ΒΙΒΛΙΟΓΡΑΦΙΑ

Adams, C. & Tavares, S. (1990). "The Structured Design of Cryptographically Good S-Boxes", Journal of Cryptology 3(1), pp. 27–41.

Adleman, L., "A subexponential algorithm for the discrete logarithm problem with applications to cryptography", Proceedings 20th IEEE Symposium on Foundations of Computer Science, pp. 55-60, October 1979.

Aiello, W. & Venkatesan, R. (1996). "Benes: A Non-Reversible Alternative to Feistel", EUROCRYPT 96, Vol. LNCS 1070 of Advances in Cryptology, Springer-Verlag, Espoo, Finland, May 31 - June 4, pp. 307–320.

Andelman, D. & Reeds, J. (1982). "On the Cryptanalysis, of Rotor Machines and Substitution-Permutation Networks", IEEE Trans. Inf. Theory IT 28(4), pp. 578–584.

Anderson, R. (1995). "The Classification of Hash Functions", Cryptography and coding IV, Springer-Verlag, pp. 83–93.

Anderson, R. (1995). "Searching for the Optimum Correlation Attack", K.U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag.

Aronsson, H. (1995). "Zero Knowledge Protocols and Small Systems", http://www.niksula.cs.hut.fi/haa/study/zeroknowledge.html.

Bauer, F. (1997). Decrypted Secrets: Methods and Maxims of Cryptology, Springer-Verlag.

Beker, H. & Piper, F. (1982). Cipher Systems: The Protection of Communications, Northwood.

Bell, D. & LaPadula, E. (1974). "Secure Computer Systems: Mathematical Foundations and Model", MITRE corp.

Benaloh, J. (1987). "Secret Sharing Homomorphisms: Keeping Shares of a Secret",CRYPTO 86, Vol. LNCS 263 of Advances in Cryptology, Springer-Verlag, pp. 213–222.

Berlekamp, E. (1984). Algebraic Coding Theory, Aegean Park Press.

Bertsekas, D. & Tsitsiklis, J. (2002). Introduction to Probability,Athena Scientific.

Beth, T. & Piper, F. (1984). "The Stop-and-Go Generator", EUROCRYPT 84, Vol. LNCS 209, Springer-Verlag, Paris, France, April 9-11, pp. 88–92.

Biham, E. (1993). "On Modes of Operation", Fast Software Encryption, Vol. LNCS 809, Springer-Verlag, Cambridge, U.K., December 9-11.

Biham, E. (1994). "Cryptanalysis of Multiple Modes of Operation", ASIACRYPT 94, Vol. LNCS 917, Springer-Verlag, Wollongong, Australia, November 28 – December 1.

Biham, E. (1995) "On Matsui's Linear Cryptanalysis", Proceedings, EUROCRYPT 94, pp. 398-412.

Biham, E. (1996). "Cryptanalysis of Triple-Modes of Operation", Technical Report CS0885, Technion Israel Institute of Technology.

Biham, E. & Shamir, A. (1991). "Differential Cryptanalysis of DES-like Cryptosystems",CRYPTO 90, Vol. LNCS 537 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 11-15, pp. 2–21.

Biham, E. & Shamir, A. (1992). "Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and LUCIFER", CRYPTO 91, Vol. LNCS 576 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 11-15, pp. 156–171.

Biham, E. & Shamir, A. (1993). Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag.

Biham, E. & Shamir, A. (1993). "Differential Cryptanalysis of the Full 16-round DES", CRYPTO 92, Vol. LNCS 740 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 16-20, pp. 487–511.

Biham, E. & Shamir, A. (1997). "Differential Fault Analysis of Secret Key Cryptosystems", CRYPTO 97, Vol. LNCS 1294 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 17-21, pp. 513–525.

Blakeley, G. (1979). "Safeguarding Cryptographic Keys", Proc. of the National Computer Conference, American Federation of Information Processing Societies, pp. 242–268.

Blum, M. & Micali S. (1984). "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits", SIAM J. on Computing 13, pp. 850–64.

