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

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA
Tel: +1 801 581 5254
FAX: +1 801 581 4148
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

09 January 2018
Version 1.283

Title word cross-reference

#14 [2262]. #15949 [867]. #4059 [1237]. #8373 [2085].

(0, 1) [1049]. (0, s) [2517, 2900]. (a^n - 1)/(a - 1) [913]. (j, c) [726]. (n^2 \alpha) [2470]. (n^k \alpha) [2471]. (n\alpha) [2470]. (t, m, s) [2029, 2860, 2035, 2334]. (t, s) [2612, 2029, 2325, 2860, 2035]. (X^2 - Y^2)^{1/2} [488]. 0.1(0 \times 1)0 \times 9 [139]. 1 [733, 871, 2813, 171, 301, 708, 2935, 2937]. 1, 2, 3 [3445]. 1.13198824... [2494]. 10, 000 [282]. $10.00 [168]. 10^{2357} [2465]. 10^{1355} [2027]. 1200 \mu [3094]. 128 [3119]. 13 [270]. 16 [270]. 2 [2813, 2104, 925, 3059, 2479, 2793, 2939]. 2, 000 [86]. $24.95 [2072]. 2^{-31} - 1 [833, 926]. 2^{15} [2122]. 2^{-31} - 1 [3494, 798, 969, 1002, 1190, 1191]. 2^{31} - 69 [3341]. 2^{32} - 1 [1082]. 2^9 [1467, 2222]. 2^3 [1310, 1473, 1718]. 2^k [2593]. 2^{k-1} [2593]. 2^p [3205]. 2^p - 1 [2255]. 3 [1772, 3620]. 32 [3575]. 4 [270]. 48 [245]. 5 [270]. $52.95 [3544].
$[0, 1] \ [217, 843] \cdot 2 \ [3094] \cdot \tau \ [2356, 1942] \cdot a \ [363] \cdot a = \pm 2^q + 2^r \ [2388, 2458] \cdot a_n \ [647] \cdot \alpha \lambda \ [710, 711] \cdot b \ [2119, 3296] \cdot b = 2, 3, 5, 6, 7, 10, 11, 12 \ [1029, 1295, 2600] \cdot b^q \pm 1 \ [1029, 1295, 2600] \cdot \beta = 32 \ [1310] \cdot \beta = 48 \ [1310]$

$\beta \simeq 32 \ [1473] \cdot \beta \simeq 48 \ [1473] \cdot \left\{ \frac{a}{m^2} \bigg\} \bigg\{ \frac{a}{m} (j + r)^2 \bigg\} \ [323] \cdot \text{mod} 1$

$[296, 297, 401, 639, 719, 644] \cdot \text{mod} \ [2188] \cdot C^\infty \ [1255] \cdot C \exp(-\lambda|x|^r) \ [1455] \cdot \chi^2 \ [343, 921, 1079, 1080, 1081, 6, 7] \cdot D \ [2360, 1792, 2947, 2063] \cdot d^2 \ [92] \cdot e \ [80, 1490, 86, 366] \cdot e [1895] \cdot F_2 \ [2981, 2990, 3194] \cdot F_{2w} \ [2794] \cdot G \ [443, 444] \cdot \Gamma \ [1211, 1185] \cdot j [1922] \cdot k \ [2175, 1443, 1751, 2096, 1034, 1312, 1902, 1100, 1349, 1950] \cdot k > 1 \ [1339] \cdot L^2 \ [2015, 1946] \cdot L_2 \ [2114] \cdot L_p \ [2385] \cdot \lambda [2783] \cdot M \ [1423, 1195, 1161, 826, 460, 1036, 1006, 437, 247, 1343, 2139, 2320, 2057, 2163, 2165, 2252, 1110, 229] \cdot F_2 \ [3062, 3413] \cdot F_{2w} \ [2938] \cdot F_q \ [3172, 3466] \cdot F_{q^n} \ [3172, 3466] \cdot F_2 \ [3414] \cdot GF(2^n) \ [1547] \cdot \mu [3152] \cdot N \ [1128, 890, 267, 1300, 1663, 1664, 2209, 707, 203, 604, 194, 2757, 199, 1506, 3703, 780, 205, 423, 783] \cdot \Omega(3) \ [1549] \cdot O(n(1 + \log(N/n))) [1911] \cdot P \ [6, 705, 3098, 2405, 2156, 3298, 2169, 2352] \cdot \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + (K/y)(\partial u/\partial y) = 0 \ [195] \cdot \pi \ [2826, 80, 1490, 86, 282, 285, 2878] \cdot \pm 1 \ [647] \cdot \pm 2^{k_1} \pm 2^{k_2} \ [2255] \cdot \pm 2^{m_1} \pm 2^{m_2} \ [2585] \cdot q \ [2483] \cdot S \ [1001, 1853] \cdot \sigma \ [1549] \cdot \sqrt{2} \ [404, 432] \cdot \sum a_n / n \ [647] \cdot T \ [2548, 2810, 1843, 827, 1853, 1298, 2985, 935, 940, 39] \cdot U(0, 1) \ [2695] \cdot X(I + 1) = A X(I) \mod 2^{31} \ [761] \cdot x^2 \mod N \ [1975] \cdot X_{n+1} = a_n X_n + b_n \mod (p) \ [1777] \cdot X_I = X_{I-3p} \oplus X_{I-3q} \ [1476] \cdot y = [(a + x) \sin(hx)] \mod 1 \ [2332] \cdot Z/nZ \ [1886] \cdot Z_p \ [1379]$

*good* [2643].
0.57pJ [3218]. 0.57pJ/bit [3218]. '05 [3867, 3871]. '07 [3877]. '08 [3881].

1 [743, 1038, 1907, 1908, 3325]. 1.04 [3152]. 1.1 [3640]. 1.6 [3576]. '10
'13 [3914]. 133 [265, 266, 303, 309]. 134 [871]. 13th [3840]. 14th
[3878, 3807]. 153 [924, 1080, 1081]. 155 [921, 1081]. 157 [972]. 16
[1465, 2946, 907]. 16-Bit [1258, 1851, 739, 1465, 2159]. 16-bit-PC [1465].

2 [194, 219, 2240, 3326]. 2.4GHz [3336]. 20 [2072, 2406]. 200 [298, 358].
29th [3785, 3769]. 2nd [3742, 3755].

3 [3064, 3648, 1928, 3327]. 3-Key [2842]. 3.0 [2614]. 3.x [2261]. 30 [3456].
30th [3775, 3796]. 31 [2535]. 31-bit [750]. 31st [3781]. 32-Bit
[1207, 2919, 2989, 1726, 3340]. 32-bit-word [532]. 334 [425, 470]. 33rd
[504, 606]. 38th [3827]. 39th [3877].

4 [456, 655, 3328]. 4086 [2827]. 40th [3881]. 41st [3848]. 42 [674, 675].
48-Bit [1016]. 488 [657]. 4Gbps [3218].

5.0 [1626]. 5.2 [2730]. 500 [3270, 317]. 51st [3898]. 52 [867]. 52nd [3913].
5th [3882].

60th [3915]. 61 [1226]. 623-dimensionally [2319]. 64-bit


82g [1038]. 82h [1007]. 84 [3754]. 85 [1997]. '86 [3765]. '87 [3762]. '88 [3780].


9th [3896].

= [3721, 3731].


<table>
<thead>
<tr>
<th>Term</th>
<th>Page Numbers</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearer [3182]</td>
<td>[2027, 2555]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Cleve [2027]</td>
<td>[2555]</td>
<td>CKv12</td>
</tr>
<tr>
<td>CMOS [3270, 3064, 3315, 3218, 3336]</td>
<td>[168]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Co-evolving [2161]</td>
<td>[168, 2161]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Code [3143, 2095, 3166, 979, 3299, 2157, 3546, 2681, 968, 3183, 1913, 2044, 3715, 1051]</td>
<td>[138]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clever [3182]</td>
<td>[2027, 2555]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Client-server</td>
<td>[1929]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Club [1284]</td>
<td>[1820, 2245]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clock [1965]</td>
<td>[2165]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clock-controlled [1965]</td>
<td>[2556]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clock-flipping</td>
<td>[1965]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clipped [609]</td>
<td>[2025]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Close [2457, 1141, 2633]</td>
<td>[2457]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Cloudier [3663]</td>
<td>[2025]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Coin [3689, 1069, 2087, 3261, 1746, 2521, 3288, 1421, 161, 1172]</td>
<td>[138]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Coin-Tossing</td>
<td>[1746]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Collector</td>
<td>[3725, 1957]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Collector</td>
<td>[142]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Cluster-flipping</td>
<td>[1820]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clustered-rocket</td>
<td>[253]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clustered</td>
<td>[253]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Cluster-flipping</td>
<td>[253]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Clustering</td>
<td>[3179, 3176]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combined</td>
<td>[3728, 2203]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combined</td>
<td>[142]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combined</td>
<td>[3729, 2697]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combined</td>
<td>[3729, 2697]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combination</td>
<td>[392, 503, 474, 362, 1756, 1088, 2769, 438, 439, 61]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combination</td>
<td>[392, 503, 474, 362, 1756, 1088, 2769, 438, 439, 61]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combinatorial</td>
<td>[617, 3564, 201, 2312, 1516, 2075, 235, 3409, 749]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combinatorics</td>
<td>[3779, 2697]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combiners [1703]</td>
<td>[2340]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combiners [1703]</td>
<td>[2340]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combining</td>
<td>[878, 879, 1564, 3166, 2524, 3052]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Combining</td>
<td>[878, 879, 1564, 3166, 2524, 3052]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Comment [292, 1561, 168, 2518, 837, 1038, 930, 1585, 933, 842, 938, 2850, 939, 844, 2568, 946, 855, 851]</td>
<td>[138]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Commentary</td>
<td>[2128]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Commentary</td>
<td>[2128]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Commitment [1514, 1605]</td>
<td>[1280]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Commodore</td>
<td>[1115]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Common</td>
<td>[1179, 499, 1257, 1684, 2995, 1708, 1528, 787, 2119, 1091, 3526, 1809, 1057, 730, 3488, 2509, 2187, 1086, 1677, 886, 753, 709, 892, 1331, 2384, 1808, 2030, 914, 1441, 1630]</td>
<td>[138]</td>
</tr>
<tr>
<td>Commun [1997, 2118]</td>
<td>[1280]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Communications [494, 2632, 3871, 3801, 2676]</td>
<td>[138]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compatible</td>
<td>[1478, 1506, 3504]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compatible</td>
<td>[1478, 1506, 3504]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Comparing</td>
<td>[1194, 886, 1782, 2126, 3244]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Comparative</td>
<td>[1306, 395, 491, 3168, 2060]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compatibility</td>
<td>[1306, 395, 491, 3168, 2060]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compatibility</td>
<td>[1306, 395, 491, 3168, 2060]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compatible</td>
<td>[1478, 1506, 3504]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Competing</td>
<td>[1478, 1506, 3504]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Compiled</td>
<td>[69]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Complete</td>
<td>[1261, 989, 909, 2344, 2751, 2751]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Completed</td>
<td>[927]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Complex</td>
<td>[3568, 663, 3826, 3658]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Complex</td>
<td>[3568, 663, 3826, 3658]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Complex</td>
<td>[3568, 663, 3826, 3658]</td>
<td>CKv12</td>
</tr>
<tr>
<td>Complex</td>
<td>[3568, 663, 3826, 3658]</td>
<td>CKv12</td>
</tr>
</tbody>
</table>
Confidence
configurable [2498]. configuration [1159]. Confusion
Congrès [3721]. Congress [3721]. Congruence
congruences [1311, 187]. congruent [2141]. Congruential
Convergent [310].
Convolutional [3647]. Convolutions [666, 2546, 1548]. Cooperation [3524].
Cope [2423]. Copenhagen [3768]. Coprocessor [2531, 3572]. copula [3023].
Copulas [3023]. Copyright [2264]. CORDIC [3578, 3624]. Core.
Corfu [1935, 2733, 1837]. Correspondence [655, 2005, 1801, 2046].
Corrigendum [1007, 2469, 1344, 525, 612, 3545].
Cryptanalytic [2301]. CRYPTO
Cryptography
Cryptology

[1117, 3754, 3744, 3762, 3763, 3783, 3793, 3752, 3807, 3780, 3879, 3765]

Cryptosystem [3224, 1334, 3647]. cryptosystems [2386, 1348, 3125].

