

Áèáëèî ãðàòèÿ

1. C. M. Adams and S.E. Tavares, "Generating and Counting Binary Bent Sequences", in *IEEE Trans. Inf. Theory*, vol 36, no 5, 1990
2. C. M. Adams and S.E. Tavares, "The use of bent sequences to achieve higher-order strict avalanche criterion", Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990
3. A.V. Aho, J.E. Hopcroft and J.D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company, 1974
4. S.V.B. Aiyer, M. Niranjan, F. Fallside. A theoretical investigation into the performance of the Hopfield model, *IEEE Trans. On Neural Networks*, 1(2): 204-215, 1990
5. W. Alexi, B. Chor, O. Goldreich, and C. P. Schnorr, "RSA and Rabin functions: Certain parts are as hard as the whole," *SIAM J. Comput.*, vol. 17, pp. 194-209, April 1988.
6. N. Alon, O. Goldreich, J. Hastad and R. Peralta. Simple constructions of almost k-wise independent random variables. In 31th *Annual Symposium on Foundations of Computer Science, St.Louis, Missouri*, pp 544-553, 1990.
7. R. Anderson. "Solving a class of stream ciphers", *Cryptologia*, 14(3):285-288,1990
8. R. Anderson. "Faster attack on certain stream ciphers", *Electr. Lett.*, 29(15):1322-1323, July 1993
9. R. Anderson. "Derived Sequence Attacks on Stream Ciphers", presented at the rump session of Crypto 93
10. R. Anderson. Preface to "Fast Software Encryption - Cambridge Security Workshop", pages V-VI, Springer-Verlag, Berlin, 1994.
11. R. Anderson, post to Newsgroups: sci.crypt (from rja14@cl.cam.ac.uk), 17 Jun 1994, Subject: A5
12. R. Anderson. "Why Cryptosystems Fail", in *Communications of the ACM* , v 37 no 11 (November 1994) pp 32-40
13. R. Anderson. "Searching for the optimum correlation attack". Fast Software Encryption - Second International Workshop, Leuven, December 1994, Springer-Verlag, Berlin, 1995, pp 137-143

-
14. R. Anderson. "On Fibonacci Keystream Generators". Fast Software Encryption - Second International Workshop, Leuven, Dec. 1994, Springer-Verlag, Berlin, 1995, pp 346-352
 15. R. Anderson and C. Manifavas, "Chameleon - A New Kind of Stream Cipher", in Fast Software Encryption - Fourth International Workshop, Haifa, Israel, Jan. 1997, Springer-Verlag, Berlin, 1997.
 16. K.B. Athreya and P.E.Ney, *Branching Process*. Berlin, Springer-Verlag, 1972
 17. S. Babbage. "A Space/Time Trade-Off in Exhaustive Search Attacks Stream Ciphers", 9 April 1996, presented at the rump session of Eurocrypt 96
 18. A.D. Barnard, J.R. Silvester, W.G. Chambers, "Guaranteeing the period of linear recurring sequences (mod 2^e)", IEE Proceedings-E, 140, 243-245, (Sept 1993).
 19. U. Baum and S. Blackburn. Clock-controlled pseudorandom generators on finite groups. Fast Software Encryption - Second International Workshop, Leuven, December 1994, Springer-Verlag, Berlin, 1995
 20. H. Beker and F. Piper, *Cipher Systems: the Protection of Communications*, London: Northwood Books, 1982.
 21. K. Beker and M. Dorfler. *Dynamic systems and fractals*. Cambridge University Press, New York, 1989.
 22. B. Benjauthrit and I. S. Reed, "Galois switching functions and their applications," *IEEE Trans. Comput.*, vol. C-25, pp. 78-86, Jan. 1976.
 23. C.H. Bennett, G. Brassard and J.M. Robert, "Privacy amplification by public discussion", *SIAM J. Computing*, vol. 17, pp. 210-229, 1988
 24. M. Ben-Or, Probabilistic algorithms in finite fields, *Proceedings of the 22nd IEEE Foundations of Computer Science Symposium*. 1981. Pp. 394-398
 25. E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.
 26. J. Bernasconi and C. G. Günther, "Analysis of a nonlinear feedforward logic for binary sequence generators," *BBC Tech. Rep.*, 1985.
 27. T. Beth and Zong-duo Dai. "On the complexity of pseudo-random sequences - or: If you can describe a sequence it can't be random". In J.J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - Eurocrypt '89*, pages 533-543, Springer-Verlag, Berlin, 1990.

-
28. T. Beth and F. Piper, "The stop-and-go generator," in *Lecture Notes in Computer Science 209; Advances in Cryptology: Proc. Eurocrypt '84*, T. Beth, N. Cot, and I. Ingemarsson, Eds., Paris, France, April 9-11, 1984, pp. 88-92. Berlin: Springer-Verlag. 1985.
 29. J. Bierbrauer, K. Gopalakrishnan and D.R. Stinson. "Bounds on resilient functions and orthogonal arrays," in *Advances in Cryptology: Proc. Crypto '94*, 1994 vol 839, LNCS, pp 247-256, Springer-Verlag, Berlin
 30. E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.
 31. E. Biham and P. Kocher. A known plaintext attack on the PKZIP encryption. *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995
 32. S.R. Blackburn. A generalisation of the discrete Fourier transform: an algorithm to determine the minimum polynomial of a periodic sequence. September 1993. Preprint.
 33. R. E. Blahut, "Transform techniques for error-control codes," *IBM J. Res. Develop.* vol. 23, pp. 299-315, 1979.
 34. R.E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.
 35. R.E. Blahut. *Fast Algorithms for Digital Signal Processing*. Addison-Wesley, 1985.
 36. A. Blake and A. Zisserman. *Visual Reconstruction*, MIT Press, Cambridge Mass., 1987
 37. W. Blaser and P. Heinzmann, "New cryptographic device with high security using public key distribution," *Proc. IEEE Student Paper Contest 1979-80*, pp.145-153,1982.
 38. U. Blöcher and M. Dichtl. Fish: A Fast Software Stream Cipher. In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 41-44, Springer-Verlag, Berlin, 1994.
 39. M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850-863, 1984.
 40. L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM J. Comput.*, vol. 15, pp. 364-383, 1986.
 41. J. Boyar (Plumstead). Inferring sequences produced by a linear congruential generator missing low-order bits. *Journal of Cryptology*, 1(3):177-184, 1989.

-
42. J. Boyar (Plumstead). "Inferring sequences produced by pseudo-random number generators", *Jour. Of ACM*, Vol.36, No.1, 1989, pp. 262-280.
 43. R.P. Brent, "On the periods of generalised Fibonacci sequences", in *Mathematics of Computation* v 63 no 207 (July 1994) pp 389-401
 44. E.F. Brickell. Breaking iterated knapsacks. In G.R. Blakley and D.Chaum, editors, *Advances in Cryptology - Crypto '84*, pages 342-358, Springer-Verlag, New York, 1985.
 45. E.F. Brickell and A.M. Odlyzko , "Cryptanalysis. A Survey of Recent Results", in G.J. Simmons, editor. *Contemporary Cryptology, The Science of Information Integrity*; pp 501-540. IEEE Press, New York, 1992.
 46. J. O. Brüer, "On nonlinear combinations of linear shift register sequences," in *Proc. IEEE ISIT*, les Arcs, France, June 21-25 1982
 47. J. O. Brüer, "On pseudo random sequences as crypto generators," in *Proc. Int. Zurich Seminar on Digital Communication*, Switzerland, 1984.
 48. N.G. de Bruijn. A combinatorial problem. *Nederl. Akad. Wetensch. Proc.*, 49:758-764, 1946.
 49. L. Brynielsson, "On the linear complexity of combined shift register sequences," in *Lecture Notes in Computer Science 219; Advances in Cryptology: Proc. Eurocrypt '85*, F. Pichler, Ed., Linz, Austria, April 1985, pp. 156-166. Berlin: Springer-Verlag, 1986.
 50. L. Brynielsson, "Wie man den richtigen Schlüssel in einem Heuhaufen findet," *Kryptologie Aufbauseminar J.*, Kepler Universität, Linz, Austria, 1987.
 51. L. Brynielsson, "Below the unicity distance," *Workshop on Stream Ciphers*, Karlsruhe, Germany 1989.
 52. TR Cain, AT Sherman, "How to Break Gifford's Cipher", in *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (ACM, Nov 94) pp 198-209
 53. T.R. Cain and A.T. Sherman , "How to break Gifford's Cipher", *CRYPTOLOGIA*, vol XXI, 1997, n 3, pp 237-286
 54. P. Camion and A. Canteaut "Construction of t-Resilient Functions over a Finite Alphabet", in *Lecture Notes in Computer Science; Advances in Cryptology: Eurocrypt '96 Proc.*, Springer-Verlag 1996, pp. 283-293

-
55. P. Camion, C. Carlet, P. Charpin and N. Sendrier, "On correlation-immune functions," in *Lecture Notes in Computer Science vol.576; Advances in Cryptology: Crypto '91 Proc.*, pp 87-100. Berlin: Springer-Verlag, 1991.
 56. C. Carlet, "Partially-bent functions", *Advances in Cryptology - Crypto '92*, pages 280-291, Springer-Verlag, New York, 1993.
 57. C. Carlet, "Two New Classes of Bent Functions", in *Lecture Notes in Computer Science vol. 765; Advances in Cryptology: Eurocrypt '93 Proc.*, Springer-Verlag 1994, pp. 77-101
 58. C. Carlet, J. Seberry and X.-M. Zhang "Comments on 'Generating and Counting Binary Bent Sequences'", in *IEEE Trans. Inf. Theory*, vol 40, no 2, page 600, 1994.
 59. C. Carlet, "Hyper-bent functions", in *Proceedings of the 1st Int. Conference on the theory and Applications of Cryptology, Pragocrypt '96*, CTU Publishing House, 1996, pp 145-155
 60. C. Carlet, "More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings ", in *LNCS 1233; Proc. Eurocrypt '97*, Berlin: Springer-Verlag, 1997.
 61. J. Carrol and L. Robins, Computer Cryptanalysis, *Technical Report No.223*, 1988, Department of Computer Science, The University of Western Ontario, London, Ontario.
 62. G.J. Chaitin. Information, Randomness and Incompleteness. World Scientific Publishing, Singapore, 1987.
 63. G.J. Chaitin. On the length of programs for computing finite binary sequences. *J. ACM*, 13(4):547-569, October 1966.
 64. C.M. Campbell, "Design and specification of cryptographic capabilities," *IEEE Commun. Soc. Mag.*, vol. 16, pp. 15-19, 1978.
 65. W.G. Chambers and S. M. Jennings, "Linear equivalence of certain BRM shift-register sequences," *Electron. Lett.*, vol. 20, Nov. 1984.
 66. W.G. Chambers, "Clock-controlled shift registres in binary sequence generators," *IEE Proc. E.*, vol. 135, pp. 17-24, 1988.
 67. W.G. Chambers and D. Gollmann, "Generators for sequences with nearmaximal linear equivalence," *IEE Proc. E.*, vol. 135, pp. 67-69, 1988.
 68. W.G. Chambers and Z.-D. Dai, "On binary sequences from recursion modulo 2^e made non-linear by the bit-by-bit XOR-fuction", *Lecture Notes in Computer Science vol 547 Advances in Cryptology:Proc. Eurocrypt'91*, Springer-Verlag., pp 200-204, 1992

-
69. W.G. Chambers, "Two Stream Ciphers", In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 51-55, Springer-Verlag, Berlin, 1994.
 70. W.G. Chambers, "On Random Mappings and Random Permutations", *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995, pp 22-28
 71. A.H. Chan. On quadratic m-sequences. In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 166-173, Springer-Verlag, Berlin, 1994.
 72. A. H. Chan and R. A. Games, "On the linear span of binary sequences obtained from finite geometries," in *Lecture Notes in Computer Science 263; Advances in Cryptology: Proc. Crypto '86*, A. M. Odlyzko, Ed., Santa Barbara, CA, Aug. 11-15, 1986, pp. 405-417. Berlin: Springer-Verlag, 1987.
 73. A.H. Chan and R.A. Games. On the quadratic spans of periodic sequences. In G. Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 82-89, Springer-Verlag, New York, 1990.
 74. A.H. Chan and R.A. Games. "On the linear span of binary sequences from finite geometries, q odd". *IEEE Transactions on Information Theory* 36, 548-552 (1990)
 75. A. H. Chan, M. Goresky, and A. Klapper, "Correlation functions of geometric sequences," *Proc. Eurocrypt 90*, I. Damgard, Ed., Springer Verlag .
 76. D. Chaum and J. H. Evertse, "Cryptanalysis of DES with a reduced number of rounds," in *Lecture Notes in Computer Science 218; Advances in Cryptology: Proc. Crypto '85*, H. C. Williams, Ed., Santa Barbara, CA, Aug. 18-22, 1985, pp. 192-211. Berlin: Springer-Verlag, 1986.
 77. U. Cheng. Properties of Sequences. PhD thesis, University of Southern California, 1981.
 78. V. Chepyzhov and B. Smeets. On a fast correlation attack on certain stream ciphers. In D.W. Davies, editor, *Advances in Cryptology - Eurocrypt '91*, pages 176-185, Springer-Verlag, Berlin, 1991.
 79. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. "The bit extraction problem or t-resilient functions," *IEEE Symposium on Foundations of Computer Science*, vol. 26, pp. 396-407, 1985.
 80. G.C. Clark and J.B. Cain. *Error-Correcting Coding for Digital Communications*. New York: Plenum Press, 1982

-
81. A. Clark, J. Goliã, E. Dawson. "A Comparison of Fast Correlation Attacks". In *Fast Software Encryption - Third International Workshop*, Cambridge, February 1996, pp. 145-157, Springer-Verlag, Berlin, 1996
 82. D. Coppersmith, H. Krawczyk, and Y. Mansour. The shrinking generator. In D.R. Stinson, editor, *Advances in Cryptology - Crypto '93*, pages 22-39, Springer-Verlag, New York, 1994.
 83. C. Coveyou and R.D. MacPherson, "Fourier Analysis of Uniform Random Number Generators," *Journal of the ACM*, v. 14, n. 1, 1967, pp. 100-119.
 84. Zong-duo Dai. Binary sequences derived from ML-sequences over rings. 1986. Preprint.
 85. Zong-duo Dai, "Proof of Rueppel's linear complexity conjecture," *IEEE Trans. inform. Theory*, vol. 32, pp. 440-443, May 1986.
 86. Zong-duo Dai and Kencheng Zeng, "Continued Fractions and the Berlekamp-Massey Algorithm," In *J. Seberry and J. Pieprzyk, editors, Advances in Cryptology - Auscrypt '90*, pages 24-31, Springer Verlag, Berlin, 1990.
 87. J. Daemen, R. Govaerts, and J. Vandewalle. On the Disign of High Speed Self-Synchronizing Stream Ciphers. In *Singapore ICSS/ISITA '92 Conference Proceedings*, IEEE 1992, pages 279-283.
 88. J. Daemen, R. Govaerts, and J. Vandewalle. Cryptanalysis of MUX-LFSR based scramblers. In *State and Progress in the Research of Cryptography*, 1993, pages 55-61, 1993.
 89. J. Daemen, R. Govaerts, and J. Vandewalle. "Resynchronization weakness in synchronous stream ciphers". *Advances in Cryptology - Eurocrypt '93, LNCS vol 765*, pages 159-167, Springer-Verlag, 1994.
 90. J. Daemen. Cipher and Hash Function Design. PhD thesis, Katholieke Universiteit Leuven, 1995.
 91. D.W. Davies and W.L. Price. *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*. John Wiley & Sons, New York, 1984.
 92. E. Dawson and B.Goldburg, "Universal logic sequences", In *J. Seberry and J. Pieprzyk, editors, Advances in Cryptology - Auscrypt '90*, pages 426-432, Springer Verlag, Berlin, 1990.
 93. E. Dawson and A.Clark, "Cryptanalysis of Universal Logic Sequences", *Advances in Cryptology - Eurocrypt '93*, Springer Verlag, Berlin.