Boneh, D., Demilio, R., Lipton, R. (1997). "On the Importance of Checking Cryptographic Protocols for Faults", EUROCRYPT 97, Vol. LNCS 1233 of Advances in Cryptology, Springer-Verlag, Konstanz, Germany, May 11-15, pp. 37–51.

Brassard, G. (1979). "A Note on the Complexity of Cryptography", IEEE Trans. on Information Theory IT-25(2), pp. 232–33.

Brickell, E. & Stinson, D. (1990). "The Detection of Cheaters in Threshold Schemes", CRYPTO 88, Vol. LNCS 403 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 21-25, pp. 564–577.

Brickell E., Simmons, G. (1983), "A Status Report on Knapsack Based Public Key Cryptosystems", Sandia Report, SAND 83-0042, Sandia National Laboratories, February.

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

Campbell, K. & Wiener, M. (1993). "DES is not a Group", CRYPTO 92, Vol. LNCS 740 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 16-20, pp. 512–520.

Carlet, C. (1993). "Partially-Bent Functions", CRYPTO 92, Vol. LNCS 740 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 16-20, pp. 280–91.

Chatterjee S. & Price, B. (1977). Regression Analysis by Example, Wiley.

Chaum, D. & Evertse, J. (1986). "Cryptanalysis of DES with a Reduced Number of Rounds; Sequences of Linear Factors in Block Ciphers", CRYPTO 85, Vol. LNCS 218 of Advances in Cryptology, Santa Barbara, California, USA, August 18-22, pp. 192–211.

Coppersmith, D. (1994). "The Data Encryption Standard and its Strength Against Attacks", IBM Journal of Research and Development 38(3): 243–250.

Coppersmith, D. (1996). "Luby-Rackoff: Four Rounds is not Enough", IBM Research Report, RC 20674.

Cormen, T., Leiserson, C., Rivest, R., Stein, C. (2001). Introduction to algorithms, MIT Press, 2nd Ed.

Cusick, T. & Wood, M. (1991). "The REDOC II Cryptosystem", CRYPTO 90, Vol. LNCS 537 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 11-15, pp. 545–563.

Dai, Z & Yang, J. (1991). "Linear Complexity of Periodically Repeated Random Sequences", EUROCRYPT 91, Vol. LNCS 547 of Advances in Cryptology, Springer-Verlag, Brighton, UK, April 8-11, pp. 168–175.

Damgard, I., "A Design Principle for Hash Functions", Proceedings CRYPTO 89, 1989 New York, Springer-Verlag.

Damgard., I. & Knudsen, L. (1994). "The Breaking of the AR Hash Function", EURO-CRYPT 93, Vol. LNCS 765 of Advances in Cryptology, Springer-Verlag, Lofthus, Norway, May 23-27, pp. 286–292.

Damgard., I. & Knudsen, L. (1996). "Multiple Encryption with Minimum Key", Vol. LNCS 1029, Springer-Verlag, pp. 156–164.

Davies, D. & Price, W. (1984). Security for Computer Networks, Wiley.

Davis, D. & Swick, R. (1990). "Network Security via Private-Key Certificates", MIT Project Athena.

Delfs, H. & Knebl, H. (2002). Introduction to cryptography. Springer, Berlin Heidelberg New York.

Denning, D., Sacco, G. (1981). "Timestamps in key distribution protocols", Comm. ACM, 24, No.8, 533-536, August.

Desmedt, Y. (1991). "The 'A' Cipher Does Not Necessarily Strengthen Security", Cryptologia 15(3): 203–6.

Desmedt, Y. & Frankel, Y. (1990). "Threshold Cryptosystems", CRYPTO 89, Vol. LNCS 435 of Advances in Cryptography, Springer-Verlag, Santa Barbara, California, USA, August 20-24, pp. 307–315. Desmedt, Y. & Frankel, Y. (1992). "Shared Generation of Authentication and Signatures", CRYPTO 91, Vol. LNCS 576 of Advances in Cryptography, Springer-Verlag, Santa Barbara, California, USA, August 11-15, pp. 457–469.