Crystal [3839, 53, 3854, 3748, 3795]. crystallography [3186].

CSD [2051].

Cuba [2836]. cube [416, 1540, 783]. Cubic [1571, 2197, 1816].

CUDA [3476, 3066, 3192, 3537].


Customer [2684]. Cusum [1168]. Cusum-Shewhart [1168].

cut [2524].


Frequency [1999, 2113, 3671, 2867, 1018, 609, 540, 1321, 3199, 2661, 691].
Frequency-Modulated [2867]. frog [2282]. frontiers [3886, 3865].
frustration [3232]. FTTN77 [1881]. Fukuoka [3784].
2593, 1847, 3151, 1754, 3602, 1872, 2691, 3610, 1893, 2011, 1036, 3427, 1804, 1267, 2947, 2666, 1036
generator


generators [3662, 3033, 1642, 1118, 2819, 1026, 2820, 1174, 1967, 1646, 2599, 2682, 2966, 2359, 880, 1456, 1649, 2821, 1176, 698, 3042, 3600, 1855, 3045, 3559, 3392, 1856, 2093, 2184, 533, 2185, 1860, 1974, 2094, 2186, 997, 1861, 3158, 2274, 1301, 1462, 1463, 3160, 1382, 1450, 1460, 3395, 1564, 1659, 2685, 2825, 3051, 3161, 1303, 1383, 616, 2826, 3163, 3164, 1568, 400, 1384, 2688, 2193, 2591, 2439, 1466, 3167, 1386, 1387, 1469, 1667, 1308, 2828, 1875, 1876, 1900, 2106, 2203, 2281, 2282, 2370, 2514, 2515, 1674, 1129, 1765, 833, 925, 926, 1190, 1191, 1310, 1766, 1993].

generators [3697, 430, 1004, 272, 2286, 836, 971, 2832, 2979, 3698, 1317, 3607, 2834, 3409, 2696, 1678, 1771, 749, 467, 1198, 1252, 1319, 2524, 2622, 2698, 2699, 3060, 3566,
2042, 3324, 1820, 3458, 3459, 2879, 2958]. **Goodness**
[3758, 579, 2857, 18, 815, 68, 87, 101, 3042, 1132, 1037, 1143, 97, 607].
**Goodness-of-Fit** [2857, 815, 3758, 3042, 1132, 1037, 1143, 607].
**Gossip** [3824]. **GP** [3857, 3531]. **GP-2001** [3857]. **GP-GPU** [3537]. **GPU** [3628, 3372, 3554, 3596, 3563, 3278, 3634, 3902, 3912, 3517, 3884, 3317, 3531, 3440, 3359]. **GPU-enabled** [3317]. **GPUs** [3596, 3389, 3639].
**Gradient** [3184, 1503]. **Graduate** [3843]. **Grand** [3835].
**Grande** [2363]. **Graph** [2901, 505, 1853, 2828, 1992, 2758, 1896, 1948].
**Graphic** [3331, 3586, 3254]. **Graphical** [1434, 1618, 1731]. **Graphics** [3395, 3317, 3253, 3557, 3082, 3525, 1431, 1613, 3360, 3472]. **graphs** [1841, 2115].
**gray** [1664]. **gray-scale** [1664].
**Greater** [871, 460]. **Greatest** [499, 1257, 1091, 1057, 730]. **Greece** [3880].
**Greedy** [3337]. **Green** [1273].
**growth** [3310]. **Guangdong** [3903].
**guarantee** [1248]. **guaranteed** [3627]. **Guarantees** [1677, 1958].
**Guest** [2273, 3020].
**Guide** [3476, 1028, 1235, 2543, 2639, 2558, 989, 2129, 2992, 2557]. **Guidelines** [1677, 1531].
**Guitar** [2684].
hiding \[3283\].  hierarchical \[3068, 2926\].  Hierarchy \[2136, 3346, 1563\].  High \[2354, 3364, 2083, 3631, 2601, 3045, 3180, 3181, 3218, 3072, 3671, 3315, 1161, 3016, 3018, 100, 3467, 1029, 1295, 2618, 2683, 2606, 2685, 2972, 3055, 3167, 2515, 2759, 3281, 2980, 1682, 1894, 2118, 117, 3082, 3192, 128, 3429, 1912, 3434, 3435, 1919, 771, 2326, 225, 2942, 2868, 2952, 3429, 3457, 121, 2419, 2493, 3469, 2883].  High-density \[2601\].  high-dimensional \[2606, 2685, 2326, 2952, 3625\].  High-entropy \[3045\].  high-functioning \[2942\].  high-order \[2980\].  High-Performance \[3072, 3188, 3525, 3429\].  high-period \[2972\].  High-Quality \[2083, 2515, 1894, 2118, 1912, 2419, 2493\].  Higher \[1655, 2380, 3150, 3419, 1217, 2877\].  Higher-Order \[1655\].  Highly \[1578, 2938\].  highly-uniform \[2938\].  Hilbert \[2935\].  Hill \[168, 3861, 866, 1753, 3096\].  Hilton \[3782, 3776\].  Hirschberg \[1839\].  Histogram \[3389, 1579\].  Histograms \[3585, 1278\].  Historical \[2672\].  History \[70, 88, 700, 2703, 2721, 67, 1350, 368\].  Hit \[1744, 1977, 1750\].  Hit-and-Run \[1744, 1750\].  Hitachi \[2068\].  Hitting \[2377\].  HK97 \[3472\].  Hlawka \[847, 454\].  HMAC \[3710\].  HMAC-DRBG \[3710\].  Hoare \[3846\].  Hoeffding \[2242\].  Home \[2448\].  homogeneous \[12, 1580\].  Homomorphism \[505, 2360\].  homomorphisms \[3140\].  Hong \[3860\].  Honolulu \[3840, 3897\].  honor \[3886, 3915\].  honour \[3846\].  Hopfield \[3345\].  Hörmann \[2894\].  Horner \[2496, 239\].  Horseshoes \[2302\].  Horton \[1865\].  Hot \[3833\].  HotBits \[2809\].  Hotel \[3778, 3724, 3821, 3776, 3748, 3750, 3795, 3810, 3861, 3760, 3835\].  Houston \[3745\].  Huge \[2996\].  hundred \[1195\].  Hurst \[2286\].  HW \[3089\].  Hyatt \[3839, 3913, 3835\].  Hybrid \[3164, 348, 2193, 3224, 3026, 3150, 544\].  hyperbolas \[2066, 2347\].  Hyperbolic \[2729, 872, 993, 1754, 1903, 1935\].  Hypercube \[3759, 907, 908, 1325\].  Hypercubes \[3773\].  Hypergeometric \[1327, 1142\].  hyperplane \[2193\].  Hyperplanes \[2195\].  hyperspheres \[3248, 2952\].  Hypotheses \[173\].  Hypothesis \[433\].

I. \[866\].  IBM \[3722, 701, 792, 660, 1392, 1478, 469, 2531, 153, 1506, 481, 453\].  IBM-Compatible \[1478, 1506\].  ibre \[1023\].  IC \[2683, 3400, 3280, 2380, 2480, 3343\].  ICCMSE \[3880\].  ICGA \[3857\].  ICGA-2001 \[3857\].  ICICTA \[3903\].  icosahedral \[165\].  ideal \[792, 660\].  identical \[928\].  Identically \[2497, 3287\].  Identification \[1421\].  Identifying \[3185\].  identities \[1357\].  identity \[2507, 1903\].  IEEE \[3852, 3897, 3898, 3913\].  If \[1453\].  IFIP \[3896\].  II \[3842, 1229, 3258, 1664, 1757, 2204, 1774, 1884, 1202, 251, 1921, 2024, 2396, 636, 1604, 677, 1433, 520, 2579, 863, 2167, 1546, 2069\].  II.5 \[743\].  IIASA \[3792\].  iid \[3157\].  III \[3831, 2205, 2001, 2395, 776\].  Illiac \[151\].  Illinois \[3767, 3862, 3743\].  Illumination \[2037\].  illusion \[2908\].  Illustrated \[24\].  illustrations \[7\].  Illustrative \[2876\].  IMA \[3841, 3872\].  IMACS \[3828\].  Image \[3399, 3446, 3447, 3234, 3243, 3416, 3428, 1425, 3355\].  Images
[2750, 2363, 3504, 2779, 3650, 3005]. Java-implemented [3005]. JavaTalk
[3798, 3822, 3738, 3717, 3815, 3836, 3890, 3732, 3857, 3804]. Jump
[2981, 3062, 3063]. June [3811, 3862, 3877, 3891, 3900, 3914, 3728, 3869, 3831,
3908, 3786, 3742, 3717, 3897, 3726, 3816, 3843, 3890, 3855, 3804, 3817, 3844].
Jungles [2329]. Justification [2189, 984].
Kakutani [3206]. kappa [3591]. KASUMI [2534]. Keccak [3484]. KENO
[3364, 3255, 2267, 3043, 3273, 887, 2448, 2842, 2927, 1601, 2025, 1513, 2482,
1936, 1627, 3035, 2386, 3304, 1925, 3106]. Key-Stream [3364]. Keys
[3687, 3502, 1601, 3680, 2872]. keystream [3177, 3447]. keystreams [1764].
Kloosterman-type [1761]. KMCLib [3640]. Known
[1805, 3269, 2281, 780]. Knoxville [3759]. Knuth [1696, 676, 713]. Kochen
[3474]. Koen [2969]. Kolmogorov
[63, 398, 71, 1132, 766, 2713, 97, 815, 188, 3450]. Kong [3860]. Kongruenz
[1023]. Kongruenz-Generatoren [1023]. konvexe [32]. konvexer [718].
Korea [3870]. Körper [32]. kriging [3488]. krivoi [34]. Kronecker [3487]. KY
[3882].
L [529, 578, 620]. Laboratory [3716, 3718]. Lag [593]. Lagged
Laplace [2519, 666, 3000, 3213]. laptops [2268]. Large
[3716, 3259, 3493, 3494, 838, 666, 26, 2852, 2143, 185, 3210, 1528, 2963, 2825,
3051, 3161, 1320, 64, 73, 244, 95, 1052, 604, 230]. Large-Order [3493, 3494].
Large-Scale [3716, 185, 2143, 2963, 95]. large-size [73]. largely [960].
Laser [3212, 3282, 3297, 457, 3239]. Lasers [3009, 3126, 3200]. Last [2164].
Latin [2326]. LatMRG [2129]. Lattice
[530, 566, 1970, 2893, 2434, 699, 2610, 2829, 2296, 2916, 2634, 3616, 3672, 2709,
588, 2401, 2724, 2950, 3009, 3117, 3217, 1538, 2672, 1023, 1114, 1169, 1283,
2085, 1860, 2757, 1467, 1762, 1307, 1308, 1130, 2523, 3413, 3414, 2913, 1136,
1137, 2445, 3186, 2222, 671, 707, 2226, 2228, 2391, 2460, 2538, 3294, 2461,
2545, 1912, 847, 2935, 2937, 1059, 3010, 3116, 3451, 2247, 1828, 391, 454, 3672].
lattice-bases [1136]. lattice-sublattice [3186]. lattices [2094, 2772, 2800].
Lausanne [3888]. lava [2718]. LavaRnd [2565]. Law
[3391, 3210, 1528, 2169, 3054, 2689, 3173, 15, 197, 2111, 244, 16, 3097, 780,
2334, 3377, 3256, 3068, 2932, 2801, 882]. Laws [838, 1498, 2729, 560].
Laxenburg [3792]. LC [2867]. LCG [2610]. LCGs [2205, 2515, 2229].
Leading [2917, 616, 1035]. leads [1850]. leads-to [1850]. Leakage [2423].
Leap [3241, 2282]. leap-frog [2282]. learnability [2171]. Learning
[3118, 1943]. Least [733, 531, 104, 1405]. Least-Remainder [104]. Lécons
Lehmer [1658, 2193, 2194, 745, 3574, 891, 246, 2151, 480, 2053, 231].
Lemmas [2521]. Length [3688, 181, 369, 458, 1238, 238, 1572, 1078, 1003, 807, 1805,
1852, 1242, 461, 1386, 1468, 1667, 1130, 841, 1893, 2449, 1411, 582, 583, 1697,
3104, 642, 1949, 3225, 3466, 3022].
[465, 1201, 1798, 2946, 483]. letters [2864]. Levels
[3556, 2473, 1123, 2987, 1785, 3003, 2732]. Lewis [740]. Lexington [3882].
Leydold [2894]. LFSR [2270, 3156, 2392, 3304, 3703, 3241]. LFSR-Based
[3703]. Libgcrypt [3666]. Liblice [3726]. libraries [2117]. Library
[3376, 3692, 1032, 1304, 1196, 2543, 2639, 2924, 2992, 2640, 2138, 1438, 1554, 1634,
3374, 3554, 3596, 2816, 3272, 3171, 3563, 3667, 2896, 2991, 2468, 2469].
Lie [1930]. Life [2355, 3535]. light [3457]. Lightweight [3677, 3353]. Like
[2684, 468, 2025, 3621, 3346]. Likelihood [2285, 1000, 1128]. Limit
[695, 1236, 2437, 1470, 2519, 2932, 2152, 2801, 2338, 3465, 560, 63, 2979, 3287,
1697, 3435, 3643, 409, 2721, 1159, 188, 2090]. limiting [1704]. Limits
[616, 85, 38, 2253, 2346]. Lin [2771]. Lindberg [1373]. Line
[2095, 2681, 438, 439, 3215]. linéaire [1336]. linéaires [2479, 2793]. Linear
[392, 2868, 1374, 2510, 2823, 1974, 921, 3496, 2282, 2283, 1079, 1080, 1081,
3405, 1085, 835, 2904, 2763, 1996, 2981, 3062, 3063, 2216, 2530, 2838, 3503,
3508, 3509, 503, 759, 1338, 1339, 2388, 2459, 2990, 3194, 2550, 2583, 1796, 845,
474, 587, 807, 3439, 3000, 596, 849, 1811, 1055, 362, 2575, 3540, 2340, 367,
2670, 3545, 209, 1169, 1363, 3597, 566, 1454, 1027, 1376, 2359, 1649, 3046,
1860, 2094, 111, 3049, 1463, 1303, 569, 1756, 1384, 1469, 1188, 1246, 1308,
2203, 2281, 2369, 3270, 925, 1311, 1250, 1313, 3172, 2832, 2979, 1679, 2622].
linear [2699, 2980, 3560, 1088, 3413, 3414, 2529, 975, 3075, 936, 1144, 2919,
1336, 2129, 2226, 2239, 2391, 2635, 2847, 1145, 2232, 843, 3432, 2642, 252,
2317, 2784, 2719, 2997, 2651, 1706, 3001, 677, 775, 776, 850, 1155, 1516,
2792, 2479, 2793, 2794, 2938, 2939, 901, 1353, 1717, 1718, 942, 1014, 3620,
2799, 2800, 2946, 1725, 1220, 957, 1275, 2874, 3014, 3222, 3340, 3458, 2956,
3017, 2877, 1622, 13, 2810, 3355, 1835, 2256, 1023]. Linear-Algebra [1811].
[975]. Linearily [3141, 3251, 3121, 1949]. Link [3202]. linkage [3737]. links
Load [2204]. loaded [2453]. Loads [3044].
Local [3550, 3259, 712, 588, 1343, 1510, 1599, 1812, 3477, 1325, 2994, 1159].
Locality [3550, 3477]. localization [1645, 3270]. Log
[737, 2442, 2328, 1075, 1892, 2446]. log-concave [1075, 1892, 2446].
Log-Normal [737]. Logarithm [2831, 2655, 2169, 3373, 244, 2801].
log-concave [1075, 1892, 2446]. Logistic [3266, 3000, 2040, 3150].
logspace [1369, 1638]. logspace-hard [1369]. Lois [780]. Long
[3550, 877, 1859, 1463, 1753, 2368, 3181, 437, 2465, 1805, 1353, 1952, 1282, 3477,
2966, 1301, 2606, 2685, 1918, 2027, 2939, 684, 2675]. log-concave [1075, 1892, 2446]. Log-Normal [737]. Logarithm [2831, 2655, 2169, 3373, 244, 2801].
Log-concave [1075, 1892, 2446]. Long-Cycle [2606, 2685]. Long-Period
[877, 3181, 1952, 2966, 1472, 750, 2299, 2636, 1918, 2027, 2939, 684, 2675].
Log-Normal [737]. Logarithm [2831, 2655, 2169, 3373, 244, 2801].
Log-concave [1075, 1892, 2446]. Long-Cycle [2606, 2685]. Long-Period
[877, 3181, 1952, 2966, 1472, 750, 2299, 2636, 1918, 2027, 2939, 684, 2675].
Long-Range [2368, 1463, 1753, 1301, 1387]. Low-Dimensionality [2807]. Low-Discrepancy [2615, 2147, 2324, 1539, 1846, 1214, 1345, 1710, 876, 1644, 2912, 2461, 2710, 1709, 3534, 2055].
Low-Dimensional [1748, 2069]. Log-Normal [737]. Logarithm [2831, 2655, 2169, 3373, 244, 2801].
Log-concave [1075, 1892, 2446]. Low-Dimensionality [2807]. Low-Discrepancy [2615, 2147, 2324, 1539, 1846, 1214, 1345, 1710, 876, 1644, 2912, 2461, 2710, 1709, 3534, 2055].
low-cost [3581, 3437]. Long-Degree [3298]. Low-Degree [3298]. low-dimensional [1748, 2069].
Low-Dimensionality [2807]. Low-Discrepancy [2615, 2147, 2324, 1539, 1846, 1214, 1345, 1710, 876, 1644, 2912, 2461, 2710, 1709, 3534, 2055].
Low-Dimensional [1748, 2069].
Marginals [2508]. margins [2248]. Mark [3760]. Markov

