References

1. ABA Bank Card Standard, "Management and   Use of Personal Information Numbers, "   Aids from ABA, Catalog no. 207213, American Bankers Association, 1979.

2. ABA Document 4.3, "Key Management Standard," American Bankers Association, 1980.

3. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle," Proceedings of the 19th ACM Symposium on the Theory of Computing, 1987, pp. 195-203.

4. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle," Journal of Computer and System Sciences, v.39, n.1, Aug 1989, pp.21-50.

5. M. Abadi and R. Needham, "Prudent Engineering Practice for Cryptographic Protocols," Research Report 125, Digital Equipment Corp Systems Research Center, Jun 1994.

6. C.M. Adams, "On Immunity Against Biham and Shamir's Differential Cryptanalysis,' " Information Processing Letters, v. 41, 14 Fob 1992, pp. 77-80.

7. C.M. Adams, "Simple and Effective Key Scheduling for Symmetric Ciphers, " Workshop on Selected Areas in Cryptography Workshop Record, Kingston, Ontario, 5-6 May 1994, pp.129-133.

8. C.M. Adams and H. Mailer, "Security Related Comments Regarding McEliece's Public-Key Cryptosystem, " Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 224-230.

9. C.M. Adams and S.E. Tavares, "The Structured Design of Cryptographically Good SBoxes," journal of Cryptology v. 3, n. 1, 1990, pp. 27-41.

10. C.M. Adams and S.E. Tavares, "Designing S-Boxes for Ciphers Resistant to Differential Cryptanalysis," Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography Rome, Italy, 15-16 Feh 1993, pp. 181-190.

11. W. Adams and D. Shanks, "Strong Primality Tests That Are Not Sufficient, " Mathematics of Computation, v. 39, 1982, pp. 255-300.

12. W.W Adams and L.J. Goldstein, Introduction to Number Theory, Englewood Cliffs, N.J.: Prentice-Hall, 1976.

13. B.S. Adiga and P. Shankar, "Modified LuLee Cryptosystem," Electronics Letters, v 21, n. 18, 29 Aug 1985, pp. 794-795.

14. L.M. Adleman, "A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography," Proceedings of the IEEE 20th Annual Symposium of Foundations of Computer Science, 1979, pp.55-60.

15. L.M. Adleman, "On Breaking Generalized Knapsack Public Key Cryptosystems, " Proceedings of the 15th ACM Symposium on Theory of Computing, 1983, pp. 402412.

16. L.M. Adleman, "Factoring Numbers Using Singular Integers," Proceedings of the 23rd Annual ACM Symposium on the Theory of Computing, 1991, pp. 64 71.

17. L.M. Adleman, "Molecular Computation of Solutions to Combinatorial Problems," Science, v. 266, n. 11, Nov 1994, p. 1021.

18. L.M. Adleman, D. Estes, and K. McCurley, "Solving Bivariate Quadratic Congruences in Random Polynomial Time," Mathematics of Computation, v. 48, n. 177, Jan 1987, pp. 17-28.

19. L.M. Adleman, C. Pomerance, and R.S. Rumeley, "On Distinguishing Prime Numbers from Composite Numbers, " Annals of Mathematics, v. 117, n. 1, 1983, pp. 173-206.

20. L.M. Adleman and R.L. Rivest, "How to Break the Lu-Lee {COMSAT) Public-Key Cryptosystem, " MIT Laboratory for Computer Science, Jul 1979.

21. G.B. Agnew, "Random Sources for Cryptographic Systems, " Advances in Cryptology EUROCRYPT '8 7 Proceedings, Springer-Verlag, 1988, pp. 77-81.

22. G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, and S.A. Vanstone, "An Implementation for a Fast Public-Key Cryptosystem," Journal of Cryptology, v. 3, n. 2, 1991, pp. 63-79.

23. G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "A Fast Elliptic Curve Cryptosystem," Advances in Cryptology EUROCRYPT '89 Proceedings, Spnnger-Verlag, 1990, pp. 706-708.

24. G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "Improved Digital Signature Scheme Based on Discrete Exponentiation, " Electronics Letters, v. 26, n. 14, 5 Jul 1990, pp. 1024 1025.

25. G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "On the Development of a Fast Elliptic Curve Cryptosystem," Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 482

26. G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "An Implementation of Elliptic Curve Cryptosystems over F:155," IEEE Selected Areas of Communications, v. 11, n. 5, Jun 1993, pp. 804-813.

27. A. Aho, J. Hopcroft, and J. Ullman. The 40. Design and Analysis of Computer Algorithms, Addison-Wesley, 1974.

28. S.G. Akl, "Digital Signatures: A Tutorial Survey." Computer, v. 16, n. 2, Feb 1983, pp. 15-24.

29. S.G. Akl, "On the Security of Compressed Encodings," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 209-230.

30. S.G. Akl and H. Meijer, "A Fast Pseudo-Random Permutation Generator with Applications to Cryptology," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 269-275.

31. M. Alabbadi and S.B. Wicker, "Security of Xinmei Digital Signature Scheme," Electronics Letters, v. 28, n. 9, 23 Apr 1992, pp. 890-89 1.

32. M. Alabbadi and S.B. Wicker, "Digital Signature Schemes Based on Error-Correcting Codes," Proceedings of the 1993 IEEE-ISIT, IEEE Press, 1993, p. 199.

33. M. Alabbadi and S.B. Wicker, "Cryptanalysis of the Harn and Wang Modification of the Xinmei Digital Signature Scheme, " Electronics Letters, v. 28, n. 18, 27 Aug 1992, pp. 1756-1758.

34. K. Alagappan and J. Tardo, "SPX Guide: Prototype Public Key Authentication Service, " Digital Equipment Corp.. May 1991.

35. W. Alexi, B.-Z. Chor, O. Goldreich, and C.R Schnorr, "RSA and Rabin Functions: Certain Parts Are as Hard as the Whole," Proceedings of the 25th IEEE Symposium on the Foundations of Computer Science, 1984, pp. 449-457.

36. W. Alexi, B.-Z. Chor, O. Goldreich, and C.R Schnorr, "RSA and Rabin Functions: Certain Parts are as Hard as the Whole," SIAM 1ournal on Computing, v. 17, n. 2, Apr 1988, pp. 194 209.

37. Ameritech Mobile Communications et al., "Cellular Digital Packet Data System Specifications: Part 406: Airlink Security," CDPD Industry Input Coordinator. Costa Mesa, Calif.. Jul 1993.

38. H.R. Amirazizi, E.D. Karnin, and J.M. Reyneri, "Compact Knapsacks are Polynomial Solvable," ACM SIGACT News, v.15, 1983, pp. 20-22.

39. R.J. Anderson, "Solving a Class of Stream Ciphers," Cryptologia, v. 14, n. 3, Jul 1990, pp. 285-288.

40. R.J. Anderson, "A Second Generation Electronic Wallet," ESORICS 92, Proceedings of the Second European Symposium on Research in Computer Security, Springer 54. Verlag, 1992, pp. 411 418.

41. R.J. Anderson, "Faster Attack on Certain Stream Ciphers, " Electronics Letters, v. 29, n. 15, 22 Jul 1993, pp. 1322-1323.

42. R.J. Anderson! "Derived Sequence Attacks on Stream Ciphers, " presented at the rump session of CRYPTO '93, Aug 1993.

43. R.J. Anderson, "Why Cryptosystems Fail," lst ACM Conference on Computer and Communications Security ACM Press, 1993, pp. 215-227.

44. R.J. Anderson, "Why Cryptosystems Fail," Communications of the ACM, v. 37, n. 11,   Nov 1994, pp. 32 40.

45. R.J. Anderson, "On Fibonacci Keystream 58. Generators, " K. U. Lezzven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

46. R.J. Anderson, "Searching for the Optimum Correlation Attack, " K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995. to appear.

47. R.J. Anderson and T.M.A. Lomas, "Fortifying Key Negotiation Schemes with Poorly Chosen Passwords," Electronics Letters, v. 30, n. 13, 23 Jun 1994, pp. 1040-1041.

48. R.J. Anderson and R. Needham, "Robustness Principles for Public Key Protocols," Advances in Cryptology CRYPTO '95 Proceedings, Springer-Verlag, 1995, to appear,

49. D. Andleman and J. Reeds, "On the Cryptanalysis of Rotor Machines and Substitution-Permutation Networks," IEEE Trans   actions on Information Theory, v. IT-28, n.   4, Jul 1982, pp. 578-584.

50. ANSI X3.92, "American National Standard for Data Encryption Algorithm   (DEA)," Ameriean National Standards   Institute, 1981.

51. ANSI X3.105, "American National Standard for Information Systems Data Link   Encryption, " Ameriean National Standards Institute, 1983.

52. ANSI X3.106, "American National Standard for Information Systems Data   Encryption Algorithm Modes of Operation," Ameriean National Standards Institute, 1983.

53.   ANSI X9.8, "American National Standard for Personal Information Number (PIN) Management and Security, " American   Bankers Association, 1982.

54.   ANSI X9.9 (Revised, "American National   Standard for Financial Institution Message Authentication (Wholesales), " American   Bankers Association, 1986.

55. ANSI X9.17 (Revised. "American   National Standard for Financial Institution   Key Management (Wholesales)" American   Bankers Assoeiation, 1985.

56. ANSI X9.19, "American National Standard for Retail Message Authentication,"   Ameriean Bankers Assoeiation, 1985.

57. ANSI X9.23, "American National Standard for Financial Institution Message   Encryption, " American Bankers Assoeiation, 1988.

58. ANSI X9.24, "Draft Proposed Ameriean National Standard for Retail Key Management," Ameriean Bankers Assoeiation,   1988.

59. ANSI X9.26 (Revised). "American   National Standard for Financial Institution   Sign-On Authentication for Wholesale   Financial Transaction," American Bankers   Association, 1990.

60. ANSI X9.30, "Working Draft: Public Key Cryptography Using irreversible Algorithms for the Financial Services   Industry'" Ameriean Bankers Association,   Aug 1994.

61. ANSI X9.31, "Working Draft: Public Key   Cryptography Using Reversible Algorithms for the Financial Services   Industry," Ameriean Bankers Association,   Mar 1993.

62. K. Aoki and K. Ohta, "Differential-Linear   Cryptanalysis of FEAL-8," Proceedings of   the 1995 Symposium on Cryptography   and Information Security (SCIS by),   Innyama, Japan, 24-27 Jan 1995, pp.   A3.4.1-11. (In Japanese)

63. K. Araki and T. Sekine, "On the Conspiracy Problem of the Generalized Tanaka's Cryptosystem," IEICE Transactions, v.   E74, n. 8, Aug 1991, pp. 2176-2178.

64. S. Araki, K. Aoki, and K. Ohta, "The Best   Linear Expression Search for FEAL," Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS   95), Inuyama, Japan, 24-27 Jan 1995, pp.   A4.4.1-10.

65. C. Asmuth and J. Bloom, "A Modular   Approach to Key Safeguarding," IEEE   Transactions on Information Theory, v. IT-   29, n. 2, Mar 1983, pp. 208 210.

66. D. Atkins, M. Graff, A.K. Lenstra, and RC.   Leyland, "The Magic Words are Squeamish Ossifrage, " Advances in Cryptology   ASIA CRYPT '94 Proceedings, Springer-   Verlag, 1995, pp. 263-277.

67. AT&T, "T7001 Random Number Generator," Data Sheet, Aug 1986.

68. AT&LT, "ATTEST Readying New Spy-Proof   Phone for Big Military and Civilian Markets," The Report on ATTEST, 2 Jun 1986,   pp. 6-7.

69. AT&T, "T7002/T7003 Bit Slice   Multiplier," product announcement, 1987.

70. AT&T, "Telephone Security Device TSD   3600 User's Manual, " ATTEST, 20 Sep   1992.

71. Y. Aumann and U. Feige, "On Message   Proof Systems with Known Space Verifiers," Advances in Cryptology CRYPTO   '93 Proceedings, Springer-Verlag, 1994, pp.   85-99.

72. R.G. Ayoub, An Introduction to the Theory of Numbers, Providence, Rl: American Mathematical Society, 1963.

73. A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks," IEEE Personal Communications, v. l, n. 1, 1994, pp. 25-31.

74. A. Bahreman and J.D. Tygar, "Certified Electronic Mail," Proceedings of the Internet Society 1994 Workshop on Network and Distributed System Secunty, The Internet Society, 1994, pp. 3-19.

75. D. Balenson, "Automated Distribution of Cryptographic Keys Using the Financial Institution Key Management Standard, " IEEE Communications Magazine, v. 23, n. 9. Sep 1985, pp. 41-46.

76. D. Balenson, "Privacy Enhancement for Internet Electronic Mail: Part 111: Algo 91. rithms, Modes, and Identifiers, " RFC 1423, Feb 1993.

77. D. Balenson, C.M. Ellison, S.B. Lipner, and S.T. Walker, "A New Approach to Software Key Escrow Encryption," TIS Report #520, Trusted Information Systems, Aug 94

78. R. Ball, Mathematical Recreations and Essays, New York: MacMillan, 1960.

79. J. Bamford, The Puzzle Palace, Boston: 93. Houghton Mifflin, 1982.

80. J. Bamford and W. Madsen, The Puzzle Palace, Second Edition, Penguin Books, 1995.

81. S.K. Banerjee, "High Speed Implementa- tion of DES," Computers ed Security, v. l, 1982, pp. 261-267.

82. Z. Baodong, "MC-Veiled Linear Transform Public Key Cryptosystem," Acta Electron- ica Sinica, v. 20, n. 4, Apt 1992, pp. 21-24. {In Chinese 1

83. P.H. Bardell, "Analysis of Cellular Automata Used as Pseudorandom Pattern Generators," Proceedings of 1990 Interna- tional Test Conference, pp. 762-768.

84. T. Baritaud, H. Gilbert, and M. Girault, "FFT Hashing is not Collision-Free, " Advances in Cryptology EUR OCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 35-44.

85. C. Barker, "An Industry Perspective of the CCEP, " 2nd Annual AIAA Computer Security Conference Proceedings, 1986.

86. W.G. Barker, Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

87. R Barrett, "Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp 311-323.

88. T.C. Bartee and D.l. Schneider, "Computation with Finite Fields," Information and Control, v. 6, n. 2, Jun 1963, pp. 79-98.

89. U. Baum and S. Blackburn, "Clock Controlled Pseudorandom Generators on Finite Groups," K.U Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

90. K.R. Bauer, T.A. Bersen, and R.J. Feiertag, "A Key Distribution Protocol Using Event Markers," ACM Transactions on Computer Systems, v. 1, n. 3, 1983, pp. 249-255.

91. F. Bauspiess and F. Damm, "Requirements for Cryptographic Hash Functions," Computers Security, v. l l, n. 5, Sep 1992, pp. 427 437.

92. D. Bayer, S. Haber, and W.S. Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping, " Sequences '91: Methods in Communication, Security, and Computer Science, Springer-Verlag, 1992, pp. 329-334.

93. R. Bayer and J.K. Metzger, "On the Encipherment of Search Trees and Random Access Files," ACM Transactions on Data base Systems, v. l, n. 1, Mar 1976, pp. 37-52.

94. M. Beale and M.F. Monaghan, "Encrytion Using Random Boolean Functions," Cryptography and Coding, H.J. Beker and F.C. Piper, eds., Oxford: Clarendon Press, 1989, pp. 219-230.

95. P. Beauchemin and G. Brassard, "A Gener- alization of Hellman's Extension to Shannon's Approach to Cryptography," lournal of Cryptology, v. 1, n. 2, 1988, pp. 129-132.

96. R Beauchemin, G. Brassard, C. Crepeau, C. Goutier, and C. Pomerance, "The Generation of Random Numbers that are Probably Prime, " Journal of Cryptology, v. 1, n. 1, 1988, pp. 53-64.

97. D. Beaver, J. Feigenbaum, and V Shoup, "Fliding Instances in Zero-Knowledge Proofs, " Advances in Cryptology CR YPTO '90 Proceedings, Springer-Verlag, 1991, pp. 326-338.

98. H. Beker, J. Friend, and P. Halliden, "Simplifying Key Management in Electronic Funds Transfcr Points of Sale Systems," Electronics Letters, v. 19, n. 12, Jun 1983, pp. 442 444.

99. H. Beker and F. Piper, Cipher Systems: The Protection of Communications, London: Northwood Books, 1982.

100. D.E. Bell and L.J. LaPadula, "Secure Computer Systems: Mathematical Foundations, " Report ESD-TR-73-275, MITRE Corp., 1973.

101. D.E. Bell and L.J. LaPadula, "Secure Computer Systems: A Mathematical Model," Report MTR-2547, MITRE Corp., 1973.

102. D.E. Bell and L.J. LaPadula, "Secure Computer Systems: A Refinement of the Mathematical Model," Report ESD-TR-73-278, MITRE Corp., 1974.

103. D.E. Bell and L.J. LaPadula. "Secure Com- puter Systems: Unified Exposition and Multics Interpretation," Report ESD-TR- 75-306, MITRE Corp., 1976.

104. M. Bellare and S. Goldwasser, "New Paradigms for Digital Signatures and Message Authentication Based on Non-interactive Zero Knowledge Proofs, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 194-211.

105. M. Bellare and S. Micali, "Non-interactive Oblivious Transfer and Applications, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp.547-557.

106. M. Bellare, S. Micali, and R. Ostrovsky, "Perfect Zero-Knowledge in Constant Rounds," Proceedings of the 22nd ACM Symposium on the Theory of Computing, 1990, pp. 482-493.

107. S.M. Bellovin, "A Preliminary Technical Analysis of Clipper and Skipjack," unpublished manuscript, 20 Apr 1993.

108. S.M. Bellovin and M. Merritt, "Limitations of the Kerberos Protocol, " Winter 1991 USENIX Conference Proceedings, USENIX Association, 1991, pp. 253-267.

109. S.M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," Proceedings of the 1992 IEEE Computer Society Conference on Research in Security and Privacy, 1992, pp. 72-84.

110. S.M. Bellovin and M. Merritt, "An Attack on the Interlock Protocol When Used for Authentication, " IEEE Transactions on Information Theory, v. 40, n. 1, Jan 1994, pp. 273-275.

111. S.M. Bellovin and M. Merritt, "Cryptographic Protocol for Secure Communications, " U.S. Patent #5,241,599, 31 Aug 93.

112. J. Ben-Aroya and E. Biham, "Differential Cryptanalysis of Lucifer, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 187-199.

113. J.C. Benaloh, "Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, 213-222.

114. J.C. Benaloh, "Secret Sharing Homorphisms: Keeping Shares of a Secret Secret, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987. pp. 251-260.

115. J.C. Benaloh, "Verifiable Secret-Ballot Elections, " Ph.D. dissertation, Yale University, YALEU/DCS/TR-561, Dec 1987.

116. J.C. Benaloh and M. de Mare, "One-Way   Accumulators: A Decentralized Alternative to   Digital Signatures," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 274 285.

117. J.C. Benaloh and D. Tuinstra, "Receipt Free Secret Ballot Elections," Proceedings   of the   26th ACM Symposium on the Theory of Computing, 1994, pp. 544-553.

118. J.C. Benaloh and M. Yung, "Distributing   the Power of a Government to Enhance   the   Privacy of Voters, " Proceedings of the 130. 5th ACM Symposium on the Principles   in   Distributed Computing, 1986, pp.   52-62.

119. A. Bender and G. Castagnoli, "On the   Implementation of Elliptic Curve Cryptosystems, "   Advances in Cryptology   CRYPTO '89 Proceedings, Springer-Verlag,   1990, pp. 186-192.

120. S. Bengio, G. Brassard, Y.G. Desmedt, C. Goutier, and J.-J. Quisquater, "Secure   Implementation of Identification   Systems, " Journal of Cryptology, v. 4, n. 3,   1991, pp.   175-184.

121. C.H. Bennett, F. Bessette, G. Brassard, L.   Salvail, and J. Smolin, "Experimental   Quantum   Cryptography, " Advances in   Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag,   1991, pp. 253-265.

122. C.H. Bennett, F. Bessette, G. Brassard, L.   Salvail, and J. Smolin, "Experimental   Quantum   Cryptography, "Journal of Cryptology, v. 5, n. 1, 1992, pp. 3-28.

123. C.H. Bennett and G. Brassard, "Quantum   Cryptography: Public Key Distribution and Coin   Tossing, " Proceedings of the   IEEE International Conference on Computers, Systems, and   Signal Processing,   Banjalore, India, Dec 1984, pp. 175-179.

124. C.H. Bennett and G. Brassard, "An Update   on Quantum Cryptography," Advances in   Cryptology: Proceedings of CRYPTO 84,   Springer-Verlag, 1985, pp. 475-480.

125. C.H. Bennett and G. Brassard, "Quantum   Public-Key Distribution System, " IBM   Technical Disclosure Bulletin, v. 28, 1985,   pp. 3153-3163.

126. C.H. Bennett and G. Brassard, "Quantum Public Key Distribution Reinvented, "   SIGACT   News, v. 18, n.4, 1987, pp. 51-53.

127. C.H. Bennett and G. Brassard, "The Dawn of a New Era for Quantum Cryptography: The   Expenmental Prototype is Working!"   SIGACT News, v. 20, n. 4, Fall 1989, pp.   78-82.

128. C.H. Bennett, G. Brassard, and S. Breidbart,   Quantum Cryptography 11: How to Re-Use a   One-Time Pad Safely Even if P=NP,   unpublished manuscript, Nov 1982.

129. C.H. Bennett, G. Brassard, S. Breidbart, and S. Weisner, "Quantum Cryptography, or   Unforgeable Subway Tokens," Advances   in Cryptology: Proceedings of Crypto 82,   Plenum Press, 1983, pp. 267-275.

130. C.H. Bennett, G. Brassard, C. Crepeau, and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer, " Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 351-366.

131. C.H. Bennett, G. Brassard, and A.K. Ekert, "Quantum Cryptography," Scientific American, v. 267, n.4, Oct 1992, pp. 50-57.

132. C.H. Bennett, G. Brassard, and N.D. Mermin, "Quantum Cryptography Without Bell's Theorem, " Physical Review Letters, v.68, n.5, 3 Feb 1992, pp. 557-559.

133. C.H. Bennett, G. Brassard, and J.-M. Robert, "How to Reduce Your Enemy's Information," Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 468-476.

134. C.H. Bennett, G. Brassard, and J.-M. Robert, "Privacy Amplification by Public Discussion," SIAM Journal on Computing, v. 17, n.2, Apr 1988, pp. 210-229.

135. J. Bennett, "Analysis of the Encryption Algorithm Used in WordPerfect Word Processing Program," Cryptologia, v. l l, n. 4, Oct 1987, pp. 206-210.

136. M. Ben-Or, S. Goldwasscr, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, " Proceedings of the 20th ACM Symposium on the Theory of Computing, 1988, pp. 1-10.

137. M. Ben-Or, O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali, and R Rogaway, "Everything Provable is Provable in Zero-Knowledge," Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 37-56.

138. M. Ben-Or, O. Goldreich, S. Micali, and R.L. Rivest, "A Fair Protocol for Signing Contracts," IEEE Transactions on Information Theory, v. 36, n. 1, Jan 1990, pp. 40 46.

139. H.A. Bergen and W.J. Caelli, "File Security in WordPerfect 5.0," Cryptologia, v. 15, n. 1, Jan 1991, pp. 57-66.

140. E.R. Berlekamp, Algebraic Coding Theory, Aegean Park Press, 1984.

141. S. Berkovits, "How to Broadcast a Secret," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 535-541.

142. S. Berkovits, J. Kowalchuk, and B. Schanning, "Implementing Public-Key Scheme, " IEEE Communications Magazine, v. 17, n. 3, May 1979, pp. 2-3.

143. D.J. Bernstein, Bernstein vs. U.S. Depart- ment of State et al., Civil Action No. C95-0582-MHP, United States District Court for the Northern District of California, 21 Feb 1995.

144. T. Berson, "Differential Cryptanalysis Mod 2^{32} with Applications to MD5, " Advances in Cryptology EUROCRYPT '92 Proceedings, 1992, pp. 71-80.

145. T. Beth, Verfahren der schnellen Fourier-Transformation, Teubner, Stuttgart, 1984. (In German.)

146. T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards," Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 77-84.

147. T. Beth, B.M. Cook, and D. Gollmann, "Architectures for Exponentiation in $GF|2n|$," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 302-310.

148. T. Beth and Y. Desmedt, "Identification Tokens or: Solving the Chess Grandmastcr Problem," Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 169-176.

149. T. Beth and C. Ding, "On Almost Nonlinear Permutations, " Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 65-76.

150. T. Beth, M. Frisch, and G.J. Simmons, eds., Lecture Notes in Computer Science 578; Public Key Cryptography: State of the Art and Future Directions, Springer-Verlag, 1992.

151. T. Beth and F.C. Piper, "The Stop-and-Go Generator," Advances in Cryptology: Procedings of EUROCRYPT 84, Springer-Verlag, 1984, pp. 88-92.

152. T. Beth and F. Schaefer, "Non Supersingular Elliptic Curves for Public Key Cryptosystems," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 316-327.

153. A. Beutelspacher, "How to Say 'No', " Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 491-96.

154. J. Bidzos, letter to NIST regarding DSS, 20 Sep 1991.

155. J. Bidzos, personal communication, 1993. 169.

156. R Bieber, "A Logic of Communication in a Hostile Environment," Proceedings of the Computer Security Foundations Workshop, IEEE Computer Society Press, 1990, pp. 14-22.

157. E. Biham, "Cryptanalysts of the Chaotic- Map Cryptosystem Suggested at EUROCRYPT '91, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 532-534.

158. E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys, " Technical Report #753, Computer Science Department, Technion Israel Institute of Technology, Sep 1992.

159. E. Biham, "On the Applicability of Differential Cryptanalysis to Hash Functions,"   lecture at EIES Workshop on Cryptographic Hash Functions, Mar 1992.

160. E. Biham, personal communication, 1993.

161. E. Biham, "Higher Order Differential   Cryptanalysis, " unpublished manuscript,   Jan 1994.

162. E. Biham, "On Modes of Operation," Fast   Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag,   1994,pp. 116-120.

163. E. Biham, "New Types of Cryptanalytic   Attacks Using Related Keys," Journal of Cryptology, v. 7, n. 4, 1994, pp. 229-246.

164. E. Biham, "On Matsui's Linear Cryptanalysis, " Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag,   1995, pp. 398-412.

165. E. Biham and A. Biryukov, "How to   Strengthen DES Using Existing   Hardware, " Advances in Cryptology   ASIACKYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

166. E. Biham and P.C. Kocher, "A Known   Plaintext Attack on the PKZIP Encryption," K.U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995,   to appear.

167. E. Biham and A. Shamir, "Differential   Cryptanalysis of DES-like   Cryptosystems," Advances in Cryptology- CRYPTO 90 Proceedings, Springer-   Verlag, 1991, pp. 2-21.

168. E. Biham and A. Shamir, "Differential   Cryptanalysis of DES-like   Cryptosystems," Journal of Cryptology, v.   4, n. 1, 1991, pp 3-72.

169. E. Biham and A. Shamir, "Differential   Cryptanalysis of Feal and N-Hash, "   Advances in Cryptology EUROCRYPT   '91 Proceedings, Springer-Verlag, 1991, pp. 181. 1-16.

170. E. Biham and A. Shamir, "Differential   Cryptanalysis of Snefru, Khafre, REDOC-   II, LOKI, and Lucifer," Advances in Cryptology CRYPTO '91 Proceedings, 1992,   pp. 156-171.

171. E. Biham and A. Shamir, "Differential   Cryptanalysis of the Full 16-Round DES," Advances in Cryptology CRYPTO '92   Proceedings, Springer-Verlag, 1993, 487- 496.

172. E. Biham and A. Shamir, Differential   Cryptanalysis of the Data Encryption   Standard, Springer-Verlag, 1993.

173. R. Bird, I. Gopal, A. Herzberg, R Janson, S.   Kutten, R. Molva, and M. Yung, "Systematic Design of Two-Party Authentication   Protocols, " Advances in Cryptology   CRYPTO'91 Proceedings, Springer-Verlag,   1992, pp. 44-61.

174. R. Bird, I. Gopal, A. Herzberg, P. Janson, S.   Kutten, R. Molva, and M. Yung, "System- atic Design of a Family of Attack-Resistant   Authentication Protocols, " IEEE journal   of Selected Areas in Communication, to   appear.

175. R. Bird, I. Gopal, A. Herzberg R Janson, S. Kutten, R. Molva, and M. Yung, "A Modular Family of Secure Protocols for Authentication and Key Distribution," IEEE/ACM Transactions on Networking, to appear.

176. M. Bishop, "An Application for a Fast Data Encryption Standard Implementation, " Computing Systems, v. 1, n. 3, 1988, pp. 221-254.

177. M. Bishop, "Privacy-Enhanced Electronic Mail," Distributed Computing and Cryptography, J. Feigenbaum and M. Merritt, eds., American Mathematical Society, 1991, pp. 93-106.

178. M. Bishop, "Privacy-Enhanced Electronic Mail, " Internetworking: Research and Experience, v. 2, n. 4, Dec 1991, pp. 199-233.

179. M. Bishop, "Recent Changes to Privacy Enhanced Electronic Mail," Internetworking: Research and Experience, v. 4, n. 1, Mar 1993, pp. 47-59.

180. I.F. Blake, R. Fuji-Hara, R.C. Mullin, and S.A. Vanstone, "Computing Logarithms in Finite Fields of Characteristic Two, " SIAM Journal on Algebraic Discrete Methods, v. 5, 1984, pp. 276-285.

181. I.F. Blake, R.C. Mullin, and S.A. Vanstone, "Computing Logarithms in GF (2n), " Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 73-82.

182. G.R. Blakley, "Safeguarding Cryptographic Keys," Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, v. 48. 1979, pp. 313-317.

183. G.R. Blakley, "One-Time Pads are Key Safeguarding Schemes, Not Cryptosystems Fast Key Safeguarding Schemes (Threshold Schemes Exist), " Proceedings of the 1980 Symposium on Security and Privacy, IEEE Computer Society. Apr 1980, pp. 108-113.

184. G.R. Blakley and I. Borosh, "Rivest-Shamir-Adleman Public Key Cryptosystems Do Not Always Conceal Messages," Computers and Mathematics with Applications, v. 5, n. 3, 1979, pp. 169-178.

185. G.R. Blakley and C. Meadows, "A Database Encryption Scheme which Allows the Computation of Statistics Using Encrypted Data," Proceedings of the 1985 Symposium on Security and Privacy, IEEE Computer Society, Apr 1985, pp. 116-122.

186. M. Blaze, "A Cryptographic File System for UNIX," 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 9-16.

187. M. Blaze, "Protocol Failure in the Escrowed Encryption Standard, " 2nd ACM Conference on Computer and Communications security, ACM Press, 1994, pp. 59-67.

188. M. Blaze, "Key Management in an Encrypting File System, " Proceedings of   the Summer 94 USENIX Conference,   USENIX Association, 1994, pp. 27-35.

189. M. Blaze and B. Schneier, "The MacGuffin Block Cipher Algorithm, " K. U. Leuven Workshop on Cryptographic Algorithms,   Springer-Verlag, 1995, to appear.

190. U. Blocher and M. Dichtl, "Fish: A Fast   Software Stream Cipher," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994,   pp. 41-44.

191. R. Blom, "Non-Public Key Distribution," Advances in Cryptology: Proceedings of   Crypto 82, Plenum Press, 1983, pp.   231-236.

192. K.J. Blow and S.J.D. Phoenix, "On a Fundamental Theorem of Quantum Cryptography, " Journal of Modern Optics, v. 40, n. 1,   Jan 1993, pp. 33-36.

193. L. Blum, M. Blum, and M. Shub, "A Simple   Unpredictable Pseudo-Random Number Generator," SIAM Journal on Computing,   v. 15, n. 2, 1986, pp. 364-383.

194. M. Blum, "Coin Flipping by Telephone: A   Protocol for Solving Impossible   Problems," Proceedings of the 24th IEEE   Computer Conference (CompCon), 1982,   pp. 133-137.

195. M. Blum, "How to Exchange Secret Keys, " ACM Transactions on Computer Systems, v. 1, n. 2, May 1983, pp. 175-193.

196. M. Blum, "How to Prove a Theorem So No Onc Else Can Claim It," Proceedings of   the International Congress of Mathematicians, Berkeley, CA, 1986, pp. 1444-1451.

197. M. Blum, A. De Santis, S. Micali, and G. Persiano, "Noninteractive Zero-Knowledge, " SIAM Journal on Computing, v. 20,   n. 6, Dec 1991. pp. 1084-1118.

198. M. Blum, P. Feldman, and S. Micali, "Non   Interactivc Zero-Knowledge and Its Applications, " Proceedings of the 20th ACM   Symposilzm on Theory of Computing, 1988, pp. 103-112.

199. M. Blum and S. Goldwasser, "An Efficient   Probabilistic Public-Key Encryption   Scheme Which Hides All Partial Information," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985,   pp. 289-299.

200. M. Blum and S. Micali, "How to Generate Cryptographically-Strong Sequences of Pseudo-Random Bits," SIAM Journal on Computing, v. 13, n. 4, Nov 1984, pp.   850-864.

201. B. den Boer. "Cryptanalysts of F.E.A.L.,"   Advances in Cryptology EUROCRYPT   '88 Proceeding.s, Springer-Verlag, 1988, pp.   293-300.

202. B. den Boer and A. Bosselaers, "An Attack on the Last Two Rounds of MD4, "   Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 194-203.

203. B. den Boer and A. Bosselaers, "Collisions for the Compression Function of MD5," Advances in Cryptology EUROCRYPT 93 Proceedings, Springer-Verlag, 1994, pp. 293

204. J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, R de Rooij, B. Schoenmakers, M. Schunter, L. Vallee, and M. Waidner, "Digital Payment Systems in the ESPRIT Project CAFE, " Securicom 94, Paris, France, 2-6 Jan 1994, pp. 35-45.

205. J.-R Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pcdersen, B. Pfitzmann, P. de Rooij, B. Schoen makers, M. Schunter, L. Vallee, and M. Waidner, "The ESPRIT Project CAFE High Security Digital Payment System," Computer Security ESORICS 94, Springer-Verlag, 1994, pp. 217-230.

206. D.J. Bond, "Practical Primality Testing," Proceedings of IKE International Conference on Secure Communications Systems, 22-23 Feb 1984, pp. 50-53.