Diffie, W. & Hellman, M. (1976). "New Directions in Cryptography", IEEE Trans. Inf. theory IT-22(6), pp. 644–654.

Diffie, W., Hellman, M. (1976), "Multiuser Cryptographic Techniques", IEEE Trans. Info. Theory, November.

Diffie, W., Van Oorschot, Wiener, M. (1992). "Authentication and Authenticated Key Exchanges", Designs, Codes and Cryptography 2, pp. 107–125.

Eastlake, D. & Jones, P. (2001). US Secure Hash Algorithm 1 (SHA1). RFC3174.

Even, S. & Goldreich, O. (1985). "On the Power of Cascaded Ciphers", ACM Trans. on Computer Systems 3(2), pp. 108–116.

Even, S., Goldreich, O., Lempel, "A randomized Protocol for signing contracts", Comm. ACM, v28 n6, Jun 1985, pp.637-647.

Feige, U., Fiat, A., Shamir, A. (1987). "Zero-Knowledge Proofs of Identity", Proc. of the 19th ACM Symposium on Theory of Computing, pp. 210–217.

Feistel, H. (1974). "Block Cipher Cryptographic System", U.S. Patent #3,798,359.

Feistel, H., Notz, W., Smith, J. (1975). "Some Cryptographic Techniques for Machine-to-Machine Data Communications", Proc. of the IEEE 63(11), pp. 1545–1554.

Freirer, A., Karlton P., Kocher, P. (1996). "The SSL Protocol Version 3.0", Internet Draft.

Garret, P. (2001), Making, Breaking Codes, Prentice-Hall.

Garey., M. & Johnson, D. (1979). Computers and Intractability: A Guide to the Theory of NP-Completeness, Freeman.

Garon, G. & Outerbridge, R. (1991). "DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's", Cryptologia 15(3), pp. 177–93.

Geffe, P. (1973). "How to Protect Data with Ciphers that are Really Hard to Break", Electronics 46(1), pp. 99–101.

Goldreich, O., Goldwasser, S., Micali, S. (1984). "How to Construct Random Functions", Proceedings of the 25th Annual Symposium on Foundations of Computer Science.

Goldwasser, S.,Micali, S., Rivest, S. (1988). "A Digital Signature Scheme Secure Against Adaptive Chosen Message Attacks", SIAM J. in Computing 17, pp. 281–308.

Golomb, S. (1967). Shift register sequences, Holden-Day.

Good, J. (1957). "On the Serial Test for Random Sequences", Ann. Math. Statistics 28, pp. 262–264.

Heys, H. & Tavares, S. (1996). "Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis", Journal of Cryptology 9(1), pp. 1–19.

Ingemasson, I. & Simmons, G. (1991). "A Protocol to Set Up Shared Secret Schemes without the Assistance of a Mutually Trusted Party", EUROCRYPT 90, Vol. LNCS 473 of Advances in Cryptology, Springer-Verlag, Aarhus, Denmark, May 21-24, pp. 266–282.

ISO/IEC 9796 (1991). "Information Technology- Security Techniques- Digital Signature Scheme Giving Message Recovery".

Jansen, C. & Boekee, D. (1988). "Modes of Blockcipher Algorithms and their Protection Against Active Eavesdropping", EUROCRYPT 87, Vol. LNCS 304 of Advances in Cryptology, Springer-Verlag, pp. 281–286.

Knudsen, L. (1994a). "Block Ciphers - Analysis, Designs, Applications", PhD thesis, Aarhus University.

Knudsen, L. (1994b). "Practically Secure Feistel Ciphers", Fast Software Encryption 93, Vol. LNCS 809, Springer-Verlag, Cambridge, U.K., December 9-11, pp. 211–221.

Knuth, D. (1981). The Art of Computer Programming, Vol. 2, Addison-Wesley.

Koblitz, N. (1987). A Course in Number Theory and Cryptography, Springer-Verlag.

Koyama, K. & Terada, R. (1993). "How to Strengthen DES-like Cryptosystems Against Differential Cryptanalysis", IEICE Trans. Fundamentals E76-A(1), pp. 63–69.

