219] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [3865], page ?? ISBN 3-901608-11-7. LCCN ???.

Hellekalek:1997:NPNa


Hellekalek:1997:NPNb


Herendi:1997:FGR


[228] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. On the lattice structure of pseudo-random numbers generated by the modified inversive congruential generator with modulus $2^n$. *Japan Journal of Industrial and
REFERENCES


REFERENCES


[2239] George Marsaglia. A random number generator for C. Posted to the sci.math.num-analysis news group, September 29, 1997. URL http://mathforum.org/kb/thread.jspa?messageID=1607565. From the posting: “Keep the following six lines of code somewhere in your files. #define znew ((z=36969*(z&65535)+(z>>16))<<16) #define wnew ((w=18000*(w&65535)+(w>>16))&65535) #define IUNI (znew+wnew) #define UNI (znew+wnew)*4.656613e-10 static unsigned long z=362436069, w=521288629; void setseed(unsigned long i1,unsigned long i2)z=i1; w=i2; Whenever you need random integers or random reals in your C program, just insert those six lines at (near?) the beginning of the program. In every expression where you want a random real in [0, 1) use UNI, or use IUNI for a random 32-bit integer. No need to mess with ranf() or ranf(lastI), etc, with their requisite overheads. Choices for replacing the two multipliers 36969 and 18000 are given below. Thus you can tailor your own in-line multiply-with-carry random number generator.”.


REFERENCES


REFERENCES

Eichenauer-Herrmann:1998:SQI


Ellison:1998:CRN


Emmerich:1998:EPC


Emmerich:1998:SIP


Entacher:1998:BSW


Entacher:1998:LCG


Entacher:1998:LIP

Evans:1998:RVG


Fuster-Sabater:1998:LPS


Gammel:1998:HRR


Garcia:1998:GCE


Gentle:1998:RNG


Hellekalek:1998:WST


Hickernell:1998:LRH


Homan:1998:RNG


Jakobsson:1998:PSP


Kao:1998:RNG


Kao:1998:SET

REFERENCES


[2318] Chi-Jen Lu. Improved pseudorandom generators for combinatorial rectangles. Lecture Notes in Computer Science, 1443:223–??,


REFERENCES


REFERENCES


REFERENCES

Soto:1998:STR

Sugita:1998:LTS

Takashima:1998:RWT

Tanaka:1998:OLA

Tezuka:1998:FAM

Thomlinson:1998:NBP

Trotter:1998:RTS


REFERENCES


REFERENCES


Chu:1999:DTF


Coddington:1999:IIR


deRaadt:1999:COO


Durrant:1999:RND


Eichelsbacher:1999:CPA


REFERENCES

Fernandez:1999:ANRa


Fernandez:1999:ANRb


Gartner:1999:PCP


Gartner:1999:RCZ


Goldreich:1999:IDB


Goldreich:1999:MCP


Gonzalez:1999:RNG

[2385] Jorge A. González and Ramiro Pino. A random number generator based on unpredictable chaotic functions. Computer Physics Communications,
Grin:1999:DNR


Haastad:1999:PGO


Intel:1999:IRN


Jun:1999:IRN


Kleinman:1999:SBO


Koldobsky:1999:PDD

Koshiba:1999:UPN


Larcher:1999:ADS


LEcuyer:1999:BLC


LEcuyer:1999:GPI


LEcuyer:1999:SRU


LEcuyer:1999:TLC

REFERENCES


[2424] Dietrich Stauffer. Ising model as test for simple random number generators. *International Journal of Modern Physics C* [Physics and Com-


[2433] 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

Beichl:2000:MA

Borkowf:2000:BRB

Brent:2000:TYA

Chen:2000:RRI

Couture:2000:LCR


REFERENCES


REFERENCES


[2458] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of AES finalists — RC6, Serpent, MARS and Twofish (abstract only). In


REFERENCES


[2472] George Marsaglia. The monster, a random number generator with period
over $10^{2^{857}}$ times as long as the previously touted longest-period one. Technical report ???, Florida State University, Tallahassee, FL, USA, ???. 2000.