94. E. Dawson and A.Clark, "Divide and conquer attacks on certain classes of stream ciphers", *Cryptologia* XVIII, N 1, 1994 pp 25-40.
95. E. Dawson and A.Clark, "Discrete Optimisation: A Powerful Tool for Cryptanalysis?", in *Proceedings of the 1st Int. Conference on the theory and Applications of Cryptology, Pragocrypt '96*, CTU Publishing House, 1996, pp 425-450
96. D. E. Denning, *Cryptography and Data Security*, Reading, MA: Addison-Wesley, 1983.
97. Y. Desmedt, J. J. Quisquater, and M. Davio, "Dependence of output on input of DES: Small avalanche characteristics," in *Lecture Notes in Computer Science 196; Advances in Cryptology: Proc. Crypto '84*, G. R. Blakley and D. Chaum, Eds., Santa Barbara, CA, Aug. 19-22, 1984, pp. 359-376. Berlin: Springer-Verlag, 1985.
98. Y. G. Desmedt, "Cryptanalysis of conventional and public key cryptosystems," *Proc. SPRCI'89*, Rome, Nov. 23-24, 1989.
99. L. Dickson. *History of the Theory of Numbers*. Chelsea Pub. Co., London, 1919.
100. W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Informat. Theory*, vol. IT-22, pp. 644-654, Nov. 1976.
101. W. Diffie and M. Hellman, "Privacy and authentication: An introduction to cryptography," *Proc. IEEE*, vol. 67, pp. 397-427, 1979.
102. W. Diffie, Private communication with R.Rueppel, July 1984.; (in "Contemporary Cryptology", G.Simmons, Ed. , IEEE Press, New York, p. 124, 1992)
103. J. F. Dillon, "A survey of bent functions", *The NSA Technical Journal* (1972), pp 191-215 (unclassified)
104. J. F. Dillon, "Elementary Hadamard difference sets", *Ph..D. Thesis*, University of Maryland, 1974
105. J. F. Dillon, "Elementary Hadamard difference sets," *Proc. 6th Southeastern Conf. Combinatorics, Graph Theory, and Computing*, Boca Raton, FL, pp. 237- 249, 1975; in *Congressus Numerantium* No. XIV, Utilitas Math., Winnipeg, Manitoba, 1975.
106. C Ding, G Xiao, W Shan, "*The Stability Theory of Stream Ciphers*" , Springer LNCS v 561 (1991)
107. C. Ding, "The Differential Cryptanalysis and Design of Natural Stream Ciphers". In *Fast Software Encryption*, Cambridge Security Workshop, December 1993, pages 101-115, Springer-Verlag, Berlin, 1994

-
108. H. Dobbertin, "Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity", *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995, pp 61-74
 109. M.W. Dodd, "Simultaneous Correlation to Many Linear Functionals: a New Cryptanalytic Technique which Can Almost Halve the Effective Key Size of Certain Stream Ciphers", *Proc. 4th IMA Conference on Cryptography and Coding*, Cirencester, 1993, (published by the IMA, ed. P.G.Farrell, 1995).
 110. R. Durbin and D. Willshaw, An analogue approach to the travelling salesman problem using an elastic net method, *Nature* 326: 689-91 (1987)
 111. Specification of the Systems of the MAC/Packet Family. EBU Technical Document 3258-E, October 1986.
 112. H.D. Ebbinghaus et al., *Numbers*, Graduate Texts in Mathematics vol. 123, Springer Verlag, N.Y., 1990.
 113. E.D. Erdmann. Empirical Tests of Binary Keystreams. Master's thesis, University of London, 1992.
 114. J. H. Evertse, "Linear structures in block cyphers," in *Lecture Notes in Computer Science 304; Advances in Cryptology: Proc. Eurocrypt '87*, D. Chaum and W. L. Price, Eds., Amsterdam, The Netherlands, April 13-15, 1987, pp. 249-266. Berlin: Springer-Verlag, 1988.
 115. P. Fahn. Answers to Frequently Asked Questions About Today's Cryptography. RSA Laboratories, September 1993. Version 2.0.
 116. L. J. Folks, Combination of Independent Tests, *Handbook of Statistics*, 4, Elsevier, 1984, 113-121.
 117. R.P.Feynman. *Statistical Mechanics*, W.A.Benjamin, Inc. (1972)
 118. R. Forré, "The strict avalanche criterion: Spectral properties of boolean functions and an extended definition," in *Lecture Notes in Computer Science 403; Advances in Cryptology: Proc. Crypto '88*, pp. 450-468. Berlin: Springer-Verlag, 1990.
 119. R. Forré, "A fast correlation attack on nonlinearly feedforward filtered shift-register sequences," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt '89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 586-595. Berlin: Springer-Verlag, 1990.
 120. A.M. Frieze, J. Hastad, R. Kannan, J.C. Lagarias, and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM Journal on Computing*, 17(2):262-280, April 1988.

-
121. A.M. Frieze, R. Kannan, and J.C. Lagarias. Linear congruential generators do not produce random sequences. *IEEE Symposium on Foundations of Computer Science*, 480-484, 1984.
 122. J. Gait, "A new nonlinear pseudorandom number generator," *IEEE Trans. Software Eng.*, vols. S E3, no. 5, pp. 359-363, Sept. 1977.
 123. R. G. Gallager, "Low-density parity-check codes," Cambridge, MA: MIT Press 1963.
 124. R.A. Games. There are no de Bruijn sequences of span n with complexity 2^n . *Journal of Combinatorial Theory, Series A*, 34:248-251, 1983.
 125. R.A. Games and A.H. Chan. A fast algorithm for determining the complexity of a binary sequence with period 2^n . *IEEE Transactions on Information Theory*, IT-29:144-146, 1983.
 126. R.A. Games, A.H. Chan, and E.L. Key. On the complexities of de Bruijn sequences. *Journal of Combinatorial Theory, Series A*, 33:233-246, 1982.
 127. M. R. Garey and D. S. Johnson, *Computers and Intractability*, New York: W. H. Freeman, 1979.
 128. A.H. Gee and R.W. Prager. Polyhedral combinatorics and neural networks, *Neural Computation* 6: 161-180, (1994)
 129. P. R. Geffe, "How to protect data with ciphers that are really hard to break," *Electronics*, Jan. 4, 1973, pp 99-101
 130. D.K. Gifford, J.M. Lucassen and S.T. Berlin, "The Application of Digital Broadcast Communication to Large Scale Information Systems", *IEEE Journal on Selected Areas in Communications*, v 3, n 3, May 1985, pp. 457-467.
 131. A. Gill, *Linear Sequential Circuits*, McGraw-Hill, New York, 1966
 132. J. Gleick, *Chaos: Making a New Science*. Viking Penguin: New York, 1987.
 133. S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial information," *J. Comput. Sys. Sci.*, vol. 28, no. 2, Apr. 1984.
 134. O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, no. 4, pp. 792-807, 1986.
 135. J. Goliã and M. V. Zivkoviã, "On the linear complexity of nonuniformly decimated pn-sequences," *IEEE Trans. inform. Theory*, vol 34, pp. 1077-1079, Sept. 1988.
 136. J. D. Goliã, "On the linear complexity of functions of periodic GF(q)-sequences," *IEEE Trans. Inform. Theory*, vol. IT-35, pp. 69-75, Jan. 1989.

-
137. J. D. Goliã and M.J. Mihaljeviã, "A noisy clock-controlled shift register cryptanalytic concept based on sequence comparison approach," *Advances in Cryptology - Eurocrypt '90, Lecture Notes in Computer Science vol. 473*; I. Damgård, Ed., pp. 487-491, Springer-Verlag, 1990.
 138. J. D. Goliã and M.J. Mihaljeviã, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance," *Journal of Cryptology* , 3(3):201-212, 1991
 139. J. Goliã and S.V. Petroviã, "A generalized correlation attack with a probabilistic constrained edit distance," In R.A. Rueppel, ed, *Advances in Cryptology - Eurocrypt '92, Lecture Notes in Computer Science vol. 658*; pages 472-476, Springer-Verlag, Berlin, 1993.
 140. J. Goliã and S.V. Petroviã, "Constrained edit distance for a memoryless function of strings," invited introductory paper, *Proceedings of the Second Spanish Conf. Cryptology*, Madrid, pp. 1-23, Oct. 1992.
 141. J. Goliã, Correlation via linear sequential circuit approximation of combiners with memory. In R.A. Rueppel, editor, *Advances in Cryptology - Eurocrypt '92*, pages 113-123, Springer-Verlag, Berlin, 1993.
 142. J. Goliã, "On the security of shift register based keystream generators". In *Fast Software Encryption*, Cambridge Security Workshop, December 1993, pages 90-100, Springer-Verlag, Berlin, 1994
 143. J. D. Goliã and L. O'Connor. Embedding and probabilistic correlation attacks on clock-controlled shift registers. In *Advances in Cryptology - Eurocrypt '94*, pages 230-343, Springer-Verlag, Berlin.
 144. J. Goliã, Intrinsic statistical weakness of keystream generators. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - Asiacrypt '94*, pages 91-103, Springer-Verlag, Berlin, 1995.
 145. J. Goliã, Linear cryptanalysis of stream ciphers. In *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995
 146. J. D. Goliã, Towards fast correlation attacks on irregularly clocked shift registers. In L.C. Guillou and J.J. Quisquater, editors, *Advances in Cryptology - Eurocrypt '95*, pages 248-262, Springer-Verlag, Berlin, 1995.
 147. J. Goliã, M. Salmasizadeh, A. Clark, A. Khodkar and E. Dawson, "Discrete Optimisation and Fast Correlation Attacks", *Cryptographic Policy and Algorithms - Brisbane '95, Lecture Notes in Computer Science 1029*; E. Dawson and J. Goliã, Eds., pp. 188-202, Springer-Verlag, 1996.

-
148. J. Goliã, "On the Security of Nonlinear Filter Generators". In *Fast Software Encryption - Third International Workshop, Cambridge, February 1996*, pp. 173-188, Springer-Verlag, Berlin, 1996
 149. J. Goliã, "Correlation Properties of a General Binary Combiner with Memory", *J.Cryptology* (1996) 9: 111-126
 150. J. Goliã, "Linear models for keystream generators", *IEEE Trans. Computers*, vol. C-45, pp. 41-49, Jan. 1996.
 151. J. D. Goliã, "Linear Statistical Weakness of Alleged RC4 Keystream generator", in *Lecture Notes in Computer Science 1233; Advances in Cryptology: Proc. Eurocrypt '97*, W. Fumy, Ed., May 1997, pp. 226-238, Berlin: Springer-Verlag, 1997
 152. J. D. Goliã, "Cryptanalysis of Alleged A5 Stream Cipher", in *Lecture Notes in Computer Science 1233; Advances in Cryptology: Proc. Eurocrypt '97*, W. Fumy, Ed., May 1997, pp. 239-255, Berlin: Springer-Verlag, 1997
 153. J. Goliã, A. Clark and E. Dawson, "Generalized inversion attack on nonlinear filter generators", submitted
 154. D. Gollman, "Pseudo random properties of cascade connections of clock controlled shift registers," in *Lecture Notes in Computer Science 209; Advances in Cryptology: Proc. Eurocrypt '84*, T. Beth, N. Cot, and I. Ingemarsson, Eds., Paris, France, April 9-11, 1984, pp. 93-98. Berlin: Springer-Verlag, 1985.
 155. D. Gollmann. *Linear Recursions of Cascaded Sequences*. Contributions to General Algebra 3, Hoelder-Pichler-Tempsky, Wien, Teubner, Stuttgart, 1985
 156. D. Gollmann. Correlation analysis of cascaded sequences. December 1986. Talk presented at 1st IMA Conference on Cryptography and Coding.
 157. D. Gollman and W. G. Chambers, "Lock-in effect in cascades of clock-controlled shift-registers," in *Lecture Notes in Computer Science 330; Advances in Cryptology: Proc. Eurocrypt '88*, C. G. Günther, Ed., Davos, Switzerland, May 25-27, 1988, pp. 331-343. Berlin: Springer-Verlag, 1988.
 158. D. Gollmann and W. G. Chambers, "Clock-controlled shift registers: A review," *IEEE J. Selected Areas Commun.*, vol. 7, pp. 525-533, May 1989.
 159. D. Gollmann and W. G. Chambers, "A cryptanalysis of step_{k,m}-cascades.," *Advances in Cryptology: Proc. Eurocrypt '89, LNCS vol 434*, J.-J. Quisquater, J. Vandevallè Eds., Springer-Verlag, pages 680-687, 1990.
 160. D. Gollmann, "Automata Theory and Cryptography", *Proc. Cryptography and Coding 1989*, C.J. Mitchell (ed.), Oxford University Press, pp. 67-74, 1992

-
161. D. Gollmann, "Cryptanalysis of Clock Controlled Shift Registers", *In R. Anderson, editor, Fast Software Encryption - Cambridge Security Workshop*, pages 121-126, Springer-Verlag, Berlin, 1994.
 162. S. W. Golomb, "Deep space range measurements," Jet Propulsion Laboratory, Pasadena, CA Research Summary, No. 36-1, 1960.
 163. S. W. Golomb, *Shift Register Sequences*, San Francisco: Holden Day, 1967. (and also reprint: Aegan Park Press, 1982)
 164. J.A. Gordon, "Very Simple Method to Find the Minimal Polynomial of an Arbitrary Non-Zero Element of a Finite Field," *Electronic Letters*, v. 12, n. 25, 9 Dec 1976, pp. 663-664.
 165. R. Gottfert and H. Niederreiter. A general lower bound for the linear complexity of the product of shift-register sequences. In *Advances in Cryptology - Eurocrypt '94*, Springer-Verlag, Berlin.
 166. E. J. Groth, "Generation of binary sequences with controllable complexity," *IEEE Trans. Inform. Theory*, vol. IT-17, no. 3, May 1971.
 167. C. G. Günther, "On some properties of the sum of two pseudorandom sequences," paper presented at Eurocrypt'86, Linköping, Sweden, May 20-22, 1986.
 168. C. G. Günther, "Alternating step generators controlled by de Bruijn sequences," in *Lecture Notes in Computer Science 304; Advances in Cryptology: Proc. Eurocrypt' 87*, D. Chaum and W. L. Price, Eds., Amsterdam, The Netherlands, April 13-15, 1987, pp. 5-14. Berlin: Springer-Verlag, 1988.
 169. C. G. Günther, "A universal algorithm for homophonic coding," in *Lecture Notes in Computer Science 330; Advances in Cryptology: Proc. Eurocrypt'88*, C. G. Günther, Ed., Davos, Switzerland, May 25-27, 1988, pp. 405-414. Berlin: Springer-Verlag, 1988.
 170. H.M.Gustafson, E.P.Dawson and J.Dj.Goliæ, "Randomness Measures Related to subset occurrence", in *Lecture Notes in Computer Science 1029; Advances in Cryptology: Proc. Cryptography: Policy and Algorithms*, Ed Dawson, J.Golic (Eds.), Brisbane, Queensland, Australia, July 1995, pp. 132-143. Berlin: Springer-Verlag, 1996.
 171. T.H.Harris, *The Theory of Branching Processes*. Berlin, Springer-Verlag, 1963
 172. J. Hastad and A. Shamir. The cryptographic security of truncated linearly related variables. In *Proceedings of the 17th ACM Symposium on Theory of Computing*, pages 356-362, 1985.

173. J. Hastad, B. Just, J. Lagarias and C.P. Schnorr. "Polynomial time algorithms for finding integer relations among real numbers", *SIAM J. Comput.*, vol. 18, pp. 859-881, 1989.
174. T. Herlestam, "On the complexity of functions of linear shift register sequences," *Int. Symp. Inform. Theory*, Les Arc, France, 1982.
175. T. Herlestam, "On functions of linear shift register sequences," in *LNCS 219; Advances in Cryptology: Eurocrypt'85*, pp. 119-129. Berlin: Springer-Verlag, 1986.
176. J.J. Hopfield and D.W.Tank. Neural computation of decisions in optimization problems, *Biological Cybernetics* 52: 1-25, (1985)
177. C. J. Jansen, "Investigations on nonlinear stream cipher systems: Construction and evaluation methods", Ph.D. thesis, Eindhoven University of Technology, The Netherlands, 1989.
178. C. J. Jansen and D.E. Boekke, "A Binary Sequence Generator Based on Ziv-Lempel Source Coding". In J.Seberry and J.Pieprzyk, eds., *Advances in Cryptology - Auscrypt '90*, pages 156-164, Springer Verlag, Berlin, 1990.
179. R.J. Jenkins, "ISAAC", In *Fast Software Encryption - Third International Workshop*, Cambridge, February 1996, pp. 41-49, Springer-Verlag, Berlin, 1996
180. S.M. Jennings. A Special Class of Binary Sequences. PhD thesis, University of London, 1980.
181. S. M. Jennings, "Multiplexed sequences: Some properties of the minimum polynomial," in *Lecture Notes in Computer Science 149; Cryptography: Proc. Workshop Cryptography*, T. Beth, Ed., Burg Feuerstein, Germany, March 29-April 2, 1982, pp. 189-206. Berlin: Springer-Verlag, 1983.
182. S. M. Jennings, "Autocorrelation function of the multiplexed sequence," *IEE Proc.*, vol. 131, no. 2, pp. 169-172, Apr. 1984.
183. B. Kaliski, A pseudo random bit generator based on elliptic logarithms, M. Sc. thesis, Massachusetts Institute of Technology, 1987.
184. E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 732-763, Nov. 1976.
185. L.H. Khachaturian. The lower bound of the quadratic spans of de Bruijn sequences. *Designs, Codes and Cryptography*, 3:29-32, 1993.
186. S. Kirkpatrick, C.D. Gelatt and M.P. Vecchi, "Optimization by simulated annealing", *Science*, 220 (4598):671-680, 1983.