207. H. Bonnenberg, Secure Testing of VSLI Cryptographic Equipment, Series in Microelectronics, Vol. 25, Konstanz: Hartung Gorre Verlag, 1993.

208. H. Bonnenberg, A. Curiger, N. Felber, H. Kacslin, and X. Lai, "VLSI Implementation of a New Block Cipher," Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD 91), Oct 1991, pp. 510-513.

209. K.S. Booth, "Authentication of Signatures Using Public Key Encryption," Communications of the ACM, v. 24, n. 11, Nov 1981, pp. 772-774,

210. A. Bosselaers, R. Govaerts, and J. Vanderwalle, Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 175-186.

211. D.R Bovet and P. Crescenzi, Introduction to the Theory of CompiexiLy, Englewood Cliffs, N.J.: Prenticc-Hall, 1994.

212. J. Boyar, "Inferring Scqucnccs Produced by a Linear Congruential Generator Missing Low-Order Bits." Journal of Cryptology, v. 1, n. 3, 1989, pp. 177-184.

213. J. Boyar, D. Chaum, and I. Damgard, "Convertible Undeniable Signatures," Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 189-205.

214. J. Boyar, K. Fricdl, and C. Lund, "Practical Zero-Knowledge Proofs: Giving Hints and Using Deficiencies, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 155-172.

215. J. Boyar, C. Lund, and R. Peralta, "On the Communication Complexity of Zero Knowledge Proofs, " Journal of Cryptology, v.6, n.2, 1993, pp.65-85.

216. J. Boyar and R. Peralta, "On the Concrete   Complexity of Zero-Knowledge Proofs, "   Advances in Cryptology CRYPTO '89   Proceedings, Springer-Verlag 1990, pp.   507-525.

217. C. Boyd, "Some Applications of Multiple Key Ciphers," Advances in Cryptology   EUROCRYPT '88 Proceedings, Springer   Verlag, 1988, pp. 455-467.

218. C. Boyd, "Digital Multisignatures," Cryptography and Coding, H.J. Beker and F.C. Piper,   eds., Oxford: Clarendon Press, 1989, pp. 241-246.

219. C. Boyd, "A New Multiple Key Cipher and an Improved Voting Scheme," Advances in   Cryptology EUROCRYPT '89 Proceed   ings, Springer-Verlag, 1990, pp. 617 625.

220. C. Boyd, "Multisignatures Revisited,"   Cryptography and Coding, M.J. Ganley,   ed.,   Oxford: Clarendon Press, 1993, pp.   21-30.

221. C. Boyd and W. Mao, "On the Limitation of BAN Logic, " Advances in Cryptology   EUROCRYPT '93 Proceedings, Springer   Verlag, 1994, pp. 240-247.

222. C. Boyd and W. Mao, "Designing Secure   Key Exchange Protocols," Computer Security   ESORICS 94, Springer-Verlag, 1994,   pp. 217-230.

223. B. O. Brachtl, D. Coppersmith, M.M.   Hyden, S.M. Matyas, C.H. Meyer, J. Oseas,   S.   Pilpel, and M. Schilling, "Data Authentication Using Modification Detection   Codes Based   on a Public One Way Function," U.S. Patent #4,908,861, 13 Mar 1990.

224. J. Brandt, I.B. Damgard, R Landrock, and T. Pederson, "Zero-Knowledge Authentication   Scheme with Secret Key Exchange,"   Advances in Cryptology CRYPTO '88,   Springer-   Verlag, 1990, pp. 583-588.

225. S.A. Brands, "An Efficient Off-Line Electronic Cash System Based on the Representation   Problem," Report CS-R9323,   Computer Science / Department of Algorithms and   Architecture, CWI, Mar 1993.

226. S.A. Brands, "Untraceable Off-line Cash in Wallet with Observers," Advances   in   Cryptology CRYPTO '93, Springer Verlag, 1994, pp. 302-318.

227. S.A. Brands, "Electronic Cash on the Internet," Proceedings of the Internet Society   Symposium on Network and Distributed Systems Secunty, IEEE Computer Society Press   1995, pp 64-84.

228. D.K. Branstad, "Hellman's Data Does Not   Support His Conclusion," IEEE Spectrum,   v.   16, n. 7, Jul 1979, p. 39.

229. D.K. Branstad, J. Gait, and S. Katzke,   "Report on the Workshop on Cryptography in   Support of Computer Security, "   NBSIR 77-1291, National Bureau of Standards, Sep 21-   22, 1976, September 1977.

230. G. Brassard, "A Note on the Complexity of Cryptography, " IEEE Transactions on Information Theory, v. IT-25, n. 2, Mar 1979, pp. 232-233.

231. G. Brassard, "Relativized Cryptography," Proceedings of the IEEE 20th Annual Symposium on the Foundations of Computer Science, 1979, pp. 383-391.

232. G. Brassard, "A Time-Luck Trade-off in Relativized Cryptography, " Proceedings of the IEEE 21st Annual Symposium on the Foundations of Computer Science, 1980, pp. 380-386.

233. G. Brassard, "A Time-Luck Tradeoff in Relativized Cryptography," Journal Of Computer and System Sciences, v. 22, n.3, Jun 1981, pp. 280-311.

234. G. Brassard, "An Optimally Secure Relativized Cryptosystem," SIGACT News, v. 15, n. 1, 1983, pp. 28-33.

235. G. Brassard, "Relativized Cryptography," IEEE Transactions on Information Theory, v. IT-29, n. 6, Nov 1983, pp. 877-894.

236. G. Brassard, Modern Cryptology: A Tutorial, Springer-Verlag, 1988.

237. G. Brassard, "Quantum Cryptography: A Bibliography," SIGACT News, v. 24, n. 3, Oct 1993, pp. 16-20.

238. G. Brassard, D. Chaum, and C. Crepeau, "An Introduction to Minimum Disclosure," CWI Quarterly v. 1, 1988, pp. 3-17.

239. G. Brassard, D. Chaum, and C. Crepeau, "Minimum Disclosure Proofs of Knowledge," Journal of Computer and System Sciences, v. 37, n.2, Oct 1988, pp. 156-189.

240. G. Brassard and C. Crepeau, "Non-Transitive Transfer of Confidence: A Perfect Zero-Knowledge Interactive Protocol for SAT and Beyond," Proceedings of the 27th IEEE Symposium on Foundations of Computer Science, 1986, pp. 188-195.

241. G. Brassard and C. Crepeau, "Zero-Knowledge Simulation of Boolean Circuits," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 225-233.

242. G. Brassard and C. Crcpeau, "Sorting Out Zcro-Knowlcdge, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springcr-Vcrlag, 1990, pp. 181-191.

243. G. Brassard and C. Crcpcau, "Quantum Bit Commitment and Coin Tossing Protocols, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 49-61.

244. G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, "A Quantum Bit Commitment Schcmc Provably Unbreakable by Both Parties, " Proceedings of the 34th IEEE Symposium on Foundations of computer Science, 1993, pp. 362-371.

245. G. Brassard, C. Crepeau, and J.-M. Robert, "Information Theoretic Reductions Among Disclosure Problems, " Proceedings of the 27th IEEE Symposium on Foundations of Computer Science, 1986, pp. 168-173.

246. G. Brassard, C. Crcpeau, and J.-M. Robert, "All-or-Nothing Disclosure of Secrets, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 234-238.

247. G. Brassard, C. Crepeau, and M. Yung, "Everything in NP Can Be Argued in Perfect Zero-Knowledge in a Bounded Number of Rounds," Proceedings on the 16th International Colloquium on Automata, Languages, and Programming, Springer-Verlag, 1989, pp. 123-136.

248. R.P. Brent, "An Improved Monte-Carlo Factorization Algorithm," BIT v. 20, n. 2, 1980, pp. 176-184.

249. R.P. Brent, "On the Periods of Generalized 261. Fibonacci Recurrences, Mathematics of Computation, v 63, n. 207, Jul 1994, pp. 389-401.

250. R.R Brent, "Parallel Algorithms for Integer Factorization," Research Report CMA-R49-89, Computer Science Laboratory The Australian National University, Oct 1989.

251. D.M. Bressotid, Factorization and Primality Testing, Springer-Verlag, 1989.

252. E.F. Brickcll, "A Fast Modular Multiplication Algorithm with Applications to Two Key Cryptography," Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1982, pp. 51-60.

253. E.F. Brickell, "Are Most Low Density Polynomial Knapsacks Solvable in Polynomial Timer" Proceedings of the 14th Southeastern Conference on Combinatorics, Graph Theory, and Computing, 1983.

254. E.F. Brickell, "Solving Low Density Knapsacks," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 25-37.

255. E.F. Brickell, "Breaking Iterated Knapsacks," Advances in Cryptology: Proceedings of Crypto 84, Springer-Verlag, 1985, pp. 342-358.

256. E.F. Brickell, "Cryptanalysts of the Uagisawa Public Key Cryptosystem," Abstracts of Papers, EUROCRYPT '86, 20-22 May 1986.

257. E.F. Brickell, "The Cryptanalysis of Knapsack Cryptosystems, " Applications of Discrete Mathematics, R.D. Ringeisen and F.S. Roberts, eds., Society for Industrial and Applied Mathematics, Philadelphia, 1988, pp. 3-23.

258. E.F. Brickell, "Survey of Hardware Implementations of RSA, " Advances in Cryptology CRYPTO '89 Proceedings, Springcr-Verlag, 1990, pp. 368-370.

259. E.F. Brickell, D. Chaum, I.B. Damgard, and J. van de Graff, "Gradual and Verifiable Release of a Secret," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 156-166.

260. E.F. Brickell, J.A. Davis, and G.J. Simmons, "A Preliminary Report on the Cryptanalysis of Merkle-Hellman Knapsack, " Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 289-303.

261. E.F. Brickell and J. DeLaurentis, "An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 28-32.

262. E.F. Brickell, D.E. Denning, S.T. Kent, D.R Maher, and W. Tuchman, "SKIPJACK Review Interim Report, " unpublished manuscript, 28 Jul 1993.

263. E.F. Brickell, J.C. Lagarias, and A.M. Odlyzko, "Evaluation of the Adleman Attack of Multiple Iterated Knapsack Cryptosystems," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 39-42.

264. E.F. Brickell, RJ. Lee, and Y. Yacobi,   "Secure Audio Teleconference," Advances   in Cryptology CRYPTO '87 Proceedings,   Springer-Verlag, 1988, pp. 418 426.

265 . E. F. Brickell and K. S. McCurley, "An Interactive Identification Scheme Based on Discrete Logarithms and Factoring, "   Advances in Cryptology EUROCRYPT   '90 Proceedings, Springer-Verlag, 1991, pp.   63-71.

266. E.F. Brickell, J.H. Moore, and M.R. Purtill,   "Structure in the S-Boxes of the DES," Advances in Cryptology CRYPTO '86   Proceedings, Springer-Verlag, 1987, pp.   3-8.

267. E.F. Brickell and A.M. Odlyzko, "Crypt analysis: A Survey of Recent Results," Pro ceedings of the IEEE, v. 76, n. 5, May 1988, 279.   pp. 578-593.

268. E.F. Brickell and A.M. Odlyzko, "Crypt analysis: A Survey of Recent Results," Contemporary Cryptology: The Science of   Information Integnty, G.J. Simmons, ed., IEEE Press, 1991, pp. 501-540.

269. E.F. Brickell and G.J. Simmons, "A Status   Report on Knapsack Based Public Key Cryptosystems, " Congressus Numeran   tium, v. 7, 1983, pp. 3-72.

270. E.F. Brickell and D.R. Stinson, "The Detection of Cheaters in Threshold Schemes," Advances in Cryptology CRYPTO '88   Proceedings, Springer-Verlag, 1990, pp.   564-577.

271. A.G. Broscius and J.M. Smith, "Exploiting   Parallelism in Hardware Implementation   of the DES, " Advances in Cryptology   CRYPTO '91 Proceedings, Springer-Verlag,   1992, pp. 367-376.

272. L. Brown, M. Kwan, J. Pieprzyk, and J. Seberry, "Improving Resistancc to Differential Cryptanalysis and the Redesign of LOKI, " Advances in Cryptology ASIACRYPT '91 Proceedings, Springer-Verlag, 1993, pp. 36-50.

273. L. Brown, J. Pieprzyk, and J. Seberry, "LOKI: A Cryptographic Primitive for Authentication and Secrecy Applications," Advances in Cryptology AUSCRYPT ' 90 Proceedings, Springer Verlag, 1990, pp. 229-236.

274. L. Brown, J. Pieprzyk, and J. Seberry, "Key Scheduling in DES Type Cryptosystems," Advances in Cryptology A IJSCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 221-228.

275. L. Brown and J. Seberry, "On the Design of Permutation P in DES Type Cryptosystems," Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 696-705.

276. W. Brown, "A Quantum Leap in Secret Communications, " New Scientist, n. 1585, 30 Jan 1993, p. 21.

277. J.O. Bruer, "On Pseudo Random Sequences as Crypto Generators," Proceedings of the International Zurich Seminar on Digital Communication, Switzerland, 1984.

278. L. Brynielsson "On the Linear Complexity of Combined Shift Register Sequences," Advances in Cryptology EUROCRYPT '85, Springer-Verlag, 1986, pp. 156-166.

279. J. Buchmann, J. Loho, and J. Zayer, "An Implementation of thc General Number Field Sieve, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 159-165.

280. M. Burmester and Y. Desmedt, "Broadcast Interactive Proofs," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 81-95.

281. M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System, " Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

282. D. Burnham, "NSA Seeking 500,000 'Secure' Telephones," The New York Times, 6 Oct 1994.

283. M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication, " Research Report 39, Digital Equipment Corp. Sys- tems Research Center, Feb 1989.

284. M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Trans- actions on Computer Systems, v. 8, n. 1, Feb 1990, pp. 18-36.

285. M. Burrows, M. Abadi, and R. Needham, "Rejoinder to Nessett," Operating System Review, v. 20, n. 2, Apr 1990, pp. 39 40.

286. J.J. Cadc, "A Modification of a Broken Public-Key Cipher," Advances in Cryptology - CRYPTO '86 Proceedillgs, Springer- Verlag, 1987, pp. 64-83.

287. T.R. Cain and A.T. Sherman, "How to Break Gifford's Cipher, " Proceedings of the 2nd Annual ACM Conference Computer and Communications Security 300 ACM Press, 1994, pp. 198-209.

288. C. Calvelli and V Varadharajan, "An Analysis of Some Delegation Protocols for Distributed Systems, " Proceedings of the Computer Security Foundations Workshop V, IEEE Computer Society Press, 1992, pp. 92-110.

289. J.L. Camenisch, J.-M. Piveteau, and M.A. Stadler, "An Efficient Electronic Payment System Protecting Privacy," Computer Security ESORICS 94, Springer-Verlag, 1994, pp. 207-215,

290. P. Camion and J. Patarin, "The Knapsack Hash Function Proposed at Crypto '89 Can Be Broken," Advances in Cryptology EUROCRYPT '91, Springer-Verlag, 1991, pp. 39-53.

291. C.M. Campbell, "Design and Specification of Cryptographic Capabilities," IEEE Computer Society Magazine, v. 16, n. 6, Nov 1978, pp. 15 19.

292. E.A. Campbell, R. Safavi-Naini, and PA. Pleasants, "Partial Belief and Probabilistic Reasoning in the Analysis of Secure Protocols," Proceedings of the Computer Security Foundations Workshop V, IEEE Computer Society Press, 1992, pp. 92-110.

293. K.W. Campbell and M.J. Wiener, "DES Is Not a Group," Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, pp. 512-520.

294. Z.F. Cao and G. Zhao, "Some New MC Knapsack Cryptosystems, " CHINACRYPT 307 . '94, Xidian, China, 11-15 Nov 1994, pp. 70-75. (In Chinese.)

295. C. Carlet, "Partially-Bent Functions, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 280-291.

296. C. Carlet, "Partially Bent Functions," Designs, Codes and Cryptography. v. 3, 1993, pp. 135-145.

297. C. Carlet, "Two New Classes of Bent Functions" Advances in Cryptology EUROCRYPT '93 Proceedings, Springer Vcrlag, 1994, pp. 77-101.

298. C. Carlet, J. Seberry, and X.M. Zhang, "Comments on Generating and Counting Binary Bent Sequences,' " IEEE Transac tions on Information Theory v. IT-40, n. 2, Mar 1994, p. 600.

299. J.M. Carroll, Computer Security, 2nd cdition, Butterworths 1987.

300. J.M. Carroll, "The Three Faces of Information Security," Advances in Cryptology AUSCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 433-450.

301. J.M. Carroll, "'Do-it-yourself' Cryptography," Computers & Security v. 9, n. 7, Nov 1990, pp. 613-619.

302. T.R. Caron and R.D. Silverman, "Parallel Implementation of the Quadratic Scheme," Journal of Supercomputing, v. 1, n. 3, 1988, pp. 273-290.

303. CCITT, Draft Recommendation X.509, "The Directory Authentication Framework," Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1987.

304. CCITT, Recommendation X.509, "The Directory Authentication Framework, " Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989.

305. CCITT, Recommendation X.800, "Security Architecture for Open Systems Interconnection for CCITT Applications, " International Telephone and Telegraph. International Telecommunications Union, Geneva, 1991.

306. F. Chabaud, "On the Security of Some Cryptosystems Based on Error-Correcting Codes," Advances in Cryptology EURO- CRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

307. F. Chabaud and S. Vaudenay, "Links Between Differential and Linear Cryptanalysis, " Advances in Cryptology- EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

308. W.G. Chambers and D. Gollmann, "Generators for Sequences with Near-Maximal Linear Equivalence," IKE l'roceedings, V. 135, Pt. E, n. 1, Jan 1988, pp. 67-69.

309. W.G. Chambers and D. Gollmann, "Lock-In Effect in Cascades of Clock-Controlled Shift Registers, " Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 331-343.

310. A. Chan and R. Games, "On the Linear Span of Binary Sequences from Finite Geometries, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 405-417.

311. J.R Chandler, D.C. Arrington, D.R. Berkel- hammer, and W.L. Gill, "Identification and Analysis of Foreign Laws and Regulations Pertaining to the Use of Commercial Encryption Products for Voice and Data Communications, " National Intellectual Property Law Institute, George Washing- ton University, Washington, D.C., Jan 1994.

312. C.C. Chang and S.J. Hwang, "Cryptographic Authentication of Passwords, " Proceedings of the 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, Taipei, Taiwan, 1-3 Oct 1991, pp. 126-130.

313. C.C. Chang and S.J. Hwang, "A Strategy for Transforming Public-Key Cryptosystems into Identity-Based Cryptosystems." Proceedings of the 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, Taipei, Taiwan, 1-3 Oct 1991, pp. 68-72.

314. C.C. Chang and C.H. Lin, "An ID-Based Signature Scheme Based upon Rabin's Public Key Cryptosystem, " Proceedings of the 25th Annual 1991 IEEE International Carahan Conference on Secunty Technology, Taipei, Taiwan, 1-3 Oct 1991, pp. 139-141.

315. C. Charnes and J. Pieprzyk, "Attacking the SL2 Hashing Scheme," Advances in Cryptology ASIACRYPT '94 Proceedings, Springer-Verlag, 1995, pp. 322-330.

316. D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, " Communications of the ACM,v.24,n.2,Febl981,pp.84 88.

317. D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 199-203.

318. D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete, " Communications of the ACM, v. 28, n. 10, Oct 1985, pp. 1030-1044.

319. D. Chaum, "Demonstrating that a Public Predicate Can Be Satisfied without Revealing Any Information about How, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 159-199.

320. D. Chaum, "Blinding for Unanticipated Signatures," Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Vcrlag, 1988, pp. 227-233.

321. D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability, " Journal of Cryptology, v. 1, n. 1, 1988, pp. 65-75.

322. D. Chaum, "Elections with Unconditionally Secret Ballots and Disruptions Equivalent to Breaking RSA," Advances in Cryptology EUROCRYPT '88 Proceedings. Springer-Verlag, 1988, pp. 177-181.

323. D. Chaum, "Blind Signature Systems, " U.S. Patent #4,759,063, 19 Jul 1988.

324. D. Chaum, "Blind Unanticipated Signature Systems," U.S. Patent #4,759,064, 19 Jul 1988.

325. D. Chaum, "Online Cash Checks, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springcr-Verlag, 1990, pp. 288-293.

326. D. Chaum, "One-Show Blind Signature Systems," U.S. Patent #4,914,698, 3 Apr 1990.

327. D. Chaum, "Undeniable Signature Systems," U.S. Patent #4,947,430, 7 Aug 1990.

328. D. Chaum, "Returned-Value Blind Signature Systems," U.S. Patent #4,949,380, 14 Aug 1990.

329. D. Chaum, "Zero-Knowledge Undeniable Signatures, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 458-464.

330. D. Chaum, "Group Signatures," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 2.57-265.

331. D. Chaum, "Unpredictable Blind Signature Systems," U.S. Patent #4,991,210, 5 Feb 1991.

332. D. Chaum, "Achieving Electronic Privacy," Scientific American, v. 267, n. 2, Aug 1992, pp. 96-101.

333. D. Chaum, "Designated Confirmer Signatures," Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

334. D. Chaum, C. Crepeau, and I.B. Damgard, "Multiparty Unconditionally Secure Protocols, " Proceedings of the 20th ACM Symposium on the Theory of Computing, 1988, pp. 11-19.

335. D. Chaum, B. den Boer, E. van Heyst, S. Mjolsnes, and A. Steenbeek, "Efficient Offline Electronic Checks," Advances in Cryptology E UK OCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 2Y4-301.

336. D. Chaum and J.-H. Evertse, "Cryptanalysis of DES with a Reduced Number of Rounds; Scqucnces of Linear Factors in Block Ciphers, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 192-211.

337. D. Chaum, J.-H. Evertse, and J. van de Graff, "An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations, " Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1988, pp. 127 141.

338. D. Chaum, J.-H. Evertse, J. van de Graff, and R. Peralta, "Demonstrating Possession of a Discrete Logarithm without Revealing It, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 200-212.

339. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 319-327.

340. D. Chaum and T. Pedersen, "Transferred Cash Grows in Size," Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 391-407.

341. D. Chaum and T. Pedersen, "Wallet Databases with Observers," Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 89-105.

342. D. Chaum and J. Schaumuller-Bichel, eds., Smart Card 2000, North Holland: Elsevier Science Publishers, 1989.

343. 1). Chaum and H. van Antwcrpen, "Undeniable Signaturcs," Advances in Cryptology CRYPTO '89 Proceedings, Springcr-Verlag, 1990, pp. 212-216.

344. D. Chaum, E. van Heijst, and B. Pfitzmann, "Cryptographically Strong Undeniable Signatures, Unconditionally Secure for thc Signer, " Advances in Cryptology CRYPTO '91 Proceedings. Springer-Verlag, 1992, pp. 470-484.

345. T.M. Chee, "The Cryptanalysis of a New Public-Key Cryptosystem Based on Modular Knapsacks, " Advances in Cryptology CKYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 204-212.

346. L Chen, "Oblivious Signatures," Computer Security ESORICS 94, Springcr-Verlag, 1994, pp. 161-172,

347. L. Chen and M. Burminster, "A Practical Secret Voting Scheme which Allows Voters to Abstain," CHINACRYPT '94, Xidian, China, 11-15 Nov 1994, pp. 100-107.

348. L. Chen and T.P Pedersen "New Group Signature Schemes, " Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

349. J. Chenhui, "Spectral Characteristics of Partially-Bent Functions," CHINACRYPT '94, Xidian, China, 11-15 Nov 1994, pp. 48-51.

350. V. Chepyzhov and B. Smeets, "On a Fast Correlation Attack on Certain Stream Ciphers," Advances in Cryptology EUR OCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 176-185.

351. T.C. Cheung, "Management of PEM Public Key Certificates Using X.500 Directory Service: Some Problems and Solutions," Proceedings of the lnternet Society 1994 Workshop on Network and Distnhuted System Security. The Internet Society, 1994, pp. 35 42.

352. G.C. Chiou and W.C. Chen, "Secure Broadcasting Using the Secure Lock, " IEEE Transactions on Software Engineenng, v. SE-15, n. 8, Aug 1989, pp. 929-934.

353. Y.J. Choie and H.S. Hwoang, "On the Cryptosystem Using Elliptic Curves, " Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryp tography, Seoul, Korca, 24-26 Oct 1993, pp. 105-113.

354. B. Chor and O. Goldreich, "RSA/Rabin Least Significant Bits are 1/2+1/... Secure, " Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 303-313.

355. B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults," Proceedings of the 26th Amlual IEEE Symposium on the Foundations of Computer Science, 1985, pp. 383-395.

356. B. Chor and R.L. Rivcst, "A Knapsack Typc Public Key Cryptosystem Based on Arith-mctic in Finitc Fields," Advallces ill Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 54-65.

357. R Christoffersson, S.-A. Ekahll, V. Fak, S. Herda, R Mattila, W. Price, and H.-O. Wid-man, Crypto Users Handbook: A Guide for Implementors of Cryptographic Protection in Computer Systems, North Holland Elscvicr Scicncc Publishcrs, 1988.

358. R. Cleve, "Controlled Gradual Disclosure Schemes for Random Bits and Their Applications, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 572-588.

359. J.D. Cohen, "Improving Privacy in Cryptographic Elections," Yale University Computer Science Department Technical Report YALEU/DCS/TR-454, Feb 1986.

360. J.D. Cohen and M.H. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme, " Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science, 1985. pp. 372-382.

361. R. Cole, "A Model for Security in Dis tributed Systems," Computers and Security, v.9 , n.4, Apr 1990, pp.319-330.

362. Comptroller General of the United States, "Matter of National Institute of Standards and Technology Use of Electronic Data Interchange Technology to Create Valid Obligations," File B-245714, 13 Dec 1991.

363. M.S. Conn, letter to Joe Abernathy, National Security Agency, Ser: Q43-111 92, 10 Jun 1992.

364. C. Connell, "An Analysis of NewDES: A Modified Version of DES," Cryptologia, v. 14, n. 3, Jul 1990, pp. 217-223.

365. S.A. Cook, "The Complexity of Theorem Proving Procedures," Proceedings of the 3rd Annual ACM Symposium on the The oryofComputing, 1971,pp. 151-158.

366. R.H. Cooper and W. Patterson, "A Generalization of the Knapsack Method Using Galois Fields," Cryptologia, v. 8, n. 4, Oct 1984, pp. 343-347.

367. R.H. Cooper and W. Patterson, "RSA as a Benchmark for Multiprocessor Machines, " Advances in Cryptology AUSCRYPT'90 Proceedings, Springer-Verlag, 1990, pp. 356-359.

368. D. Coppersmith, "Fast Evaluation of Logarithms in Fields of Characteristic Two," IEEE Transactions on Information Theory, v.30,n.4,Jull984,pp.587-594.

369. D. Coppersmith, "Another Birthday Attack, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 14-17.

370. D. Coppersmith, "Cheating at Mental Poker, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 104-107.

371. D. Coppersmith, "The Real Reason for Rivest's Phenomenon, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 535-536.

372. D. Coppersmith, "Two Broken Hash Functions," Research Report RD 18397, IBM T.J. Watson Center, Oct 1992.

373. D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks," Technical Report RC 18613, IBM T.J. Watson Center, Dec 1992.

374. D. Coppersmith, "The Data Encryption Standard (DES) and its Strength against Attacks, " IBM /ournal of Research and Development, v. 38, n. 3, May 1994, pp. 243-250.

375. D. Coppersmith, "Attack on the Cryptographic Scheme NIKS-TAS," Advances in Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 294-307.

376. D. Coppersmith, personal communication, 1994.

377. D. Coppersmith and E. Grossman, "Generators for Certain Alternating Groups with Applications to Cryptography, " SIAM Journal on Applied Mathematics, v. 29, n. 4, Dec 1975, pp. 624-627.

378. D. Coppersmith, H. Krawczyk, and Y. Mansour, "The Shrinking Generator, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 22-39.

379. D. Coppersmith, A. Odlykzo, and R. Schroeppel, "Discrete Logarithms in GF(p)," Algorithmica, v. 1, n. 1, 1986, pp. 1-16.

380. D. Coppersmith and R Rogaway, "Software Efficient Pseudo Random Function and the Use Thereof for Encryption," U.S. Patent pending, 1995.

381. D. Coppersmith, J. Stern, and S. Vaudenay, "Attacks on the Birational Signature Schemes, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 435-443.

382. V. Cordonnier and J.-J. Quisquater, eds.. CARD1S '94 Proceedings of the First Smart Card Research and Advanced Application Conference, Lille, France, 24-26 Oct 1994.

383. C. Couvreur and J.-J. Quisquater, "An Introduction to Fast Generation of Large Prime Numbers," Philips /ournal Research, v. 37.   n. 5 6, 1982, pp. 231-264.

384. C. Couvreur and J.-J. Quisquater, "An Introduction to Fast Generation of Large Prime Numbers," Philips journal Research, v. 38,   1983, i' 77

385. C. Coveyou and R.D. MacPherson,   "Fourier Analysis of Uniform Random   Number Gcncrators," lournal of the ACM,   v. 14, n. 1, 1967, pp. 100-119.

386. T.M. Cover and R.C. King, "A Convergent   Gambling Estimate of the Entropy of   English," IEEE Tran.saction.s on Informa-   tion Theory, v. IT-24, n. 4, Jul 1978, pp.   413-421.

387. R.J.F. Cramer and T.R Pedersen, "Improved   Privacy in Wallets with Observers,"   Advances in Cryptology EZJROCRYPT   '93 Proceedings, Springer-Verlag, 1994, pp.   329-343.

388. R.E. Crandell, "Method and Apparatus for   Public Key Exchange in a Cryptographic System," U.S. Patent #5,159,632, 27 Oct   1992.

389. C. Crepeau, "A Secure Poker Protocol   That Minimizes the Effect of Player Coalitions," Advances in Cryptology   CKYP'I'O '85 Proceedings, Springer-Verlag,   1986, pit. 73-86.

390. C. Crepcau, "A Zcro-Knowlcdge Poker   Protocol that Achieves Confidentiality of   the Players' Strategy, or How to Achieve   an Electronic Poker Face, " Advances in   Cryptology CRYPTO '86 Proceedings,   Springer-Verlag, 1987, pp. 23Y-247,

391. C. Crepeau, "Equivalence Between Two   Flavours of Oblivious Transfer," Advances   in Cryptology CRYPTO 87 Proceedings,   Springer-Verlag, 1988, pp. 350-354.

392. C. Crepeau, "Correct and Private Reductions among Oblivious Transfers," Ph.D. dissertation, Department of Electrical   Engineering and Computer Science, Massachusetts Institute of Technology, 1990.

393. C. Crcpcau, "Quantum Oblivious Transfcr, " journal of Modern Optics, v. 41, n. 12,   Dec 1994, pp. 2445-2454.

394. C. Crepeau and J. Kilian, "Achieving   Oblivious Transfer Using Weakened Security Assumptions, " Proceedings of the   29th Amllzal Symposiurn on the Foundatijns of Computer Science, 1988, pp.   42-.32.

395. C. Crepeau and J. Kilian, "Weakening   Security Assumptions and Oblivious Transfer, " Advances in Cryptology   CRYPTO '88 Proceedings, Springer-Verlag,   1990, pp. 2-7.

396. C. Crepeau and L. Salvail, "Quantum Oblivious Mutual Identification, " Advances in Cryptology EUROCRYPT '95 Proceed-   ings, Springer-Verlag 1995, pp. 133-146.

397. A. Curiger, H. Bonnenberg, R. Zimmermann, N. Felber, H. Kaeslin and W. Fichtner, "VINCI: VLSI Implementation of the   New Block Cipher IDEA," Proceedings of   IEEE CICC '93, San Diego, CA, May 1993,   pp. 15.5.1-15.5.4.

398. A. Curiger and B. Stuber, "Specification for   the IDEA Chip, " Technical Report No.   92/03, Institut fur Integrierte Systeme,   ETH Zurich, Feb 1992.

399. T. Cusick, "Boolean Functions Satisfying a   Higher Order Strict Avalanche Criterion," Advances in Cryptology EUROCRYPT   '93 Proceedings, Springer-Verlag, 1994, pp.   102-117.

400. T.W. Cusick and M.C. Wood, "The   REDOC-II Cryptosystem," Advances in   Cryptology CRYPTO '90 Proceedings,   Springer-Verlag, 1991, pp. 545-563.

401. Cylink Corporation, Cylink Corporation   vs. RSA Data Security, Inc., Civil Action   No. C94-02332-CW, United States District   Court for the Northern District of Califor-   nia, 30 Jun 1994.

402. J. Daeman, "Cipher and Hash Function   Design, " Ph.D. Thesis, Katholieke Univer-   siteit Leuven, Mar 95.

403. J. Daeman, A. Bosselaers, R. Govaerts, and   J. Vandewalle, "Collisions for Schnorr's   Hash Function FFT-Hash Presented at   Crypto '91," Advances in Cryptology   ASIA CRYPT '91 Proceedings, Springer-   Verlag, 1993, pp. 477-480.

404. J. Daeman, R. Govaerts, and J. Vandewalle,   "A Framework for the Design of One-Way Hash Functions Including Cryptanalysis of   Damgard's Onc-Way Function Based on Cellular Automata, " Advances in Cryp-   tology ASIA CRYPT '91 Proceedings,   Springer-Verlag, 1993, pp. 82-96.

405. J. Daeman, R. Govaerts, and J. Vandewalle,   "A Hardware Design Model for Crypto-   graphic Algorithms, " ESORICS 92, Pro-   ceedings of the Second European Sympo-   sium on Research in Computer Security,   Springer-Verlag, 1992, pp. 419 434.

406. J. Daemcn, R. Govacrts, and J. Vandewalle, "Block Ciphers Based on Modular Arith-
metic, " Proceedings of the 3rd Symposium   on State and Progress of Research in Cryptography, Rome, Italy, 15-16 Feb 1993, pp. 418.   80-89.

407. J. Daemen, R. Govaerts. and J. Vandewalle,   "Fast Hashing Both in Hardware and Soft ware," presented at the rump session of   CRYPTO '93, Aug 1993.

408. J. Daeman, R. Govaerts, and J. Vandewalle,   "Resynchronization Weaknesses in Syn chronous Stream Ciphers," Advances in   Cryptology E UR O CRYPT '93 Proceed   ings, Springer-Verlag, 1994, pp. 159-167.