[2473] George Marsaglia and Wai Wan Tsang. A simple method for generating
gamma variables. *ACM Transactions on Mathematical Software*, 26(3):
363–372, September 2000. CODEN ACMSCU. ISSN 0098-3500 (print),
1557-7295 (electronic).

[2474] George Marsaglia and Wai Wan Tsang. The ziggurat method for
www.jstatsoft.org/v05/i08; http://www.jstatsoft.org/v05/
i08/rnorrexp.c; http://www.jstatsoft.org/v05/i08/updates;
http://www.jstatsoft.org/v05/i08/ziggurat.pdf. See [2858,
2953].

scalable library for pseudorandom number generation. *ACM Transactions
ACMSCU. ISSN 0098-3500 (print), 1557-7295 (electronic). URL
http://doi.acm.org/10.1145/358407.358427. See correction [2476].

[2476] Michael Mascagni and Ashok Srinivasan. Corrigendum: Algorithm 806:
SPRNG: a scalable library for pseudorandom number generation. *ACM


Niederreiter:2000:IES


Nishimura:2000:TBM


NIST:2000:RNG


Panneton:2000:GNA

François Panneton. Générateurs de nombres aléatoires utilisant des récurrences linéaires modulo 2. (French) [random-number generators using linear recurrences modulo 2]. Thèse (M.Sc.), Département d’informatique et de recherche opérationnelle, Université de Montréal, Montréal, QC, Canada, 2000. xiii + 179 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.

Petrie:2000:NBI


Proykova:2000:HIR


RSA:2000:PKC

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2530] 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 $A = 31 167 285 = 0x1db_9335$ and modulus $M = 2^{48}$, implemented to require only 32-bit signed integer arithmetic.

REFERENCES


[2537] J. C. Hernández, A. Ribagorda, P. Isasi, and J. M. Sierra. Genetic algorithms can be used to obtain good linear congruential generators.
REFERENCES


Krause:2001:MHC


Kuang:2001:CSA


LEcuyer:2001:CQR


LEcuyer:2001:PBS


LEcuyer:2001:RN


LEcuyer:2001:RNG

REFERENCES


REFERENCES


[2577] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. *A Statistical Test Suite For Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute for Standards and Technology, Gaithersburg, MD,
REFERENCES


REFERENCES


[2592] 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.


REFERENCES


[2607] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of b^n ± 1, b = 2, 3, 5, 6, 7, 10, 11, 12*
REFERENCES


L.-Y. Deng and H. Xu. Design, search, and implementation of high-dimensional, efficient, long-cycle, and portable uniform random variate
REFERENCES


REFERENCES


[2640] ëfIü. P. (ëfIUriî Petrovitch) Kunchenko. Polynomial parameter estimations of close to Gaussian random variables. Berichte aus der Kommu-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Moon:2002:IDC


Murray:2002:IYP


Niederreiter:2002:ADI


Niederreiter:2002:ICS


Niederreiter:2002:RAT

REFERENCES


REFERENCES


REFERENCES


[2686] Anonymous. */dev/random*. Web site., June 8, 2003. From the site: “Thus, in 1994 noted Linux kernel hacker Theodore Ts’o wrote a driver for Linux, which takes information about hard to predict events like keyboard and mouse use, packet and disk drive timings, and so on, and uses it to seed a cryptographically secure random number generator. A process can then open up the ‘file’ */dev/random* (usually a character device), and read out random bytes. The driver keeps an estimate of how much entropy remains in the pool — if it goes below 0 then any reads will block until more entropy is added.” Also this: “the actual driver is implemented in drivers/char/random.c in the Linux source tree.”.

REFERENCES


[2691] 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).