187. K. Kjeldsen and E. Andresen, "Some randomness properties of cascaded sequences," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 227-232, March 1980.
188. A. Klapper. The vulnerability of geometric sequences based on fields of odd characteristic. *Journal of Cryptology*, 7(1):33-52, 1994.
189. A. Klapper and M. Goresky. 2-adic shift registers. In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 174-178, Springer-Verlag, Berlin, 1994.
190. A. Klapper. Feedback with carry shift registers over finite fields. *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995
191. A. Klapper and M. Goresky. Feedback registers based on ramified extensions of the 2-adic numbers, *Advances in Cryptology - Eurocrypt '94 (LNCS vol 950)*, pages 215-222, Springer-Verlag, Berlin, 1995.
192. A. Klapper and M. Goresky. Large period nearly de Bruijn FCSR sequences. In L.C. Guillou and J.J. Quisquater, editors, *Advances in Cryptology - Eurocrypt '95*, pages 248-262, Springer-Verlag, Berlin, 1995.
193. A. Klapper and M. Goresky. Cryptanalysis based on 2-adic rational approximation. *Advances in Cryptology - Crypto '95 (LNCS vol 963)*, pages 262-273, Springer-Verlag, Berlin, 1995.
194. A. Klapper. On the Existence of Secure Feedback Registers, *Advances in Cryptology - Eurocrypt '96 (LNCS vol 1070)*, pages 256-267, Springer-Verlag, Berlin, 1996.
195. A. Klapper and M. Goresky. Arithmetic cross-correlation of FCSR sequences. University of Kentucky technical report no. 262-96, 1996
196. A. Klapper and M. Goresky. Feedback Shift Registers, 2-Adic Span, and Combiners with Memory, *Journal of Cryptology* (1997) 10: 111-147
197. D.E. Knuth. *The Art of Computer Programming. Volume 2*, Addison-Wesley, Reading, Mass., 2nd edition, 1981.
198. D.E. Knuth. Deciphering a Linear Congruential Encryption. Technical Report 024800, Stanford University, 1980.
199. N. Koblitz. *P-Adic Numbers, p-Adic Analysis, and Zeta Functions*. Graduate Texts in Mathematics Vol. 58, Springer-Verlag, New York, 1984
200. N. Koblitz. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1987.

201. À. Í. Êîèì íáíðíá. Òðè ìíäöíäà è ìíðäááéáí èð "èíèè-áñòàà èí òíðì àöèè", *Í ðíáéèì ù íáðäáà-è èí òíðì àöèè*, 1:3-11, 1965.
202. A.G. Konheim, *Cryptography: A Primer*, John Wiley and Sons, New York, 1981
203. E. Kranakis, *Primality and Cryptography*, Stuttgart: Teubner, Wiley, 1986.
204. H. Krawczyk. How to predict congruential generators. In G. Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 138-153, Springer-Verlag, New York, 1990.
205. H. Krawczyk. "How to predict congruential generators," *Journal of Algorithms*, v.13, n. 4, Dec 1992, pp. 527-545
206. H. Krawczyk. "The Shrinking Generator: Some Practical Considerations", *Fast Software Encryption, Cambridge Security Workshop Proceedings*, Springer-Verlag, 1994, pp. 45-46
207. P. V. Kumar and R. A. Scholtz, "Bounds on the linear span of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 854-862, Nov. 1983.
208. P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinatorial Theory*, Ser. A 40, pp. 90-107, 1985.
209. E. Kushilevitz and Y. Mansour. Learning decision trees using the Fourier spectrum. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp 455-464, May 1991.
210. GJ Kühn, "Algorithms for Self-Synchronising Ciphers", in *Proc COMSIG 88*
211. G Kühn, F Bruwer, W Smit, "Vinnige Veeldoelige Enkripsievlokkie", supplementary paper to *Proceedings of Infosec 1990*
212. J.C. Lagarias and J.A. Reeds. Unique extrapolation of polynomial recurrences. *SIAM Journal on Computing*, 17(2):342-362, April 1988.
213. P. L'Ecuyer, "Efficient and Portable Combined Random Number Generators", *Communications of the ACM*. v. 31 , n. 6, Jun 1988, pp. 742-749,774.
214. P. L'Ecuyer, Random numbers for simulation. *Communications of the ACM*. 1990, 33(10): 86-97.
215. A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 865-868, Nov. 1982.
216. A. Levenshtein, Binary codes capable of correcting deletions, insertions, and reversals. *Sov. Phy. Dokl.*, Volume 10, (1966) 707-710

217. R. Lidl and H. Niederreiter, "Finite Fields," in *Encyclopedia of Mathematics and Its Applications, Vol. 20*, Reading, MA: Addison-Wesley, 1983.
218. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, London, Cambridge University Press, 1986.
219. S. Lin and D.J.Jr. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1983
220. S. Lloyd, "Counting functions satisfying a higher order strict avalanche criterion," in *LNCS 434: Advances in Cryptology; Eurocrypt'89*, pp.63-74. Springer-Verlag, 1990.
221. S. Lloyd. Counting binary functions with certain cryptographic properties. *Journal of Cryptology*, 5(2):107-131, 1992.
222. D. L. Long and A. Wigderson, "How discrete is the discrete log?" in *Proc. 15th ACM Symposium on Theory of Computation*, Apr. 1983.
223. R. Lorentzen and R. Nilsen, "Application of linear programming to the optimal difference triangle set problem," *IEEE Trans. Inform.Theory*, vol. IT-37, pp 1486-1488, Sep 1991
224. M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," *SIAM J. Comput.* vol. 17, pp. 373-386, 1988.
225. R. Matthews, On the Derivation of a "Chaotic" Encryption Algorithm. *Cryptologia*. 1989. 13: 29-42.
226. DJC MacKay, "A Free Energy Minimization Framework for Inference Problem in Modulo 2 Arithmetic". Fast Software Encryption - Second International Workshop, Leuven, December 1994, Springer-Verlag, Berlin, 1995, pp 179-195
227. F. J. MacWilliams and N. J. A. Sloane, "The theory of error correcting codes," Amsterdam: North-Holland, 1977.
228. D. Mandelbaum, Arithmetic codes with large distance. *IEEE Trans. Info. Theory*, vol. IT-13, 1967 pp.237-242
229. G. Marsaglia. Random numbers fall mainly in the planes. *Proc. N.A.S.*, 61:25-28, 1968.
230. P. Martin-Löf. The definition of random sequences. *Inform. Contr.*, 9:602-619, 1966.
231. J. L. Massey, *Threshold Decoding*. Cambridge, MA: MIT Press, 1963

232. J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-127, Jan. 1969.
233. J. L. Massey, A. Gubser, A. Fischer, P. Hochstrasser, B. Huber, and R. Sutler, "A self-synchronizing digital scrambler for cryptographic protection of data," in *Proceedings of International Zurich Seminar*, March, 1984.
234. J. L. Massey and R. A. Rueppel, "Linear ciphers and random sequence generators with multiple clocks," in *Lecture Notes in Computer Science 209; Advances in Cryptology: Proc. Eurocrypt'84*, T. Beth, N. Cot, and I. Ingemarsson, Eds., Paris, France, April 9-11, 1984, pp. 74-87. Berlin: Springer-Verlag, 1985.
235. J. L. Massey and I. Ingemarsson, "The Rip van Winkle cipher - a simple and provably computationally secure cipher with a finite key," in *Abstracts of Papers. IEEE Int. Symp. Inform. Theory*, Brighton, England, June 24-28, 1985.
236. J. L. Massey, "Delayed-decimation/square sequences," *Proc. 2nd Joint Swedish-Soviet Workshop on Information Theory*, Granna, Sweden, Apr. 14-19, 1985.
237. J. L. Massey and M. Z. Wong, "The characterization of all binary sequences with perfect linear complexity profiles," in *Abstracts of Papers, Eurocrypt'86*, Linkoping, Sweden, May 20-22, 1986, pp. 3-4A-3-4B.
238. J. L. Massey, "Cryptography and System Theory," *Proc. 24th Allerton Conf. Commun., Control, Comput.*, Oct. 1-3, 1986.
239. J. L. Massey, "Probabilistic encipherment," *Elektrotechnik und Maschinenbau*, vol. 104, no. 12, Dec. 1986.
240. J. L. Massey and R. A. Rueppel, "Method of, and apparatus for, transforming a digital sequence into an encoded form", U.S. Patent No. 4,797,922, 1989.
241. J. L. Massey, "Contemporary Cryptology: An Introduction", in G.J. Simmons, editor. *Contemporary Cryptology, The Science of Information Integrity*, pp 1-40. IEEE Press, New York, 1992.
242. J.L. Massey and S. Serconek. A Fourier transform approach to the linear complexity of nonlinearly filtered sequences. In Y. Desmedt, editor, *Advances in Cryptology - Crypto '94*, pages 332-340, Springer-Verlag, New York, 1994.
243. J.L. Massey and S. Serconek. "Linear Complexity of Periodic Sequences: A General Theory". *Advances in Cryptology - Crypto '96*, pages 358-371, Springer-Verlag, New York, 1996.
244. J. L. Massey, "Applied digital information theory," Lecture Notes, Swiss Federal Institute of Technology, Zurich.

-
245. M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseeth, editor, *Advances in Cryptology - Eurocrypt '93*, pages 386-397, Springer-Verlag, Berlin, 1994.
246. U. Maurer and J. L. Massey, "Perfect local randomness in pseudo-random sequences," in *Lecture Notes in Computer Science 435; Advances in Cryptology: Proc. Crypto'89*, G. Brassard, Ed., Santa Barbara, CA, Aug. 20-24. 1981 110-112. Berlin: Springer-Verlag, 1990.
247. U. Maurer, "A provable-secure strongly-randomized cipher," in *Lecture Notes in Computer Science 473; Advances in Cryptology: Proc. Eurocrypt'90*, I. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 361-373. Berlin: Springer-Verlag.
248. U.M. Maurer. New approaches to the design of self-synchronizing stream ciphers. In D.W. Davies, editor, *Advances in Cryptology - Eurocrypt '91*, pages 458-471, Springer-Verlag, Berlin, 1991.
249. U.M. Maurer. "A universal statistical test for random bit generators, " *J. Cryptol.*, vol. 5, no. 2, pp. 89-105, 1992.
250. G Mayhew, R Frazee, M Bianco, "The Kinetic Protection Device", in *Proceedings of the 15th National Computer Security Conference* (NIST, 1992) pp 310-318
251. G Mayhew, "A Low Cost, High Speed Encryption System and Method", in *Proc 1994 IEEE Computer Society Symposium on Research in Security and Privacy* (IEEE, 1994) pp 147-154
252. L. McCarthy , post to Newsgroups: sci.crypt (from lmccarth@cs.umass.edu), 27 Aug 1996, Subject: Elementrix and POTP encryption
253. R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combinatorial Theory*, Ser. A, 15, pp. 1-10, 1973.
254. W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, vol. I, no. 3, pp. 159-176, 1989.
255. W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt'89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 549-562. Berlin: Springer-Verlag, 1990.
256. W. Meier and O. Staffelbach, "Correlation properties of combiners with memory in stream ciphers," in *Lecture Notes in Computer Science 473; Advances in Cryptology: Proc. Eurocrypt'90*, I. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 204-213. Berlin: Springer-Verlag.

-
257. W. Meier and O. Staffelbach. Correlation properties of combiners with memory in stream ciphers. *Journal of Cryptology*, 5(1):67-86, 1992.
 258. W. Meier and O. Staffelbach. Analysis of pseudo random sequences generated by cellular automata. In D.W. Davies, editor, *Advances in Cryptology - Eurocrypt '91*, pages 186-199, Springer-Verlag, Berlin, 1992.
 259. W. Meier and O. Staffelbach. The self-shrinking generator. In *Advances in Cryptology - Eurocrypt '94*, Springer-Verlag, pp. 205-214
 260. R. Menicocci. Cryptanalysis of a two-stage Gollmann cascade generator. In *Proceedings of SPRC '93*, W.Wolfowicz (ed.), pp. 62-69, 1993
 261. R. Menicocci. Short Gollmann cascade generators may be insecure. In *Proceedings of the 4th IMA Conference on Cryptography and Coding*, Cirencester, 1993
 262. R. Menicocci. "A systematic attack on clock controlled cascades." In *Advances in Cryptology - Eurocrypt '94*, pages 450-455, Springer-Verlag, Berlin.
 263. R.C. Merkle, "Secure communication over insecure channels," *Comm. ACM*, vol. 21, pp. 294-299, Apr. 1978.
 264. N. Metropolis, A.W. and M.N. Rosenbluth, A.H. and E. Teller. "Equations of state calculations by fast computing machines". *Journal of Chemical Physics*, 21(6):1087-1092, 1953.
 265. S. Micali and C. P. Schnorr, "Efficient, perfect random number generators," preprint, Massachusetts Institute of Technology, University of Frankfurt, 1988
 266. M.J. Mihaljeviæ and J. Goliæ. A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology - Auscrypt '90*, pages 165-175, Springer Verlag, Berlin, 1990.
 267. M.J. Mihaljeviæ and J. Goliæ. "A comparison of cryptanalytic principles based on iterative error correction ", In D.V. Davies, editor, *Advances in Cryptology - Eurocrypt '91*, pages 527-531, Springer-Verlag, Berlin, 1992.
 268. M.J. Mihaljeviæ and J. Goliæ. "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence", In R.A. Rueppel, editor, *Advances in Cryptology - Eurocrypt '92*, pages 124-137, Springer-Verlag, Berlin, 1993.
 269. M.J. Mihaljeviæ. "An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure", *Advances in Cryptology - Auscrypt '92*, pages 349-356, Springer-Verlag, Berlin, 1993.

-
270. M.J. Mihaljeviæ and J. Goliæ. "A parity-check weight distribution for maximum-length sequences", *Abstracts of the Second International Conference on Finite Fields*, University of Nevada, Las Vegas, p. 35, 1993.
271. M.J. Mihaljeviæ. A correlation attack on the binary sequence generators with time-varying output function. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - Asiacrypt '94*, pages 67-79, Springer-Verlag, Berlin, 1995.
272. L. M. Milne-Thomson, "The calculus of finite differences," London: Macmillan and Co., 1951.
273. D. Mitchell, Nonlinear Key Generators. *Cryptologia*. 1990. 14: 350-354.
274. S. Mund. Ziv-Lempel complexity for periodic sequences and its cryptographic application. In D.W. Davies, editor, *Advances in Cryptology - Eurocrypt '91*, pages 114-126, Springer-Verlag, Berlin, 1992.
275. J. Naor and M. Naor. Small bias probability spaces: efficient construction and applications. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, Baltimore, Maryland*, pp 213-223, May 1990.
276. National Institute of Standards and Technology (NIST). FIPS Publication 180: Secure Hash Standard (SHS). May 11, 1993.
277. National Institute of Standards and Technology (NIST). FIPS Publication 46-2: Data Encryption Standard. December 30, 1993.
278. National Institute of Standards and Technology (NIST). FIPS Publication 81: DES Modes of Operation. December 2, 1980. Originally issued by National Bureau of Standards.
279. G. Nicolis and I. Prigogine. *Exploring Complexity*. W. H. Freeman and Company: New York, 1989.
280. H. Niederreiter, "Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences," contributions to General Algebra 5, Proc. Conf. Salzburg, Teubner, Stuttgart, 1986.
281. H. Niederreiter, "Sequences with almost perfect linear complexity profile," in *Lecture Notes in Computer Science 304; Advances in Cryptology: Proc. Eurocrypt'87*, D. Chaum and W. L. Price, Eds., Amsterdam, The Netherlands, April 13-15, 1987, pp. 37-51. Berlin: Springer-Verlag, 1988.
282. H. Niederreiter, "Probabilistic theory of linear complexity," in *Lecture Notes in Computer Science 330; Advances in Cryptology: Proc. Eurocrypt'88*, C. G. Günther, Ed., Davos, Switzerland, May 25-27, 1988, pp. 191-209. Berlin: Springer-Verlag, 1988.