Nonparametric [654, 541, 1131, 1676, 2693, 3406, 3508, 3509, 289].
nonprobabilistic [1583]. nonrandom [608]. Nonrandomness [3337, 1329].
Nonrecursive [535, 3138, 2675]. nonskewed [1220]. nonsuccessive [2667].
Nonuniform [962, 2970, 2895, 1186, 2766, 2816, 2817, 2894, 758, 1819, 3495].


Phenomena

Physics

Pseudo

Pseudo-aléatoire

Pseudo-aléatoires

Pseudo-disturbance

Pseudo-Inversen

Pseudo-Casuali

Pseudo-Random
2717, 2995, 1804, 3679, 2719, 2997, 1512, 3525, 3204, 984, 3681, 2145, 638, 850, 1012, 1100, 1215, 1216, 1267, 1346, 1347, 1349, 1428, 1517, 1519, 1711, 1712, 1810, 1923, 2031, 2474, 2475, 2476, 2559, 2560, 2561, 2656.
pseudorandom
[2862, 3102, 1715, 3310, 3311, 3313, 599, 3583, 3650, 1611, 513, 2039, 814, 942, 449, 1933, 1103, 1614, 1434, 1731, 1951, 2877, 1735, 2586, 910, 3542, 3128, 3129, 3350, 2060, 482, 690, 2168, 1547, 2065, 2066, 2170, 2347, 2424, 1956, 2881, 3022, 2675, 231, 788, 1552, 1959, 3396, 3235].
pseudorandom-number
[2593].
Pseudorandomness
[2885, 2174, 3261, 3487, 703, 2619, 2443, 3507, 2451, 2532, 2627, 2534, 2544, 2134, 3300, 2473, 1605, 2588, 2503, 2081, 2378, 3020, 2673, 2072].
pseudozufallsvektoren [1319]. Pseudozufallszahlenfolgen [605].
psevdosluchainykh [345].
PSI [1391].
PUB [1814].
Publications [259, 388].
Publicly [3048].
PUF [3706].
Public-Key [887, 2448, 2482].
Public-Key [887, 2448, 2482]. Public [2267, 887, 2448, 1925, 2482, 3184, 2386].
Public-Key [887, 2448, 2482].
punched [35].
punctured [3647].
Pure [3701].
purposes [1053].
purposes [2853].
PVT [3336]. PVT-variation [3336]. pW [3270].
pyramids [1425]. Python [3614, 3515, 2315, 2316].
Quadrature [890, 765, 712, 1011, 390, 2445]. Quality [2083, 3392, 1780, 2628, 3638, 2020, 1062, 3016, 3124, 2880, 3144, 3254, 1861, 2515, 1890, 1894, 2118, 3082, 3192, 1912, 3434, 1919, 590, 2407, 2408, 2419, 2493, 2881, 2883].
Quantitative [3032, 719, 3893, 3618]. quantity [225]. Quantum [3362, 3363, 3473, 2747, 3367, 3386, 3039, 3605, 3277, 3699, 1583, 3074, 3291, 3511, 3577, 3518, 3680, 1936, 3443, 3623, 518, 2577, 3011, 3454, 3019, 3239, 3247, 3474, 3262, 3560, 371, 3055, 3562, 3698, 3285, 3287, 2452, 3420, 3073, 11, 3523, 3582, 3322, 3333, 2734, 2490, 3220, 3457, 3226, 3230, 3543, 3463, 2957, 3237].

récursifs [2585]. recursion [1476, 975, 13]. Recursions
[2982, 2021, 2022, 1971, 1920]. Recursive [2598, 2361, 3050, 3493, 3494, 1567,
2833, 2380, 3415, 2389, 2458, 3616, 2852, 585, 2146, 2804, 527, 3478, 3042,
3151, 2825, 3051, 3161, 1246, 622, 2220, 2221, 2300, 3421, 2845, 2988, 1793,
2127, 2129, 2228, 2306, 2031, 2033, 3115, 1732, 2584, 2667, 2668, 2738, 2739,
2873, 2875, 2954, 2955, 3222, 3339, 3341, 3459, 2585, 3133]. recursively [621].
recycle [1401]. Redefining [3442]. Rédei [3060, 2997]. Redondo [3848].
Reduced [112, 2528, 2652, 1114, 566, 2822, 1136, 1137]. reduced-round [2822]. reducible [1831]. Reducing [2433, 2121]. reduction [3413, 3414, 3290, 3493, 3494, 1567,
2833, 2380, 3415, 2389, 2458, 3616, 2852, 585, 2146, 2804, 527, 3478, 3042,
3151, 2825, 3051, 3161, 1246, 622, 2220, 2221, 2300, 3421, 2845, 2988, 1793,
2127, 2129, 2228, 2306, 2031, 2033, 3115, 1732, 2584, 2667, 2668, 2738, 2739,
2873, 2875, 2954, 2955, 3222, 3339, 3341, 3459, 2585, 3133]. recursively [621].
recycle [1401]. Redefining [3442]. Rédei [3060, 2997]. Redondo [3848].
Reference [2079, 3171]. Refutation [2928]. Regarding [2876, 1229].
Regency [3839, 3913]. Regenerative [1968, 886, 889]. REG [3713].
region [1414]. Regional [3785, 3401, 3796]. Regions [1107]. Register
[1180, 1297, 1078, 1003, 2904, 403, 1489, 2459, 631, 633, 845, 477, 3439, 3540,
1538, 2353, 2356, 1239, 3046, 1472, 703, 1005, 2217, 978, 3432, 1595, 1698,
2017, 1267, 1348, 1518, 3620, 1725, 2049, 1034]. Registers
[2510, 505, 1527, 3119, 3344, 2670, 1679, 2011, 328, 305, 1104]. Regression
[1684, 3049, 723]. Regular [3260, 3599, 3659]. Regularities [475, 509].
Regularity [2839, 3173]. Regularly [3585, 2976]. Rehearsal [3024].
Reinfall [2376]. Reingold [3617, 2575]. Rejection
[1474, 435, 1394, 1779, 1891, 2006, 2116, 1092, 2016, 819, 784, 1836, 3660, 992,
2817, 3695, 751, 1781, 2984, 3505, 1496, 980, 1007, 2641, 1061, 823].
Rejection-inversion [2116]. Rejoinder [918, 857]. Rekursion [975].
rekursiv [621, 622]. rekursiv-erzeugte [622]. Related
[1840, 3255, 325, 766, 872, 1860, 1383, 2771, 905, 947]. Related-Key [3255].
Reliable [2961, 2892, 3317, 3596]. Remainder [531, 104, 105, 1268, 2666].
Remark [266, 1080, 1081, 374, 1138, 839, 2706, 470, 303, 252, 1152, 679, 385,
601, 606, 1019, 785, 1226, 1387, 1671, 1080, 1081, 748, 1138, 839, 1152, 785].
Remarks [313, 877, 194, 247, 1801, 1346, 414, 1834, 3170, 2050]. removal
[2217]. Renaissance [3825]. rendering [3539]. rendus [3721].
renormalization [757]. Rényi [398]. Repeatable [507, 508]. Repeating
[2695, 222]. Repetition [2906, 2833, 2142]. Repetitions [1938].
Replacement [2016]. replica [3658]. replica-exchange [3658]. replication
[994]. Reply [2518, 1492, 651]. Report [1745, 3323, 103]. Representation
[2224, 943, 1852, 663, 270, 1434, 648, 1731, 690]. Representations
[1849, 1555]. Reprise [2936]. reproducibility [1248]. Reproducible
Requirement [2684]. Requirements [2564, 3639]. Requires [3503].
requiring [2702]. rescaled [2286]. Research