REFERENCES


REFERENCES


REFERENCES


[2717] Xueqing Li, Wenping Wang, Ralph R. Martin, and Adrian Bowyer. Using low-discrepancy sequences and the Crofton formula to compute surface areas of geometric models. Computer Aided Design, 35(9):771–782, August 2003. CODEN CAIDA5. ISSN 0010-4485 (print), 1879-
REFERENCES

Lodwick:2003:EVC


Louchard:2003:ARS


Marsaglia:2003:EKD


Marsaglia:2003:RNG


Marsaglia:2003:TOS


Marsaglia:2003:XR

xorshift generators and the well-understood linear feedback shift register generators. See also [3456, 3549, 3639] for the failure of Marsaglia’s xorwow() generator from this paper. See [2871, 3699] for detailed analysis.


REFERENCES


Timothy C. Brown. Transforming a random variable to a prescribed distribution: An application to school-based assessment. *Journal of Applied
Conflitti:2004:MDS


Deng:2004:GMP


Dorfer:2004:CFE


Feige:2004:SIR


Fung:2004:AIH

E. Fung, K. Leung, N. Parimi, M. Purnaprajna, and V. C. Gaudet. ASIC implementation of a high speed WGNG for communication channel emulation [white Gaussian noise generator]. In IEEE, editor, 2004 *IEEE Workshop on Signal Processing Systems Design and Implementation proceedings: October 13–15, 2004, Crowne Plaza Hotel, Austin,
REFERENCES


Guan:2004:PNG


Gupta:2004:DBG


Gutmann:2004:CSA


Haldir:2004:HCL


Hernandez:2004:STN


Hong:2004:DCT


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[2826] Vincent Bénony, François Recher, Éric Wegrzynowski, and Caroline Fontaine. Cryptanalysis of a particular case of Klimov–Shamir pseudo-random generator. In Helleseth et al. [3907], pages
Blackburn:2005:PNP


Bogdanov:2005:PGL


Calvayrac:2005:RNG


Castro:2005:NRG


Contini:2005:SAA

[2831] Scott Contini and Igor E. Shparlinski. On Stern’s attack against secret truncated linear congruential generators. *Lecture Notes*
REFERENCES


REFERENCES


REFERENCES


[2850] Sharon S. Keller. *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES*
REFERENCES


Kemp:2005:PRN


Konuma:2005:DEH


Kung:2005:SGT


Larrondo:2005:ISC


LEcuyer:2005:FRN


[2874] B. Ya. Ryabko and V. A. Monarev. Using information theory approach to randomness testing. *Journal of Statistical Planning and In-
REFERENCES


Wic


Wiese:2005:IPN


Wiese:2005:PRP


Zhang:2005:ZBH


Zuquete:2005:EHQ

REFERENCES


Barker:2006:RRN


BenAtti:2006:BMA


Brent:2006:FRR


Cools:2006:CEL


Creutzig:2006:BRW


Devroye:2006:NRV

REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Title and Authors</th>
</tr>
</thead>
</table>
REFERENCES


REFERENCES


REFERENCES


Maffre:2006:WKT


Marsaglia:2006:RCS


Matsumoto:2006:PNG


Matsumoto:2006:UPN


McCullough:2006:RT


Miller:2006:MCL


REFERENCES


[2971] Heiko Bauke and Stephan Mertens. Random numbers for large-scale
distributed Monte Carlo simulations. *Physical Review E (Statistical
physics, plasmas, fluids, and related interdisciplinary topics)*, 75(6(part
2)):066701, June 2007. CODEN PLEEE8. ISSN 1539-3755 (print), 1550-

[2972] Verónica Becher, Santiago Figueira, and Rafael Picchi. Turing’s unpublished
algorithm for normal numbers. *Theoretical Computer Science*, 377
1879-2294 (electronic).

functional algorithms for simulation optimization. *ACM Transactions
CODEN ATMCEZ. ISSN 1049-3301 (print), 1558-1195 (electronic).