-
283. H. Niederreiter, "Keystream sequences with a good linear complexity profile for every starting point," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt'89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 523-532. Berlin: Springer-Verlag, 1990.
284. H. Niederreiter. The linear complexity profile and the jump complexity of keystream sequences. In I.B. Damgård, editor, *Advances in Cryptology - Eurocrypt '90*, pages 174-188, Springer-Verlag, Berlin, 1991.
285. K. Nyberg, "Construction of bent functions and difference sets," in *Lecture Notes in Computer Science 473; Advances in Cryptology:Proc. Eurocrypt'90*, I. Damgård, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 151-160. Berlin: Springer-Verlag.
286. K. Nyberg, "Perfect Nonlinear S-boxes" in *Lecture Notes in Computer Science 547; Advances in Cryptology:Proc. Eurocrypt'91*, Springer-Verlag, 1992
287. K. Nyberg, "New Bent Mappings Suitable for Fast Implementation", In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 179-184, Springer-Verlag, Berlin, 1994.
288. P. Nyffeler, *Binare Automaten und ihre linearen Rekursionen*, Ph.D. thesis, University of Berne, 1975.
289. L. O'Connor and T. Snider. Suffix trees and string complexity. In R.A.Rueppel, editor, *Advances in Cryptology - Eurocrypt '92*, pages 138-152, Springer-Verlag, Berlin, 1993.
290. Y. Ohnishi, *A study on data security*. Master thesis (in Japanese), Tohoku University, Japan, 1988.
291. J.D. Olsen, R.A. Scholtz and L.R.Welch. "Bent functions sequences", *IEEE Transactions on Information Theory*, IT-28 No 6, 858-864
292. B.J. Oommen, Recognition of noisy subsequences using constrained edit distance. *IEEE Trans Pattern Analysis Mach. Intell.*, Volume PAMI-9, September (1987) 636-685
293. B.J. Oommen, Correction to recognition of noisy subsequences using constrained edit distance. *IEEE Trans Pattern Analysis Mach. Intell.*, Volume PAMI-10, November (1988) 983-984
294. S.-J. Park, S.-J. Lee and S.-Ch. Goh. On the Security of the Gollmann Cascades. *Advances in Cryptology - Crypto '95 (LNCS vol 963)*, pages 148-156, Springer-Verlag, Berlin, 1995.

-
295. W. T. Penzhorn and G. J. Kühn, " Computation of Low-Weight Parity Checks for Correlation Attacks on Stream Ciphers". *Proc. 5th IMA Conference Cryptography and Coding*, Cirencester, England, Dec. 1995, pages 74-83, Springer-Verlag, 1995.
 296. W. T. Penzhorn, "Correlation Attacks on Stream Ciphers: Computing Low-Weight Parity Checks Based on Error-Correcting Codes". In *Fast Software Encryption - Third International Workshop*, Cambridge, February 1996, pp. 159-172, Springer-Verlag, Berlin, 1996
 297. C. Peterson and B. Soderberg. A new method for mapping optimization problems onto neural networks, *Int. Journal Neural Systems*, (1989)
 298. S.V. Petroviæ and J. Goliæ, "String editing under a combination of constraints," *Information Sciences*,74:151-163, 1993.
 299. S.V. Petroviæ and J. Goliæ, "A divide and conquer attack on clock-controlled shift registers combined by a function with memory", submitted, 1993
 300. C. Pickover, Pattern Formation and Chaos in Networks. *Communications of the ACM*, 1988, 31: 136-151..
 301. F. Piper, "Stream ciphers," *Elektrotechnik und Maschinenbau*, vol. 104, no. 12, pp. 564-568, 1987.
 302. V. S. Pless, "Encryption schemes for computer confidentiality," *IEEE Trans. Comput.*, vol. C-26, pp. 1133-1136, Nov. 1977.
 303. J. Plumstead (Boyar). Inferring a sequence generated by a linear congruence. In *Proceedings of 23rd IEEE Symposium on Foundations of Computer Science*, pages 153-159, 1982.
 304. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functions," in *Lecture Notes in Computer Science 473; Advances in Cryptology: Proc. Eurocrypt'90*, 1. Damgard, Ed., Aarhus, Denmark, May 21-24. 1990, pp. 161-173. Berlin: Springer-Verlag.
 305. B. Preneel, R. Govaerts, and J. Vandewalle, "Boolean functions satisfying higher order propagation criteria" in *Lecture Notes in Computer Science 547; Advances in Cryptology: Proc. Eurocrypt'91*,1991, pp. 141-152. Berlin: Springer-Verlag.
 306. B. Preneel, "Introduction". *Fast Software Encryption - Second International Workshop*, Leuven, December 1994, Springer-Verlag, Berlin, 1995, pp 1-5
 307. W.H.Press, B.P.Flannery, S.A. Teukolsky and W.T. Vetterling, *Numerical Recipes in C: The Art of Scientific Computing*, Cambridge University Press, 1988.

-
308. *Pr Newswire*, "Elementrix announces revolutionary encryption for Internet and all digital communication", September 29, 1995
309. N. Proctor. A self-synchronizing cascaded cipher system with dynamic control of error-propagation. In G.R. Blakley and D. Chaum, editors, *Advances in Cryptology - Crypto '84*, pages 174-190, Springer-Verlag, New York, 1985.
310. M. O. Rabin, "Probabilistic Algorithm for Testing Primality," *SIAM Journal on Computing*, v. 9, n. 2, May 1980, pp. 273-280
311. M. O. Rabin, "Fingerprinting by Random Polynomials," Technical Report TR-15-81, Center for Research in Computing Technology, Harvard University, 1981.
312. S. Rasband, *Chaotic Dynamics of Nonlinear Systems*. John Wiley & Sons: New York, 1990.
313. J.A. Reeds. "Cracking a random number generator." *Cryptologia*, 1, January 1977.
314. J.A. Reeds. "Cracking a Multiplicative Congruential Encryption Algorithm", in *Information Linkage Between Applied Mathematics and Industry*, P.C.C Wang, ed., Academic Press, 1979, pp.467-472.
315. J.A. Reeds, "Solution of Challenge Cipher," *Cryptologia*, v. 3, n. 2, Apr 1979, pp. 83-95.
316. J.A. Reeds and N.J.A. Sloane. Shift register synthesis (modulo m). *SIAM Journal on Computing*, 14(3):505-513, 1985.
317. E. Rietman, *Exploring the Geometry of Nature*. Windcrest Books, Blue Ridge Summit, PA., 1989.
318. T. Ritter. The Efficient Generation of cryptographic Confusion Sequences. *Cryptologia*, 1991, 15(2): 81-139
319. R.L. Rivest. The RC4 Encryption Algorithm. RSA Data Security, Inc., March 12, 1992.
320. R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120-126, February 1978.
321. M.J.B. Robshaw. Block Ciphers. Technical Report TR - 601, RSA Laboratories, revised July 1995.
322. M.J.B. Robshaw. Stream Ciphers. Technical Report TR - 401, RSA Laboratories, revised July 1995.

323. M.J.B. Robshaw. On Binary Sequences with Certain Properties. PhD thesis, University of London, 1992.
324. M.J.B. Robshaw. On evaluating the linear complexity of a sequence of least period 2^n Designs, Codes and Cryptography, 4:263-269, 1994.
325. M.J.B. Robshaw. Security of RC4. Technical Report TR - 401, RSA Laboratories.
326. P. Rogaway and D. Coppersmith. A software-optimized encryption algorithm. In R. Anderson, editor, Fast Software Encryption - Cambridge Security Workshop, pages 56-63, Springer-Verlag, Berlin, 1994.
327. C.A. Ronce. Feedback Shift Registers. Volume 169 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1984.
328. O. S. Rothaus, "On bent functions," *J. Combinatorial Theory*, vol. 20, pp. 300-305, 1976.
329. F. Rubin "Decrypting a stream cipher based on J - K flip-flops," *IEEE Trans Comput.*, vol. C-28, no. 7, pp. 483-487, July 1979.
330. R.A. Rueppel. New Approaches to Stream Ciphers. PhD thesis, Swiss Federal Institute of Technology, Zurich, 1984.
331. R. A. Rueppel, "Linear complexity and random sequences," in *Lecture Notes in Computer Science 219; Advances in Cryptology: Proc. Eurocrypt'85*, F. Pilcher, Ed., Linz, Austria, April 1985, pp. 167-188. Berlin: Springer-Verlag, 1986.
332. R. A. Rueppel and J. L. Massey, "The knapsack as a nonlinear function," *IEEE Int. Symp. Inform. Theory*, Brighton, UK, May 1985.
333. R. A. Rueppel, "Correlation immunity and the summation combiner," in *Lecture Notes in Computer Science 218; Advances in Cryptology: Proc. Crypto'85*, H. C. Williams Ed., Santa Barbara, CA, Aug. 18-22, 1985, pp. 260-272. Berlin: Springer-Verlag, 1986.
334. R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Berlin: Springer-Verlag, 1986.
335. R. A. Rueppel and O. Staffelbach, "Products of sequences with maximum linear complexity," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 1, pp. 124-131, Jan. 1987.
336. R. A. Rueppel, "When shift registers clock themselves," in *Lecture Notes in Computer Science 304; Advances in Cryptology: Proc. Eurocrypt'87*, D. Chaum and W. L. Price, Eds., Amsterdam, The Netherlands, April 13-15, 1987, pp. 53-64. Berlin: Springer-Verlag, 1988.

-
337. R. A. Rueppel, "On the security of Schnorr's pseudo random sequence generator," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt'89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 423-428. Berlin: Springer-Verlag, 1990.
338. R. A. Rueppel, "Security models and notions for stream ciphers," *Proc. 2nd IMA Conf. Cryptography and Coding*, Cirencester, England, Dec. 1989.
339. R. A. Rueppel, "Stream ciphers," in G.J. Simmons, editor. *Contemporary Cryptology, The Science of Information Integrity*, pp 65-134. IEEE Press, New York, 1992.
340. A. Fuster-Sabater and P. Caballero-Gil. On the linear complexity of nonlinearly filtered PN-sequences. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology - Asiacrypt '94*, pages 80-90, Springer-Verlag, Berlin, 1995.
341. A. Fuster-Sabater and P. Caballero-Gil. "Linear Span of a Set of Periodic Sequence Generators". *Proc. 5th IMA Conference Cryptography and Coding*, Cirencester, England, Dec. 1995, pages 22-33, Springer-Verlag, 1995.
342. M. Salmasizadeh, J. Golic, E. Dawson and L. Simpson. "A Systematic Procedure for Applying Fast Correlation Attacks to Combiners with Memory", *Proc. of Fourth Annual Workshop on Selected Areas in Cryptography - SAC '97*, Ottawa, August 1997, preprint.
343. D. Sankoff and J.B. Kruskal, *Time Warps, String Edits and Macro Molecules: The Theory and Practice of Sequence Comparison*. Reading, MA: Addison-Wesley, 1983
344. J. E. Savage, Some simple self-synchronizing digital data scramblers. *Bell Sys.Tech. J.*, vol. 46, no. 2, pp. 449-487, Feb. 1967.
345. T. Schaub, A linear complexity approach to cyclic codes, Ph.D. thesis, Swiss Federal Institute of Technology, Zurich, 1988.
346. B. Schneier, *Applied Cryptography*, 2nd edition, John Wiley & Sons, New York, 1996
347. B. Schneier "Cryptography, Security and the Future", *Communications of the ACM*, v. 40, n. 1, Jan 1997.
348. C. P. Schnorr, "On the construction of random number generators and random function generators," in *Lecture Notes in Computer Science 330; Advances in Cryptology: Proc. Eurocrypt'88*, C. G. Gunther, Ed., Davos, Switzerland, May 25-27, 1988, pp. 225-232. Berlin: Springer-Verlag, 1988.
349. J. Seberry and M. Yamada. "Hadamard Matrices, Sequences and Block Designs". In J.H.Dinitz and D.R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, chapter 11, pages 431-559, John Wiley and Sons, Inc, 1992.

350. J. Seberry and X.M. Zhang. "Highly Nonlinear 0-1 balanced functions satisfying strict avalanche criterion". Presented at AUSCRYPT '92, 1992.
351. J. Seberry, X.M. Zhang, and Y. Zheng. "Nonlinearly balanced Boolean functions and their propagation characteristics". In D.R. Stinson, editor, *Advances in Cryptology - Crypto '93*, pages 49-60, Springer-Verlag, New York, 1994.
352. J. Seberry, X.M. Zhang and Y. Zheng, "On Constructions and Nonlinearity of Correlation Immune Functions" In T. Helleseth, editor, *Advances in Cryptology - Eurocrypt '93*, pages 181-199, Springer-Verlag, Berlin, 1994.
353. J. Seberry, X.-M. Zhang and Y. Zheng, "Nonlinearity and Propagation Characteristics of Balanced Boolean Functions", *Information and Computation*, Vol. 119, No 1, pp 1-13, 1995
354. E. S. Selmer, *Linear recurrence relations over finite fields*. Lecture Notes, University of Bergen, Bergen, Norway, 1966.
355. J. A. Serret, "Cours d'algebre superieure," Tome II, p. 154, Gauthier-Villars, Paris, 1886.
356. E.H. Sibley, "Random Number Generators: Good Ones Are Hard to Find", *Communications of the ACM*, v.31, n.10, Oct 1988, pp. 1192-1201
357. A. Shamir, "On the generation of cryptographically strong pseudo-random sequences," *8th Int. Colloquium of Automata, Languages, and Programming, Lecture Notes in Computer Science 62*, Springer-Verlag, 1981.
358. A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Transactions on Information Theory*, IT-30(5):699-704, Sept. 1984.
359. C. E. Shannon , "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol.27, pp. 379-423, 623-656, July and October 1948
360. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol.28, pp. 656-715, Oct. 1949
361. T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 776-780, Oct. 1984.
362. T. Siegenthaler, "Cryptanalyst's representation of nonlinearly filtered ml-sequences," in *Lecture Notes in Computer Science 219; Advances in Cryptology: Proc. Eurocrypt'85*, F. Pilcher, Ed., Linz, Austria, April 1985, pp. 103-110. Berlin: Springer-Verlag, 1986.