Kullback, Solomon, Statistical methods in cryptanalysis, Aegean Park Press, Laguna Hills, California, 1976.

Kumar, I. (1997), Cryptology, Laguna Hills, CA: Aegean Park Press.

Lai, X. (1992). On the Design and Security of Block Ciphers, Vol. 1 of ETH Series in Information Processing, Konstanz: Hartung-Gorre Verlag.

Lai, X., & Massey, J. (1991). "A proposal for a New Block Encryption Standard", EUROCRYPT 90, Vol. LNCS 473 of Advances in Cryptology, Springer-Verlag, Aarhus, Denmark, May 21-24, pp. 389–404.

Lai, X., Massey, J., Murphy S. (1991). “Markov Ciphers and Differential Cryptanalysis”, EUROCRYPT 91, Vol. LNCS 547 of Advances in Cryptology, Springer-Verlag, Brighton, UK, April 8-11, pp. 17–38.

Luby, M. & Rackoff, C. (1986). “Pseudo-random Permutation Generators and Cryptographic Composition”, Proc. 18th Annual Symposium on Theory of Computing, pp. 356–63.

Luby, M. & Rackoff, C. (1988). “How to Construct Pseudorandom Permutations from Pseudorandom Functions”, SIAM J. Computing 17(2), pp. 373–86.

Martin, K. (1993). “Untrustworthy Participants in Perfect Secret Sharing Schemes”, in M. Ganley (ed.), Cryptography and Coding III, Clarendon Press, pp. 255–264.

Matsui, M. (1994). “Linear Cryptanalysis Method for DES Cipher”, EUROCRYPT 93, Vol. LNCS 765 of Advances in Cryptology, Springer-Verlag, Lofthus, Norway, May 23-27, pp. 386–397.

Maurer, U. (1993). “A Simplified and Generalized Treatment of Luby-Rackoff Pseudorandom Permutation Generators”, EUROCRYPT 92, Vol. LNCS 658 of Advances in Cryptology, Springer-Verlag, Balatonfured, Hungary,May 24-28, pp. 239–255.

Menezes, A. (1993). Elliptic Curve Public Key Cryptosystems, Kluwer.

Merkle, R. (1979). “Secrecy, Authentication, and Public Key Systems”, PhD thesis, Stanford University.

Merkle, R. (1990). “A Fast Software One-Way Hash Function”, J. of Cryptology 3(1), pp. 43–58.

Merkle, R. (1989). “One Way Hash Functions and DES”, Proceedings CRYPTO 89, New York, Springer-Verlag.

Meyer, C. & Matyas, M. (1982). Cryptography: A New Dimension In Computer Data Security, Willey.

Meyer, C. & Schilling, M. (1988). “Secure Program Load with Manipulation Detection Code”, SECURICOM 88, pp. 111–130.

Mund, S., Gollman, D., Beth, T. (1988). “Some Remarks on the Cross Correlation Analysis of Pseudorandom Generators”, EUROCRYPT 87, Vol. LNCS 304 of Advances in Cryptology, Springer-Verlag, pp. 25–35.

Murphy S. & Robshaw, M. (2002). “Essential Algebraic Structure within the AES”, CRYPTO 2002, LNCS 2442, Springer-Verlag, pp.1 –16,

Naor, M., Ostrovsky, R., Venkatesan, R., Yung, M. (1992). “Perfect Zero-Knowledge Arguments for NP Can Be Based on General Complexity Assumptions”,ftp://ftp.icsi.Berkeley.edu/pub/techreports/1992/tr-92-082.ps.Z.

National Institute of Standards & Technology (1992). “Proposed Federal Information Processing Standard for Secure Hash Standard (DSS)”, Federal Register 57(21): 29–40.

Needham, R. (1994). “Denial of Service: An Example”, Communications of the ACM 37(11), pp. 42–46.

Needham, R. & Schroeder, M. (1978). “Using encryption for authentication in large networks of computers”, Comm. ACM, 21, No.12, 993-999, December.

O’Connor (1994). “An Analysis of a Class of Algorithms for S-box Construction”, J. of Cryptology 7(3), pp. 133–152.