[2974] Richard Pierce Brent. Some long-period random number generators
using shifts and xors. *The ANZIAM Journal*, 48(??):C188–C202,
???? 2007. CODEN AJNOA2. ISSN 1446-1811 (print), 1446-8735
ANZIAMJ/article/view/40/79. Proceedings of the Computational Tech-
niques and Applications Conference.

the NIST SP 800-90 elliptic curve random number generator. In
Menezes [3916], pages 466–481. ISBN 3-540-74142-9 (paperback). LCCN
1777777.1777815.

Hardware generation of arbitrary random number distributions from un-
iform distributions via the inversion method. *IEEE Transactions on Very
CODEN IEVSE9. ISSN 1063-8210 (print), 1557-9999 (electronic). URL
REFERENCES

Chiu:2007:CKC


Cowles:2007:BRB


Delfs:2007:ICP


Doornik:2007:CHP


Dorrendorf:2007:CRNa


Dorrendorf:2007:CRNb

[2982] Leo Dorrendorf, Zvi Guterman, and Benny Pinkas. Cryptanalysis of the random number generator of the Windows operating system. In Rebecca N. Wright, Paul F. Syverson, and David Evans, editors, *CCS ’07: proceedings of the 14th ACM Conference on Computer and Communications Security*: Alexandria, Virginia, USA, October 29–November 2,


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[3030] Sastra Wijaya, Syn Kiat Tan, and Sheng-Uei Guan. Permutation and sampling with maximum length CA or pseudorandom number genera-


REFERENCES


REFERENCES


[3060] Lih-Yuan Deng, Rui Guo, Dennis K. J. Lin, and Fengshan Bai. Improving random number generators in the Monte Carlo simulations


REFERENCES


Hiroshi Haramoto, Makoto Matsumoto, and Pierre L’Ecuyer. A fast jump ahead algorithm for linear recurrences in a polynomial space. In

Holleman:2008:WCT


Hou:2008:LPD


Howes:2008:U


Inaltekin:2008:ANE


Jang:2008:CDH


Joe:2008:CSS


REFERENCES


Jovanovic-Dolecek:2008:UMT


Kalos:2008:MCM


Kang:2008:HPP


Kato:2008:QSC


Katsoprinakis:2008:QRN


Katti:2008:SPR

REFERENCES


Katz:2008:RRNa


Katz:2008:RRNb


Kiessler:2008:BRBe


Killmann:2008:DPR


Kim:2008:TRG

REFERENCES


Masaro:2008:RODb


Matsumoto:2008:MPR


McCullough:2008:ASP


McCullough:2008:MEW


Miller:2008:OSB


Moler:2008:NCM

REFERENCES


REFERENCES


Rumley:2008:PRN


Saito:2008:SOF


Schlier:2008:SHS


Schneier:2008:SSR


Shen:2008:RRL


Sinescu:2008:CLR

REFERENCES


REFERENCES

Varbanets:2008:ICGa


Varbanets:2008:ICGb


Walker:2008:EPN


Wang:2008:DCP


Wikramaratna:2008:ACR


Willink:2008:UPN


Wold:2008:AER

REFERENCES


REFERENCES

Czernik:2009:CRN


Danko:2009:IPR


DeMicco:2009:QR


Deng:2009:SPM


Devroye:2009:RVG


Dodson:2009:IGT

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

???? 2009. CODEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic).


REFERENCES

CODEN JIOSDC. ISSN 0252-2667.

S. K. Tawfeeq. A random number generator based on single-photon
avalanche photodiode dark counts. Journal of Lightwave Technology,
27(24):5665–5667, 2009. CODEN JLTEDG. ISSN 0733-8724
stamp/stamp.jsp?tp=&arnumber=5286273.

N. M. Thamrin, G. Witjaksono, A. Nuruddin, and M. S. Abdullah. An
whois:2009:RNG

Tian Tian and Wen-Feng Qi. Periods of termwise exclusive ors of
maximal length FCSR sequences. Finite Fields and their Applica-
science/article/pii/S1071579708000762.

Simone Tisa and Franco Zappa. One-chip quantum random number
generator. Proceedings of the SPIE — The International Society for
Optical Engineering, 7236(1):72360J, 2009. CODEN PSISDG. ISSN
link/?PSI/7236/72360J/1. Quantum Communications Realized II.