sanners [1750]. Samples
[1181, 1938, 1945, 8, 827, 64, 73, 17, 39, 134, 33, 230]. Sampling
[561, 653, 915, 1116, 1960, 3489, 830, 1243, 1458, 2098, 269, 741, 742, 1083,
1474, 702, 48, 837, 1196, 500, 3609, 24, 3417, 2006, 1327, 1403, 3669, 842, 1911,
2313, 844, 3619, 1, 643, 856, 857, 858, 609, 161, 1167, 100, 613, 960, 1286, 1364,
3592, 2071, 867, 12, 1559, 237, 149, 42, 2976, 575, 576, 116, 65, 73, 74, 2219,
94, 155, 3290, 25, 30, 31, 1333, 3424, 2463, 1695, 1097, 157, 281, 27, 2326, 550,
257, 187, 1272, 2491, 2737, 958, 12, 1559, 237, 149, 42, 2976, 575, 576, 116, 65,
73, 74, 2219, 94, 155, 3290, 25, 30, 31, 1333, 3424, 2463, 1695, 1097, 157, 281,
27, 2326, 550, 257, 187, 1272, 2491, 2737, 958, 121, 368, 9, 106, 208, 135, 2063,
3022, 69, 28].
Samuel [3886]. San [3877, 3900, 3766, 3812, 3892, 3857, 3837, 3861]. Santa
[3719, 3807, 3879]. SAR [3860]. Satisfied [406, 542]. Satisfying
[406, 542]. Satisfy [1311, 3211, 450, 13]. Satiety [517, 452, 13]. Saturday
[3869]. Saturday-Wednesday
[3869]. Saunders [3086]. Savage [2464]. SC'11 [3904]. Scalable
[3161, 3196, 3711, 3563, 2778, 2468, 2469, 2268, 3084]. Scale
[2171, 3716, 766, 185, 10, 2963, 14, 1664, 95, 1423, 2143, 1052].
Scale-sensitive [2171]. Scaling [2245, 3229]. Scan [3432]. Scan-based
Schedules [652]. scheduling [1790, 3308]. schemata [2590].
schemata-based [2590]. Scheme [3259, 1930, 2957, 3300, 772, 1611, 3447].
Schemes [1768, 2473, 722, 1168, 1400, 2314, 157]. Schnorr [1529]. School
[2754, 3737, 629]. School-Based [2754]. Schwinger [2263]. Sci [1038].
Science [3740, 3851, 3745, 3733, 3743, 3746, 3749, 3764, 3769, 3755, 3781,
3791, 3814, 3823, 3827, 3848, 3852, 3898, 3913, 3905, 3755, 3747, 3802, 3875,
3880, 3866, 3735, 3770, 3771, 3753, 3846, 3834, 3865, 3734, 3535, 3793].
siences [3856]. Scientific
[3728, 2892, 1121, 3727, 1139, 1722, 2487, 3803, 3171, 2715, 3816, 3732].
Scientists [625, 274, 1199]. scores [428]. Scrambled [3206, 3684, 3113].
Scrambling [2361]. scramblings [2725, 3709]. screening [3221, 2584].
scroll [3149, 3178]. SEAC [89]. SEAL [2614]. Search
[3493, 969, 1391, 3611, 811, 907, 908, 2606, 3051, 2515, 926, 2913, 707, 1336,
1793, 1512, 2802, 2582, 3458, 3459]. Searches [2610, 2220, 1414]. Searching
[2845, 2804]. Seattle [3772, 3904]. secant [1754]. Second
[3716, 3759, 30, 3853, 3003, 860, 3828, 3777, 3845, 3222]. Second-level [3003].
second-order [3222]. Secondary [2880]. Secret [2823, 1275, 2423]. Secure
[3372, 2680, 3255, 1452, 3486, 2108, 2531, 2632, 3075, 3641, 3094, 3013, 1111,
1166, 2677, 3634, 3418, 1400, 2298, 1334, 3089, 3318, 3106, 2944, 2335, 1275,
3543, 2676, 1845]. Securely [3680]. sécuritaire [1845]. Security
[3839, 3375, 3663, 2365, 1866, 2827, 3169, 3499, 2694, 2762, 2627, 3871, 2556,
2722, 2564, 3307, 3649, 3583, 1529, 3114, 2953, 2803, 3817, 3837, 3710, 3906,
2082, 2967, 3779, 3430, 1419, 772, 3204, 3209, 3215, 2870]. Seed
[3688, 2361, 3231, 1120, 2449, 1725, 3347, 3415]. Seeding
[1315, 2321, 3548, 976, 3319]. Seeds [2715, 3763, 1205, 3216]. seeming [2567].
Segmentation [1741, 2926]. Select [2509]. Selected
[3847, 636, 3876, 3878, 2203, 3870, 2864, 1225, 3878]. Selecting [1205].
Selection
Selective [44]. Self
self-adaptive [3446]. self-assembly [3693]. Self-Avoiding
Self-Excited [3044]. Self-Similarity [3875]. self-test
Self-testing [3538]. selfish [3067]. Semi
Spectrum [2837, 3298, 3654]. Speed
[2354, 3181, 3671, 634, 3315, 3212, 100, 3467, 3240, 3631, 2683, 3055, 3167,
2759, 3281, 1681, 117, 2126, 128, 2462, 771, 225, 550, 1161, 2868, 121].
Speedy [1621]. Sphere [194, 199, 586, 1540, 1110, 423]. Spheres
[203, 1141, 3232, 267]. Spherical [336, 337]. Spherically [167]. Spin
[3484]. spongy [3621]. sponsored [3728, 3735]. Spontaneous [3352].
Spooler [2043]. Spreading [3635, 3183]. spreadsheet [2788]. Spritz [3621].
SRPN [2268, 2468, 2469]. sprout [3216]. Square
[801, 43, 384, 3306, 1663, 1664, 2523, 93, 1587, 3085, 87]. squared
[1321, 1143]. Squarefree [2898]. squares [1405, 159]. squaring [1278].
Squeeze [855, 954, 806, 1061]. SR [3589]. SRAM [3185]. SRS [1898]. SRU
[592]. SSE2 [3374]. St [3781]. Stability [314, 1768, 670, 388, 2177, 2537].
Stable [738, 3417, 2450, 2915, 2385, 1237, 3162, 1351]. Stack [2797]. STACS
[3755]. Stage [1071, 3400, 157]. staircase [1706, 1835]. Standard
[1457, 3491, 1385, 2448, 1814, 3648, 3537, 792, 660, 1900, 1589, 1614, 2983,
3850, 2413, 2488]. Standards [90, 2482, 165]. Stanford [3833]. Star
[2896, 2916, 3009, 3117, 3217, 3010, 3451]. Start [568, 3206]. Start-Up [568].
STATCOM [3044]. State
[1069, 3185, 2996, 118, 3016, 1172, 3694, 3274, 1907, 1908, 3739, 132, 3471].
state-of-the-art [3739]. State-transition [3016]. States
[3277, 2142, 3523, 3582, 3333]. stationary [795]. Stationary
[344, 670, 763, 2987, 2537, 3104, 3314]. Statist [1237, 1038, 1007, 674, 675].
Statistic [126, 924, 1080, 815, 1234, 1194, 1587, 1010]. Statistical
[871, 2961, 2506, 793, 696, 828, 1655, 921, 2189, 999, 569, 493, 1763, 2280, 924,
1079, 1080, 1081, 23, 46, 72, 113, 114, 169, 170, 1002, 1195, 1313, 836, 541,
1131, 1676, 2693, 3406, 1392, 747, 748, 2621, 2834, 1134, 972, 2698, 495, 3182,
753, 407, 242, 1138, 839, 1039, 1201, 1899, 934, 2768, 628, 2305, 3671, 763,
2550, 3905, 1600, 2396, 1152, 86, 2563, 777, 850, 1012, 1147, 1519, 3530, 282,
720, 2570, 2571, 2485, 820, 859, 2337, 2412, 2414, 2415, 2416, 3338, 3707, 1438,
2167, 785, 1021, 1113, 1226, 960, 3722, 3373, 3478]. statistical
[1292, 1643, 2181, 2182, 2597, 3257, 234, 3272, 1756, 883, 1874, 2609, 833, 2286,
345, 3742, 1324, 3570, 1254, 2299, 3726, 2846, 2547, 1702, 2397, 2648, 2788, 2859,
3095, 1267, 3732, 1103, 1356, 2403, 2797, 387, 2584, 3627, 207, 959, 1958, 458].
Statistically [837, 842, 844, 856, 857, 858, 3650]. statisticheskii [345].
Statisticians [3736]. Statistics [1961, 3722, 795, 3166, 2608, 3740, 2899,
1767, 3745, 3911, 2209, 3742, 623, 3733, 53, 682, 524, 289, 3770, 3771, 3736,
3753, 3729, 213, 3768, 3863, 2697, 1135, 1321, 2626, 511, 3097, 1222, 2338].
STATLIB [1438]. Steady [1907, 1908]. Steady-state [1907, 1908]. Steady-state
[3556]. Stein [2366]. Step [3004, 1100, 1349]. steps [492]. Stern [2823]. Still
[353]. Stimulated [336]. STOC [3867, 3877, 3881, 3914]. STOC’12 [3907].
1389, 2130, 774, 1012, 513, 1616, 1620, 557, 649. Tb [3576]. TDIST [2810].
TEA [2822, 2528, 2623, 2624, 2701, 2765, 2652, 2238, 2067]. Teach [2684].
Teaching [3166, 3070]. Technical
[2079, 2005, 1801, 2715, 2046, 3828, 3844, 3640, 236, 318, 402, 399].
Technique [1394, 2006, 807, 3461, 992, 74, 2702]. Techniques
[3752, 3384, 3389, 3762, 2362, 1861, 269, 2632, 1503, 2715, 636, 3029, 3758,
463, 544, 155, 1544, 3469, 99]. Technology [2268, 3733, 3903, 3885, 3834].
Teil [519, 520]. Telegraphic [1796]. Temperature [3218, 3452].
[3421, 2845, 2988, 2954, 3339, 3459]. terms [2221, 249, 1161]. termwise
[3225]. Terrain [2041]. TES [1602]. Test
[2263, 2506, 995, 126, 917, 918, 3385, 236, 2098, 493, 743, 2906,
747, 748, 2695, 2833, 142, 579, 2764, 1138, 930, 839, 1039, 933, 3574, 2768,
938, 939, 2927, 43, 1151, 2857, 2646, 1600, 119, 849, 1610, 3003, 1815, 3703,
3323, 946, 2570, 1818, 1062, 724, 2336, 2051, 3338, 1825, 3707, 2740, 2807,
3127, 3131, 785, 87, 865, 3248, 694, 3028, 731, 233, 2091, 2602, 315, 1752, 464,
1307, 1308, 1876, 2369, 1129, 116, 172, 404, 432, 3279, 92, 667, 2295, 1398,
1485, 3065, 222, 408, 2841, 2221, 2124, 2013, 2551, 2464, 3520, 2320, 2717].
test [1702, 3205, 1100, 1155, 1349, 1428, 3530, 2039, 45, 2797, 2798, 607, 2417,
1949, 2057, 2163, 2165, 2739, 3222, 1277, 1951, 50, 230, 28, 3028, 2837, 1582].
Test-Pattern [724]. tested [1855, 3285, 2300, 3644]. Testing
[2506, 2080, 2507, 1238, 3047, 1032, 1304, 1305, 2099, 2100, 2613, 798, 405, 3415,
840, 3286, 153, 1901, 223, 1690, 2543, 2639, 2924, 2992, 3516, 2552, 506, 1262,
1051, 2478, 3315, 1016, 2571, 3110, 2337, 2412, 2413, 2414, 2415, 2416, 2488, 610,
860, 1221, 2735, 1623, 2064, 1112, 825, 487, 2428, 456, 1642, 2969, 1861, 3163,
968, 740, 1764, 90, 91, 345, 3279, 200, 2129, 2308, 2991, 1910, 156, 158, 129,
599, 680, 339, 2866, 3538, 1822, 555, 49, 163, 910, 2422, 3715, 2065, 2349, 1025].
TESTRAND [1051, 968, 1032, 1304]. Tests
[654, 916, 62, 2093, 1655, 967, 618, 2204, 1392, 1478, 972, 198, 82, 3182, 22,
3080, 1684, 628, 2132, 2230, 2305, 2457, 2638, 766, 1799, 2137, 2644, 2563,
3208, 3003, 3530, 903, 173, 2572, 1222, 1223, 2425, 2501, 457, 427, 1644, 103,
3042, 41, 3272, 3604, 923, 1245, 1982, 2978, 239, 1993, 1195, 1313, 836, 1132,
1037, 116, 1134, 1322, 2913, 3570, 1201, 2119, 1898, 1143, 2769, 2227, 2228,
2309, 2539, 761, 2232, 762, 769, 2145, 850, 1012, 2241, 1717, 942, 3319, 2661,
519, 520, 1819, 607, 162, 2164, 2251, 2252, 2339, 2667, 959]. tests
[2742, 1954, 1955, 2062, 2132, 2018, 973]. TESTU01
[2931, 2543, 2639, 2991, 2924, 2992]. Texas [3745, 3837, 3750]. Texture
[789, 929]. Textured [1741]. theatres [1219]. thefts [3561]. Their
[500, 2632, 2457, 2550, 1023, 3, 3496, 1867, 1579, 3698, 3882, 3870, 2217, 3186,
438, 439, 1606, 2476, 3008, 364, 147, 3454, 2676]. Theme [3771]. Theorem
[1373, 2631, 105, 3474, 235, 1036, 3412, 3287, 32, 3435, 3643, 409, 2721, 3100,
639, 1159, 2338, 2666, 1236, 2519, 2932, 2801]. theorem-based [3412].
Theorems
[1961, 3259, 2090, 71, 349, 588, 2152, 2659, 680, 564, 1470, 63, 640, 188, 3465].
Truly...
uniform
[1223, 2956, 3017, 3589, 910, 5, 1833, 2674, 3271, 2983, 2922, 419, 1274].
uniform-Gaussian [2218].
uniformément [1223, 2956, 3017, 3589, 910, 5, 1833, 2674, 3271, 2983, 2922, 419, 1274].
Uniformity [1163]. Uniformly [2084, 967, 841, 2638, 483, 2903, 2552, 2141, 1100, 1824].
Uniformization [1163]. Uniformly-distributed [176]. Uniforms [1891, 2120, 1625, 1361, 1890, 2121, 2463, 1537].
Unimodal [1074, 2191, 1097]. Unique [3277, 1335, 3134]. unit [423].
Univariate [1044, 501, 1897, 2548]. Universal [2817, 2096, 1323, 2549, 2640, 1165, 690, 1440].
universe [3910]. University [2640]. UNIX [3817]. Unknown [2266, 1179, 766, 38, 983].
unleash [2718]. unperceivable [2264]. Unpredictability [2386]. Unpredictable [1173, 3455, 2379, 1416, 3436].
USA [3862, 3867, 3877, 3831, 3807, 3840, 3882, 3849, 3853, 3879, 3816, 3843, 3805, 3819, 3891, 3900, 3907, 3914, 3773, 3869, 3740, 3852, 3898, 3913, 3871, 3850, 3854, 3803, 3817, 3818, 3844]. usable [3383, 1697]. Usage [3652, 1933].
Usenix [3844]. User [2543, 2639, 2992, 2129, 2732]. user-level [2732]. users [2930].