-
363. T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Comput.*, vol. C-34, pp. 81-85, Jan. 1985.
364. G.J. Simmons, editor. *Contemporary Cryptology, The Science of Information Integrity*. IEEE, New York, 1992.
365. B. Smeets, "A note on sequences generated by clock-controlled shift registers," in *Lecture Notes in Computer Science 219; Advances in Cryptology: Proc. Eurocrypt'85*, F. Pilcher, Ed., Linz, Austria, April 1985, pp. 40-42. Berlin: Springer-Verlag, 1986.
366. B. Smeets, "The linear complexity profile and experimental results on a randomness test of sequences over the field F_q ," *IEEE Int. Symp. Inform. Theory*, Kobe, Japan, June 19-24, 1988.
367. B. Smeets and W.G. Chambers, "Windmill pn-sequences generators", *IEE Proceedings-E*, vol 136, pp 401-404 (Sept 1989).
368. O. Staffelbach and W. Meier, "Cryptographic significance of the carry for ciphers based on integer addition," In A.J. Menezes and S.A. Vanstone, editors, *Advances in Cryptology - Crypto '90*, pages 601-615, Springer-Verlag, New York, 1990.
369. J. Stern, "Secret Linear Congruential Generators Are Not Cryptographically Secure", *Proceedings of the 28th Symposium on Foundations of Computer Science*, 1987, pp.421-426.
370. M. A. Stephens and R.B.D. D'Agostino, *Tests Based on EDF Statistics, Goodness of Fit Techniques, Statistics, Textbooks and Monographs*, 68, Marcell Dekker Inc., 1986, 97-193.
371. D.R. Stinson, "Resilient functions and large sets of orthogonal arrays," *Congressus numerantium*, vol. 92, pp. 105-110, 1993
372. D.R. Stinson and J.L. Massey, "An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions", *Journal of Cryptology*, vol.8(3), pp. 167-173, 1995
373. R. C. Tittsworth, "Optimal ranging codes," *IEEE Trans. Space Electron. Telemetry*, pp. 19-30, March 1964.
374. S. A. Tretter, "Properties of PN^2 sequences," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 295-297, March 1974.
375. PC van Oorschot, MJ Wiener, "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms", in *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (ACM, Nov 94) pp 210-218

376. G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *J. Amer. Inst. Elec. Eng.*, vol. 45, pp. 109-115, 1926.
377. R. Vogel, "On the linear complexity of cascaded sequences," in *Lecture Notes in Computer Science 209; Advances in Cryptology: Proc. Eurocrypt'84*, T. Beth, N. Cot, and I. Ingemarsson, Eds., Paris, France, April 9-11, 1984, pp. 99-109. Berlin: Springer-Verlag, 1985.
378. D. Wagner, B. Schneier and J. Kelsey, "Cryptanalysis of ORYX", *Preprint*, May 4, 1997
379. M. Z. Wang and J. L. Massey, "The characteristics of all binary sequences with perfect linear complexity profiles," paper presented at Eurocrypt'86, Linkoping, Sweden, May 20-22, 1986.
380. M. Wang, "Linear complexity profiles and continued fractions," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt'89*, J.-J. Quisquater and J. Vandewalle, Eds., Houthalen, Belgium, April 10-23, 1989, pp. 571-585. Berlin: Springer-Verlag, 1990.
381. M.Z. Wang, "Algorithm for recursively generating irreducible polynomials", *Electronic Letters* , v 32 no 20 (26/9/96) p 1875
382. M. Ward. The arithmetical theory of linear recurring series. Transactions of the American Mathematical Society, 35:600-628, (July 1933).
383. A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Lecture Notes in Computer Science 218; Advances in Cryptology: Proc. Crypto'85*, H. C. Williams, Ed., Santa Barbara, CA, Aug. 18-22, 1985, pp. 523-534. Springer-Verlag, 1986.
384. B.M.M. de Weger, Approximation lattices of p-adic numbers, *J. Num. Th.* Vol. 24, 1986, pp. 281-292.
385. L.R. Welch and R.A. Scholtz, Continued fractions and Berlekamp's algorithm. *IEEE Trans. Info. Theory* vol. 25, 1979 pp. 19-27.
386. D.D. Wheeler, Problems with Chaotic Cryptosystems. *Cryptologia*. 1989. 13(3): 243-250.
387. D.D. Wheeler and R. Matthews, Supercomputer Investigations of a Chaotic Encryption Algorithm. *Cryptologia*. 1989. 15(2): 140-152.
388. D.J. Wheeler, "A Bulk Data Encryption Algorithm", In R. Anderson, editor, *Fast Software Encryption - Cambridge Security Workshop*, pages 125-134, Springer-Verlag, Berlin, 1994.

-
389. B.A. Wichman and I.D. Hill, "An Efficient and Portable Pseudo-Random Number Generator", *Applied Statistics*, v. 31, 1982, pp. 188-190.
390. S. Wolfram, "Cryptography with cellular automata," in *Lecture Notes in Computer Science 218; Advances in Cryptology: Proc. Crypto'85*, H. C. Williams, Ed., Santa Barbara, CA, Aug. 18-22, 1985, pp. 429-432. Berlin: Springer-Verlag, 1986.
391. C.-K. Wu, "Boolean functions in cryptology," Ph.D. thesis, Xidian University, China, 1993
392. G. Z. Xiao and J. L. Massey, "A spectral characterization of correlation-immune functions," *IEEE Trans. Inform. Theory*, vol. 34, no. 3, pp. 569-571, May 1988.
393. E. Yanovsky, "Protected communication method and system". European Patent No EP 667691, 1995.
394. A. C. Yao, "Theory and applications of trapdoor functions," *Proc. 25th IEEE Symp. Foundations Comput. Sci.*, New York, 1982.
395. R. Yarlagadda and J.E.Hershey, "Analysis and synthesis of bent sequences," *Proc. IEE*, vol. 136, pt. E., pp. 112-123, March 1989.
396. L. E. Zegers, Common bandwidth transmission of data signals and wide-band pseudonoise synchronization waveforms," *Philips Res. Reports Suppl.*, no. 4, 1972
397. K. Zeng and M. Huang, "On the linear syndrome method in cryptanalysis," in *LNCS 403; Advances in Cryptology: Crypto'88*, S. Goldwasser, Ed., Santa Barbara, CA, Aug. 21-25, 1987, pp. 469-478. Berlin: Springer-Verlag, 1990.
398. K. Zeng, C.H. Yang, and T.R.N. Rao. An improved linear syndrome algorithm in cryptanalysis with applications. In A.J. Menezes and S.A. Vanstone, editors, *Advances in Cryptology - Crypto '90*, pages 34-47, Springer-Verlag, New York, 1990.
399. K. Zeng, C.H. Yang, and T.R.N. Rao. On the linear consistency test in cryptanalysis with applications. In G. Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 167-174, Springer-Verlag, New York, 1990.
400. K. Zeng, C.H. Yang, D.Y. Wei, and T.R.N. Rao. Pseudorandom bit generators in stream-cipher cryptography. *Computer* n 24, pp 8-17, February 1991.
401. X.-M. Zhang and Y.Zheng, "On nonlinear resilient functions," *Advances in Cryptology - Eurocrypt '95, Lecture Notes in Computer Science*, vol.921, L.C. Guillou ed., Springer-Verlag, pp. 274-288, 1995
402. X.-M. Zhang and Y.Zheng, "Cryptographically resilient functions," *IEEE Transactions on Information Theory*, September 1997

403. Y. Zheng, T. Matsumoto, and H. Imai, "Impossibility and optimality results on constructing pseudorandom permutations," in *Lecture Notes in Computer Science 434; Advances in Cryptology; Proc. Eurocrypt'89*, 1989, pp. 412-422. Berlin: Springer-Verlag, 1990.
404. N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, vol. 7, no.1, pp. 31-48, March 1959.
405. N. Zierler, "Primitive Trinomials Whose Degree Is a Mersenne Exponent," *Information and Control*, vol. 15, pp. 67-69, 1969.
406. N. Zierler and J. Brillhart, "On Primitive Trinomials (mod 2)," *Information and Control*, vol. 13, no. 6, pp. 541-544, Dec. 1968.
407. N. Zierler and W. H. Mills, "Products of linear recurring sequences," *J. Algebra*, vol. 27, no. 1, pp. 147-157, Oct. 1973.
408. J. Ziv and A. Lempel. On the complexity of finite sequences. *IEEE Trans. Information Theory*, 22:75-81, 1976.
409. J. Ziv and A. Lempel. A universal algorithm for sequential data compression. *IEEE Trans. Information Theory*, 23(3):337-343, 1977.
410. M.V.Živkoviã, "On two probabilistic decoding algorithms for binary linear codes", *IEEE Trans. Information Theory*, 37:1707-1716, Nov. 1991.
411. M.V.Živkoviã, "An algorithm for the initial state reconstruction of the clock-controlled shift register", *IEEE Trans. Information Theory*, 37:1488-1490, Sep. 1991.

Àí ãèí-ðóññèé ì ðàäì àòí ùé óèàçàòàèü

òàðì èí í à àí àèèéñèíì ÿçùéà	òàðì èí í à ðóññèíì ÿçùéà	ñòðàí èòà
1/p generator	ãáí àðàòì ð "1/p"	252
2-adic complexity	2-ààè-àñèàÿ ñèí æí í ñòü	236
2-adic numbers	2-ààè-àñèèà +èñèà	210
2-adic span	2-ààè-àñèèé ðàçì àð	65,211,236
2-adic value (of a register)	2-ààè-àñèí à çì à-áí èà (ðáàèñòðà)	210,232
A5 (algorithm)	èðèì òí àèáí ðèòì À5	257
adaptive algorithm	àààì òèáí ùé àèáí ðèòì	211,237
additive generator	àààèòèáí ùé àáí àðàòì ð	180,255
additive natural stream cipher	àààèòèáí ùé àñòàñòàáí í ùé ì ì òí +í ùé øèòð	297
affine function	àòòèí í àÿ óóí èöèÿ	122,143
algebraic degree (of a function)	àèãááðàè-àñèàÿ ñòàí áí ü óóí èöèè	122,142
algebraic normal form (ANF)	àèãááðàè-àñèàÿ í ì ðì àèüí àÿ òí ðì à (ÁÍ Õ)	54,142
algorithm resetting	ì àðàçàððóçèà àèáí ðèòì à	96
almost bent function	ì ì +òè ááí ò-òóí èöèÿ	109
alternating step generator	ãáí àðàòì ð ñ í àðàì àæàðùèì ñÿ øááí ì	158
ANF transformation	ì ðàí àðàçì àáí èà ÁÍ Õ	55,123
asymmetric cipher	àñèì ì àððè-í ùé øèòð	2
asynchronous cipher	àñèí òðì í í ùé øèòð	8
augmented function	ì ì ì èí áí í àÿ óóí èöèÿ	108
autocorrelation function	óóí èöèÿ ààòì èí ððáèÿöèè	36
autocorrelation test	òàñò ààòì èí ððáèÿöèè	39
balanced function	ñáàèáí ñèðì àáí í àÿ óóí èöèÿ	122,143
balanced sequence	ñáàèáí ñèðì àáí í àÿ ì ì ñèááí ààòàèüí ì ñòü	27,143
base polynomial	ààçì àùé ì ì í àí +éáí	272
Ben-Or algorithm	àèáí ðèòì Ááí -Ì ðà	28
bent mapping	ááí ò-ì òí àðàæáí èà	133
bent function	ááí ò-òóí èöèÿ	109,120,129, 132,144
bent sequence	ááí ò-ì ì ñèááí ààòàèüí ì ñòü	144
bent triple	ááí ò-ððì èéà (Áí áááððèí à)	137
Berlekamp-Massey algorithm	àèáí ðèòì Áàðèàèà ì à-Ì ÿññè	26,44
binary derivative	àáí è-í àÿ ì ðì èçáí áí àÿ	262
binary symmetric channel (BSC)	àáí è-í ùé ñèì ì àððè-í ùé èáí àè (ÄÑÈ)	84,94
birthday paradox	ì àðàáí èñ "áí àé ðì æááí èé"	259

Áεάέεεί áðàöèÿ è εί ääēñ ðáðì εί í á

block cipher	áεί ÷ í úé øèòð	2,141
Blum-Micali generator	ääí áðàòì ð Áεβι à-Ì èεάεε	324
BRM-generator (Binary Rate Multiplier)	ääí áðàòì ð BRM (í áðàì í í æáí èÿ äáí è÷ í úò ñòáí áí áé)	156
carry (operation)	í áðáí í ñ (í í áðàöèÿ)	211
cascade generator	éñéááí úé äáí áðàòì ð	154,159,163
CDPD	ñòáí äáðò ðáéáòí í í í é ñí òí áí é ñáÿçè CDPD	260
cellular automaton	éεáòì ÷ í úé äáðì ì àò	250
Chameleon	"Óàì áεáí í " (éðèì òí εί í ñòðóεèÿ)	283
chaotic cipher	òáí ðè÷-áñéé øèòð	319,334
chosen-ciphertext attack	àòáεà ñ í í áí áðáí í úì øèòððáéñòì	1
chosen-plaintext attack	àòáεà ñ í í áí áðáí í úì í ðèðúòúì ðáéñòì	1
cipher feedback mode	ðáæèí í áðàòì í é ñáÿçè í ð øèòððáéñòá	8
ciphertext	øèòððáéñò	1
ciphertext-only attack	àòáεà òí εüéí í í øèòððáéñòò	1
cleartext	í ðèðúòúé ðáéñò	1
clock-controlled shift register	ðááéñòð ñáéεà ñ í áðááí í ì áðí úì äáεæáí εáì	154
combination generator, combiner	éí ì áéí εðòβúéé äáí áðàòì ð, -- óçæ	69,77
conditional complementing shift register (CCSR)	ðááéñòð ñáéεà ñ òñéí áí úì áí í í éí áí εáì (ĐÑÑÓÄ)	287
congruential generator	éí í áðóÿí òí úé äáí áðàòì ð	20
connection polynomial	í í ééí ì ì í áðàòì í é ñáÿçè	25
constrained edit distance (CED)	ðáñòì ÿí εá í áðáí è÷ áí í í áí ðáááεèðí ááí èÿ (ĐÍ Đ)	212
constrained embedding attack	àòáεà í áðáí è÷ áí í úì áñòðáéááí εáì	191
constrained Levenshtein distance	í áðáí è÷ áí í í á ðáñòì ÿí εá Éáááí øðáéí à	190
correlation attack	éí ððáÿÿèéí í í äÿ àòáεà	80,84
correlation coefficient	éí ÿòöèøéáí ò éí ððáÿÿèé	127
correlation immune function	éí ððáÿÿèéí í í í -éì ì óí í äÿ óóí èðèÿ	119,122
cost function	óóí éøèÿ ñòì èì í ñè	302
Counterpane Systems	éí í ñáεèéí áí äáÿ εðèì òí òèðì à Counterpane Systems	279
critical branching process	éðèðè÷-áñééé ááðáÿúééñÿ í ðí óáññ	259
critical noise probability	éðèðè÷-áñéáÿ ááðí ÿòí í ñòü øóí à	103
cross-correlation function	óóí éøèÿ éðí ññ-éí ððáÿÿèé	84,127
Crypto AG	Éðèì òí ÄÄ, éðèì òí òèðì à	2,4,50
cryptoanalysis	éðèì òí áí áéεç	1
cryptogram	éðèì òí áðáì ì à	1
cryptography	éðèì òí áðàöèÿ	1

Áεάέεεεεεε εε εε εεεε εεεε εε εε εε

cryptology	έεεεεε εε εε εεεε	1
cyclic code	εεεεεε-εεεεεε εε εε	90
De Bruijn function	εεεε εεεεεε εε εε εεεεεε	110
De Bruijn property	εεεε εεεεεε εε εε εεεεεε	27
De Bruijn sequence	εεεεεεεεεεεεεεεεεε εεεεεε εε εεεεεεεε	27,50,252
degenerate initial loading	εεεεεεεεεε εε εε εε εεεεεε εε εεεε εεεε εεεε	234
deletion rate	εεεεεε εε εε εεεεεε εε	197,201
dense polynomial	εεεεεε εε εε εεεεεε	33
[d,k]-self-decimation generator	εεεε εεεεεε εε [d,k]-εεεε εεεεεε-εεεε εεεε	161
decimation of sequence	εεεεεε-εεεε εε εε εεεεεε εεεεεεεεεε εεεε	154,190
DES (Data Encryption Standard)	εεεε εεεεεε εεεε-εεεε εε εεεεεε εεεε εεεε DES	2,173
difference decimation sequence	εεεεεεεεεε εεεεεεεεεε εεεεε εεεεε εεεεε-εεεε εεεε	157
difference set	εεεεεεεεεε εεεεε εεεεεε	132
differential cryptanalysis	εεεεεεεεεε εεεεεεεε εε εεεεεε εε εεεεεε	297
Diffie's randomized cipher	εεεε εεεε εεεεεε εεεε εεεε εεεεεε εεεεεε	330
digital signal processor (DSP)	εεεε εεεεεεεεεεεεεε εεεε εεεε εεεεεεεε εε DSP	272
directed acyclic word graph	εεεε εεεεεεεε εεεε εεεεεεεε-εεεεεε εεεεε εεεε εε	64
direct matching algorithm	εεεεε εεεεε εεεε εεεεεεεεεεεεεε εεεε εεεεεεεεεεεε	197
discrepancy	εεεεεε εεεεεε εε	65
distance between functions	εεεεεεεε εεεε εε εεεεε εεεεεεεεεε εε	129
divide-and-conquer attack	εεεεεε "εεεεεεεεεε-εεεεεεεεεε"	80,85
D-transform	D-εεεε εεεεεεεεεε εεεε εε	225
ε-bias distribution	ε-εεε εεεεεε εεε εεεεε εεεεεεεεεε εε	176
Elementrix Technologies	εεεεε εε εεεεεε εεεεε εεεεε εεεεε, εεεεε εε	334
embedding attack	εεεεε εεεεεεεεεεεεεε εεεε	196
equidistant set	εεεεεεεεεεεεεε εεεεε εεεεεεεεεε	114
error-free information set	εεεε εεεεε εεε εεε εεεεεε εεε εεεεεε εεεεεε εεεεε-εεεε	103
evolution program	εεεε εεεεεεεεεεεεεε εεεε εεεε εεεε εε	306
exhaustive search	εεεεεεεεεε εεεε εεεεεεεεεε	81,162,178
fast correlation attack	εεεεεεεεεε εεεεεεεεεεεεεε εεεε εεεεεε	81,86
fast resetting	εεεεεεεεεε εεεεεεεεεεεεεε	97
feedback clock control	εεεε εεεε εεεεεεεε εε εεεεεεεεεε εεε εεεεεεεεεε εεεεεε	154
feedback integer	εεεεε εε-εεεεε εεεεεεεεεε εεεεεεεεεε	210,231
feedback polynom	εεεεεεεεεε εεεεεεεεεε εεεεεε	26
feedback shift-register	εεεεεεεεε εεεεεεεε εεεεεεεεεε εεεεεεεεεε	25