409. J. Daeman, R. Govaerts, and J. Vandewalle,   "Weak Keys for IDEA, " Advances in Cryptology CRYPTO '93 Proceedings,   Springer-Verlag, 1994, pp. 224-230.

410. J. Daemen, R. Govaerts, and J. Vandewalle,   "A New Approach to Block Cipher Design," Fast Software Encryption, Cam   bridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 18-32.

411. Z.-D. Dai, "Proof of Rueppel's Linear Complexity Conjecture," IEEE Transactions on Information Theory, v. IT-32, n. 3, May   1986, pp. 440 443.

412. I.B. Damgard, "Collision Free Hash Functions and Public Key Signature Schemes," Advances in Cryptology EUROCRYPT   '87 Proceedings, Springer-Verlag, 1988, pp. 203-216.

413. I.B. Damgard, "Payment Systems and Credential Mechanisms with Provable Secu   rity Against Abuse by Individuals, "   Advances in Cryptology CRYPTO '88   I'roceedings, Springer-Verlag, 1990, pp.   328-335

414. I.B. Damgard, "A Design Principle for   Hash Functions, " Advances in Cryptol428.   ogy CRYPTO '89 Proceedings, Springer   Verlag, 1990, pp. 416 427.

415. I.B. Damgard, "Practical and Provably   Secure Release of a Secret and Exchangc of Signatures, " Advances in Cryptology   EUROCRYPT '93 Proceedings, Springer   Verlag, 1994, pp. 200-217.

416. 1.B. Damgard and L.R. Knudsen, "The   Rreaking of the AR Hash Function, "   Advances in Cryptology EUROCRYPT   '93 Proceedings, Springer-Verlag, 1994, pp.   286-292.

417. I.B. Damgard and R Landrock, "Improved   Bounds for the Rabin Primality Test, " 431. Cryptography and Coding III, M.J. Ganley, ed., Oxford: Clarendon Press, 1993, pp.   117-128.

418. I.B. Damgard, P. Landrock and C. Pomerance, "Average Case Error Estimates for   the Strong Probablc Prime Test," Mathematics of Computation, v. 61, n. 203, Jul 1993, pp. 177-194.

419. H.E. Daniels, Jr., letter to Datapro   Research Corporation regarding CCEP, 23   Dec 1985.

420. H. Davenport, The Higher Arithmetic,   Dover Books, 1983.

421. G.I. Davida, "Inverse of Elements of a   Galois Field," Electronics Letters, v. 8, n.   21, 19 Oct 1972, pp. 518-520.

422. G.I. Davida, "Hellman's Scheme Breaks   DES in Its Basic Form," IEEE Spectrum, v.   16, n. 7, Jul 1979, p. 39.

423. G.I. Davida, "Chosen Signature Cryptanalysis of the RSA iMITJ Public Key Cryptosystem," Technical Report TR-CS-82-2,   Department of EECS, University of Wis-   consin, 1982.

424. G.I. Davida and G.G. Walter, "A Public   Key Analog Cryptosystem," Advances in   Cryptology E UR O CRYPT '8 7 Proceedings, Springer-Verlag, 1988, pp. 143-147.

425. G.I. Davida, D. Wells, and J. Kam, "A   Database Encryption System with Subkeys," ACM   Transactions on Database   Systems,v.6,n.2,Junl981,pp.312-328.

426. D.W. Davies, "Applying the RSA Digital   Signature to Electronic Mail," Computer,   v. 16,   n. 2, Feb 1983, pp. 55-62.

427. D.W. Davies, "Some Regular Properties of   the DES," Advances in Cryptology: Pro-   ceedings of Crypto 82, Plenum Press, 1983,   pp. 89-96.

428. D.W. Davics, "A Message Authentication   Algorithm Suitable for a Mainframe Com-   puter," Advances in Cryptology: Proceed-   ings of Crypto 82, Springer-Verlag, 1985,   pp.   393 400.

429. D.W. Davies and S. Murphy, "Pairs and   Triplets of DES S-boxes, " Cryptologia, v. 8,   n. 1,   1995, pp. 1-25.

430. D.W. Davies and G.I.P. Parkin, "The Average Size of thc Key Stream in Output Feedback   Encipherment, " Cryptography Proceedings of the Workshop of cryplograpy   Burg   Feuer.stein, Germany, March 29-April   2, 1982, Springer-Verlag, 1983, pp. 263-279.

431 D.W. Davies and G.I.R Parkin, "The Average Size of the Key Stream in Output Feedback   Mode, " Advances in Cryptology: Pro ceedings of Crypto 82, Plenum Press, 1983,   pp. 97-   98.

432. D.W. Davies and W. L. Price, "The Applica tion of Digital Signatures Based on Public-   Key   Cryptosystems, " Proceedings of the   Fifth International Computer Communications   Conference, Oct 1980, pp. 525-530.

433. D.W. Davies and W.L. Price, "The Applica-   tion of Digital Signatures Based on Public-   Key Cryptosystems, " National Physical   Laboratory Report DNACS 39/80, Dec   1980.

434. D.W. Davies and W.L. Price, "Digital Sig-   nature An Update," Proceedings of Inter-   national Conference on Computer Com-   munications, Sydney, Oct 1984, North   Holland: Elsevier, 1985, pp. 843-847.

435. D.W. Davies and W.L. Price, Security for   Computer Networks, second edition, John   Wiley & Sons, 1989.

436. M. Davio, Y. Desmedt, M. Fosseprez, R.   Govaerts, J. Hulsbrosch, R Neutjens, R   Piret, J -   l Quisquater, J Vandewalle, and S.   Wouters, "Analytical Characteristics of   the Data   Encryption Standard," Advances   in Cryptology: Proceedings of Crypto 83,   Plenum Press,   1984, pp. 171-202.

437. M. Davio, Y. Desmedt, l Goubert, F. Hoor-naert, and l -J Quisquater, "Efficient Hardware and Software Implementation of the DES," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 144 146.

438. M. Davio, Y. Desmedt, and l-l Quisquater, "Propagation Characteristics of the DES, " Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, 62-73.

439. D. Davis, R. Ihaka, and R Fenstermacher, "Cryptographic Randomness from Air Turbulence in Disk Drives," Advances in Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 114 120.

440. J.A. Davis, D. B. Holdbridge, and G.l. Sim-mons, "Status Report on Factoring tat the Sandia National Laboratoriesi," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 183-215.

441. R.M. Davis, "The Data Encryption Standard in Perspective," Computer Secunty and the Data Encryption Standard, National Bureau of Standards Special Publication 500-27, Feb 1978.

442. E. Dawson and A. Clark, "Cryptanalysts of Universal Logic Sequences," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, to appear.

443. M.H. Dawson and S.E. Tavares, "An Expanded Set of Design Criteria for Substitution Boxes and Their Use in Strengthening DES-Like Cryptosystems, " IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing, Victoria, BC, Canada, 9-10 May 1991, pp. 191-195.

444. M.H. Dawson and S.E. Tavares, "An Expanded Set of S-Box Design Criteria Based on Information Theory and Its Relation to Differential-like Attacks," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 352-367.

445. C.A. Deavours, "Unicity Points in Cryptanalysis," Cryptologia, v. 1, n. 1, 1977, pp. 46-68.

446. C.A. Deavours, "The Black Chamber: A Column; How the British Broke Enigma." Cryptologia, v. 4, n. 3, lU1 1980, pp. 129-132.

447. C.A. Deavours, "The Black Chamber: A Column; La Methode des Batons," Cryptologia, v. 4, n. 4, Oct 1980, pp. 240-247.

448. C.A. Deavours and L. Kruh, Machine Cryptography and Modern Cryptanalysis, Norwood MA: Artech House, 1985.

449. l.M. DeLaurentis, "A Further Weakness in the Common Modulus Protocol for the RSA Cryptosystem," Cryptologia, v. 8, n. 3, lul 1984, pp. 253-259.

450. R Delsarte, Y. Desmedt, A. Odlyzko, and P. Piret, "Fast Cryptanalysis of the Matsumoto-lmai Public-Key Scheme, " Advances in Cryptology: Proceedings of EUROCRYPT 84, Spunger-Verlag, 1985, pp. 142-149.

451. R Delsarte and R Piret, "Comment on 'Extension of RSA Cryptostructure: A Galois Approach'," Electronics Letters, v. 18, n. 13, 24 Jun 1982, pp. 582-583.

452. R. DeMillo, N. Lynch, and M. Merritt, "Cryptographic Protocols," Proceedings of the 14th Annual Symposium on the The- ory of Computing, 1982, pp. 383-400.

453. R. DeMillo and M. Merritt, "Protocols for Data Security," Computer, v. 16, n. 2, Feb 1983, pp. 39-50.

454. N. Demytko, "A New Elliptic Curve Based Analogue of RSA," Advances in Cryptolgy EUROCRYPT 93 Proceedings, Springer-Verlag, 1994, pp. 40-49.

455. D.E. Denning, "Secure Personal Comput- ing in an Insecure Network," Communi- cations of the ACM, v. 22, n. 8, Aug 1979, pp. 476-482.

456. D.E. Denning, Cryptography and Data Security, Addison-Wesley, 1982.

457. D.E. Denning, "Protecting Public Keys and Signature Keys," Computer. v. 16, n. 2, Feb 1983, pp. 27-35.

458. D.E. Denning, "Digital Signatures with RSA and Other Public-Key Cryptosys471. tems," Communications of the ACM, v. 27, n. 4, Apr 1984, pp. 388-392.

459. D.E. Denning, "The Data Encryption Standard: Fifteen Years of Public Scrutiny, " Proceedings of the Sixth Annual Com puter Security Applications Conference, IEEE Computer Society Press, 1990.

460. D.E. Denning, "The Clipper Chip: A Tech nical Summary, " unpublished manuscript, 21 Apr 1993.

461. D.E. Denning and G.M. Sacco, "Time stamps in Key Distribution Protocols, " Communications of the ACM, v. 24, n. 8, Aug 1981, pp. 533-536.

462. D.E. Denning and M. Smid, "Key Escrow ing Today," IEEE Communications Maga zine, v. 32, n. 9, Sep 1994, pp. 58-68.

463. T. Denny, B. Dodson, A.K. Lenstra, and M.S. Manasse, "On the Factorization of RSA-120," Advances in Cryptology CRYPTO 93 Proceedings, Springer-Verlag, 1994, pp. 166-174.

464. W.F. Denny, "Encryptions Using Linear and Non-Linear Codes: Implementations and Security Considerations," Ph.D. dis sertation, The Center for Advanced Com puter Studies, University of Southern Louisiana, Spring 1988.

465. Department of Defense, "Department of Defense Trusted Computer System Evalu478. ation Criteria," DOD 5200.28-STD, Dec 1985.

466. Department of State, "International Traf fic in Arms Regulations SITARS," 22 CFR 120-130, Office of Munitions Control, 479. Nov 1989.

467. Department of State, "Defense Trade Reg ulations," 22 CFR 120-130, Office of Defense Trade Controls, May 1992.

468. Department of the Treasury, "Electronic Funds and Securities Transfer Policy, " Department of the Treasury Directives Manual, Chapter TD 81, Section 80, Department of the Treasury, 16 Aug 1984.

469. Department of the Treasury, "Criteria and Procedures for Testing, Evaluating, and Certifying Message Authentication Deci- sions for Federal E.F.T. Use," Department of the Treasury, 1 May 198.~.

470. Department of the Treasury, "Electronic Funds and Securitics Transfer Policy Message Authentication and Enhanced Security," Order No. 106-09, Department of the Treasury, 2 Oct 1986.

471. H. Dobbertin, "A Survey on the Construc- tion of Bent Functions," K.U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

472. B. Dodson and A.K. Lenstra, "NFS with Four Large Primes: An Explosive Experiment," draft manuscript.

473. D. Dolev and A. Yao, "On the Security of Public-Key Protocols, " Communications of the ACM, v. 29, n. 8, Aug 1983, pp. 198-208.

474. J. Domingo-Ferrer, "Probabilistic Authentication Analysis," CARDIS 94 Proceed- ings of the First Smart Card Research and Applications Conference, Lille, France, 24-26 Oct 1994, pp. 49-60.

475. R de Rooij, "On the Security of the Schnorr Scheme Using Preprocessing, " Advances in Cryptology EUR(9CRYPT 91 I'roceed- ings, Springer-Verlag, 1991, pp. 71-80.

476. A. De Santis, G. Di Crescenzo, and G. Per- siano, "Secret Sharing and Perfect Zero Knowledge, " Advances in Cryptology CKYPTO 93 I'roceedings, Springer-Verlag, 1994, pp. 73-84.

477. A. De Santis, S. Micali, and G. Persiano, "Non-interactive Zero-Knowledge Proof Systems," Advances in Cryptology CRYPTO '87 Pro cee dings , Springer Verlag, 1988, pp. 52-72.

478. A. De Santis, S. Micali, and G. Persiano,   "Non-Interactive Zero-Knowledge with   Preprocessing," Advances in Cryptology   CRYPTO 88 Proceedings, Springer-Verlag,   1990, pp. 269-282.

479. Y. Desmedt, "What Happened with Knapsack Cryptographic Schemes" Performance limits   in Communication, Theory   and P'ractice, NATO ASI Series E: Applied   Sciences, v. 142,   Kluwer Academic Publishers, 1988, pp. 113-134.

480. Y. Desmedt, "Subliminal-Free Authentication and Signature," Advances in Cryptology   EUROCRYPT '88 Proceedings,   Springer-Verlag, 1988, pp. 23-33.

481. Y. Desmedt, "Abuses in Cryptography and   How to Fight Them," Advances in Cryptology   CRYPTO '8~3 Proceedings, Springer   Verlag, 1990, pp.375-389.

482. Y. Desmedt and M. Burmester, "An Effi   cient Zero-Knowledge Scheme for the   Discrete   Logarithm Based on Smooth   Numbers, " Advances in Cryptology   ASIA CRYPT '91   Proceedings, Springer   Verlag, 1993, pp. 360-367.

483. Y. Desmedt and Y. Frankel, "Threshold 496.   Cryptosystems, " Advances in Cryptol   ogy   CRYPTO '89 Proceedings, Springer   Verlag, 1990, pp. 307-315.

484. Y. Desmedt and Y. Frankel, "Shared Gen   eration of Authentication and Signatures, "   Advances in Cryptology CRYPTO '91   Proceedings, Springer-Verlag, 1992, pp.   457   469.

485. Y. Desmedt, C. Goutier, and S. Bengio,   "Special Uses and Abuses of the Fiat   Shamir   Passport Protocol," Advances in   Cryptology CRYPTO '87 Proceedings,   Springer-   Verlag, 1988, pp. 21-39.

486. Y. Desmedt and A.M. Odlykzo, "A Chosen   Text Attack on the RSA Cryptosystem and   Some Discrete Logarithm Problems, "   Advances in Cryptology CRYPTO '85   Proceedings, Springer-Verlag, 1986, pp.   516-522.

487. Y. Dcsmedt, J.-J. Quisquater, and M.   Davio, "Dependence of Output on Input in   DES: Small Avalanche Characteristics,"   Advances in Cryptology: Proceedings of   CRYPTO   84, Springer-Verlag, 1985, pp.   359-376.

488. Y. Desmedt, J. Vandewalle, and R. Go   vaerts, "Critical Analysis of the Security of   Knapsack Public Key Algorithms," IEEE   Transactions on Information Theory, v. IT   30,n.4,Jull984,pp.601-611.

489. Y. Desmedt and M. Yung, "Weaknesses of   Undeniable Signature Schemes, " Ad   vances   in Cryptology EUROCRYPT '91   Proceedings, Springer-Verlag, 1991, pp.   205-220.

490. W. Diffie, lecture at IEEE Information The   ory Workshop, Ithaca, N.Y., 1977.

491. W. Diftie, "Cryptographic Technology: Fif   teen Year Forecast," BNR Inc., Jan 1981.

492. W. Diffie, "The First Ten Years of Public Key Cryptography, " Proceedings of the IEEE, v 76, n. 5, May 1988, pp. 560-577.

493. W. Diffie, "Authenticated Key Exchange and Secure Interactive Communication," Proceedings of SECURICOM'90, 1990.

494. W. Diffie, "The First Ten Years of Public- Key Cryptography, " in Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons. ed., IEEE Press, 1992, pp. 135-175.

495. W. Diffie and M.E. Hellman, "Multiuser Cryptographic Techniques, " Proceedings of AFIPS National Computer Conference, 1976, pp. 109-112.

496. W. Diffie and M.E. Hellman, "New Direc- tions in Cryptography, " IEEE Transactions on Information Theory, v. IT-22, n. 6, Nov 1976, pp. 644~54.

497. W. Diffie and M.E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," Computer, v. 10, n. 6, Jun 1977, pp. 74-84.

498. W. Diffie and M.E. Hellman, "Privacy and Authentication: An Introduction to Cryp- tography," Proceedings of the IEEE, v. 67, n. 3, Mar 1979, pp. 397-427.

499. W. Diffie, L. Strawczynski, B. O'Higgins, and D. Steer, "An ISDN Secure Telephone Unit," Proceedings of the National Tele- communications Forum, v 41, n. 1, 1987, pp. 473 477.

500. W. Diffie, RC. van Oorschot, and M.J. Wiener, "Authentication and Authenti- cated Key Exchanges," Designs, Codes and Cryptography, v. 2, 1992, 107-125.

501. C. Ding, "The Differential Cryptanalysis and Design of Natural Stream Ciphers," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer- Verlag, 1994, pp. 101-115.

502. C. Ding, G. Xiao, and W. Shan, The Stahility Theory of Stream Ciphers, Springer- Verlag, 1991.

503. A. Di Porto and W. Wolfewicz, "VINO: A Block Cipher Including Variable Permuta- tions, " Fast Software Encryption, Cambridge Secunty Workshop l'roceedings, Springer- Verlag, 1994, pp. 205-210.

504. B. Dixon and A.K. Lenstra, "Factoring Inte- gers Using SIMD Sieves, " Advances in Cryptology E UR O CRYPT '93 Proceed- ings, Springer-Verlag, 1994, pp. 28-39.

505. J.D. Dixon, "Factorization and Primality Tests," American Mathematical Monthly, v.91,n.6, 1984,pp.333-352.

506. D. Dolev and A. Yao, "On the Security of Public Key Protocols," Proceedings ol the 22nd Annual Symposium on the Founda- tions of Computer Science, 1981, pp. 350- 357.

507. L.X. Duan and C.C. Nian, "Modified Lu- Lee Cryptosystems," Electronics Letters, v. 25, n. 13, 22 Jun 1989, p. 826.

508. R. Durstenfeld, "Algorithm 235: Random Permutation, " Communications of the ACM, v. 7, n. 7, Jul 1964, p. 420.

509. S. Dusse and B. Kaliski, Jr., "A Cryptographic Library for the Motorola DSP56000, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer- Verlag, 1991, pp. 230-244.

510. C. Dwork and L. Stockmeyer, "Zero- Knowledge with Finite State Verifiers, " Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 71-75.

511. D.E. Eastlake, S.D. Crocker, and J.I. Schiller, "Randomness Requirements for Security," RFC 1750, Dec 1994.

512. H. Eberle, "A High-Speed DES Implementation for Network Applications, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, pp. 521-539.

513. T. Edwards, "Implementing Electronic Poker: A Practical Exercise in Zero Knowledge Interactive Proofs, " Master's thesis, Department of Computer Science, University of Kentucky, May 1994.

514. W.F. Ehrsam, C.H.W. Meyer, R.L. Powers, J L. Smith, and W.L. Tuchman, "Product Block Cipher for Data Security, " U.S. Patent #3,962,539, 8 Jun 1976.

515. W.F. Ehrsam, C.H.W. Meyer, and W.L. Tuchman, "A Cryptographic Key Manage ment Scheme for Implementing the Data Encryption Standard," IBM Systems lour nal, v. 17, n. 2, 1978, pp. 106-125.

516. R. Eier and H. Lagger, "Trapdoors in Knap sack Cryptosystems, " Lecture Notes in Computer Science 149; Cryptography Proceedings, Burg Feuerstein 1982, Springer-Verlag, 1983, pp. 316-322.

517. A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem, " Physical Review Letters, v. 67, n. 6, Aug 1991, pp. 529. 661-663.

518. T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, " Advances in Cryptology: Proceedings of CRYPTO 84, Springer" Verlag, 1985, pp. 1~18.

519. T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Infor- mation Theory, v. IT-31, n. 4, 1985, pp. 469- 472.

520. T. ElGamal, "On Computing Logarithms Over Finite Fields," Advances in Cryptol- ogy CR YP TO '85 Pro cee dings, Springe r - Verlag, 1986, pp. 396 402.

521. T. ElGamal and B. Kaliski, letter to the edi- tor regarding LUC, Dr. Dobb's /ournal, v. 18,n.5,Mayl993,p. 10.

522. T. Eng and T. Okamoto, "Single-Term Divisible Electronic Coins," Advances in Cryptology EUROCRYPT '94 Proceed- ings, Springer-Verlag, 1995, to appear.

523. M.H. Er, D.J. Wong, A.A. Sethu, and K.S. Ngeow, "Design and Implementation of RSA Cryptosystem Using Multiple DSP Chips," 1991 IEEE International Sympo- sium on Circuits and Systems, v. 1, Singa- pore, 11-14 Jun 1991, pp. 49-52.

524. D. Estes, L.M. Adleman, K. Konpella, K.S. McCurley, and G.L. Miller, "Breaking the Ong-Schnorr-Shamir Signature Schemes for Quadratic Number Fields," Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 3-13.

525. ETEBAC, "Echanges Telematiques Entre Les Banques et Leurs Clients," Standard ETEBAC 5, Comite Fran,cais d'Organisa- tion et de Normalisation Bancaires, Apr 1989. IIn French.~

526. A. Evans, W. Kantrowitz, and E. Weiss, "A User Identification Scheme Not Requiring Secrecy in the Computer," Communica- tions of the ACM, v. 17, n. 8, Aug 1974, pp. 437-472.

527. S. Even and O. Goldreich, "DES-Like Functions Can Generate the Alternating Group, " IEEE Transactions on Informa- tion Theory, v. IT-29, n. 6, Nov 1983, pp. 863-865.

528. S. Even and O. Goldreich, "On the Power of Cascade Ciphers," ACM Transactions on Computer Systems, v. 3, n. 2, May 1985, pp. 108-116.

529. S. Even, O. Goldreich, and A. Lempel, "A Randomizing Protocol for Signing Con- tracts," Communications of the ACM, v. 28, n. 6, [un 1985, pp. 637-647.

530. S. Even and Y. Yacobi, "Cryptography and NP-Completeness," I'roceedings of the 7th International CoRoquium on Automata, Languages, and Programming, Springer -Verlag, 1980, pp. 195-207.

531. H.-H. Evertse, "Linear Structures in Block Ciphers, " Advances in Cryptology EUROCRYPT '87 Proceedings, Springer Verlag, 1988, pp. 249-266.

532. R Fahn and M.J.B. Robshaw, "Results from the RSA Factoring Challenge," Technical Report TR-501, Version 1.3, RSA Laboratories, Jan 1995.

533. R.C. Fairfield, A. Matusevich, and J. Plany, "An LSI Digital Encryption Processor (DEP)," Advances in Cryptology: Proceed ings of CRYPTO 84, Springer-Verlag 1985, pp. 115-143.

534. R.C. Fairfield, A. Matusevich, and J. Plany, "An LSI Digital Encryption Processor (DEPJ," IEEE Communications, v. 23. n. 7, Jul 1985, pp. 30-41.

535. R.C. Fairfield, R.L. Mortenson, and K.B. Koulthart, "An LSI Random Number Gen erator (RNG~," Advances in Cryptology: Proceedings of CRYPTO 84, Springer Verlag, 1985, pp. 203-230.

536. "International Business Machines Corp. License Under Patents," Federal Register, v. 40, n. 52, 17 Mar 1975, p. 12067.

537. "Solicitation for Public Key Cryptographic Algorithms," Federal Register, v. 47, n. 126, 30 Jun 1982, p. 28445.

538. "Proposed Federal Information Processing Standard for Digital Signature Standard (DSSi," Federal Register, v. 56, n. 169, 30 Aug 1991, pp. 42980-42982.

539. "Proposed Federal Information Processing Standard for Secure Hash Standard," Fed eral Register, v. 57, n. 21, 31 Jan 1992, pp. 3747-3749.

540. "Proposed Reaffirmation of Federal Infor mation Processing Standard (FIPS) 46-1, Data Encryption Standard (DES)," Federal Register, v. 57, n. 177, 11 Sep 1992, p. 41727.

541. "Notice of Proposal for Grant of Exclusive Patent License," [ederal Register, v. 58, n. 108, 8 Jun 1993, pp. 23105-23106.

542. "Approval of Federal Information Process ing Standards Publication 186, Digital Sig nature Standard (DSS)," Federal Register, v. 58, n. 96, 19 May 1994, pp. 26208-26211.

543. "Proposed Revision of Federal Information Processing Standard (FIPS) 180, Secure Hash Standard, " Federal Register, v. 59, n. 131, 11 Jul 1994, pp. 35317-35318.

544. U. Feige, A. Fiat, and A. Shamir, "Zero Knowledge Proofs of Identity," Proceed- ings of the lPth Annual ACM Symposium on the Theory of Computing, 1987, pp. 210-217.

545. U. Feige, A. Fiat, and A. Shamir, "Zero Knowledge Proofs of Identity," Journal of Cryptology v. 1, n. 2, 1988, pp. 77-94.

546. U. Feige and A. Shamir, "Zero Knowledge Proofs of Knowledge in Two Rounds, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 526-544.

547. J. Feigenbaum, "Encrypting Problem Instances, or, ..., Can You Take Advan- tage of Someone Without Having to Trust Him, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 477-488.

548. J. Feigenbaum, "Overview of Interactive   Proof Systems and Zero-Knowledge, " in   Contemporary Cryptology: The Science of   Information Integrity, G.J. Simmons, ed.,   IEEE Press, 1992, pp. 423 439.

549. J. Feigenbaum, M.Y. Liberman, E. Grosse,   and J.A. Reeds, "Cryptographic Protection   of Membership Lists," Newsletter of the   International Association of Cryptologic   Research, v. 9, 1992, pp. 16-20.

550. J. Feigenbaum, M.Y. Liverman, and R.N.   Wright, "Cryptographic Protection of   Databases and Software, " Distnbuted   Computing and Cryptography, 1 Feigen-   baum and M. Merritt, eds., American   Mathematical Society, 1991, pp. 161-172.

551. H. Feistel, "Cryptographic Coding for   Data-Bank Privacy," RC 2827, Yorktown   Heights, NY: IBM Research, Mar 1970.

552. H. Feistel, "Cryptography and Computer   Privacy, " Scientific American, v. 228, n. 5,   May 1973, pp. 15-23.

553. H. Feistel, "Block Cipher Cryptographic   System," U.S. Patent #3,798,359, 19 Mar   1974.

554. H. Feistel, "Step Code Ciphering System,"   U.S. Patent #3,798,360, 19 Mar 1974.

555. H. Feistel, "Centralized Verification Sys-   tem," U.S. Patent #3,798,605, 19 Mar   1974.

556. H. Feistel, W.A. Notz, and J.L. Smith,   "Cryptographic Techniques for Machine   to Machine Data Communications," RC   3663, Yorktown Heights, N.Y.: IBM   Research, Dec 1971.

557. H. Feistel, W.A. Notz, and J.L. Smith,   "Some Cryptographic Techniques for   Machine to Machine Data Communica   tions," Proceedings of the IEEE, v. 63, n.   11, Nov 1975, pp. 1545-1554.

558. R Feldman, "A Practical Scheme for Non   interactive Verifiable Secret Sharing,"   Proceedings of the 28th Annual Symposium   on the Foundations of Computer Science,   1987, pp. 427 437.

559. R.A. Feldman, "Fast Spectral Test for Mea   suring Nunrandomness and the DES, "   Advances in Cryptology CRYPTO '87   Proceedings, Springer-Verlag, 1988, pp.   243-254.

560. R.A. Feldman, "A New Spectral Test for   Nonrandomness and the DES, " IEEE 573.   Transactions on Software Engineering, v.   16, n. 3, Mar 1990, pp. 261-267.

561. D.C. Feldmeier and RR. Karn, "UNIX   Password Security Ten Years Later, "   Advances in Cryptology CRYPTO '89   Proceedings, Springer-Verlag, 1990, pp.   44-63.

562. H. Fell and W. Diffie, "Analysis of a Public Key Approach Based on Polynomial Substitution, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 427-437.

563. N.T. Ferguson, "Single Term Off-Line Coins," Report CS-R9318, Computer Sci577. ence/Department of Algorithms and Architecture, CWI, Mar 1993.

564. N.T. Ferguson, "Single Term Off-Line Coins," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 318-328.

565. N.T. Ferguson, "Extensions of Single-term Coins," Advances in Cryptology 579. CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 292-301.

566. A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Idcntifica tion and Signature Problems," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 186-194.

567. A. Fiat and A. Shamir, "Unforgeable Proofs of Identity," Proceedings of securicom 87, Paris, 1987, pp. 147-15~3.

568. P. Finch, "A Study of the Blowfish Encryp tion Algorithm," Ph.D. dissertation, Department of Computer Science, City University of New York Graduate School and University Center, Feb 1995.

569. R. Flynn and A.S. Campasano, "Data Dependent Keys for Selective Encryption Terminal," Proceedings of NCC, vol. 47, AFIPS Press, 1978, pp. 1127-1129.

570. R.H. Follett, letter to NIST regarding DSS, 25 Nov 1991.

571. R. Forre, "The Strict Avalanche Criterion: Spectral Properties and an Extended Definition, " Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 450-468.

572. R. Forre, "A Fast Correlation Attack or Nonlinearity Feedforward Filtered Shift Register Sequences, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 568-595.

573. S. Fortune and M. Merritt, "Poker Protocols," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 454-464.

574. R.B. Fougner, "Public Key Standards and Licenses," RFC 1170, Jan 1991.

575. Y. Frankel and M. Yung, "Escrowed Encryption Systems Visited: Threats. Attacks, Analysis and Designs," Advances in Cryptology CKYPTO '95 Proceedings'. Springer-Verlag, 1995, to appear.

576. W.F. Friedman, Methods for the Solution of Running-Key Ciphers, Riverbank Publication No. 16, Riverbank Labs, 1918.

577. W.F. Friedman, The Index of Coincidence and Its Applications in Cryptography, Riverbank Publication No. 22, Rivcrhank Labs, 1920. Reprinted by Aegean Park Press, 1987.

578. W.F. Friedman, Elements of Cryptanalysis, Laguna Hills, CA: Aegean Park Press, 1976.

579. W.F. Friedman, "Cryptology," Encyclopedia Britannica, v. 6, pp. 844-851, 1967.

580. A.M. Frieze, J. Hastad, R. Kannan, J.C. Lagarias, and A. Shamir, "Reconstructing Truncated Integer Variables Satisfying Linear Congruenccs," SIAM Journal on Computing, v. 17, n. 2, Apr 1988, pp. 262-280.

581. A.M. Frieze, R. Kannan, and J.C. Lagarias, "Linear Congruential Generators loo not Produce Random Sequences," Proceedings of the 25th IEEE Symposium on Foundations of Computer Science, 1984, pp. 480 484.

582. E. Fujiaski and T. Okamoto, "On Comparison of Practical Digitial Signature Schemes," Proceedings of the l992 Symposium on Cryptography and Information Security (SCIS 92), Tateshina, Japan, 2 4 Apr 1994, pp. lA.1-12.

583. A. Fujioka, T. Okamoto, and S. Miyaguchi, "ESIGN: An Efficient Digital Signature Implementation for Smart Cards, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 446 457.

584. A. Fujioka, T. Okamoto, and K. Ohta, "Interactive Bi-Proof Systems and Undeniable Signature Schemes," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 243-256.

585. A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections, " Advances in Cryptology AUSCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 244-251.

586. K. Gaardner and E. Snekkenes, "Applying a Formal Analysis Technique to the CCITT X.509 Strong Two-Way Authentication Protocol," lournal of Cryptology v. 3,n.2, l991,pp.81-98.

587. H.E Gaines, Cryptanalysis, American Photographic Press, 1937. Reprintcd by Dover Publications, 1956.

588. J. Gait, "A New Nonlinear Pseudorandom Number Generator, " IEEE Transactions on Software Engineering, v. SE-3, n. 5, Sep 1977, pp. 359-363.

589. J. Gait, "Short Cycling in the Kravitz-Reed Public Key Encryption System," Electronics Letters, v. 18, n. 16, 5 Aug 1982, pp. 706-707.

590. Z. Galil, S. Haber, and M. Yung, "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryp- tosystems," Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, 1985, pp. 360-371.

591. Z. Galil, S. Haber, and M. Yung, "Crypto- graphic Computation: Secure Fault- Tolerant Protocols and the Public-Key Model, " Advances in Cryptology CRYPTO '87Proceedings, Springer-Verlag, 1988, pp. 135-155.

592. Z. Galil, S. Haber, and M. Yung, "Mini- mum-Knowledge Interactive Proofs for Decision Problems, " SIAM lournal on Computing, v. 18, n. 4, 1989, pp. 711-739.

593. R.G. Gallager, Information Theory and Reliable Communications, New York:John Wiley & Sons, 1968.

594. P. Gallay and E. Depret, "A Cryptography Microprocessor," 1988 IEEE International Solid-State Circuits Conference Digest of Technical Papers, 1988, pp. 148-149.

595. R.A. Games, "There are no de Bruijn Sequences of Span n with Complexity $2n + n + 1$," Journal of Combinatorical Theory, Series A, v. 34, n. 2, Mar 1983, pp. 248-251.

596. R.A. Games and A.H. Chan, "A Fast Algo- rithm for Determining the Complexity of a Binary Sequence with 2n,'t IEEE Transactions on Information Theory, v. IT-29, n. 1, Jan 1983, pp. 144-146.

597. R.A. Games, A.H. Chan, and E.L. Key, "On the Complexity of de Bruijn Sequences," ournal of Combinatorical Theory, Series A, v. 33, n. 1, Nov 1982, pp. 233-246.

598. S.H. Gao and G.L. Mullen, "Dickson Polynomials and Irreducible Polynomials over Finite Fields," Journal of Number Theory, v. 49, n. 1, Oct 1994, pp. 18-132.

599. M. Gardner, "A New Kind of Cipher That Would Take Millions of Years to Break," Scientific American, v. 237, n. 8, Aug 1977, pp. 120-124.