V [2090, 487, 2470, 599, 3725]. v. [239]. VA [3805, 3803, 3854, 2044].
Vacuum [3277, 3333]. Valentin [2090]. valeurs [2132]. Validating [2711].
Pearson:1900:CGS

[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


57(??):228–240, 1937. CODEN PRSEAE. ISSN 0080-4541 (print), 2053-5902 (electronic).


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

on the development and practice of science and engineering in the 20th Century.” See [2429, 2430], and the Hasting–Metropolis generalization in [500]. See also [342, 643, 2703].


[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].
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 × 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


[164] C. B. Tompkins. Machine attacks on problems whose variables are permutations. In Curtiss [3719], pages 195–212. LCCN 0???


vonHoerner:1957:HZR


Walsh:1957:EMO


Bass:1958:MMC


Bauer:1958:MCM


Bendat:1958:PAR


Bofinger:1958:PPP


Box:1958:NGR

REFERENCES


Sengupta:1958:TRN


Sobol:1958:PRN


Thomson:1958:MCM


Bolshev:1959:TRV


Cashwell:1959:PMM


Cook:1959:RRP

Ehrlich:1959:MCS

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

Golenko:1959:DCS


Golenko:1959:FRN


Green:1959:ETA


Hicks:1959:EMG


IBM:1959:RNG


Lehmer:1959:CPD


Muller:1959:CMG

Muller:1959:NMG


Page:1959:PRE


Schulz-Arenstorff:1959:PDP


Sterzer:1959:RNG


Thomson:1959:EMS


Tippett:1959:RSN


Zierler:1959:LRS


Bazley:1960:AMC

REFERENCES


REFERENCES


[230] Donald D. Wall. A random number test for large samples. In Anonymous [3722], pages 7–11. LCCN ???.

REFERENCES


REFERENCES


REFERENCES


REFERENCES


MendesFrance:1962:CMF
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


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


Marsaglia:1964:RVC


Marsaglia:1964:SPIa


Marsaglia:1964:SPIb


Onicescu:1964:NSA


Poore:1964:CPG


Sobol:1964:PPR


Stockmal:1964:CPR

REFERENCES


REFERENCES


Pike:1965:ARN


Pike:1965:CAGb


Potter:1965:CNS


Pyke:1965:S


Reeves:1965:AUR


Rosenberg:1965:CNN


Scheinok:1965:DFR


Seshadri:1965:RVW

REFERENCES


REFERENCES


References


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[408] G. Itzelsberger. Some experiences with the poker test for investigating pseudorandom numbers. In Hollingdale [3727], pages 64–68. LCCN QA76.5 D55 1965.


REFERENCES


REFERENCES


REFERENCES


the hyperplane problem that linear congruential generators suffer from, although careful choice of multipliers can minimize its importance: see [397, 2194, 2193, 2439].


REFERENCES

Muller:1968:RN


Pillai:1968:NEI


Polljak:1968:APN


Show:1968:AGR


Sibuya:1968:GDE


Snow:1968:AGR


Whittlesey:1968:CCB


Zaremba:1968:GLP

REFERENCES

136

Zaremba:1968:MBM


Beasley:1969:DTS


Bell:1969:DFT


Chaitin:1969:LPC


Coveyou:1969:RNG

[459] R. R. Coveyou. Random number generation is too important to be left to chance. In Anonymous [3728], pages 70–111. LCCN QA1 S565 v. 3.

Cunsolo:1969:CNP

REFERENCES


REFERENCES


[469] 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).


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Subrahmaniam:1970:SAM


Vincent:1970:CGT


Vincent:1970:GTR


White:1970:FDC


Zaremba:1970:DI1


Ashford:1971:BRG


Beyer:1971:LSM

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Elias:1972:ECU

Ermakov:1972:NPSa

Ermakov:1972:NPSb

Everett:1972:MCS

Falk:1972:EDT

Forsythe:1972:NCMa

Forsythe:1972:NCMb

Frazer:1972:BOM
REFERENCES

Garside:1972:BRBa


Heathcote:1972:TGF


Hurst:1972:AAG


Kirschenmann:1972:CR


Kral:1972:ENA


Kral:1972:NAP


Maddocks:1972:CAG


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


Majithia:1972:CFD


Marsaglia:1972:CPS


Marsaglia:1972:SLC


Mason:1972:LTN


Mihram:1972:SV


Miyatake:1972:GUR


Nance:1972:BRN
REFERENCES


REFERENCES


Ahrens:1973:EFM


Ahrens:1973:NME


Burford:1973:BAC


Diaconis:1973:LMI

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

Dieter:1973:CMG


Durbin:1973:DTT

REFERENCES


REFERENCES

SMJCAT. ISSN 0097-5397 (print), 1095-7111 (electronic). See erratum [669].


REFERENCES


REFERENCES


REFERENCES


[666] Richard A. Handelsman and John S. Lew. Asymptotic expansion of Laplace convolutions for large argument and tail densities for certain


[676] 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


David Michael Fellows. Comments on “A general Fortran emulator for IBM 360/370 random number generator ‘RANDU’”. Technical report 6,


REFERENCES


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

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


REFERENCES


REFERENCES

Brent:1976:ABE

[736] R. P. Brent. Analysis of the binary Euclidean algorithm. In Traub [3735], 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 [2432] for an update, and a repair to an incorrect conjecture in this paper. See also [2358], where the worst case complexity is shown to be $O(\log N)$, and the number of right shifts at most $2 \log(N)$.

Chamayou:1976:DAG


Chambers:1976:MSS


Claustiaux:1976:GCN


Enison:1976:PTB


Fishman:1976:SGD

REFERENCES


REFERENCES


REFERENCES


REFERENCES


vanDooren:1976:AAN


Wallace:1976:TRG


Wedderburn:1976:SAR


Williams:1976:PRS


Witsenhausen:1976:VBC


Zakharov:1976:ECS


Zucker:1976:TMT


Ahrens:1977:URN

REFERENCES


REFERENCES


REFERENCES


REFERENCES


[826] A. C. Arvillias and D. G. Maritsas. Partitioning the period of a class of m-sequences and application to pseudorandom number generation.
REFERENCES


REFERENCES


REFERENCES


[845] D. G. Maritsas, A. C. Arvillias, and A. C. Bounas. Phase-shift analysis of linear feedback shift register structures generating pseudoran-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Anonymous:1979:BRT]


[Anonymous:1979:BRT]


[Apostolopoulos:1979:IAN]


[Atkinson:1979:CGP]


[Atkinson:1979:CGP]


[Atkinson:1979:FSA]


[Atkinson:1979:FSA]


[Atkinson:1979:RDC]


[Atkinson:1979:RDC]


[Atkinson:1979:SAA]

REFERENCES


REFERENCES


Brown:1979:CPNb


Burford:1979:AVM


Cheng:1979:SSG


delJunco:1979:HLV


Edgell:1979:SCD


Good:1979:CCR

Hammersley:1979:MCM


Heidelberger:1979:CSS


Hellman:1979:MPK


Hill:1979:CPP


Iglehart:1979:RSI


Kahaner:1979:EAD


REFERENCES


REFERENCES


REFERENCES

Bentley:1980:GSL

Brown:1980:GFG

Davies:1980:SAA

Dempster:1980:CEA

Edgington:1980:RT

Farebrother:1980:SAA

Fishman:1980:NLR

Fishman:1980:SCM
[926] George S. Fishman and Louis R. Moore III. In search of correlation in multiplicative congruential generators with modulus \( 2^{-31} - 1 \). Technical


REFERENCES


Marsaglia:1980:GRV


O'Brien:1980:PIR


Peskun:1980:TTC


Petkovic:1980:RRV


Ribeiro:1980:MOS


Rice:1980:DQF


Rubin:1980:RAE

REFERENCES


[961] F. Battaglia. Riproduzione delle autocorrelazioni nei metodi di generazione di numeri pseudo-casuali normali. (Italian) [Reproduction of
autocorrelations in the generation of pseudorandom normal numbers].

1981. CODEN IBMJAE. ISSN 0018-8646 (print), 2151-8556 (electronic).

[963] I. Deák. An economical method for random number generation and a
normal generator. Computing: Archiv für Informatik und Numerik, 27
(2):113–121, June 1981. CODEN CMPTA2. ISSN 0010-485X (print),
1436-5057 (electronic).

[964] Luc Devroye. The computer generation of Poisson random variables.

[965] Luc Devroye. On the computer generation of random variables with a
given characteristic function. Computers and Mathematics and Applica-
tions, 7(6):547–552, 1981. CODEN CMAPDK. ISSN 0898-1221
science/article/pii/0898122181900389.

[966] Persi Diaconis and Mehrdad Shahshahani. Generating a random per-
mutation with random transpositions. Zeitschrift für Wahrschein-
CODEN ZWVGAA. ISSN 0044-3719. URL http://link.springer.com/
article/10.1007/BF00535457.