Áèáèèí àðàòèý è èí áàèñ òàðì èí í á

feedback shift-register with carry operation, FCSR	ðáàèñòð ñáàèà ñ í áðàòí í é ñáýçùþ ñ í í áðàòèáé í áðáí í ñà , ÐÑÌ ÑÌ	209
Fibonacci register	ðáàèñòð Òèáí í á++è	29
Fibonacci sequence	í í ñèááí áàòáèíí í ñòü Òèáí í á++è	181
filter generator	òèèüòðòþùèè ááí áðàòí ð	69-77
finite state machine	ì áøèí à ñ èí í á+í ùì +èñèí ñ ñòí ýí èé	57
Fish (algorithm)	àèáí ðèòì øèòðí ááí èý Fish	180
fitness function	óóí èòèý ñí í òáàòñòáèý	306
forward clock control	óí ðáàèáí èà áàèæáí èàì (áèòáí è áðòáí áí ðáàèñòðá)	154
free energy minimisation	ì èí èí èçàòèý ñáí áí áí í é ýí áðèèè	97
frequency test	+àñòí òí ùé òáñò	38
Fourier transform	í ðáí áðáçí ááí èà Óòðüá	51,175
full adder	í í èí ùé ñòí ì áòí ð, ñòí ì áòí ð ñ 3 áòí ááí è	231
full positive difference set	í í èí í á ì í í æáñòáí í í èí æèòáèíí ùò ðáçí í ñòáé	114
Galois register	ðáàèñòð Áàèóá	29,32
GCHQ (Government Communications Head-Quarter)	ØÈÌ Ñ (Øòáá-èáàðòèðá í ðáàèòáèííòááí í í é ñáýçè Áàèèèí áðèòáí èè)	259
Geffe generator	ááí áðàòí ð Ááòóá	81,245
generating function	í ðí èçáí áýùàý óóí èòèý	225
generator matrix	í í ðí æááþùàý ì áððèòá	89
generator polynomial	í í ðí æááþùèé ì í í áí +èáí	90
genetic algorithm	ááí áòè+áñèèé áèáí ðèòì	302,306
geometric sequence	ááí ì áððè+áñèáý í í ñèááí áàòáèíí í ñòü	50,79
Gifford generator	ááí áðàòí ð Áèòóí ðáá	256
GOAL (algorithm)	èðèí òí àèáí ðèòì GOAL	277
Golomb postulates	í í ñòèèàòù Áí èí ì áá	36
Gretag AG	Áðáòáá ÁÁ, èðèí òí óèðí á	2,86
GSM (Group Special Mobile)	ñèñòáí à ì í áèèíí í é ñáýçè GSM	257
Hadamard matrix	áááí áðí áá ì áððèòá	54,143
Hadamard product	áááí áðí áí í ðí èçááááí èà	60
Hamming code	èí á Òýí ì èí áá	91
Hamming distance	ðáññòí ýí èá Òýí ì èí áá	86,89,120,143
Hamming weight	ááñ Òýí ì èí áá	52,79,89,123,143
historical work characteristic (of cipher)	èñòí ðè+áñèáý ðááí +áý òáðáèòáðèñòèèá (øèòðá)	15
IA (generator)	ááí áðàòí ð IA	280
IBAA (generator)	ááí áðàòí ð IBAA	281
ideally secure cryptosystem	èáááèíí í ñòí èèáý øèòðñèñòáí à	5,12,15

Àèáèèì áðàòèÿ è èí ááèñ òáðì èí í á

IBM	Àé-Áe-Ýì , òèðì à	160,263
information set	èí òíðì àðèí í í á ì í í áæñòáì	103
information vector	èí òíðì àðèí í í ùé ááèðì ð	91
initialization vector	ááèðì ð èí èòèàèèçàòèè	293
inner product generator	ááí áðàòì ð ñèàèÿðí í áì í áðàì í í áéí èÿ	249
interlacing	í áðáì èáðáí èà (í í ñèááí áàòàèüí í ñòáé)	154,160
interleaving	í ðì ñèàèááí èà (í í ñèááí áàòàèüí í ñòáé)	154,160
interleaved sequence	í ðì ñèí áí í áÿ í í ñèááí áàòàèüí í ñòü	185
intersection coefficient	èí ÿòòèðèáí ò í áðáñá-áí èÿ	114
intractability hypothesis	áèí ì ðàçà í í áðàçðàøèì í ñòè	319
inverse attack	èí ááðñèí í í áÿ àòàèà	113
iterative probabilistic decoding	èòáðàòèí í í í-ááðì ÿðí í ñòí í á ááèí áèðì ááí èà	94
ISAAC (generator)	ááí áðàòì ð ISAAC	280
Jennings generator	ááí áðàòì ð Áæáí í èí áñà	247
Kerckhoffs' assumption	áí í óùáí èà Èáðèðì òòñà	1
keystream	øèòðòð ùáÿ í í ñèááí áàòàèüí í ñòü	3
keystream generator	ááí áðàòì ð ááí ì ù	3
Khufu	èðèí òí áèáí ðèòì Khufu (áèí + í ùé)	264
knapsack generator	ðáí óááùé ááí áðàòì ð	254
Kronecker product	èðì í áéáðì áñèí á í ðì èçááááí èà	143
known-ciphertext attack	àòàèà ñ èçááñòí ùì øèòððáèñòí ì	1
known-plaintext attack	àòàèà ñ èçááñòí ùì í òèðùòùì òáèñòí ì	1
lagged Fibonacci generator	çàì áçàùááð ùéé ááí áðàòì ð Òèáí í à++è	180
Lempel-Ziv complexity	ñèí áéí í ñòü Èáì í áèà-çèáá	64
Levenshtein distance	ðáññòí ÿí èà Èáááí øòáéí á	193
LFSR-sequence	ðÑÈÌ Ñ-í í ñèááí áàòàèüí í ñòü	27
linear complexity	èèí áéí áÿ ñèí áéí í ñòü (í í ñèááí áàòàèüí í ñòè)	26,43
linear complexity profile	í ðì òèèü èèí áéí í é ñèí áéí í ñòè	56
linear complexity profile test	òáñò í á í ðì òèèü èèí áéí í é ñèí áéí í ñòè	57
linear congruential generator (LCG)	èèí áéí ùé èí í áðóÿí òí ùé ááí áðàòì ð (ÈÈÁ)	4,16,20
linear feedback shift register (LFSR)	ðááèñòð ñááèèà ñ èèí áéí í é í áðàòì í é ñáÿçüð (ðÑÈÌ Ñ)	4,24-34,
linear function	èèí áéí áÿ Òóí èòèÿ	122,143
linear cryptanalysis	èèí áéí ùé èðèí òí áí áèèç	300
linear recurrence sequence	èèí áéí áÿ ðáèóððáí òí áÿ í í ñèááí áàòàèüí í ñòü	25
linear sequential circuit approximation (LSCA)	áí í ðì èñèì áðèÿ èèí áéí í é í í ñèááí áàòàèüí í é ñòáí í é (ÀÈÌ Ñ)	192,201,224,300

Àèáèèì áðàòèÿ è èí ààèñ òàðì èí í á

linear span	èèí áéí úé ðàçì àð	26,43
linear structure function	óóí èòèÿ èèí áéí í é ñòðòéóððí é	131
local randomization	èí èàèüí àÿ ðàí áí ì èçàòèÿ	13
lock-in effect	ýòòáèò çàì èðáí èÿ	160,163
look-up table	ì ðì ñì í òðì áàÿ òààéèòà	339
<i>l</i> -sequence	<i>l</i> -ì í ñèááí ààòáèüí í ñòü	211,240
Maple	ì àòáì àèè-áñèèé ì ðì áðàì ì í úé ì àèàð Maple	241
Maurer's randomized cipher	ðáí áí ì èçèðì ááí í úé øèòð Ì áóðáðà	332
maximal period generator	ááí áðàòì ð ì àèñèì àèüí í áí ì áðèí áà	16
maximum order complexity	ñèí æí í ñòü ì àèñèì àèüí í áí ì ì ðÿáèà	64
MD5 (hash-algorithm)	àèáí ðèòì òÿøèðì ááí èÿ MD5	264
meet-in-the-middle attack	àòáèà "áñòðá-à ì í ñáðááéí á"	104,259,290
Mersenne exponent	ýèñì í í áí òà Ì áðñáí í á	273
Metropolis algorithm	àèáí ðèòì Ì áòðì í í èèñà	303
<i>m</i> -sequence	<i>m</i> -ì í ñèááí ààòáèüí í ñòü	27,70
<i>m</i> -sequence cascade	èáñèáä <i>m</i> -ì í ñèááí ààòáèüí í ñòáé	159
multiplexer generator	ì óèüòèì èáèñì ð-ááí áðàòì ð	247,290,296
National Security Agency (NSA)	Áááí òñòáí í áðèí í àèüí í é ááçì í áíí í ñèè ÑØÀ	34,132
next bit test (predictor)	òáñò ñèááóðçááí áèòà (ì ðááñèáçàòáèü)	320
nonlinearity	í áèèí áéí í ñòü	143
non-uniform decimation	í áðááí ì ì áðì í á òñá-áí èà	155
objective function	òáèááàÿ Óóí èòèÿ	302
Omnisc AG	Ì ì í èñáé ÁÁ, èðèì òí Óèðì à	2,39,317
one-time pad	í áí ì ðàçì áúé áàì ì -áéí èí ì ò	3,13
on-line algorithm	"ì í -èáéí í áúé" àèáí ðèòì	65
orthogonal code	ì ðòì áí í àèüí úé èí á	90
ORYX (algorithm)	èðèì òí àèáí ðèòì ORYX	278
Pari	ì àòáì àèè-áñèèé ì ðì áðàì ì í úé ì àèàð Pari	241
parity check	ì ðì ááðèà -áòí í ñòè	82
parity-check matrix	ì àððèòà ì ðì ááðèè -áòí í ñòè	90
parity-check polynomial	ì í í áí -èáí ì ðì ááðèè -áòí í ñòè	90
Parseval equation	óðááí áí èà Ì áðñááàèÿ	120
partial joint probability	-áñòè-í àÿ ñì áì áñòí àÿ ááðì ÿòì í ñòü	199
perfect generator	ñì ááðòáí í úé ááí áðàòì ð	319,321
perfectly secure cryptosystem	ñì ááðòáí í ì ñòì èéàÿ øèòðñèñòáì à	3,4,12
perfect nonlinear function	ñì ááðòáí í àÿ í áèèí áéí àÿ Óóí èòèÿ	120,131

Àèáèèí àðàòèý è èí ààèñ òàðì èí í à

period of register	ì àðèí à ðààèñòðà	25
period of sequence	ì àðèí à í ì ñèàáí ààòàèüí í ñòè	25,57
Philips Crypto	Ôèèèí ñ Êðèí òí, èðèí òí òèðì à	55,64,268
PIKE (algorithm)	èðèí òí àèáí ðèòì PIKE	276
plaintext	ì òèðòòòùé òàèñò	1
Pless generator	àáí àðàòì ð Ì èáññà	81,246
pn-sequence, (pseudo-noise ...)	Ì Ø-í í ñèàáí ààòàèüí í ñòù, (í ñàááí -øóí í ààý ...)	36
positive difference set	ì í í æáñòáí í í èí æèòàèüí ùò ðàçí í ñòàé	115
POTP (Power One Time Pad)	"Ì í ùí í á í áí í ðàçí áí à ààí ì èðí àáí èà"	319,334
practical security	ì ðàèòè-àñèàý ñòí èéí ñòù	15
predictor (next bit test)	ì ðàáñèàçòàèü (òáñò ñèàáòðùááí àèòà)	320
primitive polynom	ì ðèí èòèáí ùé ì í í áí -èáí	27
probabilistic constrained edit distance (PCED)	àáðì ýòí í ñòí í à ðáññòí ýí èà í áðáí è-áí í í áí ðàáàèòèðí àáí èý (ADÍ Ð)	191
propagation criterion of degree k	èðèòàðèé ðáñí ðí ñòðáí áí èý ñòáí áí è k	121,142
pseudo-random function family	ñáí àéñòáí í ñàááí ñèó-àéí ùò òóí èòèé	263
pseudo-random sequence	ì ñàááí ñèó-àéí àý í í ñèàáí ààòàèüí í ñòù	3
pseudo-random sequence generator	àáí àðàòì ð í ñàááí ñèó-àéí í é ì í ñèàáí ààòàèüí í ñòè	3
public key cryptosystem	øèòðñèñòáí à ñ ñ òèðòòòùì èèð-í ì	2
quadratic residue generator	àáí àðàòì ð èááàðàòè-í ùò àù-àòí à	327
quadratic span	èááàðàòè-í ùé ðàçí àò	64
R ³ Security Engineering	èí í ñàèòèí áí ààý èðèí òí òèðì à R ³ Security Engineering	4
Racal Comsec	Ðýééé Êí ì ñàé, èðèí òí òèðì à	307
randomized cipher	ðáí áí ì èçèðí àáí í ùé øèòð	318
randomizer	ðáí áí ì èçàòì ð	6,318,329
RC2 (algorithm)	èðèí òí àèáí ðèòì RC2 (àéí-í ùé)	260
RC4 (algorithm)	èðèí òí àèáí ðèòì RC4	260
regular clocking and no memory	ñòáí à ááç í àì ýòè ñ ðááí í ì áðí ùì ààèæáí èàí	69
regular decimation	ðááí í ì áðí í à òñá-áí èà (í í ñèàáí ààòàèüí í ñòè)	155
repetition test	òáñò í à í í áòí ðáí èý	41
resilient function	ýèáñòè-í àý òóí èòèý	121,150
resynchronization	ðáñèí òðí í èçàòèý	258,292
reversion attack	ðáááðñèí í í àý àòàèà	259
ripple adder	ñòí ì áòí ð ñí ñèáí çí ùì í áðáí í ñí ì	231
Rip van Winkle cipher	øèòð "Ðèí àáí Áéí èèü"	331
root presence test	òáñò í à í ðèñòòòàèà èí ðí ý	73

Àèáèèì áðàòèý è èí áàèñ òàðì èí í á

RSA (algorithm)	àèáí ðèòì RSA	322
RSA generator	ááí áðàòì ð RSA	326
running key generator	ááí áðàòì ð ààì ì ù	3
run test	òáñò ñáðèé	39
sampled sequence	ñýì ì èèðì ááí í àý (áúáí ðì ÷ í àý) ì ì ñèááí áàòàèüí ì ñòü	190
S-box	òàáèèöà çàì áí ù (S-áí èñ)	260,267,274
Schnorr generator	ááí áðàòì ð Øí ì ððà	13
scrambler	ñèðýì áéáð	9
SEAL (algorithm)	éðèì òì àèáí ðèòì SEAL	263
secret key	ñáèðàòì ùé èèþ÷	1
secret key cryptosystem	øèððñèñòàì à ñ ñáèðàòì ùì èèþ÷íì	2
Secure Hash Algorithm (SHA)	àèáí ðèòì òýøèðì ááí èý SHA	265,277
self-shrinking generator	ñàì ì ñæèì àþùèé ááí áðàòì ð	162,184
self-synchronizing cipher	ñàì ì ñèì òðì í èçèððþùèéñý øèòð	7,8,284
semi-infinite sequence	ì ì èóááñèí ì á÷ í àý ì ì ñèááí áàòàèüí ì ñòü	42
serial test	ì ì ñèááí áàòàèüí ùé òáñò	38
sequence of function	ì ì ñèááí áàòàèüí ì ñòü òóí èöèè	122,143
Shamir's generator	ááí áðàòì ð Øàì èðà	322
shrinking generator	ñæèì àþùèé ááí áðàòì ð	154,160,173
shrunk polynomial	ñæàòùé ì ì èèí ì ì	201
Siemens AG	Ñèì áí ñ ÆÅ, òèðì à	180
simulated annealing	ñèì óéýòì ð ì òæèáà (àèáí ðèòì)	302
singular device	ñèì áóèýðì í á òñòðì éñòáí	161
sliding window	ñèì èüçýùáá ì éí ì	103
span	ðàçì áò (ì ì ñèááí áàòàèüí ì ñòè)	43
sparse polynomial	ì ðì ðáæáí í ùé ì ì èèí ì ì	33
spectral radius	ñì áèòðàèüí ùé ðáàèóñ	139
stage	ý÷áéèà ðáàèñòðà, ñòóí áí ù èáñèááà	32
state	ñì ñòì ýí èà (áàòì ì àòà)	57,231
statistical test	ñòàòèñòè÷-áñèèé òáñò	321
"step _{k,m} "-cascade	"Øáá _{k,m} "-èáñèááí á	164
step-once-twice generator	ááí áðàòì ð ì áèí -ááà-Øááà	156
stop-and-go generator	ááí áðàòì ð ñòì ì -áí áðáá	156
stream cipher	ì ì òì ÷ í ùé øèòð	2
strict avalanche criterion, SAC	ñòðì áèè èáàèí í ùé èðèòàðèé, ÑÈÈ	121,141
substitution probability	áàðì ýòì ì ñòü çàì áí ù	199