600. M.R. Garey and D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W.H. Freeman and Co., 1979.

601. S.L. Garfinkel, POP: Pretty Good Privacy, Sebastopol, CA: O'Reilly and Associates, 1995.

602. C.W. Gardiner, "Distributed Public Key Certificate Management," Proceedings of the Privacy and Security Research Group 1993 Workshop on Network and Distributed System Security, The Internet Society, 1993, pp. 69-73.

603. G. Garon and R. Outerbridge, "DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Finan- cial Institution Information Security in the 1990's," Cryptologia, v. 15, n. 3, Jul 1991, pp. 177-193.

604. M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson, "The Digital Distributed Systems Security Architecture," Proceedings of the 12th National Computer Seezznty Conference, NIST, 1989, pp. 305-319.

605. J. von zur Gathen, D. Kozen, and S. Landau, "Functional Decomposition of Polynomials, " Proceedings of the 28tl1 IEEE Symposium on the Poundations of Computer Science, IEEE Press, 1987, pp. 127617. 131.

606. RR. Geffe, "How to Protect Data With Ciphers That are Really Hard to Break," Electronics, v. 46, n. 1, Jan 1973, pp. 99-101.

607. D.K. Gifford, D. Heitmann, D.A. Segal, R.G. Cote, K. Tanacea, and D.E. Burmaster, "Boston Community Information System 1986 Experimental Test Results, " MIT/LCS/TR-397, MIT Laboratory for Computer Science, Aug 1987.

608. 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.

609. D.K. Gifford and D.A. Segal, "Boston Community Information System 1987-1988 Experimental Test Results," MIT/LCS/ TR-422, MIT Laboratory for Computer Science, May 1989.

610. H. Gilbert and G. Chase, "A Statistical Attack on the Feal-8 Cryptosystem, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 22-33

611. H. Gilbert and R Chauvaud, "A Chosen Plaintext Attack of the 16-Round Khufu Cryptosystem," Advances in Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 259-268.

612. M. Girault, "Hash-Functions Using Modulo-N Operations," Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1988, pp. 217-226.

613. J. Gleick, "A New Approach to Protecting Secrets is Discovered, " The New York Times, 18 Feb 1987, pp. C1 and C3.

614. J.-M. Goethals and C. Couvreur, "A Cryptanalytic Attack on the Lu-Lee Public-Key Cryptosystem, " Philips lournal of Research, v. 35, 1980, pp. 301-306.

615. O. Goldreich, "A Uniform-Complexity Treatment of Encryption and Zero Knowledge, Journal of Cryptology, v. 6, n. 1, 1993, pp. 21-53.

616. O. Goldreich and H. Krawczyk, "On the Composition of Zero Knowledge Proof Systems," Proceedings on the 17th International Colloquium on Automata, Languages, and Programming, Springer" Verlag, 1990, pp. 268-282.

617. O. Goldreich and E. Kushilevitz, "A Perfect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm, " Advances in Cryptology CRYPTO '88 I'roceedings, Springer-Verlag, 1990, pp. 58-70.

618. O. Goldreich and E. Kushilevitz, "A Per- fect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm," lour- nal of Cryptology, v. 6, n. 2, law, pp. 97-116.

619. O. Goldreich, S. Micali, and A. Wigderson, "Proofs That Yield Nothing but Their Validity and a Methodology of Cryptographic Protocol Design," Proceedings of the 27th IEEE Symposium on the Foundations of Computer Science, 1986, pp. 174-187.

620. O. Goldreich, S. Micali, and A. Wigderson, "How to Prove All NP Statements in Zero Knowledge and a Methodology of Cryptographic Protocol Design, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 171-185.

621. O. Goldreich, S. Micali, and A. Wigderson, "How to Play Any Mental Game," Pro- ceedings of the 19th ACM Symposium on the Theory of Computing, 1987, pp. 218-229.

622. O. Goldreich, S. Micali, and A. Wigdcrson, "Proofs That Yield Nothing but Their Validity and a Methodology of Crypto- graphic Protocol Design," Journal of the ACM, v. 38, n. 1, Jul 1991, pp. 691-729.

623. S. Goldwasser and J. Kilian, "Almost All Primes Can Be Quickly Certified, " Pro- ceedings of the 18th ACM Symposium on the Theory of Computing, 1986, pp. 316- 329.

624. S. Goldwasser and S. Micali, "Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information," Proceedings of the 14th ACM Symposium on the Theory of Computing, 1982, pp. 270-299.

625. S. Goldwasser and S. Micali, "Probabilistic Encryption," Journal of Computer and System Sciences. v. 28, n. 2, Apr 1984, pp. 270-299.

626. S. Goldwasscr, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interac- tive Proof Systems, " Proceedings of the 17th ACM Symposium on Theory of Com- puting, 1985, pp. 291-304.

627. S.Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interac tive Proof Systems, " SIAM lournal on Computing, v. 18, n. 1, Feb 1989, pp. 186 208.

628. S. Goldwasser, S. Micali, and R.L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM lournal on Computing, v. 17,n.2,Aprl988,pp.281-308.

629. S. Goldwasser, S. Micali, and A.C. Yao, "On Signatures and Authentication," Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 211-215.

630. J.D. Golic, "On the Linear Complexity of Functions of Periodic GFIq~ Sequences," IEEE Transactions on Information Theory, v. IT-35, n. 1. Jan 1989, pp. 69-75.

631. J.D. Golic, "Linear Cryptanalysis of Stream Ciphers," K.U. Leuven Workshop on Cryptographic Algorithms, Springer Verlag, 1995, pp. 262-282.

632. J.D. Golic, "Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers," Advances in Cryptology EURO CRYPT '95 Proceedings, Springer-Verlag, 1995, to appear.

633. J.D. Golic and M.J. Mihajlevic, "A Gener alized Correlation Attack on a Class of Stream Ciphers Based on the Levenshtein Distance, " journal of Cryptology, v. 3, n.3, 1991, pp. 201-212.

634. J.D. Golic and L. O'Connor, "Embedding and Probabilistic Correlation Attacks on Clock-Controlled Shift Registers," Advances in Cryptology EUROCRYPT '94 I'roceedings, Springer-Verlag, 1995, to appear.

635. R. Golliver, A.K. Lenstra, K.S. McCurley, "Lattice Sieving and Trial Division," Pro ceedings of the Algorithmic Number Theory Symposium, Cornell, 1994, to appear.

636. D. Gollmann, "Kaskadenschaltungen takt gesteuerter Schicberegister als Pseudozu fallszahlengencratoren," Ph.D. disserta tion, Universitat Linz, 1983. (In German).

637. D. Gollmann, "Pseudo Random Properties of Cascade Connections of Clock Con trolled Shift Registers," Advances in Cryp tology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 93-98.

638. D. Gollmann, "Correlation Analysis of Cascaded Sequences," Cryptography and Coding, H.J. Beker and F.C. Piper, eds., Oxford: Clarendon Press, 1989, pp. 289-297.

639. D. Gollmann, "Transformation Matrices of Clock-Controlled Shift Registers, " Cryptography and Coding 111, M.J. Ganley, ed., Oxford: Clarendon Press, 1993, pp. 197-210.

640. D. Gollmann and W.G. Chambers, "Lock-In Effect in Cascades of Clock-Controlled Shift-Registers, " Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 331-343.

641. D. Gollmann and WG. Chambers, "Clock-Controlled Shift Registers: A Review, " IEEE lournal on Selected Areas in Communications, v. 7, n. 4, May 1989, pp. 525-533.

642. D. Gollmann and W.G. Chambers, "A Cryptanalysis of Step~-cascades," Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 680-687.

643. S.W. Golomb, Shift Register Sequences, San Francisco: Holden-Day, 1967. (Reprinted by Aegean Park Press, 1982.

644. L. Gong, "A Security Risk of Depending on Synchronized Clocks, " Operating Systems Review, v. 26, n. 1, Jan 1992, pp. 49-53.

645. L. Gong, R. Needham, and R. Yahalom, "Reasoning About Belief in Cryptographic Protocols," Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991, pp. 234-248.

646. R.M. Goodman and A.J. McAuley, "A New Trapdoor Knapsack Public Key Cryptosystem," Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 150-158.

647. R.M. Goodman and A.J. McAuley, "A New Trapdoor Knapsack Public Key Cryptosystem," IKE Proceedings, v. 132, pt. E, n. 6, Nov 1985, pp. 289-292.

648. D.M. Gordon, "Discrete Logarithms Using the Number Field Sieve," Preprint, 28 Mar 1991.

649. D.M. Gordon and K.S. McCurley, "Computation of Discrete Logarithms in Fields of Characteristic Two," presented at the rump session of CRYPTO'91, Aug 1991.

650. D.M. Gordon and K.S. McCurley, "Massively Parallel Computation of Discrete Logarithms, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 661. 1993, pp. 312-323.

651. J.A. Gordon, "Strong Primes are Easy to Find," Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 216-223.

652. J.A. Gordon, "Very Simple Method to Find the Minimal Polynomial of an Arbitrary Non-Zero Element of a Finite Field, " Electronics Letters, v. 12, n. 25, 9 Dec 1976, pp. 663-664.

653. J.A. Gordon and R. Retkin, "Are Big S- Boxes Best7" Cryptography Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, March 29-April 2, 1982, Springer-Verlag, 1983, pp. 257-262.

654. M. Goresky and A. Klapper, "Feedback Registers Based on Ramified Extension of the 2-adic Numbers," Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

655. GOST, Gosudarstvennyi Standard 28147-89, "Cryptographic Protection for Data Processing Systems," Government Committee of the USSR for Standards, 1989. (in Russian.}

656. GOST R 34.10-94, Gosudarstvennyi Standard of Russian Federation, "Information technology. Cryptographic Data Security. Produce and check procedures of Electronic

Digital Signature based on Asymmetric Cryptographic Algorithm. " Government Committee of the Russia for   Standards, 1994. (In Russian.)

657. GOST R 34.11-94, Gosudarstvennyi Standard of Russian Federation, "Information technology. Cryptographic Data Security.   Hashing function." Government Committee of the Russia for Standards, 1994. (In   Russian.)

658. R. Gottfert and H. Niederreiter, "On the   Linear Complexity of Products of Shift-Register Sequences," Advances in Cryptology EUROCRYPT '93 Proceedings,   Springer-Verlag, 1994, pp. 151-158.

659. R. Gottfert and H. Niederreiter, "A General Lower Bound for the Linear Complexity of the Product of Shift-Register   Sequences, " Advances in Cryptology   EUROCRYPT '94 Proceedings, Springer- Verlag, 1995, to appear.

660. J. van de Graaf and R. Peralta, "A Simple   and Secure Way to Show the Validity of   Your Public Key," Advances in Cryptology CRYPTO '87 Proceedings, Springer-   Verlag, 1988, pp. 128-134.

661. J. Grollman and A.L. Selman, "Complexity   Measures for Public-Key Cryptosystems," Proceedings of the 25th IEEE Symposium   on the Foundations of Computer Science, 1984, pp. 495-503

662. GSA Federal Standard 1026, "Telecommunications: General Security Requirements   for Equipment Using the Data Encryption   Standard, " General Services Administration, Apr 1982.

663. GSA Federal Standard 1027, "Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data   Link Layers of Data Communications, "   General Services Administration, Jan 1983.

664. GSA Federal Standard 1028, "Intcroperability and Security Requirements for Use   of the Data Encryption Standard with   CCITT Group 3 Facsimile Equipment, "   General Services Administration, Apr   1985.

665. R Guam, "Cellular Automaton Public Key   Cryptosystems," Complex Systems, v. 1,   1987, pp. 51-56.

666. H. Guan, "An Analysis of the Finite   Automata Public Key Algorithm, " CHINACRYPT'94, Xidian, China, 11-15 Nov   1994, pp. 120-126. (In Chinese)

667. G. Guanella, "Means for and Method for   Secret Signalling," U.S. Patent #2,405,500, 6 Aug 1946.

668. M. Gude, "Concept for a High-Performance Random Number Generator   Based on Physical Random Phenomena,"   Frequenz, v. 39, 1985, pp. 187-190.

669. M. Gude, "Ein quasi-idealer Gleichverteil-ungsgenerator basierend auf physikalischen Zufallsphinomenen," Ph.D. dissertation, Aachen University of Technology, 1987. (In German.)

670. L.C. Guillou and J.-J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 123-128.

671. L.C. Guillou and J. Quisquater, "A 'Paradoxical' Identity-Based Signature Scheme Resulting from Zero-Knowledge," Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 216- 231.

672. L.C. Guillou, M. Ugon, and J. -J. Quisquater, "The Smart Card: A Standardized Security Device Dedicated to Public Cryptology," contemporary Cryptology: The Science of Information Integrity G. Simmons, ed., IEEE Press, 1992, pp. 561-613.

673. C.G. Gunther, "Alternating Step Generators Controlled by de Bruijn Sequences," Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1988, pp. 5-14.

674. C.G. Gunther, "An Identity-based Key-exchange Protocol, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 29-37.

675. H. Gustafson, E. Dawson, and B. Caelli, "Comparison of Block Ciphers, " Advances in Cryptology AUSCRYPT '90 Proceed- ings, Springer-Verlag, 1990, pp. 208-220.

676. P. Gutmann, personal communication, 1993.

677. H. Gutowitz, "A Cellular Automaton Cryptosystem: Specification and Call for Attack," unpublished manuscript, Aug 1992.

678. H. Gutowitz, "Method and Apparatus for Encryption, Decryption, and Authentication Using Dynamical Systems," U.S. Patent #5,365,589, 15 Nov 1994.

679. H. Gutowitz, "Cryptography with Dynamical Systems, " Cellular Automata and Cooperative Phenomenon, Kluwer Academic Press, 1993.

680. R.K. Guy, "How to Factor a Number, " Fifth Manitoba Conference on Numeral Mathematics Congressus Numerantium, v. 16, 1976, pp. 49-89.

681. R.K. Guy, Unsolved Problems in Number Theory, Springer-Verlag, 1981.

682. S. Haber and W.S. Stornetta, "How to Time-Stamp a Digital Document, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 437-455.

683. S. Haber and W.S. Stornetta, "How to Time-Stamp a Digital Document, " journal of Cryptology, v. 3, n. 2, 1991, pp. 99-112.

684. S. Haber and W.S. Stornetta, "Digital Document Time-Stamping with Catenate Certificate," U.S. Patent #5,136,646, 4 Aug 1992.

685. S. Haber and W.S. Stornetta, "Method for Secure Time-Stamping of Digital Documents," U.S. Patent #5,136,647, 4 Aug 1992.

686. S. Haber and W.S. Stornetta, "Method of Extending the Validity of a Cryptographic Certificate," U.S. Patent #5,373,561, 13 Dec 1994.

687. T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E73, n. 7,1ul 1990, pp. 1041-1044.

688. T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 127-140.

689. S. Hada and H. Tanaka, "An Improvement Scheme of DES against Differential Cryptanalysis," Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp 14A. I-l l. fin Japanese. l

690. B.C.W. Hagelin, "The Story of the Hagelin Cryptos," Cryptologia, v. 18, n.3, Jul 1994, pp. 204-242.

691. T. Hansen and G.L. Mullen, "Primitive Polynomials over Finite Fields," Mathematics of Computation, v. 59, n. 200, Oct 1992, pp. 639-643.

692. S. Harada and S. Kasahara, "An ID-Based Key Sharing Scheme Without Preliminary Communication," IEICE Japan, Technical Report, ISEC89-38, 1989. (In Japanese).

693. S. Harari, "A Correlation Cryptographic Scheme," EUROCODE '90 International Symposium on Coding Theory, Springer-Verlag, 1991, pp. 180-192.

694. T. Hardjono and J. Seberry, "Authentication via Multi-Service Tickets in the Kuperee Server, " Computer Security ESORICS 94, Springer-Verlag, 1994, pp. 144 160.

695. L. Harn and T. Kiesler, "New Scheme for Digital Multisignatures," Electronics Letters, v. 25, n. 15, 20 Jul 198Y, pp. 1002- 1003.

696. L. Harn and T. Kiesler, "Improved Rabin's Scheme with High Efficiency, " Electronics Letters, v. 25, n. 15, 20 Jul 1989, p. 1016.

697. L. Harn and T. Kiesler, "Two New Efficient Cryptosystems Based on Rabin's Scheme, " Fifth Annual Computer Secunty Applications Conference, IEEE Computer Society Press, 1990, pp. 263-270.

698. L. Harn and D.-C. Wang "Cryptanalysts   and Modification of Digital Signature   Scheme Based on Error-Correeting Codes, "   Electronics Letters, v. 28. n. 2, 10 Jan 1992,   p. 157-159.

699. L. Harn and Y. Xu, "Design of Generalized   ElGamal Type Digital Signature Schemes Based on Discrete Logarithm, " Electronics   Letters, v. 30, n. 24. 24 Nov 1994, p.   2025-2026.

700. L. Harn and S. Yang, "Group-Oriented   Undeniable Signature Schemes without   the Assistance of a Mutually Trusted   Party," Advances in Cryptology   AUSCRYPT '92 Proceedings, Springer-   Verlag, 1993, pp. 133-142.

701. G. Harper, A. Menezes, and S. Vanstone,   "Public-Key Cryptosystems with Very   Small Key Lengths," Advances in Cryptology EUROCRYPT '92 Proceedings,   Springer-Verlag 1993, pp. 163-173.

702. C. Harpes, "Notes on High Order Differen-   tial Cryptanalysis of DES, " internal report, Signal and Information Processing Labora-   tory, Swiss Federal Institute of Technology, Aug 1993.

703. G.W. Hart, "To Decode Short Cryptograms," Communications of the ACM, 717.   v. 37, n. 9, Sep 1994, pp. 102-108.

704. J. Hastad, "On Using RSA with Low Exponent in a Public Key Network," Advances   in Cryptology CRYPTO '85 Proceedings,   Springer-Verlag 1986, pp. 403-408.

705 1 Hastad and A. Shamir, "The Cryptographic Secunty of Truncated Linearly   Related Variables, " Proceedings of the 1 7th Annual ACM Symposium on the Theory of Computing, 1985, pp. 356-362.

706. R.C. Hauser and E.S. Lee, "Verification and Modelling of Authentication Protocols, " ESORICS 92, Proceedings of the Second European Symposium on Research in Computer Security, Springer-Verlag 1992,   pp. 131-154.

707. B. Hayes, "Anonymous One-Time Signatures and Flexible Untraceable Electronic Cash," Advances in Cryptology   AUSCRYPT '90 Proceedings, Springer   Verlag, 1990, pp. 294-305.

708. D.K. He, "LUC Public Key Cryptosystem and its Properties," CHINACRYPT '94,   Xidian, China, 11-15 Nov 1994, pp. 60-69.   (In Chinese.)

709. J. He and T. Kiesler, "Enhancing the Security of ElGamal's Signature Scheme," IKE Proceedings on Computers and Digital   Techniques, v. 141, n.3, 1994. pp.193-195.

710. E.H. Hebern, "Electronic Coding Machine, "   U.S. Patent #1,510,441, 30 Sep 1924.

711. N. Heintze and J.D. Tygar, "A Model for   Secure Protocols and their Compositions, "

Proceedings of the 1994 IEEE Computer   Society Symposium on Research in Security and   Privacy 1994, pp. 2-13.

712. M.E. Hellman, "An Extension of the Shannon Theory Approach to Cryptography,"   IEEE Transactions on Information Theory,   v. IT-23, n. 3, May 1977, pp. 289-294.

713. M.E. Hellman, "The Mathematics of Public-Key Cryptography," Scientihc American, v. 241, n. 8, Aug 1979, pp. 146-157.

714. M.E. Hellman, "DES Will Be Totally Insecure within Ten Years, " IEEE Spectrum, v.   16, n. 7, Jul 1979, pp. 32-39.

715. M.E. Hellman, "On DES-Based Synchronous Encryption," Dept. of Electrical   Engineering Stanford University, 1980.

716. M.E. Hellman, "A Cryptanalytic Time- Memory Trade Off," IEEE Transactions on   Information Theory, v. 26, n. 4, Jul 1980,   pp. 401-406.

717. M.E. Hellman, "Another Cryptanalytic   Attack on Cryptosystem for Multiple   Communications', " Information Processing Letters, v. 12, 1981. pp. 182-183.

718. M.E. Hellman, W. Diffie, and R.C. Merkle,   "Cryptographic Apparatus and Method,"   U.S. Patent #4,200,770, 29 Apr 1980.

719. M.E. Hellman, W. Diffie, and R.C. Merkle,   "Cryptographic Apparatus and Method,"   Canada Patent #1,121,480, 6 Apr 1982.

720. M.E. Hellman and R.C. Merkle, "Public   Key Cryptographic Apparatus and   Method," U.S. Patent #4,218,582, 19 Aug   1980.

721. M.E. Hellman, R. Merkle, R. Schroeppel,   L. Washington, W. Diffie, S. Pohlig, and R   Schweitzer, "Results of an Initial Attempt   to Cryptanalyze the NBS Data Encryption   Standard," Technical Report SEL 76-042,   Information Systems Lab, Department of   Electrical Engineering Stanford University, 1976.

722. M.E. Hellman and S.C. Pohlig, "Exponentiation Cryptographic Apparatus and   Method,"   U.S. Patent #4,424,414, 3 Jan   1984.

723. M.E. Hellman and J.M. Reyneri, "Distribution of Drainage in the DES," Advances in   Cryptology: Proceedings of Crypto 82,   Plenum Prcss, 1983, pp. 129-131.

724. E Hendessi and M.R. Arcf, "A Successful   Attack Against the DES, " Third Canadian Workshop on Information Theory and   Applications, Springer-Verlag, 1994, pp.   78-90.

725. T. Herlestam, "Critical Remarks on Some 738.   Public-Key Cryptosystems, " BIT, v. 18, 1978, pp. 493-496.

726. T. Herlestam, "On Ftmctions of Linear   Shift Register Sequences", Advances in   Cryptology EUROCRYPT '85, Springer   Verlag, 1986, pp. 119-129.

727. T. Herlestam and R. Iohannesson, "On   Computing Logarithms over GF(2P)," BIT, 740.   v. 21, 1981, pp. 326-334.

728. H.M. Heys and S.E. Tavares, "On thc Security of the CAST Encryption Algorithm,"   Proceedings of the Canadian Conference on Electrical and Computer Engineenng, Halifax,   Nova Scotia, Sep 1994, pp. 332-335.

729. H.M. Heys and S.E. Tavares, "The Design of Substitution-Permutation Networks   Resistant to Differential and Linear Cryptanalysis," Proceedings of the 2nd Annual   ACM   Conference on Computer and Communications Security, ACM Press, 1994, pp. 148-155.

730. E. Heyst and T.P. Pederson, "How to Make Fail-Stop Signatures," Advances in Cryptology   EUROCRYPT '92 Proceedings,   Springer-Verlag 1993, pp. 366-377.

731. E. Heyst, T.R Pederson, and B. Pfitzmann,   "New Construction of Fail-Stop Signatures and   Lower Bounds," Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag   1993, pp. 15-30.

732. L.S. Hill, "Cryptography in an Algebraic Alphabet," American Mathematical Monthly, v. 36,   Jun-Jul 1929, pp. 306-312.

733. P.J.M. Hin, "Channel-Error-Correcting Privacy Cryptosystems," Ph.D. dissertation,   Delft   University of Technology, 1986. (In   Dutch).

734. R. Hirschield, "Making Elcctronic Refunds   Safer, " Advances in Cryptology CRYPTO '92   Proceedings, Springer-Verlag, 1993, pp. 106-112.

735. A. Hodges, Alan Turing: The Enigma of Intelligence, Simon and Schuster, 1983.

736. W. Hohl, X. Lai, T. Meier, and C. Waldvogel, "Security of Iterated Hash Functions Based   on Block Ciphers, " Advances in   Cryptology CRYPTO '93 Proceedings,   Springer-   Verlag, 1994, pp. 379-390.

737. F. Hoornaert, M. Decroos, J. Vandewalle,   and R. Govaerts, "Fast RSA-Hardware: Dream   or Reality?" Advances in Cryptology E UROCRYPT '88 Proceedings,   Springer-Verlag,   1988, pp. 257-264.

738. F. Hoornaert, J. Goubert, and Y. Desmedt,   "Efficient Hardware Implementation of   the   DES," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag,   1985, pp.   147-173.

739. E. Horowitz and S. Sahni, Fundamentals of   Computer Algonthms, Rockville, MD: Computer Science Press, 1978.

740. R Horster, H. Petersen, and M. Michels, "Meta-ElGamal Signature Schemes," Proceedings of the 2nd Annual ACM Conference on Computer and Communications Security, ACM Press, 1994, pp. 96-107.

741. R Horster, H. Petersen, and M. Michels, "Meta Message Recovery and Meta Blind Signature Schemes Based on the Discrete Logarithm Problem and their Applications, " Advances in Cryptology ASIACRYPT '94 Proceedings, Springer-Verlag, 1995, pp. 224-237.

742. L.K. Hua, Introduction to Number Theory, Springer-Verlag, 1982.

743. K. Huber, "Specialized Attack on Chor-Rivest Public Key Cryptosystem, " Electronics Letters, v.27, n. 23, 7 Nov 1991, pp. 2130-2131.

744. E. Hughes, "A Cypherpunk's Manifesto, " 9 Mar 1993.

745. E. Hughes, "An Encrypted Key Transmission Protocol," presented at the rump session of CRYPTO '94, Aug 1994.

746. H. Hule and W.B. Muller, "On the RSA- Cryptosystem with Wrong Keys," Contributions to General Algebra 6, Vienna: Verlag Holder-Pichler-Tempsky, 1988, pp. 103-109.

747. H.A. Hussain, J.W.A. Sada, and S.M. Kalipha, "New Multistage Knapsack Public-Key Cryptosystem," International Journal of Systems Science, v. 22, n. 11, Nov 1991, pp. 2313-2320.

748. T. Hwang, "Attacks on Okamoto and Tanaka's One-Way ID-Based Key Distribution System," Information Processing Letters,v.43,n.2,Aug1992, pp.83-86.

749. T. Hwang and T.R.N. Rao, "Secret Error- Correcting Codes (SECC)." Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 540-563.

750. C. Ianson and C. Mitchell, "Security Defects in CCITT Recommendation X.509 the Directory Authentication Framework," Computer Communications Review, v. 20, n. 2, Apr 1990, pp. 30-34.

751. IBM, "Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference," SC40-1675-1, IBM Corp., Nov 1990.

752. IBM, "Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference Public Key Algorithm," IBM Corp., Mar 1993.

753. R. Impagliazzo and M. Yung, "Direct Minimum-Knowledge Computations, " Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 40-51.

754. I. Ingemarsson, "A New Algorithm for the Solution of the Knapsack Problem," Lecture Notes in Computer Science 149; Cryptography: Proceedings of the Workshop on Cryptography, Springer-Verlag, 1983, pp. 309-315.

755. I. Ingemarsson, "Delay Estimation for Truly Random Binary Sequences or How to Measure the Length of Rip van Winkle's Sleep," Communications and Cryptography: Two Sides of One Tapestry, R.E. Blahut ct al., eds., Kluwer Adademic Pub- lishcrs, 1994, pp. 179-186.

756. I. Ingemarsson and G.J. Simmons, "A Protocol to Set Up Shared Secret Schemes without the Assistance of a Mutually Trusted Party," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 266-282.

757. I. Ingemarsson, D.T. Tang, and C.K. Wong, "A Conference Key Distribution System," IEEE Transactions on Information Theory, v. IT-28, n. 5, Sep 1982, pp. 714-720.

758. ISO DIS 8730, "Banking Requirements for Message Authentication Wholesale," Association for Payment Clearing Services, London, Jul 1987.

759. ISO DIS 8781-1, "Banking Approved Algorithms for Message Authentication Part 1: DEA" Association for Payment Clearing Services, London, 1987.

760. ISO DIS 8731-2, "Banking Approved Algorithms for Message Authentication Part 2: Message Authenticator Algorithm, " Association for Payment Clearing Services, London, 1987.

761. ISO DIS 8732, "Banking Key Management (Wholesaled) " Association for Payment Clearing Services, London, Dec 1987.

762. ISO/IEC 9796, "Information Technology Security Techniques. Digital Signature Scheme Giving Message Recovery," International Organization for Standardization, Jul 1991.

763. ISO/IEC 9797, "Data Cryptographic Techniques. Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm," International Organization for Standardization, 1989.

764. ISO DIS 10118 DRAFT, "Information Technology Security Techniques. Hash Functions" International Organization for Standardization, 1989.

765. ISO DIS 10118 DRAFT, "Information Technology Security Techniques. Hash Functions" International Organization for Standardization, April 1991.

766. ISO N98, "Hash Functions Using a Pseudo Random Algorithm," working document, ISO-IEC/JTC 1 /SC27/WG2, International Organization for Standardization, 1992.

767. ISO N179, "AR Fingerprint Function," working document, ISO-IEC/JTC1/SC27/ WG2, International Organization for Standardization, 1992.

768. ISO/IEC 10118, "Information Technology Security Techniques. Hash Functions Part 1: General and Part 2: Hash-Functions Using an e-Bit Block Cipher Algorithm, " International Organization for Standardization, 1993.

769. K. Ito, S. Kondo, and Y. Mitsuoka, "SXAL8/MBAL Algorithm," Technical Report, ISEC93-68, IEICE Japan, 1993. (In Japancsc.)

770. K.R. Iversen, "The Application of Cryptographic Zero-Knowledge Techniques in Computerized Secret Ballot Election Schemes, " Ph.D. dissertation, IDT-report 1991:3, Norwegian Institute of Technology, Feb 1991.

771. K.R. Iversen, "A Cryptographic Scheme for Computerized General Elections, " Advances in Cryptology CRYPTO '91 Proceedings, Springcr-Vcrlag, 1992, pp. 405-419.

772. K. Iwamura, T. Matsumoto, and H. Imai, "An Implcmcutation Method for RSA Cryptosystem with Parallel Processing ", Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J75-A, n. 8, Aug 1992, pp. 1301-1311.

773. W.J. Jaburek, "A Generalization of ElGamal's Public Key Cryptosystem, " Advances in Cryptology EUROCRYPT '89 Proceedings, 1990, Springer-Verlag, pp. 23-28.

774. N.S. James, R. Lidl, and H. Niederreiter, "Breaking the Cade Cipher," Advances in Cryptology CRYPTO '86 Proceedings, 1987, Springer-Verlag, pp. 60-63.

775. C.J.A. Jansen, "On the Key Storage Requirements for Secure Terminals'" Computers and Security, v. 5, n. 2, Jun 788. 1986, pp. 145-149.

776. C.J.A. Jansen, "Investigations on Nonlinear Strcamcipher Systems: Construction and Evaluation Methods," Ph.D. dissertation, Technical University of Delft, 1989.

777. C.J.A. Jansen and D.E. Boekee, "Modes of Blockcipher Algorithms and their Protection against Active Eavesdropping, " Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1988, pp. 281-286.

778. S.M. Jennings, "A Special Class of Binary Sequences," Ph.D. dissertation, University of London, 1980.

779. S.M. Jennings, "Multiplexed Sequences: Some Properties of the Minimum Polynomial," Lecture Notes in Computer Science 149; Cryptography: Proceedings of the Workshop on Cryptography, Springer-Verlag, 1983, pp. 189-206.

780. S.M. Jennings, "Autocorrelation Function of the Multiplexed Sequence, " IKE Pro ceedings, v. 131, n. 2, Apr 1984, pp. 169-172.

781. T. Jin, "Care and Feeding of Your Three Headed Dog, " Document Number IAG-90-011, Hewlett-Packard, May 1990.

782. T. Jin, "Living with Your Three-Headed Dog," Document Number IAG-90-012, Hewlett-Packard, May 1990.

783. A. Jiwa, J. Seberry. and Y. Zheng, "Beacon Based Authentication," Computer Security ESORICS 94, Springer-Verlag, 1994, pp. 125-141.

784. D.B. Johnson, G.M. Dolan, M.J. Kelly, A.V. Le, and S.M. Matyas, "Common Cryptographic Architecture. Cryptographic Application Programming Interface," IBM Systems journal, v. 30, n.2, 1991, pp.130-150.

785. D.B. Johnson, S.M. Matyas, A.V. Le. and J.D. Wilkins, "Design of the Commercial Data Masking Facility Data Privacy Algorithm," 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 93-96.

786. J.R Jordan, "A Variant of a Public-Key Cryptosystem Based on Goppa Codes," Sigact News, v. 15, n. 1, 1983, pp. 61-66.

787. A. Joux and L. Granboulan, "A Practical Attack Against Knapsack Based Hash Functions" Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

788. A. Joux and J. Stern, "Cryptanalysis of Another Knapsack Cryptosystem, " Advances in Cryptology ASIACRYPT '91 Proceedings, Springer-Verlag, 1993, pp. 470-476.

789. R.R. Jueneman, "Analysis of Certain Aspects of Output-Feedback Mode, " Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp.99-127.

790. R.R. Jueneman, "Electronic Document Authentication, " IEEE Network Magazine, v. 1, n.2, Apr 1978, pp. 17-23.

791. R.R. Jueneman, "A High Speed Manipulation Detection Code," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 327-346.

792. R.R. Jueneman, S.M. Matyas, and C.H. Meyer, "Message Authentication with Manipulation Detection Codes," Proceedings of the 1983 IEEE Computer Society Symposium on Research in Security and Privacy, 1983, pp. 733-54.

793. R.R. Jucncman, S.M. Matyas, and C.H. Meyer, "Message Authentication, " IEEE Communications Magazine, v. 23, n. 9, Sep 1985, pp. 29 40.

794. D. Kahn, The Codebreakers: The Story of Secret Writing, New York: Macmillan Publishing Co., 1967.

795. D. Kahn, Kahn on Codes, New York: Macmillan Publishing Co., 1983.

796. D. Kahn, Seizing the Enigma, Boston: Houghton Mifflin Co., 1991.

797. P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The Solution to Security for Open Distributed Systems," Journal of Computer communications, V. 17, n. 4, Jul 1994, pp. 501-518.

798. R. Kailar and V.D. Gilgor, "On Belief Evolution in Authentication Protocols," Proceedings of the Computer Security Foundations Workshop IV, IEEE Computer Society Press, 1991, pp. 102-116.

799. B.S. Kaliski, "A Pseudo Random Bit Generator Based on Elliptic Logarithms," Master's thesis, Massachusetts Institute of Technology, 1987.