[967] Edward J. Dudewicz and Edward C. van der Meulen. Entropy-based tests
967–974, December 1981. CODEN JSTNAL. ISSN 0162-1459 (print),
REFERENCES

Dudewicz:1981:HRN


Fishman:1981:SCM


Friedman:1981:NPP


Gentle:1981:PCR


Grafton:1981:SAA


Green:1981:BRBa


Greenwood:1981:PFA


REFERENCES

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


Blum:1982:HGC


Crigler:1982:RCP


Devroye:1982:NAR


DiDonato:1982:FSP


Dykstra:1982:MLE


Faure:1982:DSA

REFERENCES


REFERENCES


REFERENCES


Reprinted in [1135, pages 238–242]. See also the extended 32-bit generator in [2958].


REFERENCES


[1034] Masanori Fushimi and Shu Tezuka. The $k$-distribution of Generalized Feedback Shift Register pseudorandom numbers. Communications of the
REFERENCES


Jennergren:1983:AMR


Kac:1983:WR


Kachitvichyanukul:1983:DUR


Keefer:1983:TPA


Lawrance:1983:SDP


Marsaglia:1983:RNG


Marsaglia:1983:RV1


Marse:1983:IPF

REFERENCES


REFERENCES

Purdy:1983:CFA


Ripley:1983:CGR


Ripley:1983:LSP


Rosenbaum:1983:RNG


Sakasegawa:1983:SRS


Savir:1983:NET

REFERENCES


REFERENCES

Brody:1984:RNG


Brown:1984:ETS


Cheng:1984:GIG


Devroye:1984:MGR


Devroye:1984:RVG


Devroye:1984:SAG


Devroye:1984:UPI

REFERENCES


[1083] George S. Fishman and Louis R. Moore III. Sampling from a discrete
distribution while preserving monotonicity. *The American Statistician*,
38(?):219–223, ???? 1984. CODEN ASTAAJ. ISSN 0003-1305 (print),
1537-2731 (electronic).

Pseudo-random trees in Monte Carlo. *Parallel Computing*, 1(2):175–180,
December 1984. CODEN PACOEJ. ISSN 0167-8191 (print), 1872-7336
(electronic).

[1085] A. M. Frieze, R. Kannan, and J. C. Lagarias. Linear congruential gener-
ators do not produce random sequences. In IEEE [3749], pages 480–484.
CODEN ASFPDV. ISBN 0-8186-8591-3, 0-8186-0591-X (paperback), 0-
IEEE catalog number 84CH2085-9.

26(?):502–512, ???? 1984. CODEN MCSIDR. ISSN 0378-4754 (print),
1872-7166 (electronic).

[1087] Daniel Guinier. Random numbers for stochastic simulation. *ACM SIG-
BIO Newsletter*, 6(4):5–6, March 1984. CODEN SINWDG. ISSN 0163-
5697 (print), 1557-9506 (electronic).

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

[1089] C. D. Heth. A Pascal version of a pseudorandom number generator. *Be-
havior Research Methods, Instruments, and Computers*, 16(6):548–550,
???? 1984. CODEN BRMCEW. ISSN 0743-3808 (print), 1532-5970
(electronic).
REFERENCES


Marsaglia:1984:FEI


Marsaglia:1984:GCM


Modianos:1984:RNG


Niederreiter:1984:PSP


Papoulis:1984:PRV


Paulsen:1984:IRN

REFERENCES

CEW. ISSN 0743-3808 (print), 1532-5970 (electronic). URL http://www.springerlink.com/content/a25j12g243u6566n/.

Ronse:1984:FSR


Scholtz:1984:GS


Schorr:1984:PLV


Smith:1984:EMC


Thesen:1984:SER


Tolleth:1984:SSM

REFERENCES


REFERENCES


REFERENCES


REFERENCES

Griffiths:1985:ASA


Helfrich:1985:ACMa


Helfrich:1985:ACMb


Hill:1985:SAR


Hurd:1985:NEM


Imai:1985:PNG

[1140] T. Imai and Masanori Fushimi. Pseudorandom number generators whose subsequences are multidimensionally equidistributed. *Transactions of
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Vitter:1985:RSR


Yashchin:1985:ADC


Afflerbach:1986:SLS


Anderson:1986:MMC


Anon:1986:IRN


Blum:1986:IUC

Blum:1986:SUP


Bowman:1986:SRN


Brown:1986:DFP


Celmaster:1986:MVR


Chandrasekaran:1986:IAR


Chernoff:1986:NSB


Clark:1986:BSP

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Shore:1986:AID

Shore:1986:SGA

Sowey:1986:TCB

Stephens:1986:TBE

Stephens:1986:TUD

Wolfram:1986:RSG

Wolfram:1986:TAC


[1232] Gh. Barbu. A new fast method for computer generation of gamma and beta random variables by transformations of uniform variables. Statist-


REFERENCES


REFERENCES


REFERENCES


REFERENCES


[1278] Wai Wan Tsang and George Marsaglia. A decision tree algorithm for
squaring histograms in random number generation. *Ars Combinatoria.*
???? ISSN 0381-7032.

of variates from arbitrary continuous distributions. *SIAM Journal on
SIJCD4. ISSN 0196-5204.

[1280] U. V. Vazirani. Strong communication complexity or generating quasi-
random sequences from two communicating semi-random sources. *Com-
binatorica*, 7(4):375–392, ???. 1987. CODEN COMBDI. ISSN 0209-9683
(print), 1439-6912 (electronic).


[1282] Brian A. Wichmann and I. D. Hill. Building a random-number generator:
A Pascal routine for very-long-cycle random-number sequences. *BYTE
Magazine*, 12(3):127–128, ???. 1987. CODEN BYTEDJ. ISSN 0360-
5280 (print), 1082-7838 (electronic).

[1283] Lothar Afflerbach and Holger Grothe. The lattice structure of pseudo-
random vectors generated by matrix generators. *Journal of Compu-
JCAMDI. ISSN 0377-0427 (print), 1879-1778 (electronic). URL http://
www.sciencedirect.com/science/article/pii/037704278890338X.

[1284] Lothar Afflerbach and Klaus Wenzel. Normal random numbers lying
237–244, December 1988. CODEN STPAE4. ISSN 0932-5026 (print),
REFERENCES


[1291] 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


Durst:1988:TPR

Edwards:1988:CAM

Eichenauer:1988:MLT

Eichenauer:1988:MLTb

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


REFERENCES


REFERENCES

Kleijnen:1988:ASE


Kolmogorov:1988:AR


Korin:1988:TRM


Kurosawa:1988:CSP


Lagarias:1988:UEP


LEcuyer:1988:BLP


LEcuyer:1988:EPC


REFERENCES


REFERENCES

Percus:1988:LRC


Petersen:1988:SVR


Reif:1988:EPP


Ripley:1988:UAS


Rockower:1988:IIR


Sezgin:1988:MOP


Shi:1988:SRP


REFERENCES


Eichenauer-Herrmann:1989:PLP


Eichenauer-Herrmann:1989:RLR


Evans:1989:PRN


Fushimi:1989:ERB


Fushimi:1989:RNG


Gilmore:1989:RSP


Gleason:1989:STI

REFERENCES


REFERENCES


**Impagliazzo:1989:ECS**


**Impagliazzo:1989:HRR**


**Impagliazzo:1989:PRG**


**Kachitvichyanukul:1989:ABS**


**Kahaner:1989:NMS**


**Kamps:1989:CPL**

[1405] U. Kamps. Chebyshev polynomials and least squares estimation based on one-dependent random variables. Linear Algebra and its Applications,
REFERENCES


REFERENCES


REFERENCES


REFERENCES


Mertsch:1989:PAS


Niederreiter:1989:STC


Paul:1989:IRN


Percus:1989:RNG


Pickover:1989:PRG


Reber:1989:PNG


Rhee:1989:OPIa

[1433] Wansoo T. Rhee and Michel Talagrand. Optimal bin packing with items of random sizes. II. SIAM Journal on Computing, 18(1):139–151, Febru-
Richards:1989:GRP


Sezgin:1989:EPC


Tezuka:1989:ALC


Tezuka:1989:RNG


Thomas:1989:SNL


Wang:1989:SMR


Wikramaratna:1989:ANM


Asada:1990:GCH


Ascheid:1990:GWD


Baccelli:1990:EPP


Bays:1990:CIR


Behboodian:1990:EUD


Bernstein:1990:SRN

REFERENCES


REFERENCES


[1465] H. Döring. Erzeugung normalverteilter Zufallszahlen mit 16-bit-PC. (German) |Generation of normally-distributed random numbers on an
REFERENCES  286


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

Macomber:1990:DUR


Marsaglia:1990:DBR


Marsaglia:1990:RNG


Marsaglia:1990:TUR


Maurer:1990:PLR


Micali:1990:EPR

Mitchell:1990:EEA


Mitchell:1990:NKG


Naor:1990:BCU


Naor:1990:SPS


Niederreiter:1990:CAP


Niederreiter:1990:LBD


REFERENCES

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

Palmore:1990:CAC


Parrish:1990:GRD


Ripley:1990:TPN


Roggeman:1990:VFS


Rozovskii:1990:PLD


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]. Dissertation (thesis), Université de Nantes, Nantes, France, 1990.
REFERENCES


REFERENCES


REFERENCES


Dunweg:1991:BDS


Eichenauer-Herrmann:1991:ASI


Eichenauer-Herrmann:1991:CCP


Eichenauer-Herrmann:1991:CIC


Eichenauer-Herrmann:1991:DIC


Eichenauer-Herrmann:1991:DQC


Eichenauer-Herrmann:1991:ICPa

Eichenauer-Herrmann:1991:ICPb


Eichenauer-Herrmann:1991:NIC


Geers:1991:HEB


Gerasimov:1991:NOH


Gupta:1991:PAT


Hultquist:1991:GRN


Ito:1991:PEU


REFERENCES


REFERENCES

[1615] 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


Agrawal:1992:PAS


Aluru:1992:RNG


Anastasio:1992:OCL


Anderson:1992:CRN


Arno:1992:SCS


Atkinson:1992:GBT


Babai:1992:MPP

Baker:1992:PPT


Bays:1992:IRN


Bellido:1992:SBR


Berdnikov:1992:RNG


Binder:1992:MCS


Bratley:1992:ITL

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Lawrance:1992:UDF


LeCuyer:1992:TRN


Lehn:1992:PNG


Leva:1992:ANR


Leva:1992:FNR


Lloyd:1992:CBF


Lo:1992:FCA

REFERENCES


REFERENCES


Szyszkowicz:1992:GRP


Tang:1992:SDA


Tezuka:1992:AAC


Tezuka:1992:FGL


Traub:1992:MCA


Tsai:1992:AFT

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Kalkuhl:1993:PDC


Kanellakis:1993:IDM


Kankaala:1993:BLC


Karloff:1993:FAA


Karloff:1993:RAP


Kepler:1993:RVM


REFERENCES


REFERENCES


[1815] 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 [1352, 1457, 1801, 1825]. The authors report that they would now recommend the MCG \( x_{n+1} = 48\,271x_n \mod (2^{31} - 1) \) over their original \( x_{n+1} = 16\,807x_n \mod (2^{31} - 1) \).


REFERENCES


REFERENCES

- Toral:1993:GGD

- Vattulainen:1993:IIP

- Wang:1993:URP

- Weber:1993:AIG

- Willemain:1993:MGA

- Winkler:1993:SRP


REFERENCES


REFERENCES

125, May 1994. CODEN ASTAAJ. ISSN 0003-1305 (print), 1537-2731 (electronic).