Àéáèèí äðàòèÿ è èí äáèñ òáðì èí í á

suffix tree	ääðaaí ñóóòèèñí á	64,66
summation combiner	ñòì ì èðòðùèé èí ì áéí èðòðùèé óçáè, ñòì ì àòì ð	65,128,213,253
switch controlled feedback shift register	ðááèñòð ñááèää ñ èí ì ì óðèðóàì í é í áðàòì í é ñáÿçùð	270
Sylvester-Hadamard matrix	ì àððèòà Ñèèüááñòðà-Àáàì áðà	143
symmetric cipher	ñèì ì àððè-í ùé øèòð	2
synchronization loss	í ì òáðÿ ñèì òðì í éçàòèè	292
synchronous cipher	ñèì òðì í í ùé øèòð	7
taps	òì-èè ñúàì à, í òáì äü	25,174
template	øááèí í	177
theoretical security	òáì ðàðè-áñèäÿ ñòì ééí ñòü	14
threshold generator	í ì ðì áí áùé ááí áðàòì ð	248
total correlation	ñòì ì áðì äÿ èí ððáèÿòèÿ	126,127
truncated congruential generator	óñá-áí í ùé èí ì áðóÿ óí ùé ááí áðàòì ð	20
truth table of function	òááèèòà èñòèí í ì ñòè Óóí èòèè	122,143
Turing-Kolmogorov complexity	ñèí áí í ñòü Õüððèí ää-Èí èí í áí ðì ää	318
Turing machine	ì àøèí à Õüððèí ää	318
unconditionally secure cryptosystem	ááçóñèí áí í ñòì ééäÿ øèòðñèñòàì à	12
unicity distance	ðáññòì ÿí èà ááèí ñòááí í ì ñòè	12
uniform decimation	ðááí í ì áðì í á óñá-áí èà	155
uniformity test	òáñò ðááí í ááðì ÿóí í ñòè	38
universal test	óí èááðñáèüí ùé òáñò	39
variable connections	í áðàì áí í ùá òì-èè ñúàì à (ðááèñòðà)	174
Vernam cipher	øèòð Ááðì àì à	3,10,13
WAKE (algorithm)	èðèí òì áèáí ðèòì WAKE	275
Walsh-Hadamard matrix	ì àððèòà Óí èøà-Àáàì áðà	143
Walsh transformation	í ðáì áðàçí ááí èà Óí èøà	53,120,123,215
Wolfram generator	ááí áðàòì ð Áí èüòðàì à	250
work characteristic (of cipher)	ðááí -äÿ òáðàèòàðèñòèèà (øèòðà)	15,318
Ziv-Lempel compression algorithm	Àèáí ðèòì ñæàòèÿ ááí í ùó Çèää-Èáì í áèà	268

Ðóññèî-àí ãèèéñèèé ì ðààì àòì ùé óèàçàòàèü

òàðì èí í à ðóññèî ÿçùéà	òàðì èí í à àíãèèéñèè ÿçùéà	ñòðàí èòà
2-ààè-àñèèäý ñèí æí í ñòü	2-adic complexity	236
2-ààè-àñèèèà +èñèèà	2-adic numbers	210
2-ààè-àñèèèé ðàçì àð	2-adic span	65,211,236
2-ààè-àñèèí à çí à-áí èà (ðààèñòðà)	2-adic value (of a register)	210,232
Àááí òñòáí í àèèí í àèüí í é áàçì í àñí í ñòè ÑØÀ	National Security Agency (NSA)	34,132
àààì àðì àà ì àòðèòà	Hadamard matrix	54,143
àààì àðì àí ì ðì èçàáááí èà	Hadamard product	60
àààì òèáí ùé àèáí ðèòì	adaptive algorithm	211,237
ààèèòèáí ùé ááí àðàòì ð	additive generator	180,255
ààèèòèáí ùé àñòáñòááí í ùé ì ðì +í ùé øèòð	additive natural stream cipher	297
Àé-Àè-Ýì , òèðì à	IBM	160,263
àèáááðàè-àñèèäý ì ðì àèüí àý òì ðì à (ÀÍ Õ)	algebraic normal form (ANF)	54,142
àèáááðàè-àñèèäý ñòàí áí ü òóí èòèè	algebraic degree (of a function)	122,142
àèáí ðèòì RSA	RSA (algorithm)	322
àèáí ðèòì Ááí-Ì ðà	Ben-Or algorithm	28
àèáí ðèòì Áàðèèèè à-Ì ÿññè	Berlekamp-Massey algorithm	26,44
àèáí ðèòì àéí +í ì áí øèòðì ááí èý DES	DES (Data Encryption Standard)	2,173
àèáí ðèòì Ì àòðì ì ì èèñà	Metropolis algorithm	303
àèáí ðèòì í áí ì ñðááñòááí í ì áí ñí ì òááòñòàèý	direct matching algorithm	197
Àèáí ðèòì ñæàòèý ááí í ùò Çèàà-Èàì ì àèà	Ziv-Lempel compression algorithm	268
àèáí ðèòì òýøèðì ááí èý MD5	MD5 (hash-algorithm)	264
àèáí ðèòì òýøèðì ááí èý SHA	Secure Hash Algorithm (SHA)	265,277
àèáí ðèòì øèòðì ááí èý Fish	Fish (algorithm)	180
àí ì ðì èñèì àèý èèí àéí í é ì ñèááí ààòàèüí í é ñòàí í é (ÀÈÌ Ñ)	linear sequential circuit approximation (LSCA)	192,201,224,300
àñèì ì àòðè-í ùé øèòð	asymmetric cipher	2
àñèí òðì í ì ùé øèòð	asynchronous cipher	8
àòàèà "àñòðà-à ì ññáðáèé á"	meet-in-the-middle attack	104,259,290
àòàèà "ðàçááèýé-è-àñèðùáàé"	divide-and-conquer attack	80,85
àòàèà àñòðàèèááí èàì	embedding attack	196
àòàèà ì áðáí è-áí í ùì àñòðàèèááí èàì	constrained embedding attack	191
àòàèà ñ èçááñòì ùì ì ðèðòóòùì òàèñòì ì	known-plaintext attack	1
àòàèà ñ èçááñòì ùì øèòðòàèñòì ì	known-ciphertext attack	1
àòàèà ñ ì ì áí áðáí í ùì ì ðèðòóòùì òàèñòì ì	chosen-plaintext attack	1

Àèáèèí àðàòèÿ è èí ààèñ òàðì èí í à

àòàèà ñ í í àí àðàí í ùì øèòðòàèñòí ì	chosen-ciphertext attack	1
àòàèà òí èüéí í í øèòðòàèñòó	ciphertext-only attack	1
àòòèí í àÿ òóí èòèÿ	affine function	122,143
áàçí àÛé ì í í àí ÷éáí	base polynomial	272
ááçòñèí áí í ñòí ééàÿ øèòðñèñòàì à	unconditionally secure cryptosystem	12
ááí ò-í òí àðàæáí èà	bent mapping	133
ááí ò-í í ñèááí ààòàèüí í ñòü	bent sequence	144
ááí ò-òðí éèà (Áí ááàðòèí à)	bent triple	137
ááí ò-òóí èòèÿ	bent function	109,120,129, 132,144
áèí ÷í Ûé øèòð	block cipher	2,141
áÛñòðàÿ èí ððàèÿòèí í í àÿ àòàèà	fast correlation attack	81,86
áÛñòðàÿ í àðàçáàðòçèà	fast resetting	97
ááèòí ð èí èòèàèèçàòèè	initialization vector	293
ááðí ÿòí í ñòí í à ðàññòí ÿí èà í àðàí è÷áí í í àí ðááàèòèðí ááí èÿ (ÁÐÍ Ð)	probabilistic constrained edit distance (PCED)	191
ááðí ÿòí í ñòü çàì áí ù	substitution probability	199
ááñ Õÿí ì èí àà	Hamming weight	52,79,89,123,143
áÛðí æááí í í à í à÷àèüí í à çàì í èí áí èà	degenerate initial loading	234
ááí àðàòí ð "1/p"	1/p generator	252
ááí àðàòí ð [d,k]-ñàì í òñà÷áí èÿ	[d,k]-self-decimation generator	161
ááí àðàòí ð BRM (í àðàí í í æáí èÿ ááí è÷í ùò ñòáí áí áé)	BRM-generator (Binary Rate Multiplier)	156
ááí àðàòí ð IA	IA (generator)	280
ááí àðàòí ð IBAA	IBAA (generator)	281
ááí àðàòí ð ISAAC	ISAAC (generator)	280
ááí àðàòí ð RSA	RSA generator	326
ááí àðàòí ð Áèçì à-Ì èèàèè	Blum-Micali generator	324
ááí àðàòí ð Áí èüòðàì à	Wolfram generator	250
ááí àðàòí ð ááì ì ù	keystream generator	3
ááí àðàòí ð ááì ì ù	running key generator	3
ááí àðàòí ð Ááòòá	Geffe generator	81,245
ááí àðàòí ð Áèòòí ðáà	Gifford generator	256
ááí àðàòí ð Áæáí í èí áñà	Jennings generator	247
ááí àðàòí ð éáàððàòè÷í ùò áÛ÷àòí à	quadratic residue generator	327
ááí àðàòí ð ì àèñèì àèüí í áí í àðèí áá	maximal period generator	16
ááí àðàòí ð í àèí -áàà-òáá	step-once-twice generator	156
ááí àðàòí ð Ì èáññà	Pless generator	81,246

Àèáèèí àðàòèý è èí ààèñ òàðì èí í à

àáí àðàòí ð í ñàáí ñèó÷áéí í é í í ñèáí ààòáèí í ñòè	pseudo-random sequence generator	3
àáí àðàòí ð ñ í àðáí àèàðùèí ñý øááí ì	alternating step generator	158
àáí àðàòí ð ñèàèýðí í áí í àðáí í í æáí èý	inner product generator	249
àáí àðàòí ð ñòí í -áí àðáá	stop-and-go generator	156
àáí àðàòí ð Øàí èðà	Shamir's generator	322
àáí àðàòí ð Øí í ððà	Schnorr generator	13
àáí àðè÷áñèéé àèáí ðèòí	genetic algorithm	302,306
àáí ì àððè÷áñèàý í í ñèáí ààòáèí í ñòù	geometric sequence	50,79
àèí í òàçà í í àðàçðàøèí í ñòè	intractability hypothesis	319
Àðàòáá ÁÁ, èðèí òí òèðí à	Gretag AG	2,86
àáí è÷í àý í ðí èçáí áí àý	binary derivative	262
àáí è÷í ùé ñèí ì àððè÷í ùé èáí àé (ÁÑÈ)	binary symmetric channel (BSC)	84,94
àáðááí ñóòòèèñí à	suffix tree	64,66
àèòòáðáí òèàèí ùé èðèí òí áí àèèç	differential cryptanalysis	297
áí í òùáí èà Éáðèòí òòñà	Kerckhoffs' assumption	1
D-í ðáí àðàçí àáí èà	D-transform	225
çáí àçàùááðùéé àáí àðàòí ð Õéáí í à÷÷è	lagged Fibonacci generator	180
èáááèí í ñòí èéàý øèòðñèòáí à	ideally secure cryptosystem	5,12,15
èí àáðñèí í í àý àðàèà	inverse attack	113
èí òí ðí àòèí í í á ì í í æáñòáí	information set	103
èí òí ðí àòèí í í ùé àáèòí ð	information vector	91
èñòí ðè÷áñèàý ðááí ÷àý òáðàèòáðèñòèèà (øèòðà)	historical work characteristic (of cipher)	15
èòáðàòèí í í í -ááðí ýòí í ñòí í á ááéí àèðí àáí èà	iterative probabilistic decoding	94
èáñèàá m-í í ñèáí ààòáèí í ñòáé	m-sequence cascade	159
èáñèàáí ùé àáí àðàòí ð	cascade generator	154,159,163
èáááðàðè÷í ùé ðàçì àð	quadratic span	64
èèàòí ÷í ùé ààòí ì àò	cellular automaton	250
èí à Õýí ì èí àá	Hamming code	91
èí ì áéí èðòðùèé àáí àðàòí ð, -- óçáé	combination generator, combiner	69,77
èí í áðóýí òí ùé àáí àðàòí ð	congruential generator	20
èí í ñàèòèí áí ááý èðèí òí òèðí à R ³ Security Engineering	R ³ Security Engineering	4
èí í ñàèòèí áí ááý èðèí òí òèðí à Counterpane Systems	Counterpane Systems	279
èí ððáèýòèí í í àý àðàèà	correlation attack	80,84
èí ððáèýòèí í í í -èí ò í í àý òóí èöèý	correlation immune function	119,122
èí ýòòèèéáí ò èí ððáèýòèé	correlation coefficient	127

Àèàèèì àðàòèÿ è èí ààèñ òàðì èí í à

èí ÿòòèèèáí ò í àðàñà-áí èÿ	intersection coefficient	114
Èðèì òì ÆÆ, èðèì òì òèðì à	Crypto AG	2,4,50
èðèì òì àèáì ðèòì GOAL	GOAL (algorithm)	277
èðèì òì àèáì ðèòì Khufu (áèí ÷í Ûé)	Khufu	264
èðèì òì àèáì ðèòì ORYX	ORYX (algorithm)	278
èðèì òì àèáì ðèòì PIKE	PIKE (algorithm)	276
èðèì òì àèáì ðèòì RC2 (áèí ÷í Ûé)	RC2 (algorithm)	260
èðèì òì àèáì ðèòì RC4	RC4 (algorithm)	260
èðèì òì àèáì ðèòì SEAL	SEAL (algorithm)	263
èðèì òì àèáì ðèòì WAKE	WAKE (algorithm)	275
èðèì òì àèáì ðèòì Å5	A5 (algorithm)	257
èðèì òì áí àèèç	cryptoanalysis	1
èðèì òì àðàì ì à	cryptogram	1
èðèì òì àðàòèÿ	cryptography	1
èðèì òì èí àèÿ	cryptology	1
èðèòàðèé ðàñì ðì ñòðàí áí èÿ ñòáí áí è k	propagation criterion of degree k	121,142
èðèòè-àñèàÿ ààðì ÿòì í ñòù øòì à	critical noise probability	103
èðèòè-àñèèé ààòáÿ Ûèéñÿ í ðì òàññ	critical branching process	259
èðì í àèàðì àñèí á í ðì èçàáááí èà	Kronecker product	143
èèí áéí àÿ ðàèòððáí òí àÿ í í ñèááí ààòàèüí í ñòù	linear recurrence sequence	25
èèí áéí àÿ ñèí áéí í ñòù (í í ñèááí ààòàèüí í ñòè)	linear complexity	26,43
èèí áéí àÿ òóí èòèÿ	linear function	122,143
èèí áéí Ûé èí í àðóÿ òí Ûé ááí àðàòì ð (ÈÈÅ)	linear congruential generator (LCG)	4,16,20
èèí áéí Ûé èðèì òì áí àèèç	linear cryptanalysis	300
èèí áéí Ûé ðàçì àð	linear span	26,43
èí èàèüí àÿ ðàí áí ì èçàòèÿ	local randomization	13
ì àòàì àðè-àñèèé í ðì àðàì ì í Ûé í àèàð Maple	Maple	241
ì àòàì àðè-àñèèé í ðì àðàì ì í Ûé í àèàð Pari	Pari	241
ì àòðèòà í ðì áàðèè ÷àðì í ñòè	parity-check matrix	90
ì àòðèòà Ñèèüááñòðà-Åààì àðà	Sylvester-Hadamard matrix	143
ì àòðèòà Óí èøà-Åààì àðà	Walsh-Hadamard matrix	143
ì àøèí à ñ èí í á-í Ûì ÷èñèí ì ñí ñòì ÿí èé	finite state machine	57
ì àøèí à Õüððèí àà	Turing machine	318
ì èí èì èçàòèÿ ñàí áí áí í é ÿí àðàèè	free energy minimisation	97
ì í í àí ÷éáí í ðì áàðèè ÷àðì í ñòè	parity-check polynomial	90
ì í í àèñòáí ÿ í èí àèòàèüí Ûò ðàçì í ñòàé	positive difference set	115