800. B.S. Kaliski, letter to NIST regarding DSS, 4 Nov 1991.

801. B.S. Kaliski, "The MD2 Message Digest Algorithm," RFC 1319, Apr 1992.

802. B.S. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certificates and Related Services," RFC 1424, Feb 1993.

803. B.S. Kaliski, "An Overview of the PKCS Standards," RSA Laboratories, Nov 1993.

804. B.S. Kaliski, "A Survey of Encryption Standards, IEEE Micro, v. 13, n. 6, Dec 1993, pp. 74-81.

805. B.S. Kaliski, personal communication, 1993.

806. B.S. Kaliski, "On the Security and Performance of Several Triple-DES Modes," RSA Laboratories, draft manuscript, Jan 1994.

807. B.S. Kaliski, R.L. Rivest, and A.T. Sherman, "Is the Data Encryption Standard a Group?", Advances in Cryptology EUROCRYPT '85, Springer-Verlag, 1986, pp. 81-95.

808. B.S. Kaliski, R.L. Rivest, and A.T. Sherman, "Is the Data Encryption Standard a Pure Cipher? Results of More Cycling Experiments in DESK, " Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 212-226.

809. B.S. Kaliski, R.L. Rivest, and A.T. Sherman, "Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DESK," Journal of Cryptology v. 1, n. 1, 1988, pp. 3-36.

810. B.S. Kaliski and M.J.B. Robshaw, "Fast Block Cipher Proposal," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 33 40.

811. B.S. Kaliski and M.J.B. Robshaw, "Linear Cryptanalysis Using Multiple Approximations," Advances in Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 26-39.

812. B.S. Kaliski and M.J.B. Robshaw, "Linear Cryptanalysis Using Multiple Approximations and PEAL," K.U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

813. R.G. Kammer, statement before the U.S. government Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, 29 Apr 1993.

814. T. Kaneko, K. Koyama, and R. Terada, "Dynamic Swapping Schemes and Differential Cryptanalysis, Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography Seoul, Korea, 24-26 Oct 1993, pp. 292-301.

815. T. Kaneko, K. Koyama, and R. Terada, "Dynamic Swapping Schemes and Differential Cryptanalysis," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E77-A, n. 8, Aug 1994, pp. 1328-1336.

816. T. Kaneko and H. Miyano, "A Study on the Strength Evaluation of Randomized DES-Like Cryptosystems against Chosen Plaintext Attacks, " Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93), Shozenji, Japan, 28-30 Jan 1993, pp. 15C.1-10.

817. J. Karl, "A Cryptosystem Based on Propositional Logic," Machines, Languages, and Complexity: 5th International Meeting of Young Computer Scientists, Selected Contributions, Springer-Verlag, 1989, pp. 210-219.

818. E.D. Karnin, J.W. Greene, and M.E. Hellman, "On Sharing Secret Systems," IEEE Transactions on Information Theory v. IT- 29, 1983, pp. 35 41.

819. F.W Kasiski, Die Geheimschriften and die Dechiffrir-kunst, E.S. Miller und Sohn, 1863. In German.

820. A. Kehne, J. Schonwalder, and H. Langendorfer, "A Nonce-Based Protocol for Multiple Authentications," Operating Systems Review, v. 26, n. 4, Oct 1992, pp. 84-89.

821. J. Kelsey, personal communication, 1994.

822. R. Kemmerer, "Analyzing Encryption Protocols Using Formal Verification Techniques, " IEEE Journal on Selected Areas in Communications, v. 7, n. 4, May 1989, pp. 448 457.

823. R. Kemmerer, C.A. Meadows, and J. Millen, "Three Systems for Cryptographic Protocol Analysis," Journal of Cryptology v. 7, n. 2, 1994, pp. 79-130.

824. S.T. Kent, "Encryption-Based Protection Protocols for Interactive User-Computer Communications, " MIT/LCS/TR162, MIT Laboratory for Computer Science, May 1976.

825. S.T. Kent, "Privacy Enhancement for Internct Electronic Mail: Part II: Certificate Based Key Management," RFC 1422, Feb 1993.

826. S.T. Kent, "Understanding the Internet Certification System, " Proceedings of INET '93, The Internet Society, 1993, pp. BAB 1 -BAB 10.

827. S.T. Kent and J. Linn, "Privacy Enhaneement for Internet Electronic Mail: Part II: Certificate-Based Key Management," RFC 1114, Aug 1989.

828. V. Kessler and G. Wedel, "AUTOLOG An Advanced Logic of Authentication," Proceedings of the Computer Security Foundations Workshop, IEEE Computer Society Press, 1994, pp. 90-99.

829. E.L. Key, "An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators," IEEE Transactions on Information Theory v. IT-22, n. 6, Nov 1976, pp. 732-736.

830. T. Kiesler and L. Harn, "RSA Blocking and Multisignature Schemes with No Bit Expansion," Electronics Letters, v. 26, n. 18, 30 Aug 1990, pp. 1490-1491.

831. J. Kilian, Crises of Randomness in Algorithms and Protocols, MIT Press, 1990.

832. J. Kilian, "Achieving Zero-Knowledge Robustly, " Advances in Cryptology CRYPTO 90 Proceedings, Springer-Verlag, 1991, pp. 313-325.

833. J. Kilian and T. Leighton, "Failsafe Key Escrow," MIT/LCS/TR-636, MIT Laboratory for Computer Science, Aug 1994.

834. K. Kim, "Construction of DES-Like S-Boxes Based on Boolean Functions Satisfying the SAC, " Advances in Cryptology, ASIACRYPT 91 Proceedings, Springer-Verlag, 1993, pp. 59-72.

835. K. Kim, S. Lee, and S. Park, "Necessary Conditions to Strengthen DES S-Boxes Against Linear Cryptanalysis," Proceedings of the 1994 Symposium on Cryptography and Information Secunty (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp. 15D.1-9.

836. K. Kim, S. Lee, and S. Park, "How to Strengthen DES against Differential Attack, " unpublished manuscript, 1994.

837. K. Kim, S. Lee, S. Park, and D. Lee, "DES Can Be Immune to Differential Cryptanalysis, " Workshop on Selected Areas in Cryptography Workshop Record, Kingston, Ontario, 5-6 May 1994, pp. 70-81.

838. K. Kim, S. Park, and S. Lee, "How to Strengthen DES against Two Robust Attacks," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography Inuyama, Japan, 24-27 Jan 1995, 173-182.

839. K. Kim, S. Park, and S. Lee, "Reconstruction of s2DES S-Boxes and their Immunity to Differential Cryptanalysis, " Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24-26 Oct l993, pp.282-291.

840. S. Kim and B.S. Um, "A Multipurpose Membership Proof System Based on Discrete Logarithm," Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24-26 Oct 1993, pp. 177-183.

841. P. Kinnucan, "Data Encryption Gurus: Tuchman and Meyer," Cryptologia, v. 2, n. 4, Oct 1978.

842. A. Klapper, "The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic," Journal of cryptology v. 7, n. 1, 1994, pp. 33-52.

843. A. Klapper, "Feedback with Carry Shift Registers over Finite Fields," K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

844. A. Klapper and M. Goresky, "2-adic Shift Registers, " Fast Software Encryption, Cambridge Security Workshop l'roceed- ings, Springer-Verlag, 1994, pp. 174-178.

845. A. Klapper and M. Goresky, "2-adic Shift Registers," Technical Report #239-93, Department of Computer Science, University of Kentucky, 19 Apr 1994.

846. A. Klapper and M. Goresky, "Large Period Nearly de Bruijn FCSR Sequences, " Advances in Cryptology EUROCRYPT 95 Proceedings, Springer-Verlag, 1995, pp. 263-273.

847. D.V. Klein, "'Foiling the Cracker: A Survey of, and Implications to, Password Security," Proceedings of the USENIX UNIX Security Workshop, Aug 1990, pp. 5-14.

848. D.V Klein, personal communication, 1994.

849. C.S. Kline and G.J. Popek, "Public Key vs. Conventional Key Cryptosystems," Proceedings of AFIPS National Computer Conference, pp. 831-837.

850. H.-J. Knobloch, "A Smart Card Implementation of the Fiat-Shamir Identification Scheme," Advances in Cryptology EUROCRPYT '88 Proceedings, Springer-Verlag, 1988, pp. 87-95.

851. T. Knoph, J. Fropl, W. Beller, and T.Giesler, "A Hardware Implementation of a Modified DES Algorithm," Microprocessing and Microprogramming, v. 30, 1990, pp. 59-66.

852. L.R. Knudsen, "Cryptanalysts of LOKI," Advances in Cryptology ASIACRYPT '91 Proceedings, Springer-Verlag, 1993, pp. 22-35.

853. L.R. Knudsen, "Cryptanalysts of LOKI," Cryptography and Coding 111, M.J. Ganley, ed., Oxford: Clarendon Press, 1993, pp. 223-236.

854. L.R. Knudsen, "Cryptanalysts of LOKI91," Advances in Cryptology AUSCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 196-208.

855. L.R. Knudsen, "Iterative Characteristics of DES and sZDES," Advances in Cryptology CRYPTO '92, Springer-Verlag, 1993, pp. 497-511.

856. L.R. Knudsen, "An Analysis of Kim, Park and Lee's DES-Like S-Boxes," unpublished manuscript, 1993.

857. L.R. Knudsen, "Practically Secure Feistel Ciphers," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 211-221.

858. L.R. Knudsen, "Block Ciphers Analysis, Design, Applications," Ph.D. dissertation, Aarhus University, Nov 1994.

859. L.R. Knudsen, personal communication, 1994.

860. L.R. Knudsen, "Applications of Higher Order Differentials and Partial Differentials, " K. U Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

861. L.R. Knudsen and X. Lai, "New Attacks on All Double Block Length Hash Functions of Hash Rate 1, Including the Parallel-DM," Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

862. L.R. Knudsen, "A Weakness in SAFER K-64, " Advances in Cryptology-CRYPTO '95 Proceedings, Springer-Verlag, 1995, to appear.

863. D. Knuth, The Art of Computer Programming: Volume 2, Seminumerical Algorithms, 2nd edition, Addison-Wesley, 1981.

864. D. Knuth, "Deciphering a Linear Congruential Encryption," IEEE Transactions on Information Theory, v. IT-31, n. 1, Jan 1985, pp. 49-52.

865. K. Kobayashi and L. Aoki, "On Linear Cryptanalysis of MBAL, " Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS 95, Innyama, Japan, 24-27 Jan 1995, pp. A4.2.1-9.

866. K. Kobayashi, K. Tamura, and Y. Nemoto, "Two-dimensional Modified Rabin Cryptosystem," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J72-D, n. 5, May 1989, pp. 850-851. (In Japanese.)

867. N. Koblitz, "Elliptic Curve Cryptosystems, " Mathematics of Computation, v. 48, n. 177, 1987, pp. 203-209.

868. N. Koblitz, "A Family of Jacobians Suitable for Discrete Log Cryptosystems, " Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag 1990, pp. 94-99.

869. N. Koblitz, "Constructing Elliptic Curve Cryptosystems in Characteristic 2," Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag 1991, pp. 156-167.

870. N. Koblitz, "Hyperelliptic Cryptosystems," Journal of Cryptology, v. 1, n. 3, 1989, pp. 129-150.

871. N. Koblitz, "CM-Curves with Good Cryptographic Properties, " Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 279-287.

872. C.K. Koc, "High-Speed RSA Implementation," Version 2.0, RSA Laboratories, Nov 1994.

873. M.J. Kochanski, "Remarks on Lu and Lee's Proposals," Cryptologia, v. 4, n. 4, 1980, pp. 204-207.

874. M.J. Kochanski, "Developing an RSA Chip," Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 350-357.

875. J.T. Kohl, "The Use of Encryption in Kerberos for Network Authentication," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp.35-43.

876. J.T. Kohl, "The Evolution of the Kerberos Authentication Service," European Conference Proceedings, May 1991, pp. 295-313.

877. J.T. Kohl and B.C. Neuman, "The Kerberos   Network Authentication Service, " RFC 1510, Sep 1993.

878. J.T. Kohl, B.C. Neuman, and T. Ts'o, "The   Evolution of the Kerberos Authentication System," Distributed Open Systems, IEEE Computer Society Press, 1994, pp. 78-94.

879. Kohnfelder, "Toward a Practical Public Key Cryptosystem, " Bachelor's thesis,   MIT Department of Electrical Engineering,   May 1978.

880. A. G. Konheim, Cryptography: A Primer,   New York: John Wiley & Sons, 1981.

881. A.G. Konheim, M.H. Mack, R.K. McNeill,   B. Tuckerman, and G. Waldbaum, "The   IPS Cryptographic Programs," IBM Systems journal, v. 19, n. 2, 1980, pp.   253-283.

882. V.I. Korzhik and A.I. Turkin, "Cryptanalysis of McEliece's Public-Key Cryptosystem," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag,   1991, pp. 68-70.

883. S.C. Kothari, "Generalized Linear Threshold Scheme," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 231-241.

884. J. Kowalchuk, B.R Schanning, and S. Powers, "Communication Privacy: Integration   of Public and Secret Key Cryptography,"   Proceedings of the National Telecommunication Conference, IEEE Press, 1980, pp.   49.1.1 49.1.5.

885. K. Koyama, "A Master Key for the RSA Public-Key Cryptosystem," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J65-D, n. 2, Feb 1982, pp. 163-170.

886. K. Koyama, "A Cryptosystem Using the Master Key for Multi-Address Communications," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J65-D, n. 9, Sep 1982, pp. 1151-1158.

887. K. Koyama, "Demonstrating Membership of a Group Using the Shizuya-Koyama-Itoh (SKI) Protocol," Proceedings of the 1989 Symposium on Cryptography and Information Security (SCIS 89), Gotenba, Japan, 1989.

888. K. Koyama, "Direct Demonstration of the Power to Break Public-Key Cryptosystems, " Advances in Cryptology AUSCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 14-21.

889. K. Koyama, "Security and Unique Decipherability of Two-dimensional Public Key Cryptosystems," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E73, n. 7, Jul 1990, pp. 1057-1067.

890. K. Koyama, U.M. Maurer, T. Okamoto, and S.A. Vanstone, "New Public-Key Schemes Based on Elliptic Curves over the Ring Zn" Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 252-266.

891. K. Koyama and K. Ohta, "Identity-based Conference Key Distribution System," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp.175-184.

892. K. Koyama and T. Okamoto, "Elliptic Curve Cryptosystems and Their Applications, " IEICE Transactions on Information and Systems, v. E75-D, n. 1, Jan 1992, pp. 50-57.

893. K. Koyama and R. Terada, " How to Strengthen DES-Like Cryptosystems against Differential Cryptanalysis," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E76-A, n. 1, Jan 1993, pp. 63-69.

894. K. Koyama and R. Terada, "Probabilistic Swapping Schemes to Strengthen DES against Differential Cryptanalysis, " Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93), Shuzenji, Japan, 28-30 Jan 1993, pp. 15D.1-12.

895. K. Koyama and Y. Tsuruoka, "Speeding up Elliptic Cryptosystems Using a Singled Binary Window Method, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 345-357.

896. E. Kranakis, Pnmality and Cryptography, Wiler-Teubner Series in Computer Science, 1986.

897. D. Kravitz, "Digital Signature Algorithm," U.S. Patent #5,231,668, 27 Jul 1993.

898. D. Kravitz and L. Reed, "Extension of RSA Cryptostructure: A Galois Approach, " Electronics Letters, v. 18, n. 6, 18 Mar 1982, pp. 255-256.

899. H. Krawczyk, "How to Predict Congruential Generators," Advances in Cryptology CRYPTO'89 Proceedings, Springer- Verlag, 1990, pp. 138-153.

900. H. Krawczyk, "How to Predict Congruential Generators," Journal of Algorithms, v. 13, n. 4, Dec 1992, pp. 527-545.

901. H. Krawczyk, "The Shrinking Generator: Some Practical Considerations," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 45 46.

902. G.J. Kuhn, "Algorithms for Self-Synchronizing Ciphers," Proceedings of COMSIG 88, 1988.

903. G.J. Kuhn, F. Bruwer, and W. Smit, "'n Vinnige Veeldoelige Enkripsievlokkie, " Proceedings of Infosec 90, 1990. (In Afrikaans.)

904. S. Kullback, Statistical Methods in Cryptanalysis, U.S. Government Printing Office, 1935. Reprinted by Aegean Park Press, 1976.

905. RV. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized Bent Functions and their Properties," Journal of Combinational Theory, Series A, v. 40, n. 1, Sep 1985, pp. 90-107.

906. M. Kurosaki, T. Matsumoto, and H. Imai, "Simple Methods for Multipurpose Certification," Proceedings of the 1989 Symposium on Cryptography and Information Security (SCIS 89), Gotenba, Japan, 1989.

907. M. Kurosaki, T. Matsumoto, and H. Imai, "Proving that You Belong to at Least One of the Specified Groups," Proceedings of the 1990 Symposium on Cryptography and Information Security (SCIS 90), Hihondaira, Japan, 1990.

908. K. Kurosawa, "Key Changeable ID-Based Cryptosystem," Electronics Letters, v. 25, n. 9, 27 Apr 1989, pp. 577-578.

909. K. Kurosawa, T. Ito, and M. Takeuchi, "Public Key Cryptosystem Using a Reciprocal Number with the Same Intractability as Factoring a Large Number," Cryptologia, v. 12, n. 4, Oct 1988, pp. 225-233.

910. K. Kurosawa, C. Park, and K. Sakano, "Group Signer/Verifier Separation Scheme," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, 134-143.

911. G.C. Kurtz, D. Shanks, and H.C. Williams, "Fast Primality Tests for Numbers Less than 50*10" Mathematics of Computation, v. 46, n. 174, Apr 1986, pp. 691-701.

912. K. Kusuda and T. Matsumoto, "Optimization of the Time-Memory Trade-Off Cryptanalysis and Its Application to Block Ciphers, " Proceedings of the 1995 Symposium on

Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. A3.2.1-11. (In Japanese.)

913. H. Kuwakado and K. Koyama, "Security of RSA-Type Cryptosystems Over Elliptic Curves against Hastad Attack," Electronics Letters, v. 30, n. 22, 27 Oct 1994, pp. 1843-1844.

914. H. Kuwakado and K. Koyama, "A Ncw RSA-Type Cryptosystem over Singular Elliptic Curves, " IMA Conference on Applications of Finite Fields, Oxford University Press, to appear.

915. H. Kuwakado and K. Koyama, "A New RSA-Type Scheme Based on Singular Cubic Curves," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 144-151.

916. M. Kwan, "An Eight Bit Weakness in the LOKI Cryptosystem, " technical report, Australian Dcfensc Force Academy, Apr 1991.

917. M. Kwan and J. Pieprzyk, "A General Purpose Technique for Locating Key Scheduling Weakness in DES-Like Cryptosystcms, " Advances in Cryptology ASIACRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 237-246.

918. J.B. Lacy, D.P. Mitchell, and W.M. Schell, "CryptoLib: Cryptography in Software," UNIX Security Symposium Proceedings, USENIX Association, 1993, pp. 1-17.

919. J.C. Lagarias, "Knapsack Public Key Cryptosystems and Diophantine Approximations," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 3-23.

920. J.C. Lagarias, "Performance Analysis of Shamir's Attack on the Basic Merkle-Hellman Knapsack Cryptosystem, " Lec- ture Notes in Computer Science 172; Proceedings of the 11 th International Colloquium on Automata, Languages, and Programming (ICALP), Springer- Verlag, 1984, pp. 312-323.

921. J.C. Lagarias and A.M. Odlyzko, "Solving Low-Density Subset Sum Problems," Proceedings of the 24th IEEE Symposium on Foundations of Computer Science, I983, pp. 1-10.

922. J.C. Lagarias and A.M. Odlyzko, "Solving Low-Density Subset Sum Problems," Journal of the ACM, v. 32, n. 1, Jan 1985, pp. 229-246.

923. J.C. Lagarias and J. Reeds, "Unique Extraporation of Polynomial Recurrences, " SIAM Journal on Computing, v. 17, n. 2, Apr 1988, pp. 342-362.

924. X. Lai, Detailed Description and a Software Implementation of the IPES Cipher, unpublished manuscript, 8 Nov 1991.

925. X. Lai, On the Design and Secunty of Block Ciphers, ETH Series in Information Processing, v. 1, Konstanz: Hartung-Gorre Verlag, 1992.

926. X. Lai, personal communication, 1993.

927. X. Lai, "Higher Order Derivatives and Differential Cryptanalysis," Communications and Cryptography: Two Sides of One Tapestry, R.E. Blahut et al., eds., Kluwer Adademic Publishers, 1994, pp. 227-233.

928. X. Lai and L. Knudsen, "Attacks on Double Block Length Hash Functions," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 157-165.

929. X. Lai and J. Massey, "A Proposal for a New Block Encryption Standard, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 389 404.

930. X. Lai and J. Massey, "Hash Functions Based on Block Ciphers, " Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag, 1992, pp. 55-70.

931. X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 17-38.

932. X. Lai, R.A. Rueppel, and J. Woollven, "A Fast Cryptographic Checksum Algorithm Based on Stream Ciphers," Advances in Cryptology AUSCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 339-348.

933. C.S. Laih, J.Y. Lee, C.H. Chen, and L. Harn, "A New Scheme for ID-based Cryptosys tems .md Signatures," Tournal of the Chinese Institute of Engineers, v. 15, n. 2, Sep 1992, pp. 605-610.

934. B.A. LaMacchia and A.M. Odlyzko, "Computation of Discrete Logarithms in Prime Fields, " Designs, Codes, and Cryptography, v. 1, 1991, pp. 46-62.

935. L. Lamport, "Password Identification with Insecure Communications," Communications of the ACM, v. 24, n. 11, Nov 1981, pp. 770-772.

936. S. Landau, "Zero-Knowledge and the Department of Defense," Notices of the American Mathematical Society, v. 35, n. 1, Jan 1988, pp. 5-12.

937. S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Mikker, P. Neumann, and D. Sobel, "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy," Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM), Association for Computing Machinery, Jun 1994.

938. S.K. Langford and M.E. Hellman, "Cryptanalysis of DES," presented at 1994 RSA Data Security conference, Redwood Shores, CA, 12-14 Jan 1994.

939. D. Lapidot and A. Shamir, "Publicly Verifiable Non-Interactive Zero-Knowledge Proofs, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 353-365.

940. A.V. Le. S.M. Matyas, D.B. Johnson, and J.D. Wilkins, "A Public-Key Extension to the Common Cryptographic Architecture, " IBM Systems Journal, v. 32, n. 3, 1993, pp. 461-485.

941. P. L'Ecuyer, "Efficient and Portable Combined Random Number Generators, " Communications of the ACM, v. 31, n. 6, Jun 1988, pp. 742-749, 774.

942. R L'Ecuyer, "Random Numbers for Simulation," Communications of the ACM, v. 33, n. 10, Oct 1990, pp. 85-97.

943. P.J. Lee and E.E Brickcll, "An Observation on the Security of McEliece's Public-Key Cryptosystem," Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 275-280.

944. S. Lee, S. Sung, and K. Kim, "An Efficient Method to Find the Linear Expressions for Linear Cryptanalysis," Proceedings of the 1995 Korea-Japan Workshop on Information Security and Cryptography, Inuyama, Japan, 24-26 Jan 1995, pp. 183-190.

945. D.J. Lehmann, "On Primality Tests, " SIAM lournal on Computing, v. 11, n. 2, May 1982, pp. 374-375.

946. T. Leighton, "Failsafe Key Escrow Systems, " Technical Memo 483, MIT Laboratory for Computer Science, Aug 1994.

947. A. Lcmpel and M. Cohn, "Maximal Families of Bent Sequences," IEEE Transactions on Information 'Fheory, v. IT-28, n. 6, Nov 963. 1982, pp. 865-868.

948. A. K. Lenstra. " Factoring Multivariate Polynomials Over Finite Fields," Journal of Computer System Science, v. 30, n. 2, 964. Apr 1985, pp. 235-248.

949. A.K. Lenstra, personal communication, 1995.

950. A.K. Lenstra and S. Haber, letter to NIST Regarding DSS, 26 Nov 1991.

951, A.K. Lcnstra, H.W. Lenstra Jr., and L.Lovacz, "Factoring Polynomials with Rational Coefficients," Mathematische Annalen, v. 261, n. 4, 1982, pp. 515-534.

952. A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, and J.M. Pollard, "The Number Field Sieve," Proceedings of the 22nd ACM Symposium on the Theory of Computing, 1990, pp. 574-672.

953. A.K. Lenstra and H.W. Lenstra, Jr., eds., Lecture Notes in Mathematics 1554: The 967. Development of the Number Field Sieve, Springer-Verlag, 1993.

954. A.K. Lenstra, H.W. Lcnstra, Jr., M.S. Manasse, and J.M. Pollard' "The Factorization of the Ninth Fermat Number," Mathematics of Computation. v. 61, n. 203, 1993, pp. 319-349.

955. A.K. Lenstra and M.S. Manasse, "Factoring by Electronic Mail," Advances in Cryptology EUROCRYPT '89 Proceedings,   Springcr-Verlag, 1990, pp. 355-371.

956. A.K. Lenstra and M.S. Manasse, "Factoring with Two Large Primes," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 72-82.

957. H.W. Lenstra Jr. "Elliptic Curves and Number-Theoretic Algorithms, " Report   86-19, Mathematisch Instituut, Universiteit van Amsterdam, 1986.

958. H.W. Lenstra Jr. "On the Chor-Rivest Knapsack Cryptosystem, " Journal of Cryptology, v. 3, n. 3, 1991, pp. 149-155.

959. W.J. LeVequc, Fundamentals of Number Theory, Addison-Wesley. 1977.

960. L.A. Levin, "One-Way Functions and   Pseudo-Randolll Generators." Proceedings of the 17th ACM Symposium on Theory of Computing, 1985, pp. 363-365.

961. Lexar Corporation, "An Evaluation of thc DES," Scp 1976.

962. D.-X. Li, "Cryptanalysts of Public-Kcy Distribution Systcms Based on Dickson Polynomials," Electronics Letters, v. 27, n. 3,   1991, pp. 228-229.

963. F. -X. Li, "How to Break Okamoto's Cryptosystems by Continued Fraction Algorithm," ASIACRYPT '91 Abstracts, 1991,   pp. 285-289.

964. Y.X. Li and X.M. Wang, "A Coins Authcntication and Encryption Schemc Bascd on Algebraic Coding Theory," Applied Algebra, Algebraic Algonthms and Error Correcting Codes 9, Springer-Vcrlag, 1991, pp.   241-245.

965. R. Lidl, G.L. Mullen, and G. Turwald, Pitman Monographs and Surveys in Pure and Applied Mathematics 65: Dickson Polynomials, London: Longman Scicntific and Technical, 1993.

966. R. Lidl and W.B. Muller, "Permutation   Polynomials in RSA-Cryptosystems, "   Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp.   293-301.

967. R. Lidl and W.B. Mullcr, "Generalizations of the Fibonacci Pseudoprimes Test," Discrete Mathematics, v. 92, 1991, pp.   211-220.

968. R. Lidl and W.B. Muller, "Primality Testing with Lucas Functions," Advances in Cryptology A USCRYPT '92 Proceedings,   Springer-Verlag, 1993, pp. 539-542.

969. R. Lidl, W.B. Muller, and A. Oswald,   "Some Remarks on Strong Fibonacci Pscudoprimes," Applicable Algebra in Engineering, Communication and Computing,   v. 1, n. 1, 1990, pp. 59 65.

970. R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of Mathematics and its Application.s, v. 20, Addison-Wesley, 1983.

971. R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications. London: Cambridge Univcrsity Press, 1986.

972. K. Lieberherr, "Unifonn Complexity and Digital Signaturcs," Theoretical Computer Science, v. 16, n. 1, Oct 1981, pp. Y9-] 10.

973. C.H. Lim and RJ. Lee, "A Practical Electronic Cash System for Smart Cards," Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography Seoul, Korea, 24-26 Oct 1993, pp. 34-47.

974. C.H. Lim and P.J. Lee, "Security of interactive RSA Batch Verification," Electronics Letters, v. 30, n. 19, 15 Sep 1994, pp. 1592-1593.

975. H.-Y. Lin and L. Harn, "A Generalized Secret Sharing Scheme with Cheater Detection," Advances in Cryptology ASIACRYPT '91 Proceedings, Springer-Verlag, 1993, pp. 149-158.

976. M.-C. Lin, T.-C. Chang, and H.-L. Fu, "Information Rate of McEliece's Public key Cryptosystem," Electronics Letters, v. 990. 26, n. 1, 4 Jan 1990, pp. 16-18.

977. J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I Message Encipherment and Authentication Procedures, " RFC 989, Feb 1987.

978. J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I Message Encipherment and Authentication Procedures, " RFC 1040, Jan 1988.

979. J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I Message Encipher ment and Authentication Procedures, " RFC 1113, Aug 1989.

980. J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part III Algorithms, Modes, and Identifiers," RFC 1115, Aug 1989.

981. J. Linn, " Privacy Enhancement for Internet Electronic Mail: Part I Message Encipherment and Authentication Procedures, " RFC 1421, Feb 1993.

982. S. Lloyd, "Counting Binary Functions with Certain Cryptographic Properties, " Journal of Cryptology, v. 5, n. 2, 1992, pp. 107-131.

983. T.M.A. Lomas, "Collision-Freedom, Considered Harmful, or How to Boot a Computer," Proceedings of the 1995 Korea-Japan Workshop on Information Security and Cryptography, Inuyama, Japan, 24-26 Jan 1995, pp. 35-42.

984. T.M.A. Lomas and M. Roe, "Forging a Clipper Message, " Communications of the ACM, v. 37, n. 12, 1994, p. 12.

985. D.L. Long, "The Security of Bits in the Discrete Logarithm, " Ph.D. dissertation, Princeton University, Jan 1984.

986. D.L. Long and A. Wigderson, "How Discrete Is the Discrete Log," Proceedings of the 15th Annual ACM Syposium on the Theory of Computing, Apr 1983.

987. D. Longlcy and S. Rigby, "An Automatic Search for Security Flaws in Key Management Schemes," Computers and Security v. 11, n. 1, Jan 1992. pp. 75-89.

988. S.H. Low, N.F. Maxemchuk, and S. Paul, "Anonymous Credit Cards," Proceedings of the 2nd Annual ACM Conference on Computer and Communications Security, ACM Press, 1994, pp. 108-117.

989. J.H. Loxton, D.S.P Khoo, G.J. Bird, and J. Seberry, "A Cubic RSA Code Equivalent to Factorization," Journal of Cryptology, v. 5, n. 2, 1992, pp. 139-150.

990. S.C. Lu and L.N. Lee, "A Simple and Effective Public-Key Cryptosystem," COMSAT Technical Review, 1979, pp. 15-24.

991. M. Luby, S. Micali and C. Rackoff, "How to Simultaneously Exchange a Secret Bit by Flipping a Symmetrically-Biased Coin, " Proceedings of the 24nd Annual Symposium on the Foundations of Computer Science, 1983, pp. 11-22.

992. M. Luby and C. Rackoff, "How to Construct Pseudo-Random Permutations from Pseudorandom Functions," SIAM lournal on Computing, Apr 1988, pp. 373-386.

993. F. Luccio and S. Mazzone, "A Cryptosystem for Multiple Communications, " Information Processing Letters, v. 10, 1980, pp. 180-183.

994. V Luchangco and K. Koyama, "An Attack on an ID-Based Key Sharing System, Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24-26 Oct 1993, pp. 262-271.

995. D.J.C. MacKay, "A Free Energy Minimization Framework for Inferring the State of a Shift Register Given the Noisy Output Sequence, " K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

996. M.D. MacLaren and G. Marsaglia, "Uniform Random Number Generators," Journal of the ACM v. 12, n. 1, Jan 1965, pp. 83-89.

997. D. MacMillan, "Single Chip Encrypts Data at 14Mb/s," Electronics, v. 54, n. 12, 16 June 1981, pp. 161-165.

998. R. Madhavan and L.E. Peppard, "A Multiprocessor GaAs RSA Cryptosystem," Proceedings CCVLSI-89: Canadian Conference on Very Large Scale Integration, Vancouver, BC, Canada, 22-24 Oct 1989, pp. 115-122.

999. W.E. Madryga, "A High Performance   Encryption Algorithm," Computer Security: A Global   Challenge, Elsevier Science   Publishers, 1984, pp. 557-570.

1000. M. Mambo, A. Nishikawa, S. Tsujii, and E.   Okamoto, "Efficient Secure Broadcast Communication System," Proceedings of the 1993 Korea-Japan Workshop on Information   Security and Cryptography, Seoul,   Korea, 24-26 Oct 1993, pp. 23-33.

1001. M. Mambo, K. Usuda, and E. Okamoto,   "Proxy Signatures," Proceedings of the   1995   Sympusium on Cryptography and   Information Secunty (SCIS 95), Inuyama,   Japan, 24-27   Jan 1995, pp. B1.1.1-17.

1002. W. Mao and C. Boyd, "Towards Formal   Analysis of Security Protocols," Proceedings of   the Computer Security Foundations Workshop Vl, IEEE Computer Society Press, 1993, pp.   147-158.

1003. G. Marsaglia and T.A. Bray, "On-Line Random Number Generators and their Use in   Combinations, " Communications of the   ACM, v. 11, n. 11, Nov 1968, p. 757-759.

1004. K.M. Martin, "Untrustworthy Participants in Perfect Secret Sharing Schemes,"   Cryptography and Coding 111, M.J. Ganley, ed.,   Oxford: Clarendon Press, 1993, pp.   255-264.

1005. J.L. Massey, "Shift-Register Synthesis and   BCH Decoding," IEEE Transactions on   Information Theory, v. IT-15, n. 1, Jan   1969, pp. 122-127.

1006. J.L. Massey, "Cryptography and System   Theory," Proceedings of the 24th Allerton   Conference on Communication, Control,   and Computers, 1-3 Oct 1986, pp. 1-8.

1007. J.L. Massey, "An Introduction to Contemporary Cryptology, " Proceedings of the   IEEE,   v. 76, n. 5., May 1988, pp. 533-549.

1008. J.L. Massey, "Contemporary Cryptology: An Introduction," in Contemporary Cryptology: The Science of Information   Integrity, G.J. Simmons, ed., IEEE Press,   1992, pp. 1-39.

1009. J.L. Massey, "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm,"   Fast Software   Encryption, Cambridge   Security Workshop Proceedings, Springer-Verlag, 1994, pp. 1-17.