Qiaoling Tong, Xuecheng Zou, and Hengqing Tong. A RFID authen-
tication protocol based on infinite dimension pseudo random number
generator. In 2009. CSO 2009. International Joint Conference on Com-
putational Sciences and Optimization, volume 1, pages 292–294. 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=5193698.


REFERENCES

Wei:2009:QRN


Wold:2009:OST


Xiao-chen:2009:URN


Yamanashi:2009:SRN


Youssef:2009:IEU


Yu:2009:ESC

[3254] Senhua Yu and D. Dasgupta. An empirical study of Conserved Self Pattern Recognition Algorithm: Comparing to other one-class classifiers and


Afshin Akhshani, Sohrab Behnia, Amir Akhavan, Siew-Choo Lim, and Zainuriah Hassan. Pseudo random number generator based on synchronized chaotic maps. International Journal of Modern Physics C
REFERENCES


Anashin:2010:NAE


Anyanwu:2010:DCS


Banks:2010:DES


Barsegov:2010:EPR


Bastos-Filho:2010:IRN


Bellare:2010:PFP


REFERENCES


REFERENCES


REFERENCES

Doty-Humphrey:2010:PR

Duplys:2010:KRU

ElHaddad:2010:QMC

Feldman:2010:BMC

Gabizon:2010:DEW

Gabriel:2010:GUQ


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


Proshchan:2010:BQQ


Qi:2010:DFR


Quantis:2010:RNG

[3332] Quantis. Random number generation using quantum physics. ID Quantique white paper Version 3.0, ID Quantique SA, 1227 Carouge/Geneva,
REFERENCES


REFERENCES


Saiprasert:2010:OHA


Saito:2010:VMT


Segui:2010:AIP


Shen:2010:PQR


Shi:2010:MED


Shin:2010:AFG

REFERENCES


Srinivasan:2010:ADP


Stankovski:2010:GDN


Suciu:2010:PIN


Tang:2010:BHA


Tang:2010:BLC

REFERENCES


REFERENCES


Vakhania:2010:QGR


Valtchanov:2010:CRS


Varbanets:2010:ICG


Wikramaratna:2010:TEC


REFERENCES


REFERENCES

[3380] 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.”.


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Hofert:2011:SET


Hung:2011:DRD


Hwang:2011:SID


Jian:2011:TBQ


Kao:2011:EAT


Kleimo:2011:RNG


Koucky:2011:PGG


LECuyer:2011:AZV


LECuyer:2011:NUR


LECuyer:2011:URN


Leydold:2011:GGI


Li:2011:CBT


Li:2011:OOH

REFERENCES

Liu:2011:NPR

Liu:2011:PRC

Liu:2011:SBA

Liu:2011:TRN

Malik:2011:EHI
REFERENCES


[3450] Nilanjan Mukherjee, Janusz Rajski, Grzegorz Mrugalski, Artur Pogiel, and Jerzy Tyszer. Ring generator: An ultimate linear feedback shift...

**Phillips:2011:PRN**


**Qiu:2011:ATB**


**Quantis:2011:RRW**


**Ren:2011:QRN**


**Rose:2011:KBT**


**Salmon:2011:PRN**

[3456] 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. [3941], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ?????
REFERENCES


[3462] Vasile Sinescu and Pierre L’Ecuyer. Existence and construction of shifted lattice rules with an arbitrary number of points and bounded weighted


REFERENCES


REFERENCES


REFERENCES


[3491] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, and François Poucheret. Contactless electromagnetic active attack on ring oscillator
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Horstmann:2012:JEC


Horvath:2012:ARM


Horvath:2012:EGP


Impagliazzo:2012:PS


Kaczynski:2012:BNR


Kaczynski:2012:NRV


Karakostas:2012:DAC


Li:2012:TST

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

Manssen:2012:RNG


Marandi:2012:AQ


Marquardt:2012:PNG


Mascagni:2012:PRN


Masse:2012:RNS


Miles:2012:SPN

Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. Lecture Notes in Computer
Misczak:2012:GUT