[1859] 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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Ritter:1994:EPR


Rivest:1994:DBI


Schneier:1994:AAd


Shallit:1994:ALS


Shukhman:1994:GQR


Sitharam:1994:PGL

REFERENCES


REFERENCES


Zhang:1994:PEE


Zijp:1994:UTC


Ahrens:1995:OTM


Al-Hussaini:1995:UPT


Anguita:1995:CDP


Antipov:1995:COP

REFERENCES


[1977] Asit Dan, Philip S. Yu, and Jen Yao Chung. Characterization of database access pattern for analytic prediction of buffer


REFERENCES

Eichenauer-Herrmann:1995:IUB


Eichenauer-Herrmann:1995:NPE


Eichenauer-Herrmann:1995:PNG


Eichenauer-Herrmann:1995:QCP


Eichenauer-Herrmann:1995:RCM


Eichenauer-Herrmann:1995:UAA


Kessler:1995:GOC


Koc:1995:RCS


Kubota:1995:DRE


Kurita:1995:DWD


Lee:1995:CSS


Leeb:1995:DT


REFERENCES


Ong:1995:CBG


Owen:1995:RPN


Palubeckis:1995:HBB


Pattanaik:1995:AER


Penrice:1995:AEP


Percus:1995:TAM


REFERENCES


REFERENCES


REFERENCES


[2066] Stefan Wegenkittl. Are there hyperbolas in the scatter plots of inversive 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


<table>
<thead>
<tr>
<th>Reference</th>
<th>Author(s)</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
</table>
REFERENCES


Beyer:1996:CLS


Bland:1996:SRN


Boppana:1996:BCP


Bromley:1996:QNG


Brunner:1996:PCO


Bryc:1996:BRB

REFERENCES


[2096] Martin Dietzfelbinger. Universal hashing and k-wise independent random variables via integer arithmetic without primes. Lecture Notes in
REFERENCES

Dodge:1996:NRN

Dodge: 1996: NRN


Dorfman:1996:PSR

Dorfman: 1996: PSR


Dwyer:1996:TRNa

Dwyer: 1996: TRNa


Dwyer:1996:TRNb

Dwyer: 1996: TRNb


Eichenauer-Herrmann:1996:ABC

Eichenauer-Herrmann: 1996: ABC


Eichenauer-Herrmann:1996:CIC

Eichenauer-Herrmann: 1996: CIC


Eichenauer-Herrmann:1996:EPI

Eichenauer-Herrmann: 1996: EPI

Jürgen Eichenauer-Herrmann. Equidistribution properties of inversive congruential pseudorandom numbers with power of two modulus.
REFERENCES


REFERENCES


[2122] Chiang Kao and J. Y. Wong. An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus


REFERENCES


REFERENCES


[2153] Igor Radović, Ilya M. Sobol, and Robert F. Tichy. Quasi-Monte Carlo methods for numerical integration: Comparison of different low discrep-


REFERENCES


REFERENCES


Ugrin-Sparac:1996:PET


Wallace:1996:FPG


Wang:1996:LIL


Wegenkittl:1996:RSP


Alon:1997:SSD

REFERENCES


REFERENCES


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


REFERENCES


Eichenauer-Herrmann:1997:QCP


Emmerich:1997:EPQ


Entacher:1997:ASP


Entacher:1997:CSP


Entacher:1997:PPL


Entacher:1997:PPP


Fishman:1997:MCC


REFERENCES


[2213] P. Hellekalek. Good random number generators are (not so) easy to find. In Troch and Breitenecker [3828], page ?? ISBN 3-901608-11-7. LCCN ???


REFERENCES


REFERENCES

Kreckel:1997:PAM


LEcuyer:1997:BLS


LEcuyer:1997:EBT


LEcuyer:1997:ILS


LEcuyer:1997:RNG


LEcuyer:1997:TBS


LEcuyer:1997:URN


[2234] 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.”.


[2236] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In IEEE [3827], pages 458–467. CODEN ASF-
REFERENCES


Woodward:1997:ECD


Wu:1997:MCR


Zubkov:1997:PTD


Aiello:1998:DPP


Andreev:1998:NGD


Antoch:1998:RPN

REFERENCES


REFERENCES


[2272] Paul D. Coddington and Sung-Hoon Ko. Random number generator for parallel computers. In Greg Egan, Richard Brent, and Dennis Gan-
REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Tanaka:1998:OLA


Tezuka:1998:FAM


Thomlinson:1998:NBP


Trotter:1998:RTS


Vallee:1998:CAB


Vallee:1998:DBE


vanHameren:1998:GLD

REFERENCES


REFERENCES


REFERENCES


Goldreich:1999:IDB


Goldreich:1999:MCP


Gonzalez:1999:RNG


Griffin:1999:DNR


Haastad:1999:PGO


Intel:1999:IRN


Jun:1999:IRN

[2383] Benjamin Jun and Paul Kocher. The Intel random number generator. White paper prepared for Intel Corporation, Cryptography Re-


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


MRaihi:1999:CAR


Muller:1999:CRV


Niederreiter:1999:DLS


REFERENCES


REFERENCES

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


REFERENCES


[2426] 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


[Balazs:2000:ONC]


[Beichl:2000:MA]


[Borkowf:2000:BRB]


[Brent:2000:TYA]


[Chen:2000:RRI]

REFERENCES


REFERENCES

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

[Hickernell:2000:ELS]


[Hormann:2000:AAG]


[Hormann:2000:ARV]


[Impagliazzo:2000:EPR]


[Indyk:2000:SDP]

REFERENCES


REFERENCES


[2465] George Marsaglia. The monster, a random number generator with period over $10^{2857}$ times as long as the previously touted longest-period one. Technical report ????, Florida State University, Tallahassee, FL, USA, ???. 2000.


REFERENCES


REFERENCES


REFERENCES


Agrawal:2001:HSP


Alexander:2001:AMC


AlOsh:2001:SAG


Arvind:2001:PRB


Bailey:2001:RCF


Banks:2001:DES

REFERENCES


Crandall:2001:PNC


Cryan:2001:PGN


Entacher:2001:EOR


Entacher:2001:ORN


Entacher:2001:PQ


Faure:2001:VS


Fernandez:2001:RCA

REFERENCES


Fischer:2001:CLT


Fischer:2001:TRN


Folegati:2001:CLR


Gerosa:2001:FIB


Gonsalves:2001:PAS

The program contains code (near the end) for the portable ran\_nu() 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


Hernandez:2001:FNO


Hernandez:2001:GAC


Howgrave-Graham:2001:PRN


Iwata:2001:PAF


Johnson:2001:CCO


Kang:2001:PMT

[2534] Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseu-
dorandomness of MISTY-type transformations and the block ci-
REFERENCES


REFERENCES


REFERENCES


REFERENCES

www.rand.org/content/dam/rand/pubs/monograph_reports/2005/
digits.txt.zip; http://www.rand.org/pubs/monograph_reports/
MR1418.html. See also [146].

[2570] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker,
Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heck-
ert, 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,
csrc.nist.gov/rng/sts-1.5.tar; http://csrc.nist.gov/rng/
www.cs.sunysb.edu/~algorith/implement/rng/distrib/SP800-22b.pdf;

DEN TPRBAU. ISSN 0040-585X (print), 1095-7219 (electronic). URL

[2572] W. Schindler. Efficient online tests for true random number gener-
CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).
URL http://link.springer-ny.com/link/service/series/0558/
bibs/2162/21620103.htm; http://link.springer-ny.com/link/
service/series/0558/papers/2162/21620103.pdf.

FPGA implementation of neighborhood-of-four cellular automata ran-

[2574] Ronen Shaltiel and Christopher Umans. Simple extractors for all min-
entropies and a new pseudo-random generator. In IEEE [3852], pages


REFERENCES


[2585] Renée Touzin. Des générateurs récursifs multiples combinés rapides avec des coefficients de la forme $\pm 2^p1 \pm 2^p2$. (French) [Fast combined multiple recursive generators of the form $\pm 2^p1 \pm 2^p2$]. 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


Futschik:2002:EFE


Gangnon:2002:MDE


Gennaro:2002:CPG


Gilbert:2002:NRP


Gleeson:2002:TRN


Golic:2002:SWM
REFERENCES


REFERENCES

Janke:2002:PRN


Jeruchim:2002:FRV


Jeruchim:2002:MCS


Jones:2002:KTP


Karras:2002:SPB

Kunchenko:2002:PPE

Kuo:2002:CCC

LEcuyer:2002:CEG

LEcuyer:2002:OOR

LEcuyer:2002:RAR

LEcuyer:2002:SST
LEcuyer:2002:TSL


Leydold:2002:ULU


Leydold:2002:VTD


Luo:2002:CGB


Marsaglia:2002:RGB


Marsaglia:2002:SDP

REFERENCES


REFERENCES


Niederreiter:2002:RAT


NIST:2002:ERN


Papoulis:2002:PRV


Philipp:2002:MTD


Pirsic:2002:SIN


Rukhin:2002:DNW


Shackleford:2002:FIN

[2662] Barry Shackleford, Motoo Tanaka, Richard J. Carter, and Greg Snider. FPGA implementation of neighborhood-of-four cellular automata ran-

Shparlinski:2002:DDH


Sugita:2002:RNI


Tan:2002:PPP


Tang:2002:CRN


Tang:2002:LBS


REFERENCES


[2679] 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


[2684] 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


Intel:2003:IRN


Joe:2003:RAI


Kocarev:2003:CPR


LEcuyer:2003:CGC


Lemieux:2003:RPL


Li:2003:ULD

[2710] 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-


xorshift generators and the well-understood linear feedback shift register generators. See also [3445, 3537, 3626] for the failure of Marsaglia’s xorwow() generator from this paper. See [2863, 3684] for detailed analysis.


REFERENCES


REFERENCES


Tu:2003:GRI


Umans:2003:PRG


Vavriv:2003:RNG


Al-Subaihi:2004:SCM


Alekhnovich:2004:PGP


Anonymous:2004:RNG


Anonymous:2004:TRR
REFERENCES


Mascagni:2004:PPM


Mauduit:2004:CPB


McCullough:2004:BRB


McCullough:2004:FSE


McIvor:2004:IIM


Mertens:2004:EPR

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Bogdanov:2005:PGL


Calvayrac:2005:RNG


Castro:2005:NRE


Contini:2005:SAA


Damgaard:2005:CRM

[2824] Ivan Damgård and Yuval Ishai. Constant-round multiparty computation using a black-box pseudorandom generator. *Lecture Notes in Computer...
REFERENCES


REFERENCES


REFERENCES

Hamano:2005:DSD

Hess:2005:LCM

Hill:2005:RDS

Horan:2005:NRN

Kang:2005:ETP

Keller:2005:NRR

Kemp:2005:PRN


REFERENCES


REFERENCES


[Niederreiter:2005:DSN]


[Niederreiter:2005:ESD]


[Panneton:2005:XRN]


[Redei:2005:JNS]


[Ryabko:2005:NTA]


[Ryabko:2005:UIT]


REFERENCES


REFERENCES


REFERENCES

Dickinson:2006:EEL

El-Mahassni:2006:DNC

Evans:2006:DOS

Faure:2006:SCR

Feige:2006:SIR

Finnigin:2006:CPN


Zvi Gutterman, Benny Pinkas, and Tzachy Reinman. Analysis of the Linux random number generator. Report, The Hebrew University of
Jerusalem and University of Haifa, Jerusalem and Haifa, Israel, March 6, 2006. 18 pp. URL http://www.pinkas.net/PAPERS/gpr06.pdf.


REFERENCES


REFERENCES


REFERENCES


Purczyński:2006:FGF


Rinehart:2006:PRN


Ripley:2006:SS


Rose:2006:CSP


Rubin:2006:EGE


Rybakov:2006:LES


Schanze:2006:EDT


Schmidt:2006:BRJ

[2948] Volker Schmidt. Book review: James E. Gentle: Random number
generation and Monte Carlo methods. Metrika. International Journal
for Theoretical and Applied Statistics, 64(2):251–252, October
1007/s00184-006-0089-0.

Schroeder:2006:RNG

287–292. Volume 7 of Springer Series in Information Sciences [3875],
fourth edition, 2006. ISBN 3-540-26598-8, 3-540-26596-1. ISSN 0720-
678X. LCCN QA241.

Sezgin:2006:DLP

CMPTA2. ISSN 0010-485X (print), 1436-5057 (electronic). URL http:
//www.springerlink.com/openurl.asp?genre=article&issn=0010-
485X&volume=78&issue=2&spage=173.

Simka:2006:MTR

random number generator aimed at cryptographic application. In IS-
CAS 2006: 2006 IEEE International Symposium on Circuits and Sys-
tems: Circuits and systems: at crossroads of life and technology: pro-
cedings: May 21–24: Kos International Convention Centre (KICC),
Island of Kos, Greece, pages 5619–5623. IEEE Computer Society Press,
1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 2006. ISBN
ieee.org/xpl/RecentCon.jsp?punumber=11145. IEEE catalog number
06CH37717C.