1010. J.L. Massey, "SAFER K-64: One Year Later," K. U. Leuven Workshop on Crypto-   graphic Algorithms, Springer-Verlag, 1995, to appear.

1011. J.L. Massey and I. Ingemarsson, "The Rip Van Winkle Cipher A Simple and Provably   Computationally Secure Cipher with   a Finite Key," IEEE International Symposium on   Information Theory, Brighton,   UK, May 1985.

1012. J.L. Massey and X. Lai, "Device for Converting a Digital Block and the Use Thereof, "   International Patent PCT/ CH91/00117, 28 Nov 1991.

1013. J.L. Massey and X. Lai, "Device for the Conversion of a Digital Block and Usc of Same," U.S. Patent #5,214,703, 25 May 1993.

1014. J.L. Massey and R.A. Rueppel, "Linear Ciphers and Random Sequence Generators with Multiple Clocks, " Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 74-87.

1015. M. Matsui, "Linear Cryptanalysis Method for DES Cipher, " Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 386-397.

1016. M. Matsui, "Linear Cryptanalysis of DES Cipher," Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93), Shuzenji, Japan, 28-30 Jan 1993, pp. 3C.1-14. (In Japanese.)

1017. M. Matsui, "Linear Cryptanalysis Method for DES Cipher " Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp. 4A.1-11. (In Japanese.)

1018. M. Matsui, "On Correlation Between the Order of the S-Boxes and the Strength of DES," Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

1019. M. Matsui, "The First Experimental Cryptanalysis of thc Data Encryption Standard," Advances in Cryptology CRYPTO ' 94 Proceedings , Springer -Verlag, 1994, pp. 1-11.

1020. M. Matsui and A. Yamagishi, "A New Method for Known Plaintext Attack of FEAL Cipher," Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 81 -91.

1021. T. Matsumoto and H. Imai, "A Class of Asymmetric Crypto-Systems Based on Polynomials Over Finite Rings, " IEEE International Symposium on Information Theory, 1983, pp. 131-132.

1022. T. Matsumoto and H. Imai, "On the Key Production System: A Practical Solution to the Key Distribution Problem," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 185-193.

1023. T. Matsumoto and H. Imai, "On the Security of Some Key Sharing Schemes (Part 2)," IEICE Japan, Technical Report, ISEC90-28, 1990.

1024. S.M. Matyas, "Digital Signatures. An Overview, " Computer Networks, v. 3, n.2, Apr 1979, pp. 87-94.

1025. S.M. Matyas, "Key Handling with Control Vectors," IBM Systems journal, v. 30, n. 2, 1991, pp. 151-174.

1026. S.M. Matyas, A.V. Le. and D.G. Abraham, "A Key Management Scheme Based on Control Vectors," IBM Systems journal, v.30, n. 2, 1991, pp. 175-191.

1027. S.M. Matyas and C.H. Meyer, "Generation, Distribution, and Installation of Cryptographic Keys," IBM Systems Journal, v. 17, n. 2, 1978, pp. 126-137.

1028. S.M. Matyas, C.H. Meyer, and J. Oseas, "Generating Strong One-Way Functions with Cryptographic Algorithm, " IBM Technical Disclosure Bulletin, v. 27, n. 10A, Mar 1985, pp. 5658-5659.

1029. U.M. Maurer, "Provable Security in Cryptography," Ph.D. dissertation, ETH No. 9260, Swiss Federal Institute of Technology, Zurich, 1990.

1030. U.M. Maurer, "A Provable-Secure Strongly-Randomized Cipher," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 361-373.

1031. U.M. Maurer, "A Universal Statistical Test for Random Bit Generators, " Advances in Cryptology CRYPTO '90, Proceedings, Springer-Verlag, 1991, pp. 409-420.

1032. U.M. Maurer, "A Universal Statistical Test for Random Bit Generators," Journal of Cryptology, v. 5, n. 2, 1992, pp. 89-106.

1033. U.M. Maurer and J.L. Massey, "Cascade Ciphers: The Importance of Being First," Journal of Cryptology, v. 6, n. 1, 1993, pp. 55-61.

1034. U.M. Maurer and J.L. Massey, "Perfect Local Randomness in Pseudo-Random Sequences, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 110-112.

1035. U.M. Maurer and Y. Yacobi, "Non interactive Public Key Cryptography, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 498-507.

1036. G. Mayhew, "A Low Cost, High Speed Encryption System and Method," Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, 1994, pp. 147-154.

1037. G. Mayhew, R. Frazee, and M. Bianco, "The Kinetic Protection Device, " Proceedings of the 15th National Computer Security Conference, NIST, 1994, pp. 147-154.

1038. K.S. McCurley, "A Key Distribution System Equivalent to Factoring," Journal of Cryptology, v. 1, n. 2, 1988, pp. 95-106.

1039. K.S. McCurley, "The Discrete Logarithm Problem," Cryptography and Computational Number Theory (Proceedings of the Symposium on Applied Mathematics), American Mathematics Society, 1990, pp. 49-74.

1040. K.S. McCurley, open letter from the Sandia National Laboratories on the DSA of the NIST, 7 Nov 1991.

1041. R.J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," Deep Space Network Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, 1978, pp. 114-116.

1042. R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Boston: Kluwer Academic Publishers, 1987.

1043. P. McMahon, "SESAME V2 Public Key and Authorization Extensions to Kerberos, " Proceedings of the Internet Society 1Y95 Symposium on Network and Distributed Systems Security, IEEE Computer Society Press, 1995, pp. 114-131.

1044. C.A. Meadows, "A System for the Specification and Analysis of Key Management Protocols," Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991, pp. 182-195.

1045. C.A. Meadows, "Applying Formal Methods to the Analysis of a Key Management Protocol," Journal of Computer Security. v. I, n. 1, 1992,pp.5-35.

1046. C.A. Meadows, "A Model of Computation for the NRL Protocol Analyzer, " Proceedings of the Computer Security Foundations Workshop VII, IEEE Computer Society Press, 1994, pp. 84-89.

1047. C.A. Meadows, "Formal Verification of Cryptographic Protocols: A Survey," Advances in Cryptology ASIACRYPT '94 Proceedings, Springer-Verlag, 1995, pp. 133-150.

1048. G. Medvinsky and B.C. Neuman, "Net Cash: A Design for Practical Electronic Currency on the Internet," Proceedings of the 1st Annual ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 102-106.

1049. G. Medvinsky and B.C. Neuman, "Electronic Currency for the Internet," Electronic Markets, v 3, n. 9/10, Oct 1993, pp. 23-24.

1050. W. Meier, "On the Security of the IDEA Block Cipher," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer -Verlag, 1994, pp. 371-385.

1051. W. Meier and O. Staffelbach, "Fast Correlation Attacks on Stream Ciphers," Journal of Cryptology v I n. 3, 1989, pp. 159-176.

1052. W. Meier and O. Staffelbach, "Analysis of Pseudo Random Sequences Generated by Cellular Automata, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 186-199.

1053. W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 204-213.

1054. W. Meier and O. Staffelbach, "Correlation Properties of Combiners with Memory in Stream Ciphers, " Journal of Cryptology, v. 5, n. 1, 1992, pp. 67-86.

1055. W. Meier and O. Staffelbach, "The Self-Shrinking Generator," Communications and Cryptography: Two Sides of One Tapestry R.E. Blahut et al., eds., Kluwer Adademic Publishers, 1994, pp. 287-295.

1056. J. Meijers, "Algebraic-Coded Cryptosystems," Master's thesis, Technical University Eindhoven, 1990.

1057. J. Meijers and J. van Tilburg, "On the Rao-Nam Private-Key Cryptosystem Using Linear Codes," International Symposium on Information Theory, Budapest, Hun gary, 1991.

1058. J. Meijers and J. van Tilburg, "An Improved 5T-Attack on the Rao-Nam Private-Key Cryptosystem," International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, NV, 1991.

1059. A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

1060. A. Menezes, ed., Applications of Finite Fields, Kluwer Academic Publishers, 1993.

1061. A. Menezes and S.A. Vanstone, "Elliptic Curve Cryptosystems and Their Implementations," Journal of Cryptology, v. 6, n. 4, 1993, pp. 209-224.

1062. A. Menezes and S.A. Vanstone, "The Implementation of Elliptic Curve Cryptosystems, " Advances in Cryptology AUSCRYPT '90 Proceedings, Springer-Verlag, 1990, pp. 2-13.

1063. R. Menicocci, "Short Gollmann Cascade Generators May Be Insecure," Codes and Ciphers, Institute of Mathematics and its Applications, 1995, pp. 281-297.

1064. R.C. Merkle, "Secure Communication Over Insecure Channels," Communications of the ACM, v. 21, n. 4, 1978, pp. 294-299.

1065. R.C. Merkle, "Secrecy, Authentication, and Public Key Systems," Ph.D. dissertation, Stanford University, 1979.

1066. R.C. Merkle, "Method of Providing Digital Signatures," U.S. Patent #4,309,569, 5 Jan 1982

1067. R.C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 369-378.

1068. R.C. Merkle, "A Certified Digital Signature," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 218-238.

1069. R.C. Merkle, "One Way Hash Functions and DES, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 428 446.

1070. R.C. Merkle, "A Fast Software One-Way Hash Function," Journal of Cryptology, v. 3, n. 1, 1990, pp. 43-58.

1071. R.C. Merkle, "Fast Software Encryption Functions, " Advances in Cryptology CRYPTO '90, Proceedings, Springer-Verlag, 1991, pp. 476-501.

1072. R.C. Merkle, "Method and Apparatus for Data Encryption," U.S. Patent #5,003,597, 26 Mar 1991.

1073. R.C. Merkle, personal communication, 1993.

1074. R.C. Merkle and M. Hellman, "Hiding information and Signatures in Trapdoor Knapsacks," IEEE Transactions on Information Theory, v. 24, n. 5, Sep 1978, pp. 525-530.

1075. R.C. Merkle and M. Hellman, "On the Security of Multiple Encryption," Communications of the ACM, v. 24, n. 7, 1981, pp. 465-467.

1076. M. Merritt, "Cryptographic Protocols," Ph.D. dissertation, Georgia Institute of Technology, GIT-ICS-83/6, Feb 1983.

1077. M. Merritt, "Towards a Theory of Cryptographic Systems: A Critique of Crypto Complexity," Distributed Computing and Cryptography, J. Feigenbaum and M. Merritt, eds., American Mathematical Society, 1991, pp. 203-212.

1078. C.H. Meyer, "Ciphertext/Plaintext and Ciphertext/Key Dependencies vs. Number of Rounds for Data Encryption Standard," AFIPS Conference Proceedings, 47, 1978, pp. 1119-1126.

1079. C.H. Meyer, "Cryptography A State of the Art. Review, " Proceedings of CompEuro '89, VLSI and Computer Peripherals, 3rd Annual European Computer Conference, IEEE Press, 1989, pp. 150-154.

1080. C.H. Meyer and S.M. Matyas, Cryptography: A New Dimension in Computer Data Security, New York: John Wiley & Sons, 1982.

1081. C.H. Meyer and M. Schilling, "Secure Program Load with Manipulation Detection Code, " Proceedings of Securicom '88, 1988, pp. 111-130.

1082. C.H. Meyer and W.L. Tuchman, "Pseudo-Random Codes Can Be Cracked, " Electronic Design, v. 23, Nov 1972.

1083. C.H. Meyer and W.L. Tuchman, "Design Considerations for Cryptography, " Proceedings of the NCC, v. 42, Montvale, NJ: AFIPS Press, Nov 1979, pp. 594-597.

1084. S. Micali, "Fair Public-Key Cryptosystems, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag,   1993, pp. 113-138.

1085.   S. Micali, "Fair Cryptosystems," MIT/LCS/TR-579.b, MIT Laboratory for Computer Science, Nov 1993.

1086. S. Micali, "Fair Cryptosystems and Methods for Use," U.S. Patent #5,276,737, 4 Jan 1994.

1087. S. Micali, "Fair Cryptosystems and Methods for Use," U.S. Patent #5,315,658, 24   May 1994.

1088. S. Micali and A. Shamir, "An Improvemcnt on the Fiat-Shamir Identification and Signature Scheme," Advances in Cryptollgy CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 244-247.

1089. M.J. Mihajlevic, "A Correlation Attack   on the Binary Sequence Generators   with Time-Varying Output Function, "   Advances in Cryptology ASIACRYPT'94,   Proceedings, Springer-Verlag, 1995, pp.   67-79.

1090. M.J. Mihajlevic and J.D. Golic, "A Fast   Iterative Algorithm for a Shift Register   Internal State Reconstruction Given the Noisy Output Sequence, " Advances in   Cryptology AUSCRYPT '90 Proceedings,   Springer-Verlag, 1990, pp. 165-175.

1091. M.J. Mihajlevic and J.D. Golic, "Convergence of a Bayesian Iterative Error-Correction Procedure to a Noisy Shift Register Sequence," Advances in Cryptology,   EUROCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 124-137.

1092. J.K. Millen, S.C. Clark, and S.B. Freedman,   "The Interrogator: Protocol Security Analysis," IEEE Transactions on Software Engineering, v. SE-13, n.2, Feb 1987, pp.274-288.

1093. G.L. Miller, "Riemann's Hypothesis and   Tests for Primality," Journal of Computer Systems Science, v. 13, n. 3, Dec 1976, pp.   300-317.

1094. S.R Miller, B.C. Neuman, J.I. Schiller, and   J.H. Saltzer, "Section E.2.1: Kerberos Authentication and Authorization   System," MIT Project Athena, Dec 1987.

1095. V.S. Miller, "Use of Elliptic Curves in Cryptography, " Advances in Cryptology   CRYPTO '85 Proceedings, Springer-Verlag,   1986, pp. 417-426.

1096. M. Minsky, Computation: Finite and Infinite Machines, Englewood Cliffs, NJ: Prentice-Hall, 1967.

1097. C.J. Mitchell, "Authenticating Multi-Cast Internet Electronic Mail Messages Using a Bidirectional MAC Is Insecure, " draft manuscript, 1990.

1098. C.J. Mitchell, "Enumerating Boolean Functions of Cryptographic Significance," Journal of Cryptology, v. 2, n. 3, 1990, pp. 155-170.

1099. C.J. Mitchell, F. Piper, and P. Wild, "Digital Signatures, " Contemporary Cryptology: The Science of Information Integtity, G.J. Simmons, ed., IEEE Press, 1991, pp. 325-378.

1100. C.J. Mitchell, M. Walker, and D. Rush, "CCITT/ISO Standards for Secure Messagc Handling," IEEE Journal on Selected Areas in Communications, v. 7, n. 4, May 1989, pp. 517-524.

1101. S. Miyaguchi, "Fast Encryption Algorithm for the RSA Cryptographic System," Proceedings of Compcon 82, IEEE Press, pp. 1115. 672-678.

1102. S. Miyaguchi, "The FEAL-8 Cryptosystem and Call for Attack, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 624-627.

1103. S. Miyaguchi, "Expansion of the FEAL Cipher," NTT Review, v. 2, n. 6, Nov 1990.

1104. S. Miyaguchi, "The FEAL Cipher Family," Advances in Cryptology CKYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 627-638.

1105. S. Miyaguchi, K. Ohta, and M. Iwata, " 128- bit Hash Function IN-Hashl," Proceedings of SECURICOM '90, 1990, pp. 127-137.

1106. S. Miyaguchi, K. Ohta, and M. Iwata, " 128- bit Hash Function (N-Hash)," NTT Review, v. 2, n. 6, Nov 1990, pp. 128-132.

1107. S. Miyaguchi, K. Ohta, and M. Iwata, "Confirmation that Some Hash Functions Are Not Collision Free," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 326-343.

1108. S. Miyaguchi, A. Shiraishi, and A. Shimizu, "Fast Data Encipherment Algorithm FEAL-8," Review of tile Electrical Communication Laboratories, v. 36, n. 4, 1988.

1109. H. Miyano, "Differential Cryptanalysis on CALC and Its Evaluation," Proceedings of the 1992 Symposium on Cryptography and Information Security ISCIS 92, Tateshina, Japan, 2-4 Apt 1992, pp. 7B.1-8.

1110. R. Molva, G. Tsudik, E. van Hcrreweghen, and S. Zatti, "KryptoKnight Authentication and Key Distribution System," Proceedings of European Symposium on Research in completer Security, Toulouse, France, Nov 1992.

1111. P.L. Montgomery, "Modular Multiplication without Trial Division," Mathematics of computation, v. 44, n. 170, 1985, pp. 51Y-521.

1112. RL. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization," Mathematics of Computation, v.48, n. 177, Jan 19R7, pp. 243-264.

1113. P.L. Montgomery and R. Silverman, "An FFT Extension to the p-l Factoring Algorithm," Mathematics of Computation, v. 54, n. 190, 1990, pp. 839-854.

1114. J.H. Moore, "Protocol Failures in Cryptosystems," Proceedings of the IEEE, v. 76, n. 5, May 1988.

1115. J.H. Moore, "Protocol Failures in Cryptosystems," in Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, pp. 541-558.

1116. J.H. Moore and G.J. Simmons, "Cycle Structure of the DES with Weak and Semi-Weak Keys, " Advances in Cryptology CRYPTO '86 Proceedings, SpringerVerlag, 1987, pp. 3-32.

1117. T. Moriyasu, M. Moriai, and M. Kasahara, "Nonlinear Pseudorandom Number Generator with Dynamic Structure and Its Properties," Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Biwako, Japan, 27-29 Jan 1994, pp. 8A.l-ll.

1118. R. Morris, "The Data Encryption Standard Retrospective and Prospects," IEEE Communications Magazine, v. 16, n. 6, Nov 1978, pp. 11-14.

1119. R. Morris, remarks at the 1993 Cambridge Protocols Workshop, 1993.

1120. R. Morris, N.J.A. Sloane, and A.D. Wyner, "Assessment of the NBS Proposed Data Encryption Standard," Cryptologia, v. 1, n. 3, Jul 1977, pp. 281-291.

1121. R. Morris and K. Thompson, "Password Security: A Case History," Communications of the ACM, v. 22, n. 11, Nov 1979, pp. 594-597.

1122. S.B. Morris, "Escrow Encryption," lecture at MIT Laboratory for Computer Science, 2 Jun 1994.

1123. M.N. Morrison and J. Brillhart, "A Method of Factoring and the Factorization of F7," Mathematics of Computation, v. 29, n. 129, Jan 1975, pp. 183-205.

1124. L.E. Moser, "A Logic of Knowlcdgc and Belief for Reasoning About Computer Security, "Proceedings of the Computer Security Foundations Workshop 11, IEEE Computer Society Press, 1989, pp. S7 63.

1125. Motorola Government Electronics Division, Advanced Techniques in Network security' Scottsdale, AZ, 1977.

1126. W.B. Muller, "Polynomial Functions in   Modern Cryptology," contributions to   General Algebra 3: Proceedings of the Vienna Conference, Vienna: Verlag   Holder-Pichler-Tempsky' 1985, pp. 7-32.

1127. W.B. Muller and W. Nobauer, "Some   Remarks on Public-Key Cryptography, "   Studia Scientiarum Mathematicarum   Hungarica, v. 16, 1981, pp. 71-76.

1128. W.B. Muller and W. Nobauer, "Cryptanalysis of the Dickson Scheme," Advances in Cryptology EUROCRYPT '85 Proceedings, Springer-Verlag, 1986, pp. 50-61.

1129. C. Muller-Scholer, "A Microprocessor-Based Cryptoprocessor," IEEE Micro, Oct   1983, pp. 5-15.

1130. R.C. Mullin, E. Nemeth, and N. Weidenhofer, "Will Public Kcy Cryptosystems   Live Up to Their Expectations? HEP   Implementation of the Discrete Log Codebreaker," ICPP 85, pp. 193-196.

1131. Y. Murakami and S. Kasahara, "An ID-Based Key Distribution Scheme, " IEICE   Japan, Technical Report, ISEC90-26, 1990.

1132. S. Murphy, "The Cryptanalysis of FEAL-4   with 20 Chosen Plaintexts, " Journal of Cryptology, v. 2, n. 3, 1990, pp. 145-154.

1133. E.D. Mycrs, "STU-III Multilevel Secure Computer Interface," Proceedings of the   Tenth Annual Computer Security Applications Conference, IEEE Computer Society   Press, 1994, pp. 170-179.

1134. D. Naccache, "Can O.S.S. be Repaired?   Proposal for a New Practical Signature Scheme," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 233-239.

1135. D. Naccache, D. M'Raihi, D. Raphacli, and   S. Vaudenay, "Can D.S.A. be Improved: Complexity Trade-Offs with the Digital   Signature Standard, " Advances in Cryptology EUKOCRYPT '94 Proceedings,   Springer-Verlag, 1995, to appear.

1136. Y. Nakao, T. Kaneko, K. Koyama, and R.   Terada, "A Study on the Security of RDES-Cryptosystem against Linear Cryptanalysis," Proceedings of the 1995 Japan-Korea Workshop on Information Security and   Cryptography, Inuyama, Japan, 24-27 Jan   1995, pp. 163-172.

1137. M. Naor, "Bit Commitmcnt Using Pseudo-Randomness," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 128-136.

1138. M. Naor and M. Yung, "Universal One-Way Hash Functions and Their Cryptographic Application," Proceedings of the 21stAnnual ACM Symposium on the Theory of Computing, 1989, pp. 33 43.

1139. National Bureau of Standards, "Report of the Workshop on Estimation of Significant Advances in Computer Technology, " NBSIR 76-1189, National Bureau of Standards, U.S. Department of Commercc, 21-22 Sep 1976, Dec 1977.

1140. National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard, " National Bureau of Standards, U.S. Department of Commerce, Jan 1977.

1141. National Bureau of Standards, NBS FIPS PUB 46-1, "Data Encryption Standard," U.S. Department of Commerce, Jan 1988.

1142. National Bureau of Standards, NBS FIPS PUB 74, "Guidelines for Implementing and Using the NBS Data Encryption Standard, " U.S. Department of Commerce, Apr 1981.

1143. National Bureau of Standards, NBS FIPS PUB 81, "DES Modes of Operation," U.S. Department of Commerce, Dec 1980.

1144. National Bureau of Standards, NBS FIPS PUB 112, "Password Usage," U.S. Department of Commerce, May 1985.

1145. National Bureau of Standards, NBS FIPS PUB 113, "Computer Data Authentication," U.S. Department of Commerce, May 1985.

1146. National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria," NCSC-TG-005 Version 1, Jul 1987.

1147. National Computer Security Centcr, "Trusted Datahase Management System Interpretation of the Trusted Computer System Evaluation Criteria, " NCSC-TG-021 Version 1, Apr 1991.

1148. National Computer Security Center, "A Guide to Understanding Data Rememberance in Automated Information Systems," NCSC-TG-025 Version 2, Sep 1991.

1149. National Institute of Standards and Technology, NIST FIPS PUB XX, "Digital Signature Standard," U.S. Department of Commcrce, DRAFT, 19 Aug 1991.

1150. National Institute of Standards and Technology, NIST FIPS PUB 46-2, "Data Encryption Standard," U.S. Department of Commcrcc, Dec 93.

1151. National Institute of Standards and Technology, NIST FIPS PUB 171, "Key Management Using X9.17," U.S. Departmcnt of Commcrce, Apr 92.

1152. National Institute of Standards and Technology, NIST FIPS PUB 180, "Secure Hash Standard, " U.S. Department of Commerce, May 93.

1153. National Institute of Standards and Technology, NIST FIPS PUB 185, "Escrowed Encryption Standard," U.S. Department of Commerce, Feb 94.

1154. National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard, " U.S. Department of Commerce, May 1994.

1155. National Institute of Standards and Technology," Clipper Chip Technology," 30 Apr 1993.

1156. National Institute of Standards and Technology," Capstone Chip Technology," 30 Apr 1993.

1157. J. Nechvatal, "Public Key Cryptography, " NIST Special Publication 800-2, National Institute of Standards and Technology, U.S. Department of Commerce, Apr 1991.

1158. l. Nechvatal, "Public Key Cryptography," Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, pp. 177-288.

1159. R.M. Needham and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, v. 21, n. 12, Dec 1978, pp. 993-999.

1160. R.M. Ncedham and M.D. Schroeder, "Authentication Revisited," Operating Systems Review, v. 21, n. 1, 1987, p. 7.

1161. D.M. Nessett, "A Critique of the Burrows, Abadi, and Needham Logic," Operating System Review, v. 20, n. 2, Apr 1990, pp. 35-38.

1162. B.C. Ncuman and S. Stubblebine, "A Note on the Use of Timestamps as Nonces, " Operating Systems Review, v. 27, n. 2, Apr 1993, pp. 10-14.

1163. B.C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Communications Magazine, v. 32, n. 9, Sep 1994, pp. 33-38.

1164. L. Neuwirth, "Statement of Lee Nenwirth of Cylink on HR145," submitted to congressional committees considering HR145, Feb 1987.

1165. D.B. Newman, Jr. and R.L. Pickholtz, "Cryptography in the Private Sector," IEEE Communications Magazine, v. 24, n. 8, Aug 1986, pp.7-10.

1166. H. Niederreiter, "A Public-Key Cryptosystem Based on Shift Register Sequences," Advances in Cryptology EZJROCRYPT '85 Proceedings, Springer-Verlag, 1986, pp. 35-39.

1167. H. Niederreiter, "Knapsack-Type Cryptosystems and Algebraic Coding Theory," Problems of Control and Information Theory, v. 15, n. 2, 1986, pp. 159-166.

1168. H. Niederreiter, "The Linear Complexity Profile and the Jump Complexity of Keystream Sequences, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 174-188.

1169. V. Niemi, "A New Trapdoor in Knapsacks," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 405-411.

1170. V. Niemi and A. Renvall, "How to Prevent Buying of Voters in Computer Elections," Advances in Cryptology ASIACRYPT '94 Proceedings, Springer-Verlag, 1995, pp. 164-170.

1171. I. Niven and H.A. Zuckerman, An Introduction to the Theory of Numbers, New York: John Wiley & Sons, 1972.

1172. R. Nobauer, "Cryptanalysts of the Redei Scheme," Contributions to General Algebra 3: Proceedings of the Vienna Conference, Verlag Holder-Pichler-Tempsky, Vienna, 1985, pp. 255-264.

1173. R. Nobauer, "Cryptanalysts of a Public- Key Cryptosystem Based on Dickson-Polynomials," Mathematica Slovaca, v. 38, n. 4, 1988, pp. 309-323.

1174. K. Nogochi, H. Ashiya, Y. Sano, and T. Kaneko, "A Study on Differential Attack of MBAL Cryptosystem," Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS' 94), Lake Biwa, Japan, 27-29 Jan 1994, pp. 14B.1-7. (In Japanese.)

1175. H. Nurmi, A. Salomaa, and L. Santean, "Secret Ballot Elections in Computer Networks," Computers & Security, v. 10, 1991, pp. 553-560.

1176. K. Nyberg, "Construction of Bent Functions and Difference Sets," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 151-160.

1177. K. Nyberg, "Perfect Nonlinear S-Boxes," Advances in Cryptology EUROCRYPT '91 Proceedings. Springcr-Verlag, 1991, pp. 378-386.

1178. K. Nyberg, "On the Construction of Highly Nonlinear Permutations, " Advances in Cryptology EUROCRYPT '92 Proceedings, Springer-Verlag 1991, pp. 92-98.

1179. K. Nyberg, "Differentially Uniform Mappings for Cryptography," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 55-64.

1180. K. Nyberg, "Provable Security against Differential Cryptanalysis," presented at the rump session of Eurocrypt '94, May 1994.

1181. K. Nyberg and L.R. Knudsen, "Provable Security against Differential Cryptanalysis," Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 566-574.

1182. K. Nyberg and L.R. Knudsen, "Provable Security against Differential Cryptanalysis," Journal of Cryptology, v. 8, n. 1, 1995, pp. 27-37.

1183. K. Nyberg and R.A. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery," 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 58-61.

1184. K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Advances in Cryptology EUROCRYPT '94 Proceedings, Spnnger-Verlag, 1995, to appear.

1185. L. O'Connor, "Enumerating Nondegenerate Permutations," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 368-377.

1186. L. O'Connor, "On the Distribution of Characteristics in Bijective Mappings, " Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 360-370.

1187. L. O'Connor, "On the Distribution of Characteristics in Composite Permutations, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 403-412.

1188. L. O'Connor and A. Klapper, "Algebraic Nonlinearity and Its Application to Cryptography," Journal of Cryptology, v. 7, n.3, 1994, pp. 133-151.

1189. A. Odlyzko, "Discrete Logarithms in Finite Fields and Their Cryptographic Significance," Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 224-314.

1190. A. Odlyzko, "Progress in Integer Factorization and Discrete Logarithms, " unpublished manuscript, Feb 1995.

1191. Office of Technology Assessment, U.S. Congress, "Defending Secrets, Sharing Data: New Locks and Keys for Electronic Communication, " OTA-CIT-310, Washington, D.C.: U.S. Government Printing Office, Oct 1987.

1192. B. O'Higgins, W. Diffie, L. Strawczynski, and R. de Hoog, "Encryption and ISDN a Natural Fit," Proceedings of the 1987 International Switching Symposium. 1987, pp. 863-869.

1193. Y. Ohnishi, "A Study on Data Security," Master's thesis, Tohuku University, Japan, 1988. (In Japanese.)

1194. K. Ohta, "A Secure and Efficient Encrypted Broadcast Communication System Using a Public Master Key," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J70-D, n. 8, Aug 1987, pp. 1616-1624.

1195. K. Ohta, "An Electrical Voting Scheme Using a Single Administrator, " IEICE Spring National Convention, A-294, 1988, v. 1, p. 296. (In Japanese.)

1196. K. Ohta, "Identity-based Authentication Schemes Using the RSA Cryptosystem," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J72D-II, n. 8, Aug 1989, pp. 612-620.

1197. K. Ohta and M. Matsui, "Differential Attack on Message Authentication Codes," Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 200-223.

1198. K. Ohta and T. Okamoto, "Practical Extension of Fiat-Shamir Scheme," Electronics Letters, v. 24, n. 15, 1988, pp. 955-956.

1199. K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme," Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 232-243.

1200. K. Ohta and T. Okamoto, "A Digital Multisignature Scheme Bascd on the Fiat-Shamir Scheme, " Advances in Cryptology ASIA CRYPT '91 Rroceedillys, Springer-Verlag, 1993, pp. 139-148.

1201. K. Ohta, T. Okamoto and K. Koyama, "Membership Authentication for Hierarchy Multigroups Using thc Extended Fiat - Shamir Scheme, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 446-457.

1202. E. Okamoto and K. Tanaka, "Key Distribution Based on Identification Information, " IEEE journal on Selected Areas in Com- munication, v. 7, n. 4, May 1989, pp. 481-490.

1203. T. Okamoto, "Fast Public-Key Cryptosystems Using Congruent Polynomial Equations, " Electronics Letters, v. 22, n. 11, 1986, pp. 581-582.

1204. T. Okamoto, "Modification of a Public-Kcy Cryptosystem," Electronics Letters, v. 23, n. 16, 1987, pp. 814-81S.

1205. T. Okamoto, "A Fast Signature Scheme Based on Congruential Polynomial Operations," IEEE Transactions on Information Theory, v. 36, n. 1, 1990, pp. 47-53.

1206. T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes, " Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 31-53.

1207. T. Okamoto, A. Fujioka, and E. Fujisaki, "An Efficient Digital Signature Scheme Based on Elliptic Curve over the Ring Z/p" Advances in Cryptology CRYPTO '92 Proceeding.s, Springer-Verlag, 1993, pp. 54-65.

1208. T. Okamoto, S. Miyaguchi, A. Shiraishi, and T. Kawoaka, "Signed Document Transmission System," U.S. Patent #4,625,076, 25 Nov 1986.

1209. T. Okamoto and K. Ohta, ``Disposablc Zero-Knowlcdge Authentication and Their Applications to Untraceable Electronic Cash," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 134-149.

1210. T. Okamoto and K. Ohta, "How to Utilize the Randomness of zero-Knowlcdgc Proofs," Advances in Cryptology CRYPTO '90 Proceedings, Springcr-Verlag, 1991, pp. 456 475.

1211. T. Okamoto and K. Ohta, "Universal Electronic Cash," Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 324-337.

1212. T. Okamoto and K. Ohta, "Survey of Digital Signature Schemes, " Proceedings of the Third Symposium on State and Progress of Research in Cryptography, Fondazone Ugo Bordoni, Rome, 1993, pp. 17-29.

1213. T. Okamoto and K. Ohta, "Designated Confirmer Signatures Using Trapdoor Functions," Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp. 16B.l-ll.

1214. T. Okamoto and K. Sakurai, "Efficient Algorithms for the Construction of Hyper-elliptic Cryptosystems," Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 267 278.

1215. T. Okamoto and A.Shiraishi, "A Fast Signature Scheme Based on Quadratic Inequalities," Proceedings of the 1985 Symposium on Security and Privacy, IEEE, Apr 1985, pp. 123-132.

1216. J.D. Olsen, R.A. Scholtz, and L. Welch, "Bent Function Sequences," IEEE Transactions on Information Theory, v. IT-28, n. 6, Nov 1982, pp. 858-864.

1217. H. Ong and C.P Schnorr, "Signatures through Approximate Representations by Quadratic Forms," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984.

1218. H. Ong and C.R Schnorr, "Fast Signature Generation with a Fiat Shamir-Like Scheme," Advances in Cryptology EUKOCKYPT '9() Proceedings, Springer-Verlag, 1991, pp. 432-440.

1219. H. Ong, C.R Schnorr, and A. Shamir, "An Efficient Signature Scheme Based on Polynomial Equations, " Proceedings of the 16th Annual Symposium on the Theory of Computing, 1984, pp. 208 216.

1220. H. Ong, C.P. Schnorr, and A. Shamir, "Efficient Signature Schemes Based on Polynomial Equations," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 37-46.

1221. Open Shop Information Services, OSIS Security Aspects, OS1.S European Working Group, WGI, final report, Oct 1985.

1222. G.A. Orton, M.R Roy, PA. Scott, L.E. Peppard, and S.E. Tavares, "VLSI Implementation of Public-Key Encryption Algorithms, " Advances in Cryptology CRYPTO '86 Proceedings, Springcr-Verlag, 1987, pp. 277-301.

1223. H. Orup, E. Svendsen, and E. Anclreasen, "VICTOR An Efficient RSA Hardware Implementation," Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 245-252.