Molina-Gil:2012:PGS


Nandapalan:2012:HPP


Nazzal:2012:UGA


Neves:2012:FSN


NIST:2012:RRN

[3540] NIST. Recommendation for random number generation using deterministic random bit generators. Special Publication 800-90, National Insti-
tute for Standards and Technology, Gaithersburg, MD, USA, 2012. URL http://csrc.nist.gov/publications/PubsSPs.html#800-90A.


REFERENCES


REFERENCES

Zhang:2012:RAG


Afshar:2013:ESR


Anonymous:2013:ERN


Applebaum:2013:PGL


AragonArtacho:2013:WRN


Bailey:2013:NNP


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

Gugala:2013:RNG


Gutierrez:2013:PML


Haitner:2013:EIC


Hamze:2013:SAR


Hill:2013:SIP


Hladky:2013:RNG

REFERENCES

Hu:2013:PSG


IBM:2013:IPC


Imai:2013:CRN


Khoshkenar:2013:NTR


Leonenko:2013:BRD


Liberty:2013:THR


REFERENCES


Anonymous:2014:CEF

Anonymous:2014:RNG

Barabesi:2014:NUR

Barash:2014:PGA

Baron:2014:LSP

Blacher:2014:PRN

Braverman:2014:PGR
REFERENCES


REFERENCES

Fukushima:2014:SDS


Gomez-Perez:2014:AEA


Haigh:2014:ABE


Healey:2014:SPS


Hormann:2014:GGI


Hu:2014:MBA

[3624] Jiaqiao Hu, Enlu Zhou, and Qi Fan. Model-based annealing random search with stochastic averaging. ACM Transactions on Modeling and
REFERENCES


Kawai:2014:ADT


Koo:2014:CRB


Korzen:2014:PPP


Langr:2014:APP


LEcuyer:2014:LSS


Ling:2014:MDN

Mascagni:2014:HPC


Mohamed:2014:MCS


Raaphorst:2014:CSC


Rivest:2014:SSR


Saito:2014:XV


Sanguinetti:2014:QRN


REFERENCES


REFERENCES


LoRe:2015:SRN


Lubicz:2015:TOB


Malik:2015:RCL


Malkiel:2015:RWW


Miles:2015:CCP


Miles:2015:SPN


Moufek:2015:MCB

REFERENCES


REFERENCES


REFERENCES


Mandal:2016:DIW


Mandal:2016:FRI


McFerland:2016:MZA


Miller:2016:RPS


Nekrutkin:2016:CBF


NIST:2016:SDR


[3703] 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 [3710] for details of the attack.


REFERENCES


REFERENCES


[3728] Katherine Q. Ye, Matthew Green, Naphat Sanguansin, Lennart Beringer, Adam Petcher, and Andrew W. Appel. Verified correctness and secu-
REFERENCES

rity of mbedTLS HMAC-DRBG. In ACM, editor, Proceedings of CCS
17, October 30–November 3, 2017, Dallas, TX, USA, pages 1–14. ACM
???? URL http://www.cs.princeton.edu/~appel/papers/verified-
hmac-drbg.pdf.

Aletti:2018:GDR

[3729] Giacomo Aletti. Generation of discrete random variables in scal-
able frameworks. Statistics & Probability Letters, 132(?):99–106,
January 2018. CODEN SPLTDC. ISSN 0167-7152 (print), 1879-
article/pii/S0167715217302900.