Àéáèèí àðàòèÿ è èí ààèñ òàðì èí í à

ì í í æáñòáí ðàçí í ñòáé	difference set	132
"Ì í Ùí í à í áí í ðàçí áí à ààí í èðí ááí èà"	POTP (Power One Time Pad)	319,334
ì óèùòèí èáèñí ð-ááí àðàòí ð	multiplexer generator	247,290,296
í áí ðàáéáí í Ùé àòèèèè-áñèèè àðàò ñèí à	directed acyclic word graph	64
í àèèí áéí í ñòù	nonlinearity	143
í àðááí í ì áðí í à óñá-áí èá	non-uniform decimation	155
í àðáí è-áí í í à ðáññòí ÿí èá Èáááí òðáéí à	constrained Levenshtein distance	190
í áí í ðàçí áùé ààí í -áèí èí ò	one-time pad	3,13
Ì í í èñáé ÅÅ, èðèí òí òèðí à	Omnisec AG	2,39,317
"í í -èáéí í áùé" àèáí ðèòí	on-line algorithm	65
í ðòí áí í àèùí Ùé èí à	orthogonal code	90
í òèðùòùé òáèñò	cleartext	1
í òèðùòùé òáèñò	plaintext	1
í àðááí èñ "áí áé ðí æááí èé"	birthday paradox	259
í àðàçáãðóçèà àèáí ðèòí à	algorithm resetting	96
í àðáí áí í Ùá ðí -èè ñúáí à (ðáàèñòðà)	variable connections	174
í àðáí í ñ (í í àðàòèÿ)	carry (operation)	211
í àðáí èáòáí èá (í í ñèááí ààòáèùí í ñòáé)	interlacing	154,160
í àðèí à í í ñèááí ààòáèùí í ñòè	period of sequence	25,57
í àðèí à ðááèñòðà	period of register	25
í èí òí Ùé í í èèí í í	dense polynomial	33
í í èèí í í í áðàòí í é ñáÿçè	connection polynomial	25
í í èèí í í í áðàòí í é ñáÿçè	feedback polynom	26
í í èí í á ì í í æáñòáí í í èí æèòáèùí Ùò ðàçí í ñòáé	full positive difference set	114
í í èí Ùé ñòí ì àòí ð, ñòí ì àòí ð ñ 3 áòí ààí è	full adder	231
í í èóááñèí í á-í àÿ í í ñèááí ààòáèùí í ñòù	semi-infinite sequence	42
í í í í èí áí í àÿ Óóí èòèÿ	augmented function	108
í í ðí áí áùé ááí àðàòí ð	threshold generator	248
í í ðí æáàðùàÿ ì àððèòà	generator matrix	89
í í ðí æáàðùé è í í í áí -éáí	generator polynomial	90
í í ñèááí ààòáèùí í ñòù Åá Áððèí à	De Bruijn sequence	27,50,252
í í ñèááí ààòáèùí í ñòù ðàçí í ñòáé óñá-áí èÿ	difference decimation sequence	157
í í ñèááí ààòáèùí í ñòù Óèáí í à-+è	Fibonacci sequence	181
í í ñèááí ààòáèùí í ñòù Óóí èòèè	sequence of function	122,143
í í ñèááí ààòáèùí Ùé òáñò	serial test	38
í í ñòèéàò Æí èí ì áà	Golomb postulates	36

Àèáèèí àðàòèý è èí ààèñ òàðì èí í à

í í òàðý ñèí òðí í èçàòèè	synchronization loss	292
í í òí +í ùé øèòð	stream cipher	2
í í +òè ááí ò-òóí èòèý	almost bent function	109
í ðàèòè+áñèàý ñòí èéí ñòü	practical security	15
í ðááñèàçàòàèü (òáñò ñèááòðùááí áèòà)	predictor (next bit test)	320
í ðáí áðàçí ááí èà ÁÍ Õ	ANF transformation	55,123
í ðáí áðàçí ááí èà Õí èøà	Walsh transformation	53,120,123,215
í ðáí áðàçí ááí èà Õòðüà	Fourier transform	51,175
í ðèì èòèáí ùé ì í íáí +éáí	primitive polynom	27
í ðí áàðèà +àòí í ñòè	parity check	82
í ðí èçáí äýùàý òóí èòèý	generating function	225
í ðí ðáæáí í ùé í í èèí ìì	sparse polynomial	33
í ðí ñèàèááí èà (í í ñèááí áàòàèüí í ñòàé)	interleaving	154,160
í ðí ñèí áí í àý í í ñèááí áàòàèüí í ñòü	interleaved sequence	185
í ðí ñì í òðí áàý òááèèòà	look-up table	339
í ðí òèèü èéí áéí í é ñèí æí í ñòè	linear complexity profile	56
í ñáááí ñèó+æéí àý í í ñèááí áàòàèüí í ñòü	pseudo-random sequence	3
Ï Ø-í í ñèááí áàòàèüí í ñòü, (í ñáááí -òóí í áàý ...)	pn-sequence, (pseudo-noise ...)	36
ðááí +àý òàðàèòàðèñòèèà (øèòðà)	work characteristic (of cipher)	15,318
ðááí ì ì áðí í á òñá+áí èà	uniform decimation	155
ðááí ì ì áðí í á òñá+áí èà (í í ñèááí áàòàèüí í ñòè)	regular decimation	155
ðàçí àò (í í ñèááí áàòàèüí í ñòè)	span	43
ðáí áí ì èçàòì ð	randomizer	6,318,329
ðáí áí ì èçèðí ááí í ùé øèòð	randomized cipher	318
ðáí áí ì èçèðí ááí í ùé øèòð Äèòòè	Diffie's randomized cipher	330
ðáí áí ì èçèðí ááí í ùé øèòð Ì àòðàðà	Maurer's randomized cipher	332
ðáí òááùé ááí áðàòì ð	knapsack generator	254
ðáññòí ýí èà áàèí ñòááí í í ñòè	unicity distance	12
ðáññòí ýí èà Èáááí øòàéí à	Levenshtein distance	193
ðáññòí ýí èà ì áæáó òóí èòèýì è	distance between functions	129
ðáññòí ýí èà í áðáí è+áí í í áí ðáááèòèðí ááí èý (DÍ Ð)	constrained edit distance (CED)	212
ðáññòí ýí èà Õýì ì èí áá	Hamming distance	86,89,120,143
ðáñòí æááí èà	discrepancy	65
ðáááðñèí í í àý àòàèà	reversion attack	259
ðáæèñòð Áæéòà	Galois register	29,32
ðáæèñòð ñáæèà ñ èí ì ì òèèðóáí í é í áðàòí í é ñáýçùð	switch controlled feedback shift register	270

Áèáèèì áðàòèý è èí áàèñ òàðì èí í á

ðáàèñòð ñáàèää ñ èèí áéí í é í áðàòí í é ñâyçüþ (ÐÑĒĪ Ñ)	linear feedback shift register (LFSR)	4,24-34,
ðáàèñòð ñáàèää ñ í áðàáí í ì áðí ùì áàèæáí èàì	clock-controlled shift register	154
ðáàèñòð ñáàèää ñ í áðàòí í é ñâyçüþ	feedback shift-register	25
ðáàèñòð ñáàèää ñ í áðàòí í é ñâyçüþ ñ í í áðàòèáé í áðáí í ñà , ÐÑĪ ÑĪ	feedback shift-register with carry operation, FCSR	209
ðáàèñòð ñáàèää ñ óñèí áí ùì áíí í éí áí èàì (ÐÑÑÓÁ)	conditional complementing shift register (CCSR)	287
ðáàèñòð Òèáí í à++è	Fibonacci register	29
ðáæèì í áðàòí í é ñâyçè í ò øèòðòáèñòà	cipher feedback mode	8
ðáñèí òðí í èçàòèý	resynchronization	258,292
ÐÑĒĪ Ñ-í í ñèááí áàòáèúí í ñòú	LFSR-sequence	27
Ðýéèè Ēí ñáè, èðèí òí òèðì à	Racal Comsec	307
ñàì í ñæèì àþùèè ááí áðàòí ð	self-shrinking generator	162,184
ñàì í ñèí òðí í èçèðòþùèèñý øèòð	self-synchronizing cipher	7,8,284
ñàì í óí ðáàèáí èà áàèæáí èàì í ò í áðàòí í é ñâyçè	feedback clock control	154
ñáàèáí ñèðí ááí í àý í ñèááí áàòáèúí í ñòú	balanced sequence	27,143
ñáàèáí ñèðí ááí í àý Óóí èòèý	balanced function	122,143
ñáí áí áí í á í ò í øèáí è èí òí ðì àòèí í í á í í -áí	error-free information set	103
ñáí èñòáí Āá Áðþèí á	De Bruijn property	27
ñáèðàòí ùé èèþ-	secret key	1
ñàì áèñòáí í ñáááí ñèó-áéí ùò Óóí èòèè	pseudo-random function family	263
ñæàòùé í í èèí í ì	shrunk polynomial	201
ñæèì àþùèè ááí áðàòí ð	shrinking generator	154,160,173
Ñèí áí ñ ĀĀ, òèðì à	Siemens AG	180
ñèì í àòðè-í ùé øèòð	symmetric cipher	2
ñèì óèýòí ð í òæèää (áèáí ðèòì)	simulated annealing	302
ñèí áóèýðí í á óñòðí èñòáí	singular device	161
ñèí òðí í í ùé øèòð	synchronous cipher	7
ñèñòáí à í í áèèúí í é ñâyçè GSM	GSM (Group Special Mobile)	257
ñèí èüçýùáá í éí í	sliding window	103
ñèðýì áèáð	scrambler	9
ñèí æí í ñòú Ēáí í áèà-Çèää	Lempel-Ziv complexity	64
ñèí æí í ñòú ì áèñèì áèúí í áí í í ðýáèà	maximum order complexity	64
ñèí æí í ñòú Òüþðèí áà-Ēí èí í áí ðí áà	Turing-Kolmogorov complexity	318
ñí áàðøáí í àý í áèèí áéí àý Óóí èòèý	perfect nonlinear function	120,131
ñí áàðøáí í í ñòí èéàý øèòðñèñòáí à	perfectly secure cryptosystem	3,4,12
ñí áàðøáí í ùé ááí áðàòí ð	perfect generator	319,321

Àèáèèì áðàòèÿ è èí ààèñ òàðì èí í à

ñì ñòì ÿí èà (ààòì ì àòà)	state	57,231
ñì àèððàèüí Ûé ðààèòñ	spectral radius	139
ñì àòèàèèèèèðì ààí í Ûé ì ðì òàññì ð DSP	digital signal processor (DSP)	272
ñòàí ààðò òàéàòì í í í é ñì òí àí é ñàÿçè CDPD	CDPD	260
ñòàòèñòè-áñèèé òàñò	statistical test	321
ñòàí áí ù òààèáí èé	deletion rate	197,201
ñòðì àèé èààèí í Ûé èðèòàðèé, ÑĒĒ	strict avalanche criterion, SAC	121,141
ñòì ì àðì àÿ èí ððàèÿòèÿ	total correlation	126,127
ñòì ì àòì ð ñì ñèáí çí ùì ì àðáí í ñì ì	ripple adder	231
ñòì ì èðòðùèé èí ì àéì èðòðùèé óçàé, ñòì ì àòì ð	summation combiner	65,128,213,253
ñòàì à ááç ì àì ÿòè ñ ðàáí í ì àðì ùì ààèæáí èàì	regular clocking and no memory	69
ñÿì ì èèðì àáí í àÿ (àúáí ðì-í àÿ) ì ñèááí ààòàèüí í ñòü	sampled sequence	190
òàáèèòà çàì áí Ù (S-áí èñ)	S-box	260,267,274
òàáèèòà èñòèí í ñòè Òóí èòèè	truth table of function	122,143
òáí ðàòè-áñèèÿ ñòì èéí ñòü	theoretical security	14
òàñò ààòì èí ððàèÿòèè	autocorrelation test	39
òàñò í à ì ì àòì ðáí èÿ	repetition test	41
òàñò í à ì ðèñòòòòàèà èí ðì ÿ	root presence test	73
òàñò í à ì ðì Òèèü èèì áéí í é ñèí æí í ñòè	linear complexity profile test	57
òàñò ðàáí í àáðì ÿòì í ñòè	uniformity test	38
òàñò ñáðèé	run test	39
òàñò ñèááòðùááí áèòà (ì ðàáñèàçàòàèü)	next bit test (predictor)	320
òì òàèüí Ûé ì àðááí ð	exhaustive search	81,162,178
òì-èè ñúáì à, ì òáí äù	taps	25,174
óí èááðñàèüí Ûé òàñò	universal test	39
óí ðàáèáí èà ààèæáí èàì (àèòàì è áðòáí àí ðààèñòðà)	forward clock control	154
ÿèáñòè-í àÿ Òóí èòèÿ	resilient function	121,150
óðááí áí èà Ĩ àðñàáàèÿ	Parseval equation	120
óñá-áí èà ì ñèááí ààòàèüí í ñòè	decimation of sequence	154,190
óñá-áí í Ûé èí ì áðóÿí òí Ûé ááí áðàòì ð	truncated congruential generator	20
Õèèè ñ Ēðèí òí, èðèí òí òèðì à	Philips Crypto	55,64,268
òèèüòðòðùèé ááí áðàòì ð	filter generator	69-77
òóí èòèÿ ààòì èí ððàèÿòèè	autocorrelation function	36
òóí èòèÿ Äá Áððèí à	De Bruijn function	110
òóí èòèÿ èðì ññ-èí ððàèÿòèè	cross-correlation function	84,127
òóí èòèÿ èèì áéí í é ñòðòèòòðì é	linear structure function	131

óóí èöèÿ ñí í òáàòñòàèÿ	fitness function	306
óóí èöèÿ ñòí èí í ñòè	cost function	302
"Óàì áèáí í " (èðèí òí èí í ñòðóèöèÿ)	Chameleon	283
òáí òè-áñèèé øèòð	chaotic cipher	319,334
òáèááÿ óóí èöèÿ	objective function	302
òáèí á +èñèí í áðàòí í é ñáÿçè	feedback integer	210,231
òèèèè-áñèèé èí á	cyclic code	90
+áñòè-í áÿ ñí àì áñòí áÿ áaðí ÿóí í ñòü	partial joint probability	199
+áñòí óí úé òáñò	frequency test	38
øááèí í	template	177
"øää _{k,m} "-èáñèáá	"step _{k,m} "-cascade	164
øèòð "Ðèí ááí Àèí èöü"	Rip van Winkle cipher	331
øèòð Ááðí àì à	Vernam cipher	3,10,13
øèòðñèñòáì à ñ í òèðúòúì èèþ-íì	public key cryptosystem	2
øèòðñèñòáì à ñ ñáèðáóí úì èèþ-íì	secret key cryptosystem	2
øèòðòáèñò	ciphertext	1
øèòðóþùáÿ í í ñèááí áàòáèüí í ñòü	keystream	3
ØÈÍ Ñ (Øóáá-èáàððèðà í ðáàèòáèüñòááí í í é ñáÿçè Ááèèèí áðèòáí èè)	GCHQ (Government Communications Head-Quarters)	259
ÿáí èþòèí í í áÿ í ðí áðàì ì à	evolution program	306
ÿèáèèñòáí óí í á ì í í æáñòáí	equidistant set	114
ÿèñí í í áí òà Ì áðñáí í á	Mersenne exponent	273
Ýèáí áí òðèèñ Óáèí í èí áæèç, òèðì à	Elementrix Technologies	334
l-í í ñèááí áàòáèüí í ñòü	l-sequence	211,240
m-í í ñèááí áàòáèüí í ñòü	m-sequence	27,70
ε-ñí àùáí í í á ðáñí ðáááèáí èà	ε-bias distribution	176
ÿòáèò çáí èðáí èÿ	lock-in effect	160,163
ÿ-áèèà ðáàèñòðà, ñóóí áí ü èáñèááá	stage	32,159