1224. D. Otway and O. Rees, "Efficient and Timely Mutual Authentication'" Operating Systems Review, v. 21, n. 1, 1987, pp. 8-10.

1225. G. Pagels-Fick, " Implementation Issues for Master Key Distribution and Protected Keyload Procedures, " Computers and Security: A Global Challenge, Proceedings of IFIP/SEC '83, North Holland: Elsevier Science Publishers, 1984, pp. 381-390.

1226. C.M. Papadimitriou, Computational Complexity, Addison-Wesley, 1994.

1227. C.S. Park, "Improving Code Rate of McEliece's Public-key Cryptosystem, " Electronics Letters, v. 25, n. 21, 12 Oct 1989, pp. 1466-1467.

1228. S. Park, Y. Kim, S. Lee, and K. Kim, "Attacks on Tanaka's Non-interactive Key Sharing Scheme," Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. B3.4.1-4.

1229. S.J. Park, K.H. Lee, and D.H. Won, "An Entrusted Undeniable Signature, " Proceedings of the 1995 Iapan-Korea Workshop on Information Secunty and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 120-126.

1230. S.J. Park, K.H. Lee, and D.H. Won, "A Practical Group Signature," Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 127-133.

1231. S.K. Park and K.W. Miller, "Random Number Generators: Good Ones Are Hard to Find," Communications of the ACM, v. 31, n. 10, Oct 1988, pp. 1192-1201.

1232. J. Patarin, "How to Find and Avoid Collisions for the Knapsack Hash Function," Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag 1994, pp. 305-317.

1233. W. Patterson, Mathematical Cryptology for Computer Scientists and Mathematicians, Totowa, N.J.: Rowman & Littlefield, 1987.

1234. W.H. Payne, "Public Key Cryptography Is Easy to Break," William H. Payne, unpublished manuscript, 16 Oct 90.

1235. T.R Pederson, "Distributed Provers with Applications to Undeniable Signatures, " Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag 1991, pp. 221-242.

1236. S. Peleg and A. Rosenfield, "Breaking Substitution Ciphers Using a Relaxation Algorithm" Communications of the ACM, v. 22, n. 11, Nov 1979, pp. 598-605.

1237. R. Peralta, "Simultaneous Security of Bits in the Discrete Log " Advances in Cryptology EUROCRYPT '85, Springer-Verlag, 1986, pp. 62-72.

1238. I. Peterson, "Monte Carlo Physics: A Cautionary Lesson," Science News, v. 142, n. 25, 19 Dec 1992, p. 422.

1239. B. Pfitzmann, "Fail-Stop Signatures: Principles and Applications," Proceedings of COMPUSEC '91, Eighth World Conference on Computer Security, Audit, and Control, Elsevier Science Publishers, 1991, pp. 125-134.

1240. B. Pfitzmann and M. Waidner, "Formal Aspects of Fail-Stop Signatures," Fakultat fur Informatik, University Karlsruhe, Report 22/90, 1990.

1241. B. Pfitzmann and M. Waidner, "Fail-Stop Signatures and Their Application, " Securicom '91,1991, pp. 145-160.

1242. B. Pfitzmann and M. Waidner, "Unconditional Concealment with Cryptographic Ruggedness," VIS '91 Verlassliche Informationsysteme Proceedings, Darmstadt, Germany, 13-15 March 1991, pp. 3-2-320. (In German.)

1243. B. Pfitzmann and M. Waidner, "How to Break and Repair a 'Provably Secure' Untraceable Payment System," Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992, pp. 338-350.

1244. C.R Pfleeger, Security in Computing, Englewood Cliffs, N.J.: Prentice-Hall, 1989.

1245. S.J.D. Phoenix and RD. Townsend, "Quantum Cryptography and Secure Optical Communication," BT Technology Journal, v. 11, n. 2, Apr 1993, pp. 65-75.

1246. J. Pieprzyk, "On Public-Key Cryptosystems Built Using Polynomial Rings, " Advances in Cryptology EUROCRYPT '85, Springer-Verlag 1986, pp. 73-80.

1247. J. Pieprzyk, "Error Propagation Property and Applications in Cryptography, " IKE Proceedings-E, Computers and Digital Techniques, v. 136, n. 4, Jul 1989, pp. 262-270.

1248. D. Pinkas, T. Parker, and R Kaijser, "SESAME: An Introduction," Issue 1.2, Bull, JCL, and SNI, Sep 1993.

1249. F. Piper, "Stream Ciphers," Elektrotechnic und Maschinenbau, v. 104, n. 12, 1987, pp. 564-668.

1250. V.S. Pless, "Encryption Schemes for Computer Confidentiality," IEEE Transactions on Computing, v. C-26, n. 11, Nov 1977, pp. 1133-1136.

1251. J.B. Plumstead, "Inferring a Sequence Generated by a Linear Congruence," Proceedings of the 23rd IEEE Symposium on the Foundations of Computer Science, 1982, pp. 153-159.

1252. R. Poet, "The Design of Special Purposc Hardware to Factor Large Integers, " Computer Physics Communications, v. 37,   1985, pp. 337-341.

1253. S.C. Pohlig and M.E. Hellman, "An   Improved Algorithm for Computing Logarithms in GF(p) and Its Cryptographic Significance," IEEE Transactions on Information Theory, v. 24, n. 1, Jan 1978, pp.   106-111.

1254. J.M. Pollard. "A Monte Carlo Method for   Factorization," BIT v. 15, 1975, pp.331-334.

1255. J.M. Pollard and C.P. Schnorr, "An Efficient Solution of the Congruence x+ky= m (mod n)" IEEE Transactions on Infor-   mation Theory, v. IT-33, n. 5, Sep 1987, pp.   702-709.

1256. C. Pomerance, "Recent Developments in   Primality Testing," The Mathematical Intelligencer, v. 3, n. 3, 1981, pp. 97-105.

1257. C. Pomerance, "The Quadratic Sieve Factoring Algorithm," Advances in Cryptology: Proceedings of EUROCRYPT 84,   Springer-Verlag, 1985, 169-182.

1258. C. Pomerance, "Fast, Rigorous Factorization and Discrete Logarithm Algorithms," Discrete Algorithms and Complexity, New   York: Academic Press, 1987, pp. 119-143.

1259. C. Pomerance, I W. Smith, and R. Tuler,   "A Pipe-Line Architecture for Factoring   Large Integers with the Quadratic Sieve   Algorithm," SIAM lournal on Computing,   v.17, n.2, Apr l988, pp. 387-403.

1260. G.J. Popek and C.S. Kline, "Encryption and Secure Computer Networks," ACM Computing Surveys, v 11, n. 4, Dec 1979, pp.   331-356.

1261. F. Pratt, Secret and Urgent, Blue Ribbon Books, 1942.

1262. B. Preneel, "Analysis and Design of Cryptographic Hash Functions, " Ph.D. dissertation, Katholieke Universiteit Leuven, Jan 1993.

1263. B. Preneel, "Differential Cryptanalysis of   Hash Functions Based on Block Ciphers, " Proceedings of the 1st ACM Conference on   Computer and Communications Security, 1993, pp. 183-188.

1264. B. Preneel, "Cryptographic Hash Functions," European Transactions on Telecommunications, v 5, n. 4, Jul/Aug 1994, pp.   431-448.

1265. B. Preneel, personal communication, 1995.

1266. B. Preneel, A. Bosselaers, R. Govaerts, and J. Vandewalle, "Collision-Free Hash Functions Based on Block Cipher Algorithms,"   Proceedings of the 1989 Carnahan Conference on Security Technology 1989, pp.   203-210.

1267. B. Preneel, R. Govaerts, and J. Vandewalle, "An Attack on Two Hash Functions by Zheng-Matsumoto-Imai, " Advances in Cryptology ASIACRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 535-538.

1268. B. Preneel, R. Govaerts, and J. Vandewalle, "Hash Functions Based on Block Ciphers: A Synthetic Approach, " Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp.368-378.

1269. B. Preneel, M. Nuttin, V. Rijmen, and J. Buelens, "Cryptanalysts of the CFB mode of the DES with a Reduced Number of Rounds," Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 212-223.

1270. B. Preneel and V. Rijmen, "On Using Maximum Likelihood to Optimize Recent Cryptanalytic Techniques, " presented at the rump session of EUROCRYPT '94, May 1994.

1271. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation Characteristics of Boolean Functions, " Advances in Cryptology EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 161-173.

1272. W.H. Press, B.R Flannery, S.A. Teukolsky, and W.T. Vetterling, Numerical Recipes in C: The Art of Scientific Computing, Cambridge University Press, 1988.

1273. W. Price, "Key Management for Data Encipherment, " Security: Proceedings of IFIP/SEC '83, North Holland: Elsevier SciencePublishers 1983.

1274. G.R Purdy, "A High-Security Log-in Procedure," communications of the ACM, v 17, n. 8, Aug 1974, pp. 442-445.

1275. J.-J. Quisquater, "Announcing the Smart-Card with RSA Capability, " Proceedings of the Conference: IC Cards and Applications, Today and Tomorrow, Amsterdam, 1989.

1276. J.-J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public Key Cryptosystem," Electronic Letters, v. 18, 1982, pp. 155-168.

1277. J.-J. Quisquater and J.-R Delescaille, "Other Cycling Tests for DES," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 255-256.

1278. J.-J. Quisquater and Y.G. Desmedt, "Chinese Lotto as an Exhaustive Code-Breaking Machine," Computer. v. 24, n. 11, Nov 1991, pp. 14-22.

1279. J.-J. Quisquater and M. Girault, "2p-bit Hash Functions Using e-bit Symmetric Block Cipher Algorithms, Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 102-109.

1280. J.-J. Quisquater and L.C. Guillou, "Des Procedes d'Authentification Bases sur une Publication de Problemes Complexes et Personnalises dont les Solutions Maintenues

Secretes Constituent autant d'Accreditations, " Proceedings of SECURICOM '89: 7th Worldwide Congress on Computer and Communications Security and Protection, Societe d'Edition et d'Organisation d'Expositions Professionnelles, 1989, pp. 149-158. (In French.)

1281. J.-J., Myriam, Muriel, and Michael Quisquater; L., Marie Annick, Gaid, Anna, Gwenole, and Soazig Guillou; and T. Berson, "How to Explain Zero-Knowledge Protocols to Your Children," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag 1990, pp. 628-631.

1282. M.O. Rabin, "Digital Signatures," Foundations of Secure Communication, New York: Academic Press, 1978, pp. 155-168.

1283. M.O. Rabin, "Digital Signatures and Public-Key Functions as Intractable as Factorization, " MIT Laboratory for Computer Science, Technical Report, MlT/LCS/TR 212, Jan 1979.

1284. M.O. Rabin, "Probabilistic Algorithm for Testing Primality," Journal of Number Theory, v. 12, n. 1, Feb 1980, pp. 128-138.

1285. M.O. Rabin, "Probabilistic Algorithms in Finite Fields," SIAM Journal on Computing, v.9, n.2, May 1980, pp.273-280.

1286. M.O. Rabin, "How to Exchange Secrets by Oblivious Transfer," Technical Memo TR 81, Aiken Computer Laboratory, Harvard University, 1981.

1287. M.O. Rabin, "Fingerprinting by Random Polynomials, " Technical Report TR15-81, Center for Research in Computing Technology, Harvard University, 1981.

1288. T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," Proceedings of the 21st ACM Symposium on the Theory of Computing, 1989, pp. 73-85.

1289. RAND Corporation, A Million Random Digits with 100,000 Normal Deviates, Glencoe, IL: Free Press Publishers, 1955.

1290. T.R.N. Rao, "Cryposystems Using Algebraic Codes," International Conference on Computer Systems and Signal Processing, Bangalore, India, Dec 1984.

1291. T.R.N. Rao, "On Struit-Tilburg Cryptanalysis of Rao-Nam Scheme," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 458-460.

1292. T.R.N. Rao and K.H. Nam, "Private-Key Algebraic-Coded Cryptosystems, " Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp.35-48.

1293. T.R.N. Rao and K.H. Nam, "Private-Key Algebraic-Code Encryptions," IEEE Transactions on Information Theory, v. 35, n. 4, Jul 1989, pp. 829-833.

1294. J.A. Reeds, "Cracking Random Number Generator," Cryptologia, v. 1, n. 1, Jan 1977, pp. 20-26.

1295. 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.

1296. J.A. Reeds, "Solution of Challenge Cipher," Cryptologia, v. 3, n. 2, Apr 1979, pp. 83-95.

1297. J.A. Reeds and J.L. Manferdelli, "DES Has No Per Round Linear Factors," Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 377-389.

1298. J.A. Reeds and N.J.A. Sloane, "Shift Register Synthesis (Modulo m)," SIAM Journal on Computing, v. 14, n. 3, Aug 1985, pp. 505-513.

1299. J.A. Reeds and P.J. Weinberger, "File Security and the UNIX Crypt Command, " AT&T Technical Journal, v. 63, n. 8, Oct 1984, pp. 1673-1683.

1300. T. Renji, "On Finite Automaton One-Key Cryptosystems," Fast Software Encryption, Cambridge Security Workshop Proceed ings, Springer-Verlag, 1994, pp. 135-148.

1301. T. Renji and C. Shihua, "A Finite Automaton Public Key Cryptosystems and Digital Signature, " Chinese Journal of Computers, v. 8, 1985, pp. 401-409. (In Chinese.)

1302. T. Renji and C. Shihua, "Two Varieties of Finite Automaton Public Key Cryptosystems and Digital Signature, " Journal of Computer Science and Tecnology, v. 1, 1986, pp. 9-18. (In Chinese.)

1303. T. Renji and C. Shihua, "An Implementation of Identity-based Cryptosystems and Signature Schemes by Finite Automaton Public Key Cryptosystems," Advances in Cryptology CHINACRYPT '92, Bejing: Science Press, 1992, pp.87-104. (In Chinese.)

1304. T. Renji and C. Shihua, "Note on Finite Automaton Public Key Cryptosystems, " CHINACRYPT '94, Xidian, China, 11-15 Nov 1994, pp. 76-80.

1305. Research and Development in Advanced Communication Technologies in Europe, RIPE Integrity Primitives: Final Report of RACE Integrity Primitives Evaluation (R1040), RACE, June 1992.

1306. J.M. Reyneri and E.D. Karnin, "Coin Flipping by Telephone," IEEE Transactions on Information Theory, v. IT-30, n. 5, Sep 1984, pp. 775-776.

1307. P. Ribenboim, The Book of Prime Number Records, Springer-Verlag, 1988.

1308. P. Ribenboim, The Little Book of Big Primes, Springer-Verlag, 1991.

1309. M. Richter, "Fin Rauschgenerator zur   Gewinnung won quasi-idealen Zufallszahlen fur die stochastische Simulation,"   Ph.D. dissertation, Aachen University of   Technology, 1992. (In German.)

1310. R.F. Rieden, J.B. Snyder, R.J. Widman, and   W.J. Barnard, "A Two-Chip Implementation of the RSA Public Encryption Algorithm,"   Proceedings of GOMAC (Government Microcircuit Applications Conference),   Nov 1982, pp. 24 27.

1311. H. Riesel, Prime Numbers and Computer   Methods for Factorization, Boston: Birkhauscr, 1985.

1312. K. Rihaczek, "Data Interchange and Legal Security Signature Surrogates," Computers & Security, v. 13, n. 4, Sep 1994, pp. 287-293.

1313.   V. Rilmen and B. Preneel, "Improved Characteristics for Differential Cryptanalysis of Hash Functions Based on   Block Ciphers," K.U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

1314. R.L. Rivest, "A Description of a Single-Chip Implementation of the RSA Cipher, " LAMBDA Magazine, v. 1, n. 3, Fall 1980,   pp. 14-18.

1315. R.L. Rivest, "Statistical Analysis of the Hagelin Cryptograph," Cryptologia, v. 5, n. 1, Jan 1981, pp. 27-32.

1316. R.L. Rivest, "A Short Report on the RSA Chip, " Advances in Cryptology: Proceedings   of Crypto 82, Plenum Press, 1983, p. 327.

1317. R.L. Rivest, "RSA Chips (Past/Present/ Future), " Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer- Verlag, 1985, pp. 159-168.

1318. R.L. Rivest, "The MD4 Message Digest   Algorithm," RFC 1186, Oct 1990.

1319. R.L. Rivest, "The MD4 Message Digest   Algorithm," Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 303-311.

1320. R.L. Rivest, "The RC4 Encryption Algorithm, " RSA Data Security, Inc., Mar 1992.

1321. R.L. Rivest, "The MD4 Message Digest Algorithm," RFC 1320, Apr 1992.

1322. R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apt 1992.

1323. R.L. Rivest, "Dr. Ron Rivest on the Difficulty of Factoring," Ciphertext: The RSA Newsletter, v. 1, n. 1, Fall 1993, pp. 6, 8.

1324. R.L. Rivest, "The RC5 Encryption Algorithm," Dr. Dobb's Journal, v. 20, n. 1, Jan 95, pp. 146-148.

1325. R.L. Rivest, "The RC5 Encryption Algorithm, " K. U. Leuven Workshop on CryptographicAlgorithms, Springer-Verlag, 1995, to appear.

1326. R.L. Rivest, M.E. Hcllman, J.C. Anderson, and J.W. Lyons, "Responses to NIST's Proposal," Communications of the ACM, v. 35, n. 7, Jul 1992, pp. 41-54.

1327. R.L. Rivest and A. Shamir, "How to Expose an Eavesdropper," Communications of the ACM, v.27, n.4, Apr 1984, pp.393-395.

1328. R.L. Rivest, A. Shamir, and L.M. Adleman, "A Method for Obtaining Digital Signatures and Publie-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.

1329. R.L. Rivest, A. Shamir, and L.M. Adlcman, "On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, Jan 1979.

1330. R.L. Rivest, A. Shamir, and L.M. Adleman, "Cryptographic Communications System and Method," U.S. Patent #4,405,829, 20 Sep 1983.

1331. M.J.B. Robshaw, "Implementations of the Search for Pseudo-Collisions in MD5, " Technical Report TR-103, Version 2.0, RSA Laboratories, Nov 1993.

1332. M.J.B. Robshaw, "The Final Report of RACE 1040: A Technical Summary," Technical Report TR-9001, Version 1.0, RSA Laboratories, Jul 1993.

1333. M.J.B. Robshaw, "On Evaluating the Linear Complexity of a Sequence of Least Period 2n,", Designs, Codes and Cryptography, v. 4, n. 3, 1994, pp. 263-269.

1334. M.J.B. Robshaw, "Block Ciphers," Technical Report TR-601, RSA Laboratories, Jul 1994.

1335. M.J.B. Robshaw, "MD2, MD4, MD5, SHA, and Other Hash Functions, " Technical Report TR-101, Version 3.0, RSA Laboratories, Jul 1994.

1336. M.J.B. Robshaw, "On Pseudo-Collisions in MD5," Technical Report TR-102, Version 1.1, RSA Laboratories, Jul 1994.

1337. M.J.B. Robshaw, "Security of RC4," Technical Report TR-401, RSA Laboratories, Jul 1994.

1338. M.J.B. Robshaw, personal communication, 1995.

1339. M. Roe, "Reverse Engineering of an EES Device," K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995, to appear.

1340. P. Rogaway and D. Coppersmith, "A Software-Oriented Encryption Algorithm, " Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 56-63.

1341. H.L. Rogers, "An Overview of the Cand-ware Program, " Proceedings of the 3rd Annual Symposium on Physical/Electronic Security, Armed Forces Communications and Electronics Association, paper 31, Aug 1987.

1342. J. Rompel, "One-Way Functions Are Necessary and Sufficient for Secure Signatures," Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing, 1990, pp. 387-394.

1343. T. Rosati, "A High Speed Data Encryption Processor for Public Key Cryptography, " Proceedings of the IEEE Custom Integrated Circuits Conference, 1989, pp. 12.3.1-12.3.5.

1344. O.S. Rothaus, "On Bent'Functions," Journal of Combinational Theory Series A, v. 20, n. 3, 1976, pp. 300-305.

1345. RSA Laboratories, "PKCS #1: RSA Encryption Standard," version 1.5, Nov 1993.

1346. RSA Laboratories, "PKCS #3: Diffie-Hellman Key-Agreement Standard, " version 1.4, Nov 1993.

1347. RSA Laboratories, "PKCS #5: Password-Based Encryption Standard," version 1.5, Nov 1993.

1348. RSA Laboratories, "PKCS #6: Extended-Certificate Syntax Standard," version 1.5, Nov 1993.

1349. RSA Laboratories, "PKCS #7: Cryptographic Message Syntax Standard," version 1.5, Nov 1993.

1350. RSA Laboratories, "PKCS #8: Private Key Information Syntax Standard, " version 1.2, Nov 1993.

1351. RSA Laboratories, "PKCS #9: Selected Attribute Types," version 1.1, Nov 1993.

1352. RSA Laboratories, "PKCS #10: Certification Request Syntax Standard, " version 1.0, Nov 1993.

1353. RSA Laboratories, "PKCS #11 : Cryptographic Token Interface Standard, " version 1.0, Apr 95.

1354. RSA Laboratories, "PKCS #12: Public Key User Information Syntax Standard," version 1.0, 1995.

1355. A.D. Rubin and P. Honeyman, "Formal   Methods for the Analysis of Authentication Protocols," draft manuscript, 1994.

1356. F. Rubin, "Decrypting a Stream Cipher   Based on J-K Flip-Flops, " IEEE Transactions on Computing. v. C-28, n. 7, Jul l 97Y,   pp. 483 487.

1357. R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

1358. R.A. Rueppel, "Correlation Immunity and   the Summation Combiner," Advances in Cryptology EUROCRYPT '85, Springer-Verlag, 1986, pp. 260-272.

1359. R.A. Rueppel, "When Shift Registers Clock Themselves," Advances in Cryptology EUROCRYPT '87 Proceedings, Springer-Verlag, 1987, pp. 53-64.

1360. R.A. Rueppel, "Security Models and   Notions for Stream Ciphers," Cryptography and Coding 11, C. Mitchell, ed., Oxford: Clarendon Press, 1992, pp.   213 230.

1361. R.A. Rueppel, "On the Security of   Schnorr's Pseudo-Random Sequence Generator," Advances in Cryptology EUROCRYPT 89 Proceedings, Springer-Verlag, 1990, pp. 423-428.

1362. R.A. Rueppel, "Stream Ciphers," Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, pp. 65-134.

1363. R.A. Rueppel and J.L. Massey, "The Knapsack as a Nonlinear Function," IEEE International Symposium on Information Theory, Brighton, UK, May 1985.

1364. R. A. Rueppel and O. J. Staffelbaeh, " Products of Linear Recurring Sequences with Maximum Complexity, " IEEE Transactions on Information Theory, v. IT-33, n. 1, Jan 1987, pp. 124-131.

1365. D. Russell and G.T. Gangemi, Computer   Security Basics, O'Reilly and Associates, Inc., 1991.

1366. S. Russell and P. Craig, "Privacy Enhanced Mail Modules for ELM," Proceedings of the Internet Society 1994   Workshop on Network and Distributed System Security, The Internet Society,   1994, pp. 21-34.

1367. D.F.H. Sadok and J. Kelner, "Privacy Enhanced Mail Design and Implementation Perspectives," Computer Communications Review, v. 24, n. 3, Jul 1994, pp. 38-46.

1368. K Sakano, "Digital Signatures with User Flexible Reliability," Proceedings of the 1993 Symposium on Cryptography and Information Security (SCIS 93), Shuzenji, Japan, 28-30 Jan 1993, pp. 5C.1-8.

1369. K. Sakano, C. Park, and K. Kunsawa, "Threshold Undeniable Signature Scheme," Proceedings of the 1993 Korea Japan Workshop on Information Security and Cryptography, Seoul, Korea, 24-26 Oct 1993, pp. 184-193.

1370. K. Sako, "Electronic Voting Schemes Allowing Open Objection to the Tally," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E77-A, n. 1, 1994, pp. 24-30.

1371. K. Sako and J. Kilian, "Secure Voting Using Partially Compatible Homomorphisms," Advances ill Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, p. 411-424.

1372. K. Sako and J. Kilian, "Receipt-Free Mix-Type Voting Scheme A Practical Solution to the Implementation of a Voting Booth," Advances in Cryptology EUROCRYPT '95 Proceedings, Springer-Verlag, 1'995, pp. 393-403.

1373. A. Salomaa, Public-Key Cryptography, Springer-Verlag, 1990.

1374. A. Salomaa and L. Santean, "Secret Selling of Secrets with Many Buyers," ETACS Bulletin, v. 42, 1990, pp. 178-186.

1375. M. Santha and U.V Vazirani, "Generating Quasi-Random Sequences from Slightly Random Sources," Proceedings of the 25th Annual Symposium on the Foundations of Computer Science, 1984, pp. 434-440.

1376. M. Santha and U.V Vazirani, "Generating Quasi-Random Sequences from Slightly Random Sources, " 70lzrnal of Computer and System Sciences, v.33, 1986, pp. 75-87.

1377. S. Saryazdi, "An Extension to EIGamal Public Key Cryptosystem with a New Signature Scheme," Proceedings of the 1990 Bilkent International Conference On New Trends in Communication, Control, and Signal Processing, North Holland: Elsevier Science Publishers, 1990, pp. 195-198.

1378. J.E. Savage, "Some Simple Self- Synchronizing Digital Data Scramblers." Bell System Technical Journal, v. 46, n. 2, Feb 1967, pp. 448-487.

1379. B.P Sehanning, "Applying Public Key Distribution to Local Area Networks, " Computers & Security, v. 1, n. 3, Nov 1982, pp. 268-274.

1380. B.P Schanning, S.A. Powers, and J. Kowalchuk, "MEMO: Privacy and Authentication for the Automated Office, " Proceethngs of the 5th Conference on Local Computer Networks, IEEE Press, 1980, pp. 21-30.

1381. L. Schaumuller-Bichl, "Zur Analyse des Data Encryption Standard und Synthese Verwandter Chiffriersysteme," Ph.D. dissertation, Linz University, May 1981. (In German.)

1382. Sehaumuller-Bichl, "On the Design and Analysis of New Cipher Systems Related to the DES," Technical Report, Linz University, 1983.

1383. A. Scherbius, "Ciphering Machine," U.S. Patent #1,657,411, 24 Jan 1928.

1384. J.I. Schiller, "Secure Distributed Computing," Scientific American, v. 271, n.5, Nov 1994, pp. 72-76.

1385. R. Schlafly, "Complaint Against Exclusive Federal Patent License," Civil Action File No. C-93 20450, United States District Court for the Northern District of California.

1386. B. Schneier, "One-Way Hash Functions," Dr. Dobb's journal, v. 16, n. 9, Sep 1991, pp. 148-151.

1387. B. Schneier, "Data Guardians," MacWorld, v. 10, n. 2, Feb 1993, pp. 145-151.

1388. B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," Fast Software Encryption, Cambridge Secunty Workshop Proceedings, Springer-Verlag, 1994, pp. 191-204.

1389. B. Schneier, "The Blowfish Encryption Algorithm," Dr. Dobb's Journal, v. 19, n. 4, Apr 1994, pp. 38-40.

1390. B. Schneier. Protect Your Macintosh, Peachpit Press, 1994.

1391. B. Schneier, "Designing Encryption Algorithms for Real People, " Proceedings of the 1994 ACM SIGSAC New Secunty Paradigms Workshop, IEEE Computer Society Press, 1994, pp. 63-71.

1392. B. Schneier, "A Primer on Authentication and Digital Signatures," Computer Security lournal, v. 10, n. 2, 1994, pp. 38-40.

1393. B. Schneier, "The GOST Encryption Algorithm," Dr. Dobb's journal, v. 20, n. 1, Jan 95, pp. 123-124.

1394. B. Schneier, E-Mail Security (with POP and SEM) New York: John Wiley & Sons, 1995.

1395. C.P Schnorr, "On the Construction of Random Number Generators and Random Function Generators," Advances in Cryptology EUROCRYPT '88 Proceedings, Springer-Verlag, 1988, pp. 225-232.

1396. C.P Schnorr, "Efficient Signature General tion for Smart Cards," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 239-252.

1397. C.P. Schnorr, "Efficient Signature Generation for Smart Cards," Journal of Cryptology, v.4, n.3, 1991, pp. 161-174.

1398. C.P Schnorr, "Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System," U.S. Patent #4,995,082, 19 Feb 1991.

1399. C.P. Schnorr, "An Efficient Cryptographic   Hash Function, " presented at the rump session of CRYPTO '91, Aug 1991.

1400. C.P. Schnorr, "FFT-Hash II, Efficient Cryptographic Hashing, " Advances in Cryptology EUROCRYPT '92 Proceedings,   Springer-Verlag, 1993, pp. 45-54.

1401. C.P. Schnorr and W. Alexi, "RSA-bits are   0.5 + E Secure," Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 113-126.

1402. C.R Schnorr and S. Vaudenay, "Parallel   FFT-Hashing," Fast Software Encryption, Cambridge Secunty Workshop Proceedings, Springer-Verlag, 1994, pp. 149-156.

1403. C.P. Schnorr and S. Vaudenay, "Black Box Cryptanalysis of Hash Networks Based on Multipermutations, " Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

1404. W. Schwartau, Information Warfare: Chaos on the Electronic Superhighway, New York: Thunders Mouth Press, 1994.

1405. R. Scott, "Wide Open Encryption Design Offers Flexible Implementations," Cryptologia, v. 9, n. 1, Jan 1985, pp. 75-90.

1406. J. Seberry, "A Subliminal Channel in Codes for Authentication without Secrecy, " Ars Combinatorica, v. 19A,   1985, pp. 337-342.

1407. J. Seberry and J. Pieprzyk, Cryptography: An Introduction to Computer Security, Englewood Cliffs, N.l.: Prentice-Hall,   1989.

1408. J. Seberry, X.-M. Zhang, and Y. Zheng,   "Nonlinearly Balanced Boolean Functions   and Their Propagation Characteristics, "   Advances in Cryptology EUROCRYPT   '91 Proceedings, Springer-Verlag, 1994, pp.   49-60.

1409. H. Sedlack, "The RSA Cryptography Processor: The First High Speed One-Chip   Solution, " Advances in Cryptology   EUROCRYPT '87 Proceedings, Springer- Verlag, 1988, pp. 95-105.

1410. H. Sedlack and U. Golze, "An RSA Cryptography Processor," Microprocessing and Microprogramming, v. 18, 1986, pp.   583-590.

1411. E.S. Selmer, Linear Recurrence over Finite   Field, University of Bergen, Norway, 1966.

1412. J.O. Shallit, "On the Worst Case of Three Algorithms for Computing the Jacobi Symbol," Journal of Symbolic Computation, v.   10, n. 6, Dec 1990, pp. 593-610.

1413. A. Shamir, "A Fast Signature Scheme,"   MIT Laboratory for Computer Science, Technical Memorandum, MIT/LCS/TM 107, Massachusetts Institute of Technology, Jul 1978.

1414. A. Shamir, "How to Share a Secret," Communications of the ACM, v. 24, n. 11, Nov 1979, pp. 612-613.

1415. A. Shamir, "On the Cryptocomplexity of Knapsack Systems, " Proceedings of the 11th ACM Symposium on the Theory of Computing, 1979, pp. 118-129.

1416. A. Shamir, "The Cryptographic Security of Compact Knapsacks, " MIT Library for Computer Science, Technical Memorandum, MIT/LCS/TM164, Massachusetts Institute of Technology, 1980.

1417. A. Shamir, "On the Generation of Cryptographically Strong Pseudo-Random Sequences, " Lecture Notes in Computer Science 8th International Colloquium On Automata, Languages, and Programming, Springer-Verlag, 1981.

1418. A. Shamir, "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem," Advances in   Cryptology: Proceedings of Crypto 82,   Plenum Press, 1983, pp. 279-288.

1419. A. Shamir, "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, " Proceedings of the 23rd IEEE Symposium on the Foundations of Computer Science, 1982,pp. 145-152.

1420. A. Shamir, "On the Generation of Cryptographically Strong Pseudo-Ranclom Sequences," ACM Transactions on Computer Systems, v. 1, n. l, Feb 1983, pp. 38-44.

1421. A. Shamir, "A Polynomial Time Algorithm for Breaking the Basic Merkle Hellman Cryptosystem, " IEEE Transactions on Information Theory, v. IT-30, n. 5, Sep 1984, pp. 699-704.

1422. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes, " Advances in Cryptology: Proceedings of CRYPTO '84.   Springer-Verlag, 1985, pp. 47-53.

1423. A. Shamir, "On the Security of OES,"   Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp.   280-281.

1424. A. Shamir, lecture at SECURICOM '89.

1425. A. Shamir, "Efficient Signature Schemes   Based on Birational Permutations," Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 1-12.

1426. A. Shamir, personal communication, 1993.

1427. A. Shamir and A. Fiat, "Method, Apparatus and Article for Identification and Signature," U.S. Patent #4,748,668, 31 May 1988.

1428. A. Shamir and R. Zippel, "On the Security of the Merkle-Hellman Cryptographic Scheme," IEEE Transactions on Information Theory, v. 26, n. 3, May 1980, pp. 339-340.

1429. M. Shand, R Bertin, and J. Vuillemin, "Hardware Speedups in Long Integer Multiplication," Proceedings of the 2nd Annual ACM Symposium on Parallel Algorithms and Architectures, 1990, pp. 138-145.

1430. D. Shanks, Solved and Unsolved Problems in Number Theory, Washington D.C.: Spartan, 1962.

1431. C.E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal. v. 27, n. 4, 1948, pp. 379-423, 623-656.

1432. C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal. v. 28, n. 4, 1949, pp. 656-715

1433. C.E. Shannon, Collected Papers: Claude Elmwood Shannon, N.J.A. Sloane and A.D. Wyner, eds., New York: IEEE Press, 1993.

1434. C.E. Shannon, "Predication and Entropy in Printed English," Bell System Technical journal, v. 30, n. 1, 1951, pp. 50-64.

1435. A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL," Transactions of IEICE of Japan, v. J70-1, n. 7, Jul 87, pp. 1413-1423. (In Japanese.)

1436. A. Shimizu and S. Miyaguchi, "Fast Data Encipherment Algorithm FEAL, " Advances in Cryptology EUROCRYPT 87 Proceedings, Springer-Vcrlag, 1988, pp. 267-278.

1437. A. Shimizu and S. Miyaguchi, "FEAL Fast Data Encipherment Algorithm," Systems and Computers in Japan, v. 19, n. 7, 1988, pp. 20-34, 104-106.