Anderson:2018:IP

[3730] David F. Anderson, Timo O. Seppäläinen, and Benedek Valkó. Intro-
duction to Probability. Cambridge mathematical textbooks. Cambridge

Bernardini:2018:GES

[3731] Riccardo Bernardini and Roberto Rinaldo. Generalized Elias schemes
for efficient harvesting of truly random bits. International Journal of
Information Security, 17(1):67–81, February 2018. CODEN ????. ISSN

Chang:2018:CSL

[3732] Zuling Chang, Martianus Frederic Ezerman, San Ling, and Huaxiong
Wang. The cycle structure of LFSR with arbitrary characteristic poly-
nomial over finite fields. Cryptography and Communications, 10(6):
1183–1202, November 2018. CODEN ????. ISSN 1936-2447 (print),
1007/s12095-017-0273-2.

Checkoway:2018:WDL

[3733] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried,
Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Wein-
mann, Eric Rescorla, and Hovav Shacham. Where did I leave my
keys?: lessons from the Juniper Dual EC incident. Communications
of the ACM, 61(11):148–155, November 2018. CODEN CACMA2. ISSN
Deng:2018:SFE


Ermakov:2018:RRQ


Harase:2018:IBM


Lin:2018:RNG


Merali:2018:PAS


Mullner:2018:RSS

REFERENCES

Petrica:2018:FOC


Sanders:2018:EPR


Wang:2018:LBA


Gorder:2019:RSN


Lemire:2019:FRI


Poudel:2019:MTU

Quaglia:2019:RCR


Zhang:2019:REU


Basuyaux:20xx:RNG


L’Ecuyer:20xx:PNG


Wagner:20xx:WRS

[3750] 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/.

Bailey:2013:CAM

REFERENCES


REFERENCES

Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 1969. LCCN QA1 S565 v. 3.


Rice:1971:MS


Zarem:1972:ANT


Schaffner:1974:PPB


Patil:1975:MCS

REFERENCES


Oren:1980:SDM


Eddy:1981:CSS


Rubinstein:1981:SMC


Grossmann:1982:PSI


IEEE:1982:ASF


Chaum:1983:ACP

REFERENCES


REFERENCES


[3792] Kurt Mehlhorn, editor. STACS 85: 2nd Annual Symposium on Theoretical Aspects of Computer Science, Saarbrücken, January 3–5, 1985, vol-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


ACM:1989:PTF


Anonymous:1989:PFC


Beker:1989:CC


IEEE:1989:ASF


MacNair:1989:WSC

REFERENCES


REFERENCES

ACM:1992:PTF


Burr:1992:UEN


Gritzmann:1992:ORE


IEEE:1992:ASF


Pflug:1992:SOP


Simmons:1992:CCS

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


REFERENCES

LCCN QA3 .L35 v.1554.


REFERENCES


REFERENCES


IEEE:1997:ASF

Troch:1997:PSI

Wyrzykowski:1997:PNP

Banks:1998:HSP

Buhler:1998:ANT

Hellekalek:1998:RQR


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Schueller:2001:MCS


Smelser:2001:IES


Spector:2001:GPG


ACM:2002:PTF


Dror:2002:MUE

REFERENCES


USENIX:2002:PBF


ACM:2004:PAA


Gentle:2004:HCS


Niederreiter:2004:MCQ

REFERENCES


REFERENCES


REFERENCES


ACM:2008:SPA


Golomb:2008:STA


Keller:2008:MCQ


Nguyen:2008:GG


Rousseau:2008:MT


Alexopoulos:2009:AFS

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

[Belsley:2009:HCE]


[Clavier:2009:CHE]


[LEcuyer:2009:MCQ]


[Paredaens:2009:PTE]


[ACM:2010:PAI]

REFERENCES

Anon:2010:NDS


Cont:2010:EQF


Dick:2010:DNS


Feldman:2010:APS


Gollmann:2010:SCR


IEEE:2010:ISV

REFERENCES


REFERENCES


Lathrop:2011:SPI


Lovric:2011:IES


vanTilborg:2011:ECS


ACM:2012:SPA


Cooper:2012:HWC


Dunn:2012:EMC

REFERENCES


[3952] Nicholas J. Higham, Mark R. Dennis, Paul Glendinning, Paul A. Martin, Fadil Santosa, and Jared Tanner, editors. The Princeton Companion to