Skoge:2006:PHH

[2952] Monica Skoge, Aleksandar Donev, Frank H. Stillinger, and Salvatore
Torquato. Packing hyperspheres in high-dimensional Euclidean spaces.
Physical Review E (Statistical physics, plasmas, fluids, and related in-
terdisciplinary topics), 74(4):041127, October 2006. CODEN PLEEE8.
RECURSIVE PSEUDO-RANDOM NUMBER GENERATORS

Steinfeld:2006:PSE


Tang:2006:EAT


Tang:2006:TAF


Thomas:2006:NUR


Wang:2006:SQR


Wichmann:2006:GGP

generator [1021] developed for 16-bit arithmetic to a new four-part combination generator for 32-bit arithmetic with a period of $2^{121} \approx 10^{36}$.


Bhatnagar:2007:ANB


Brent:2007:SLP


Brown:2007:SAN


Cheung:2007:HGA


Chiu:2007:CKC


Cowles:2007:BRB

REFERENCES


[2976] Paul Dupuis, Kevin Leder, and Hui Wang. Importance sampling for sums of random variables with regularly varying tails. ACM Transactions on
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Nekrutkin:2007:AAO


Panditaratne:2007:TRN


Pareschi:2007:SLN


Pazo-Robles:2007:MPS


Perez:2007:RJI

REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Cordero:2008:DPV


Das:2008:ASS


Deng:2008:DIE


Deng:2008:ICS


Deng:2008:IRN


Drutarovsky:2008:CSC


REFERENCES


REFERENCES


REFERENCES

547

Katz:2008:RRNb


Kiessler:2008:BRBe


Killmann:2008:DPR


Kim:2008:TRG


Kolokotronis:2008:CPN


Langdon:2008:FHQ


[3088] 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


Uchida:2008:FPR


Udawatta:2008:TVN


Varbanets:2008:ESS


Varbanets:2008:ICGa


Varbanets:2008:ICGb


Walker:2008:EPN


Wang:2008:DCP

REFERENCES


Wikramaratna:2008:ACR


Willink:2008:UPN


Wold:2008:AER


Xiang:2008:NPR


Xu:2008:SMS

Yaguchi:2008:NNP


Yang:2008:NTR


Alhakim:2009:MSG


Anyanwu:2009:DCS


Awerbuch:2009:RRN


Aycock:2009:COU

Bastos-Filho:2009:IQR


Blacher:2009:FRN


Blacher:2009:PRN


Blaszczyk:2009:EVT


Blaszczyk:2009:HIP


Cao:2009:DSB

[3149] Fuqiang Cao and Shuguo Li. A double-scroll based true random number generator with power and throughput adjustable. In 2009. ASICON
REFERENCES


REFERENCES


[3167] Hassan M. Edrees, Brian Cheung, McCullen Sandora, David B. Nummey, and Deian Stefan. Hardware-optimized Ziggurat algorithm for
REFERENCES


Faure:2009:GHS


Feldhofer:2009:HIS


Fischer:2009:SRF


Galassi:2009:GSL


Gao:2009:MPL


REFERENCES


REFERENCES


REFERENCES


Ladd:2009:FRN


Langdon:2009:FHQ


Laracy:2009:RVG


LEcuyer:2009:LRN


Lee:2009:ERA


Lee:2009:HHA

[3196] JunKyu Lee, Yu Bi, Gregory D. Peterson, Robert J. Hinde, and Robert J. Harrison. HASPRNG: Hardware Accelerated Scalable Parallel Ran-
REFERENCES


REFERENCES

Paindaveine:2009:MRT


Pareschi:2009:PAC


Petrov:2009:SLL


Qiu:2009:CMW


Reidler:2009:USR


Ridout:2009:GRN

REFERENCES


REFERENCES

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


REFERENCES


REFERENCES

Umlauft:2009:GNS


vanMeel:2009:GFS


Verloop:2009:HTA


Volos:2009:IEP


vonzurGathen:2009:SSP


Wang:2009:NPR


REFERENCES

Yamanashi:2009:SRN


Youssef:2009:IEU


Yu:2009:ESC


Yuhua:2009:EDR


Zhu:2009:WFB


Abbott:2010:QRN

[3247] Alistair A. Abbott, Cristian S. Calude, and Karl Svozil. A quantum random number generator certified by value indefiniteness. Re-
REFERENCES


REFERENCES


[3259] A. A. Borovkov. Integro-local and local theorems on normal and large deviations of the sums of nonidentically distributed random variables in


REFERENCES


REFERENCES


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


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


Roper:2010:CRNb


Roper:2010:CRNc


Roper:2010:CRNd


Saiprasert:2010:MMM


Saiprasert:2010:OHA


Saito:2010:VMT


Segui:2010:AIP


REFERENCES


Tang:2010:BHA


Tang:2010:BLC


Tang:2010:OMR


Tarsa:2010:STR


Tavas:2010:IRN

REFERENCES


[3349] B. Valtchanov, V. Fischer, A. Aubert, and F. Bernard. Characterization of randomness sources in ring oscillator-based true random number


[3355] Hong Xin, Zhu Shujing, Chen Weibin, and Jian Chongjun. An image encryption base on non-linear pseudo-random number generator. In 2010
REFERENCES

Ying:2010:DRN


Yoo:2010:IRR


Yu:2010:NRN


Zafar:2010:GRN


Zhmurov:2010:EPR


Anonymous. Quantum random bit generator service. Project developed by Centre for Informatics and Computing, Ruđer Bošković Institute, Zagreb, Croatia, 2011. URL http://random.irb.hr/.


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.”


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


REFERENCES

Bustard:2011:QRB


Cai:2011:ADB


Carter:2011:TQS


Chan:2011:TRN


Chen:2011:ARN


Chevallier:2011:LSB


[3409] Parikshit Gopalan, Raghu Meka, Omer Reingold, and David Zuckerman. Pseudorandom generators for combinatorial shapes. In ACM [3900],


Malik:2011:EHI


Malik:2011:GHT


Marton:2011:PUR


Merhi:2011:SPR


Mohamed:2011:EAG

REFERENCES


[3445] 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. [3904], pages 16:1–16:12. ISBN 1-4503-0771-X. LCCN ????.


REFERENCES

Symul:2011:RTD


Tang:2011:ESG


Tang:2011:PES


Taylor:2011:DR


Veillette:2011:TCP


Versolatto:2011:MPR


REFERENCES


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

Becher:2012:TNN


Berger:2012:CPR


Bergman:2012:GRV


Bertoni:2012:KSF


Boldyreva:2012:NPG


Boureanu:2012:PFA


REFERENCES


REFERENCES


[3511] 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 [3457] for details.


[3516] 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


References


Troyer:2012:REQ


Vadhan:2012:CPS


Vazirani:2012:CQD


Walsh:2012:BRB


Wikramaratna:2012:CCI


Yalta:2012:CSR


REFERENCES


[3556] 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


REFERENCES


REFERENCES

Ma:2013:PQR


Malik:2013:UCB


Mascagni:2013:PPR


Meka:2013:PGP


Melia-Segui:2013:JPL


Miszczak:2013:EOQ

REFERENCES


Thomas:2013:LSF


Xi:2013:LTB


Abdul:2014:MGK


Anawis:2014:ARR


Anonymous:2014:CEF


Anonymous:2014:RNG

REFERENCES


[3601] Ching-Wei Cheng, Ying-Chao Hung, and Narayanaswamy Balakrishnan. Generating beta random numbers and Dirichlet random vectors
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[Passerat-Palmbach:2015:TSS]


[Pollack:2015:SNN]


[Potter:2015:MUE]


[Raitza:2015:RRN]


[Romano:2015:AGR]


[Sarkar:2015:FNR]


REFERENCES

Bayon:2016:FME

Chang-Fong:2016:CSC

Chattopadhyay:2016:ETS

deAndrade:2016:RNG

Dorre:2016:ELO

Guskova:2016:RPL
REFERENCES


REFERENCES

Journal of the ACM, 63(4):33:1–33:??, November 2016. CODEN JA-
COAH. ISSN 0004-5411 (print), 1557-735X (electronic).

[3681] Vladimir Nekrutkin. On the complexity of binary floating point pseudo-
random generation. Monte Carlo Methods and Applications, 22(2):109–
??, June 2016. CODEN MCMAC6. ISSN 0929-9629 (print), 1569-3961

[3682] NIST. SP 800-90B: Draft recommendation for the entropy sources used
for random bit generation. Web document, January 27, 2016. URL
http://csrc.nist.gov/publications/PubsDrafts.html#800-90B.

[3683] Naoto Ohsaka, Takuya Akiba, Yuichi Yoshida, and Ken ichi Kawarabayashi
Dynamic influence analysis in evolving networks. Proceedings of the
VLDB Endowment, 9(12):1077–1088, August 2016. CODEN ???
ISSN 2150-8097.

[3684] Sebastiano Vigna. An experimental exploration of Marsaglia’s xorshift
generators, scrambled. ACM Transactions on Mathematical Software, 42
(4):30:1–30:23, July 2016. CODEN ACMSCU. ISSN 0098-3500 (print),
1557-7295 (electronic). URL http://dl.acm.org/citation.cfm?id=
2845077.

[3685] Tomoyuki Yamakami. Pseudorandom generators against advised
context-free languages. Theoretical Computer Science, 613(??):1–27,
February 1, 2016. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-
article/pii/S0304397515009196.

[3686] Qiqing Yu and Junyi Dong. Generation of pseudo random numbers and
estimation under Cox models with time-dependent covariates. Journal
of Statistical Computation and Simulation, 86(14):2727–2739, 2016. CO-
DEN JSCSAJ. ISSN 0094-9655 (print), 1026-7778 (electronic), 1563-
5163.
Anonymous:2017:DAD

[3687] 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 [3694] for details of the attack.

Artemenko:2017:PGO


Bacher:2017:GRP


Barmpalias:2017:PCO


Barmpalias:2017:RNP


Beebe:2017:MFC


REFERENCES

Herrero-Collantes:2017:QRN


Lampropoulos:2017:BLL


Monroe:2017:NPR


Nordrum:2017:TRN


Pomeranz:2017:CSL


Popov:2017:DTP


Sibidanov:2017:RSB

REFERENCES


[3715] 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

Anonymous:1954:ADC

Curtiss:1956:NAP

Meyer:1956:SMC

Macphail:1959:PFC

Anonymous:1960:PFI

Ralston:1960:MMD

Birkhoff:1961:NRT
REFERENCES


REFERENCES


[3737] Peter C. C. Wang, editor. Information linkage between applied mathematics and industry: Proceedings of the First Annual Workshop on the
REFERENCES


Dempster:1980:SPP


Oren:1980:SDM


Eddy:1981:CSS


Rubinstein:1981:SMC


Grossmann:1982:PSI


IEEE:1982:ASF


Chaum:1983:ACP


Gentle:1983:CSS


IEEE:1983:ASF


Ralston:1983:ECS


IEEE:1984:ASF


IEEE:1984:ASF


REFERENCES


Mehlhorn:1985:SAS


ACM:1986:PEA


Arkin:1986:SOP


DAgostino:1986:GFT


Heath:1986:HMP


Abrams:1988:WSC


ACM:1988:PTA


Edwards:1988:CPC


IEEE:1988:ASF


Wegman:1988:CSS

REFERENCES


REFERENCES


REFERENCES

IEEE:1990:PSN


Pomerance:1990:CCNb


Anonymous:1991:PIS


Day:1991:PAA


Dorninger:1991:CGA


Nelson:1991:WSC


[3793] 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


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


Meadows:2005:CPA


Smart:2005:CCI


Henderson:2006:S


Niederreiter:2006:MCQ


Schroeder:2006:NTS

Manfred Robert Schroeder. Number Theory in Science and Communication: With Applications in Cryptography, Physics, Digital Information,
REFERENCES


REFERENCES


[3886] Christos Alexopoulos, David Goldsman, and James R. Wilson, editors. Advancing the frontiers of simulation: a Festschrift in honor of George
REFERENCES


Belsley:2009:HCE


Clavier:2009:CHE


LECuyer:2009:MCQ


Paredaens:2009:PTE


ACM:2010:PAI

REFERENCES


REFERENCES

IEEE:2010:PIA


Peterson:2010:IEE


ACM:2011:PAI


Gilli:2011:NMO


Hwu:2011:GCG


IEEE:2011:ICI

REFERENCES


REFERENCES


[3915] David H. Bailey, Heinz H. Bauschke, Peter Borwein, Frank Garvan, Michel Théra, Jon D. Vanderwerff, and Henry Wolkowicz, editors. *Com-