1438. A. Shimizu and S. Miyaguchi, "Data Randomization Equipment," U.S. Patent #4,850,019, 18 Jul 1989.

1439. M. Shimada, "Another Practical Public key Cryptosystem, " Electronics Letters, v. 28, n. 23, 5 Nov 1992, pp. 2146-2147.

1440. K. Shirriff, personal communication, 1993.

1441. H. Shizuya, T. Itoh, and K. Sakurai, "On the Complexity of Hyperelliptic Discrete Logarithm Problem," Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 337-351.

1442. Z. Shmuley, "Composite Diffie-Hellman Publie-Key Generating Systems Are Hard to Break," Computer Science Department, Technion, Haifa, Israel, Technical Report 356, Feb 1985.

1443. PW. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," Proceedings of the 35th Symposium on Foundations of Computer Science, 1994, pp. 124-134.

1444. L. Shroyer, letter to NIST regarding DSS, 17 Feb 1992.

1445. C. Shu. T. Matsumoto, and H. Imai, "A Multi-Purpose Proof System, Transactions of the Institute of Electronics, Information, and Communication Engineers, v. E75-A, n. 6, Jun 1992, pp. 735-743.

1446. E.H. Sibley, "Random Number Generators: Good Ones Are Hard to Find," Communications of the ACM, v. 31, n. l0, Oct 1988, pp. 1192-1201.

1447. VM. Sidenikov and S.O. Shestakov, "On Encryption Based on Generalized Reed-Solomon Codes," Diskretnaya Math, v. 4, 1992, pp. 57-63. (In Russian.)

1448. V.M. Sidenikov and S.O. Shestakov, "On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes, " unpublished manuscript, 1992.

1449. D.P Sidbu, "Authentication Protocols for Computer Networks, " Computer Networks and ISDN Systems, v. 11, n. 4, Apr 1986, pp. 297-310.

1450. T. Siegenthaler, "Gorrelation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, " IEEE Transactions on Information Theory, v. IT-30, n. 5, Sep 1984, pp. 776-780.

1451. T. Siegenthaler, "Decrypting a Class of Stream Ciphers Using Ciphcrtext Only," IEEE Transactions on Computing, v. C-34, Jan 1985, pp. 81-85.

1452. T. Siegenthaler, "Cryptanalyst's Rcpresentation of Nonlinearity Filtered ml-sequenccs," Advances in Cryptology EUROCRYYT '85, Springer-Verlag, 1986, pp. 103-110.

1453. R.D. Silverman, "The Multiple Polynomial Quadratie Sieve," Mathematics of Computation, v. 48, n. 177, Jan 1987, pp. 329-339.

1454. G.J. Simmons, "Authentication without Secrecy: A Secure Communication Problem Uniquely Solvable by Asymmetric Encryption Techniques, " Proceedings of IEEE EASCON '79, 1979, pp. 661-662.

1455. G.J. Simmons, "Some Number Theoretic Questions Arising in Asymmetric Encryption Techniques," Annual Meeting of the American Mathematical .Society, AMS Abstract 763.94.1, 1979, pp. 136-151.

1456. G.J. Simmons, "High Speed Arithmetic Using Redundant Number Systems," Proceedings of the National Telecommunications Conference, 1980, pp. 49.3.1-49.3.2.

1457. G.J. Simmons, "A 'Weak' Privacy Protocol Using the RSA Cryptosystem," Cryptologia, v.7, n,2, Apr 1983, pp.180-182.

1458. G.J. Simmons, "The Prisoner's Problem and the Subliminal Channel," Advances in Cryptology: Proceedings of CRYPTO '83, Plenum Press, 1984, pp. 51-67.

1459. G.J. Simmons, "The Subliminal Channel and Digital Signatures," Advances in Cryptology: Proceedings of EUROCRYPT 84, Springer-Verlag, 1985, pp. 364-378.

1460. G.J. Simmons, "A Secure Subliminal Channel?," Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 33-41.

1461. G.J. Simmons, "Cryptology," Encyclopedia Britannica, 16th edition, 1986, pp. 913-924B.

1462. G.J. Simmons, "How to 'Really' Share a Secret, " Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 390 448.

1463. G.J. Simmons, "Prepositioned Secret Sharing Schemes and/or Shared Control Schemes, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 436-467.

1464. G.J. Simmons, "Geometric Shares Secret and/or Shared Control Schemes, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 216-241.

1465. G.J. Simmons, ed., Contemporary Cryptology: The Science of information Integrity, IEEE Press, 1992.

1466. G.J. Simmons, "An Introduction to Shared Secret and/or Shared Control Schemes and Their Application, " in Contemporary Cryptology: The Science of Information Integrity G.J. Simmons, ed., IEEE Press, 1992, pp. 441-497.

1467. G.J. Simmons, "How to Insure that Data Acquired to Verify Treaty Compliance Are Trustworthy," in Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1992, pp. 615-630.

1468. G.J. Simmons, "The Subliminal Channels of the U.S. Digital Signature Algorithm (DSA)," Proceedings of the Third Symposium on: State and Progress of Research in Cryptography, Rome: Fondazone Ugo Bordoni, 1993, pp. 35-54.

1469. G.J. Simmons, "Subliminal Communica tion is Easy Using the USA, " Advances in Cryptology EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 218-232.

1470. G.J. Simmons, "An Introduction to the Mathematics of Trust in Security Protocols," Proceedings: Computer Security Foundations Workshop VI, IEEE Computer Society Press, 1993, pp. 121-127.

1471. G.J. Simmons, "Protocols that Ensure Fairness," Codes and Ciphers, Institute of Mathematics and its Applications, 1995, pp. 383-394.

1472. G.J. Simmons, "Cryptanalysts and Protocol Failures," Communications of the ACM, v.37, n.11, Nov 1994, pp.56-65.

1473. G.J. Simmons, "Subliminal Channels: Past and Present, " European Transactions on Telecommuncations, v. 4, n. 4, Jul/Aug 1994, pp. 459-473.

1474. G.J. Simmons and M.J. Norris, How to Cipher Fast Using Redundant Number Systems, SAND-80-1886, Sandia National Laboratories, Aug 1980.

1475. A. Sinkov, Elementary Cryptanalysis, Mathematical Association of America, 1966.

1476. R. Siromoney and L. Matthew, "A Public Key Cryptosystem Based on Lyndon Words," Information Processing Letters, v. 35, n. 1, 15 Jun 1990, pp. 33-36.

1477. B. Smeets, "A Note on Sequences Generated by Clock-Controlled Shift Registers," Advances in Cryptology EUKOCRYPT '85, Springer-Vcrlag, 1986, pp. 40 42.

1478. M.E. Smid, "A Key Notarization System for Computer Networks, " NBS Special Report 500-54, U.S. Department of Commerce, Oct 1979.

1479. M.E. Smid, "The DSS and the SHS," Federal Digital Signature Applications Symposium, Rockville, MD, 17-18 Feb 1993.

1480. M.E. Smid and D.K. Branstad, "The Data Encryption Standard: Past and Future, " Proceedings of the IEEE, v. 76, n. 5., May 1988, pp. 550-559.

1481. M.E. Smid and D.K. Branstad, "The Data Encryption Standard: Past and Future," in Contemporary Cryptology: The Science of Information Integrity, G.L. Simmons, ed., IEEE Press, 1992, pp. 43-64.

1482. J.L. Smith, "The Design of Lucifer, A Cryptographic Device for Data Communications, " IBM Research Report RC3326, 1971.

1483. J.L. Smith, "Recirculating Block Cipher Cryptographic System," U.S. Patent #3,796,830, 12 Mar 1974.

1484. J.L. Smith, W.A. Notz, and P.R. Osseck,   "An Experimental Application of Cryptography to a Remotely Accessed Data System," Proceedings of the ACM Annual Conference, Aug 1972, pp. 282-290.

1485. K. Smith, "Watch Out Hackers, Public Encryption Chips Are Coming," Electronics Week, 20 May 1985, pp. 30-31.

1486. R Smith, "LUC Public-Key Encryption," Dr. Dobb's journal, v. 18, n. l, Jan 1993, pp. 44-49.

1487. P. Smith and M. Lennon, "LUC: A New Public Key System," Proceedings of the Ninth International Conference on Infor- mation Security, IFlP/Sec 1993, North Holland: Elsevier Science Publishers, 1993, pp. 91-111.

1488. E. Snekkenes, "Exploring the BAN Approach to Protocol Analysis," Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991, pp. 171-181.

1489. B. Snow, "Multiple Independent Binary Bit Stream Generator," U.S. Patent #5,237,615, 17 Aug 1993.

1490. R. Solovay and V. Strassen, "A Fast Monte-Carlo Test for Primality, " SIAM journal on Computing, v. 6, Mar 1977, pp. 84-85; erratum in ibid, v. 7, 1978, p. 118.

1491. T. Sorimachi, T. Tokita, and M. Matsui, "On a Cipher Evaluation Method Based on Differential Cryptanalysis," Proceedings of the 1994 Symposium on Cryptography and Information Security (SCIS 94), Lake Biwa, Japan, 27-29 Jan 1994, pp. 4C.l-9. (In Japanese.)

1492. A. Sorkin, "Lucifer, a Cryptographic Algorithm," Cryptologia, v. 8, n. 1, Jan 1984, pp. 22-41.

1493. W. Stallings, "Kerberos Keeps the Ethernet Secure, " Data Communications, Oct 1994, pp. 103-111.

1494. W. Stallings, Network and Internetwork Secunty, Englewood Cliffs, N.J.: Prentice Hall, 1995.

1495. W. Stallings, Protect Your Privacy: A Guide for POP Users, Englewood Cliffs, N.J.: Prentice-Hall, 1995.

1496. Standards Association of Australia, "Australian Standard 2805.4 1985: Electronic Funds Transfer Requirements for Interfaces: Part 4 Message Authentication, " SAA, North Sydney, NSW, 1985.

1497. Standards Association of Australia, "Australian Standard 2805.5 1985: Electronic Funds Transfer Requirements for Interfaces: Part 5 Data Encipherment Algorithm," SAA, North Sydney, NSW, 1985.

1498. Standards Association of Australia, "Australian Standard 2805.5.3: Electronic Data Transfer Requirements for Interfaces: Part 5.3 Data Encipherment Algorithm   2," SAA, North Sydney, NSW, 1992.

1499. J.G. Steiner, B.C. Neuman, and J.J. Schiller,   "Kerberos: An Authentication Service for Open Network Systems," USENIX Conference Proceedings, Feb 1988, pp. 191-202.

1500. J. Stern, "Secret Linear Congruential Generators Are Not Cryptographically Secure," Proceedings of the 28th Symposium on Foundations of Computer Science, 1987, pp. 421-426.

1501. J. Stern, "A New Identification Scheme   Based on Syndrome Decoding," Advances   in Cryptology CRYPTO '93 Proceedings,   Springer-Verlag, 1994, pp. 13-21.

1502. A. Stevens, "Hacks, Spooks, and Data   Encryption," Dr. Dobb's journal, v. 15, n.   9, Sep 1990, pp. 127-134, 147-149.

1503. R. Struik, "On the Rao-Nam Private-Key   Cryptosystem Using Non-Linear Codes,"   IEEE 1991 Symposium on Information   Theory, Budapest, Hungary, 1991.

1504. R. Struik and J. van Tilburg, "The Rao- Nam Scheme Is insecure against a Chosen-Plaintext Attack, " Advances in Ctyptology CRYPTO '87 Proceedings,   Springer-Verlag, 1988, pp. 445-457.

1505. S.G. Stubblebine and V.G. Gligor, "Protecting the Integrity of Privacy-Enhanced   Mail with DES-Based Authentication   Codes," Proceedings of the Privacy and   Secunty Research Group 1993 Workshop   on Network and Distributed System Security, The Internet Society, 1993, pp. 75-80.

1506. R. Sugarman, "On Foiling Computer   Crime," IEEE Spectrum, v. 16, n. 7, Jul 79,   pp.31-32.

1507. H.N. Sun and T. Hwang, "Public-key ID- Based Cryptosystem," Proceedings of the   25th Annual 1991 IEEE International Carnahan Conference on Security Technology, Taipei, Taiwan, 1 -3 Oct 1991, pp.   142-144.

1508. RF. Syverson, "Formal Semantics for Logics of Computer Protocols, " Proceedings of   the Computer Secunty Foundations   Workshop III, IEEE Computer Society   Press, 1990, pp. 32 41.

1509. RF. Syverson, "The Use of Logic in the   Analysis of Cryptographic Protocols," Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security   and Privacy, 1991,pp. 156-170.

1510. RF. Syverson, "Knowledge, Belief, and   Semantics in the Analysis of Cryptographic Protocols," journal of Computer   Security, v. 1, n. 3, 1992, pp. 317-334.

1511. RF. Syverson, "Adding Time to a Logic Authentication," 1st ACM Conference on Computer and Communications Security, ACM Press, 1993, pp. 97-106.

1512. RF. Syverson and C.A. Meadows, "A Logical Language for Specifying Cryptographic Protocol Requirements, " Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy, 1993, pp. 14-28.

1513. RE Syverson and C.A. Meadows, "Formal Requirements for Key Distribution Protocols," Advances in Cryptology EUROCRYPT '94 Proceedings, Springer-Verlag, 1995, to appear.

1514. RF. Syverson and RC. van Oorschot, "On Unifying Some Cryptographic Protocol Logics," Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, 1994, pp. 165-177.

1515. H. Tanaka, "A Realization Scheme for the Identity-Based Cryptosystem," Advances in Cryptology CRYPTO '87 Proceedings, Springer-Verlag, 1988, pp. 340-349.

1516. H. Tanaka, "A Realization Scheme for the Identity-based Cryptosystem," Electronics and communications in Japan, Part 3 (Fundamental Electronic Science), v. 73, n. 5, May 1990, pp. 1-7.

1517. H. Tanaka, "Identity-Based Noninteractive Common-Key Generation and Its Application to Cryptosystems," Transactions of the Institute of Electronics, Information, and Communication Engineers, v. J75-A, n. 4, Apr 1992, pp. 796-800.

1518. J. Tardo and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates," Proceedings of the 1991 IEEE Computer Society symposiLlm on Security and Privacy, 1991, pp. 232-244.

1519. J. Tardo, K. Alagappan, and R. Pitkin, "Public Key Based Authentication Using Internet Certificates, " USENIX Security 11 Workshop Proceedings, 1990, pp. 121-123.

1520. A. Tardy-Corfdir and H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6, " Advances in Cryptology CRYPTO'91 Proceedings, Springer-Verlag, 1992, pp. 172- 182.

IS21. M. Tatebayashi, N. Matsuzaki, and D.B. Newman, "Key Distribution Protocol for Digital Mobile Communication System," Advances in Cryptology CRYPTO '89 Proceedings, Springcr-Verlag, 1990, pp. .324- 333.

1522. M. Taylor, "Implementing Privacy Enhanced Mail on VMS," Proceedings of the Privacy and Security Research Group 1993 Workshop on Network and Distributed System Security, The Internet Society, 1993, pp. 63-68.

1523. R. Taylor, "An Integrity Cheek Value Algorithm for Stream Ciphers," Advances in Cryptology CRYPTO '93 Proceedings, Springer-Verlag, 1994, pp. 40-48.

1524. T. Tedrick "Fair Exchange of Secrets, " Advances in Cryptology: Proceedings of CRYPTO '84, Springer-Verlag, 1985, pp. 434- 448.

1525. R. Terada and P.G. Pinheiro, "How to Strengthen FEAL against Differential Cryptanalysis, " Proceedings of the 1995 Japan-Korea Workshop on Information Security and Cryptography, Innyama, Japan, 24-27 Jan 1995, pp. 153-162.

1526. J.-P. Tillich and G. Nemor, "Hashing with Sly," Advances in Cryptology CRYPTO '94 Proceedings, Springer-Verlag, 1994, pp. 40 49.

1527. T. Tokita, T. Sorimachi, and M. Matsui, "An Efficient Search Algorithm for the Best Expression on Linear Cryptanalysis." IEICE Japan, Technical Report, ISEC93-97, 1994.

1528. M. Tompa and F. Woll, "Random Self Reducibility and Zero-Knowledge Interactive Proofs of Possession of Information," Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science, 1987, pp. 472-482.

1529. M. Tompa and H. Woll, "How to Share a Secret with Cheaters," journal of Cryptology, v. 1, n. 2, 1988, pp. 133-138.

1530. M.-J. Toussaint, "Verification of Cryptographic Protocols, " Ph.D. dissertation, Universite de Liege, 1991.

1531. M.-J. Toussaint, "Deriving the Complete Knowledge of Participants in Cryptographic Protocols," Advances in Cryptology CRYPTO '91 Proceedings, SpringerVerlag, 1992, pp. 24-43.

1532. M.-J. Toussaint, "Separating the Specification and Implementation Phases in Cryptology," ESORICS 92, Proceedings of the Second European Symposium on Research in Computer Security, Springcr-Verlag, 1992, pp. 77-101.

1533. P.D. Townsend, J.G. Rarity, and RR. Tapstcr, "Enhanced Single Photon Fringe Visibility in a 10 km-Long Prototype Quantum Cryptography Channel," Electronics Letters, v. 28, n. 14, S Jul 1993, pp. 1291

1534. S.A. Tretter, "Properties of PN2 Sequences," IEEE Transactions on Information Theory, v. IT-20, n. 2, Mar 1974, pp. 295-297.

1535 H. Truman, "Memorandum for: The Secretary of State, The Secretary of Defensc," A 20707 5/4/54/OSO, NSA TS CONTL. NO 73- 00405, 24 Oct 1952.

1536. Y.W. Tsai and T. Hwang, "ID Based Public Key Cryptosystem Based on Okamoto and Tanaka's ID Based Onc-Way Communications Scheme," Electronics Letters, v. 26, n. 10, 1 May 1990, pp. 666- 668.

1537. G. Tsudik, "Message Authentication with One-Way Hash Functions," ACM Computer Communications Review, v. 22, n. 5, 1992, pp. 29- 38.

1560. J. van Tilburg, "Cryptanalysts of the Xinmei Digital Signature Scheme," Electronics Letters, v. 28, n. 20, 24 Sep 1992, pp. 1935-1938.

1561. J. van Tilburg, "Two Chosen-Plaintext Attacks on the Li Wang Joing Authentication and Encryption Scheme, " Applied Algebra, Algebraic Algorithms and Error Correcting Codes 10, Springer-Verlag, 1993, pp. 332-343.

1562. J. van Tilburg, "Security-Analysis of a Class of Cryptosystems Based on Linear Error-Correcting Codes, " Ph.D. dissertation, Technical University Eindhoven, 1994.

1563. A. Vandemeulebroecke, E. Vanzieleghem, T. Denayer, and RG. Jespers, "A Single Chip 1024 Bits RSA Processor," Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 219-236.

1564. J. Vanderwalle, D. Chaum, W. Fumy, C. Jansen, P. Landroek, and G. Roelofsen, "A European Call for Cryptographic Algorithms: RIPE; RACE Integrity Primitives Evaluation, " Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, pp. 267-271.

1565. V. Varadharajan, "Verification of Network Security Protocols," Computers and Security, v. 8, n. 8, Aug 1989, pp. 693-708.

1566. V. Varadharajan, "Use of a Formal Description Technique in the Specification of Authentication Protocols, " Computer Standards and Interfaces, v. 9, 1990, pp. 203-215.

1567. S. Vaudenay, "FFT-Hash-II Is not Yet Collision-Free," Advances in Cryptology CRYPTO '92 Proceedings, Springer-Verlag, pp. 587-593.

1568. S. Vaudenay, "Differential Cryptanalysis of Blowfish, " unpublished manuscript, 1995.

1569. U.V. Vazirani and V.V. Vazirani, "Trapdoor Pseudo-Random Number Generators with Applications to Protocol Design, " Proceedings of the 24th IEEE Symposium on the Foundations of Computer Science, 1983, pp. 23-30.

1570. U.V. Vazirani and V.V. Vazirani, "Efficient and Secure Pseudo-Random Number Generation," Proceedings of the 25th IEEE Symposium on the Foundations of Computer Science, 1984, pp. 458 463.

1571. U.V. Vazirani and V.V. Vazirani, "Efficient and Secure Pseudo-Random Number Generation," Advances in Cryptology: Proceedings of CR YP TO '84, Springer -Verlag, 1985, pp. 193-202.

1572. I. Verbauwhede, F. Hoornaert, J. Vanderwalle, and H. De Man, "ASIC Cryptographical Processor Based on DES," Euro ASIC '91 Proceedings, 1991, pp. 292-295.

1573. I. Verbanwhede, F. Hoornaert, J. Vanderwalle, H. De Man, and R. Govaerts, "Security Considerations in the Design and Implementation of a New DES Chip, " Advances in Cryptology EUROCRYPT '87 Proceedings, Springcr-Verlag, 1988, pp. 287-300.

1574. R. Vogel, "On the Linear Complexity of Caseaded Sequences," Advances in Cryptology: Proceedings oi EUROCRYPT 84, Springer-Verlag, 1985, pp. 99-109.

1575. S. von Solms and D. Naccache, "On Blind Signatures and Perfect Crimes," Computers & Security, v. 11, 1992, pp. 581-583.

1576. V.L. Voydock and S.T. Kent, "Security Meehanisms in High-Level Networks, " ACM Computing Surveys, v. 15, n. 2, Jun 1983, pp. 135-171.

1577. N.R. Wagner, RS. Putter, and M.R. Cain, "Large-Scale Randomization Techniques," Advances in Cryptology CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 393-404.

1578. M. Waidner and B. Pfitzmann, "The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability," Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag, 1990, p. 690.

1579. S.T. Walker, "Software Key Escrow A Better Solution for Law Enforcement's Needs?" TIS Report #533, Trusted Information Systems, Aug 1994.

1580. S.T. Walker, "Thoughts on Key Eserow Acceptability, " TIS Report #534D, Trusted Information Systems, Nov 1994.

1581. S.T. Walker, S.B. Lipner, C.M. Ellison, D.K. Branstad, and D.M. Balenson, "Commercial Key Escrow Something for Everyone Now and for the Future," TIS Report #541, Trusted Information Systems, Jan 1995.

1582. M.Z. Wang and J.L. Massey, "The Characteristics of All Binary Sequences with Perfect Linear Complexity Profiles," Abstracts of Papers, EUROCRYPT '86. 20-22 May 1986.

1583. E.J. Watson, "Primitive Polynomials (Mod 2)," Mathematics of Computation, v. 16, 1962, p. 368.

1584. P. Wayner, "Mimic Functions," Cryptologia, v. 16, n. 3, Jul 1992, pp. 193-214.

1585. P. Wayner, "Mimic Functions and Tractability, " draft manuscript, 1993.

1586. A.F. Webster and S.E. Tavares, "On the Design of S-Boxes," Advances in Cryptology CRYPTO '85 Proceedings, Springer-Verlag, 1986, pp. 523-534.

1587. G. Welchman, The Hut Six Story: Breaking the Enigma Codes, New York: McGraw-Hill, 1982.

1588.   A.L. Wells Jr., "A Polynomial Form for Logarithms Modulo a Prime," IEEE Transactions on Information Theory Nov 1984,   pp. 845-846.

1589. D.J. Wheeler, "A Bulk Data Encryption   Algorithm," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 127-134.

1590. D.J. Wheeler, personal communication,   1994.

1591. D.J. Wheeler and R. Needham, "A Large   Block DES-Like Algorithm," Technical   Report 35S, "Two Cryptographic Notes,"   Computer Laboratory, University of Cambridge, Dec 1994, pp. 1-3.

1592. D.J. Wheeler and R. Needham, "TEA, A   Tiny Encryption Algorithm, " Technical   Report 355, "Two Cryptographic Notes,"   Computer Laboratory, University of Cambridge, Dee 1994, pp. 1-3.

1593. S.R. White, "Covert Distributed Processing with Computer Viruses, " Advances in Cryptology CRYPTO '89 Proceedings,   Springer-Verlag, 1990, pp. 616-619.

1594. White House, Office of the Press Secretary,   "Statement by the Press Secretary," 16 Apr 1993.

1595. B.A. Wichman and I.D. Hill, "An Efficient and Portable Pseudo-Random Number Generator," Applied Statistics, v. 31, 1982, pp. 188-190.

1596. M.J. Wiener, "Cryptanalysts of Short RSA Secret Exponents," IEEE Transactions on Information Theory, v. 36, n. 3, May 1990,   pp. 553-5.58.

1597. M.J. Wiener, "Efficient DES Key Search." presented at the rump session of CRYPTO '93, Aug 1993.

1598. M.J. Wiener, "Efficient DES Key Search,"   TR-244, School of Computer Science, Carleton University, May 1994.

1599. M.V. Wilkes, Time-Sharing Computer Systems, New York: American Elsevier, 1968.

1600. E.A. Williams, An Invitation to Cryptograms, New York: Simon and Schuster,   1959.

1601. H.C. Williams, "A Modification of the   RSA Public-Key Encryption Procedure, "   IEEE Transactions on Information Theory,   v. IT-26, n. 6, Nov 1980, pp. 726-729.

1602. H.C. Williams, "An Overview of Factoring," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 71-80.

1603. H.C. Williams, "Some Public-Key Crypto-Functions as Intractable as Factorization, " Advances in Cryptology: Proceedings of   CRYPTO 84, Springer-Verlag, 1985, pp.   66-70.

1604. H.C. Williams, "Some Public-Key Crypto-Functions as Intractable as Factorization," Cryptologia, v. 9, n. 3, Jul 1985, pp. 223-237.

1605. H.C. Williams "An M3 Public-Key Encryption Scheme," Advances in Cryptology CRYPTO 85, Springer-Verlag, 1986, pp. 358-368.

1606. R.S. Winternitz, "Producing One-Way Hash Functions from DES," Advances in Cryptology: Proceedings of Crypto 83, Plenum Press, 1984, pp. 203-207.

1607. R.S. Winternitz, "A Secure One-Way Hash Function Built from DES," Proceedings of the 1984 Symposium on Security and Privacy, 1984, pp. 88-90.

1608. S. Wolfram, "Random Sequence Generation by Cellular Automata," Advances in Applied Mathematics, v. 7, 1986, pp. 123-164.

1609. S. Wolfram, "Cryptography with Cellular Automata, " Advances in Cryptology CRYPTO '85 Proceedings , SpringerVerl ag, 1986, pp. 429-432.

1610. T.Y.C. Woo and S.S. Lam, "Authentication for Distributed Systems," Computer, v. 25, n.1, Jan 1992, pp. 39-52.

1611. T.Y.C. Woo and S.S. Lam, "'Authentication Revisited," Computer, v. 25, n.3, Mar 1992, p. 10.

1612. T.Y.C. Woo and S.S. Lam, "A Semantic Model for Authentication Protocols," Proceedings of the 1993 IEEE Computer Society Symposium on Research in Security and Privacy 1993, pp. 178-194.

1613. M.C. Wood, technical report, Cryptech, Inc., Jamestown, NY, Jul 1990.

1614. M.C. Wood, "Method of Cryptographically 1628. Transforming Electronic Digital Data from One Form to Another," U.S. Patent #5,003,596, 26 Mar 1991.

1615. M. C. Wood, personal communication, 1993.

1616. C.K. Wu and X.M. Wang, "Determination of the True Value of the Euler Totient Function in the RSA Cryptosystem from a Set of Possibilities," Electronics Letters, v. 29, n. 1, 7 Jan 1993, pp. 84-85.

1617. M.C. Wunderlich, "Recent Advances in the Design and Implementation of Large Integer Factorization Algorithms, " Proceedings of 1983 Symposium on Security and Privacy, IEEE Computer Society Press, 1983, pp. 67-71.

1618. Xerox Network System (XNS) Authentication Protocol, XSIS 098404, Xerox Corporation, Apr 1984.

1619. Y.Y. Xian, "New Public Key Distribution System," Electronics Letters, v. 23, n. 11, 1987, pp. 560-561.

1620. L.D. Xing and L.G. Sheng, "Cryptanalysts of New Modified Lu-Lee Cryptosystems," Electronics Letters, v. 26, n. 19, 13 Sep 1990, p. 1601-1602.

1621. W. Xinmei, "Digital Signature Scheme Based on Error-Correcting Codes, " Electronics Letters, v. 26, n. 13, 21 Jun 1990, p. 1634. 898-899.

1622. S.B. Xu, INK. He, and X.M. Wang, "An Implementation of the GSM General Data Encryption Algorithm A5, " CHINACRYPT '94, Xidian, China, 11-15 Nov 1994, pp. 287-291. (In Chinese.)

1623. M. Yagisawa, "A New Method for Realizing Public-Key Cryptosystem," Cryptologia, v. 9, n. 4, Oct 1985, pp. 360-380.

1624. C.H. Yang, "Modular Arithmetic Algorithms for Smart Cards, " IEICE Japan, Technical Report, ISEC92-16, 1992.

1625. C.H. Yang and H. Morita, "An Efficient Modular-Multiplication Algorithm for Smart-Card Software Implementation, " IEICE Japan, Technical Report, ISEC91-58, 1991.

1626. J.H. Yang, K.C. Zeng, and Q.B. Di, "On the Construction of Large S-Boxcs, " CHINACRYPT'94, Xidian, China, 11-15 Nov 1994, pp. 24-32. (In Chinese.)

1627. A.C.-C. Yao, "Protocols for Securc Computations, " Proceedings of the 23rd IEEE Symposium on the Foundations of Computer Science, 1982, pp. 160-164.

1628. B. Yee, "Using Secure Coprocessors, " Ph.D. dissertation, School of Computer Science, Carnegie Mellon University, May 1994.

1629. S.-M. Yen, "Design and Computation of Public Key Cryptosystems," Ph.D. dissertation, National Cheng Hung University, Apr 1994.

1630. S.-M. Yen and C.-S. Lai, "New Digital Signature Scheme Based on the Discrete Logarithm," Electronics Letters, v. 29, n. 12, 1993, pp. 1120-1121.

1631. K. Yin and K. Peterson, "A Single-Chip VLSI Implementation of the Discrete Exponential Public-Key Distribution System, " IBM Systems journal, v. 15, n. 1, 1982, pp. 102-116.

1632. K. Yiu and K. Peterson, "A Single-Chip VLSI Implementation of the Discrete Exponential Public-Key Distribution System," Proceedings of Government Microcircuit Applications Conference, 1982, pp. 18-23.

1633. H.Y. Youm, S.L. Lee, and M.Y. Rhee, "Practical Protocols for Electronic Cash," Proceedings of the 1993 Korea-Japan Workshop on Information Security and Cryptography Seoul, Korea, 24-26 Oct 1993, pp. 10-22.

1634. M. Yung, "Cryptoprotocols: Subscriptions to a Public Key, the Secret Blocking, and the Multi-Player Mental Poker Game, " Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, 439-453.

1635. G. Yuval, "How to Swindle Rabin," Cryptologia, v. 3, n. 3, Jul 1979, pp. 187-190.

1636. K.C. Zeng and M. Huang, "On the Linear Syndrome Method in Cryptanalysis, " Advances in Cryptology CRYPTO '88 Proceedings, Springer-Verlag, 1990, pp. 469-478.

1637. K.C. Zeng, M. Huang, and T.R.N. Rao, "An Improved Linear Algorithm in Cryptanalysis with Applications, " Advances in Cryptology CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 34-47.

1638. K.C. Zeng, C.-H. Yang, and T.R.N. Rao, "On the Linear Consistency Test ILCTl in Cryptanalysis with Applications," Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 164-174.

1639. K.C. Zeng, C.-H. Yang, L. Wei, and T. R.N. Rao, "Pseudorandom Bit Generators in Stream-Cipher Cryptography, " IEEE Computer, v. 24, n. 2, Feb libel, pp. 5-17.

1640. M. Zhang, S.E. Tavares, and L.L. Campbell, "Information Leakage of Boolean Functions and Its Relationship to Other Cryptographic Criteria," Proceedings of the 2nd Annual ACM Conference on Computer and Communications Security, ACM Press, 1994, pp. 156-165.

1641. M. Zhang and G. Xiao, "A Modified Dcsign Criterion for Stream Ciphers," CHINACRYPT'94, Xidian, China, 11-15 Nov 1994, pp. 201-209. (In Chinese.)

1642. Y. Zheng, T. Matsumoto, and H. Imai, "Duality between two Cryptographic Primitives," Papers of Technical Group for Information Security, IEICE of Japan, Mar 1989, pp. 47-57.

1643. Y. Zhcng, T. Matsumoto, and H. Imai, "Impossibility and Optimality Results in Constructing Pseudorandom Permutations," Advances in Cryptology EUROCRYPT '89 Proceedings, Springer-Verlag. 1990, pp. 412-422.

1644. Y. Zheng, T. Matsumoto, and H. Imai, "On the Construction of Block Ciphers Provably Sccurc and Not Relying on Any Unproved Hypotheses, " Advances in Cryptology CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 461-480.

1645. Y. Zheng, T. Matsumoto, and H. Imai, "Duality hctwccn two Cryptographic Primitives," Proceedings of the 8th International Conference on Applied Algebra. Algebraic Algorithms and Error-Correcting Codes, Springer-Verlag, 1991, pp. 379-390.

1646. Y. Zheng, J. Pieprzyk, and J. Seberry, "HAVAL A One-Way Hashing Algorithm with Variable Length of Output, " Advances in Crytology AUSCRYPT '92 Proceedings, Springer-Verlag, 1993, pp. 83-104.

1647. N. Zierler, "Linear Recurring Sequences,"   Journal Soc. Indust. Appl. Math., v. 7, n 1, Mar 1959, pp. 31 48.

1648. N. Zierler, "Primitive Trinomials Whose Degree Is a Mersenne Exponent," Information and Control, v. 15, 1969, pp.   67-69.

1649. N. Zierler and J. Brillhart, "On Primitive   Trinomials (mod 2)," Information and   Control, v. 13, n. 6, Dec 1968, pp. 541-544.

1650. N. Zicrlcr and W.H. Mills, "Products of   Linear Recurring Scqucnces," Journal of Algebra, v. 27, n. 1, Oct 1973, pp. 147-157.

1651. C. Zimmer, "Perfect Gibberish," Discover,   v. 13, n. 12, Dec 1992, pp. 92-99.

1652. P. Zimmermann, The Official PGP   User's Guide, Boston: MIT Press, 1995.

1653. P. Zimmermann, PGP Source Code and   Internals, Boston: MIT Press, 1995.