O’Connor (1994). “On the Distribution of Characteristics in Bijective Mappings”,EUROCRYPT 93, Vol. LNCS 765 of Advances in Cryptology, Springer-Verlag, Lofthus, Norway, May 23-27, pp. 360–70.

Pfleeger, C. (1989). Security in Computing, Prentice Hall.

Pieprzyk, J. (1991). “How to construct Pseudorandom Permutations, from Single Pseudorandom Functions”, EUROCRYPT 90, Vol. LNCS 473 of Advances in Cryptology, Springer-Verlag, Aarhus, Denmark, May 21-24, pp. 140–150.

Pieprzyk, J. (1996). “Cryptographic Algorithms: Properties, Design and Analysis”, Invited lecture PRAGOCRYPT 96.

Pieprzyk, J., Hardjono, T., Seberry, J. (2001). Fundamentals of computer security, Springer.

Pohlig S., Hellman, M., “An improved algorithm for computing logarithms over GF(p) and its cryptographic significance”, Trans. IEEE on information theory, IT-24 No. 1, pp.106-110, January 1978.

Preneel, B., Cryptology, Cryptology, lecture notes, May 1998.

Rabin, M. (1981). How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory.

Rivest, R. (1991). “The MD4 Message Digest Algorithm”, CRYPTO 90, Vol. LNCS 537 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 11-15, pp. 303–311.

Rivest, R. (1992). “The MD4 Message Digest Algorithm”, RFC1320.

Rivest, R. (1992). “The MD5 Message Digest Algorithm”, RFC1321.

Rivest, R. (1994). “The RC5 Encryption Algorithm”, Fast Software Encryption, Vol. LNCS 1008, Springer, pp. 86–96.

Rivest, R., Shamir, A., Adleman, M. (1978). “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM 21(2), pp. 120–126.

Rosen, K. (2000), Elementary number theory and its applications, Addison Wesley Longman, 4th Ed.

RSA Laboratories (1993). “PKCS #7: Cryptographic Message Syntax Standard”, Technical note 003-903022-150-000-000.

Rueppel, R. (1988). “When Shift Registers Clock Themselves”, EUROCRYPT 87, Vol. LNCS 304 of Advances in Cryptology, Springer-Verlag, pp. 53–64.

Scherk, J. (2000). Algebra, A Computational Introduction, Chapman &Hall/CRC.

Schneier, B. (1996). Applied Cryptography, 2nd edn, Wiley.

Schneier, B. & Kelsey, J. (1996). "Unbalanced Feistel Networks and Block Cipher Design", Fast Software Encryption, Third International Workshop, Springer-Verlag, pp. 121–144.

Schnorr, C. (1991). "Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures In A Data Exchange System", US PAT No.4,995,082.

Scott, R. (1985). "Wide Open Encryption Design Offers Flexible Implementations", Cryptologia 9(1), pp. 75–90.

Seberry, J., Zhang, X., Zheng, Y. (1995). "Pitfalls in Designing Substitution Boxes", CRYPTO 94,, Vol. LNCS 839 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 21-25, pp. 383–396.

Shamir, A. (1979). "How to Share a Secret", Communications of the ACM 24(11), pp. 612–613.

Shamir A., Zippel R. (1980). "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans. on Information Theory, IT-26, pp. 339-340.

Shamir, A (1982), "A polynomial time algorithm for breaking the Merkle-Hellman cryptosystem", Proc. 23rd IEEE Symposium on Foundations of Computer Science, pp. 145-152.

Shannon, C. (1948). "A Mathematical Theory of Communication", Bell System Technical Journal, Jully, pp.379-423.

Shannon, C. (1949). "Communication Theory of Secrecy Systems", Bell System Technical Journal, 28, pp. 656–715.

Shimizu, A. & Miyaguchi, S.Z (1988). "Fast Data Encipherment Algorithm, FEAL", EUROCRYPT 87, Vol. LNCS 304 of Advances in Cryptology, Springer-Verlag, pp. 267–278.

Silverman, J. (2001), A friendly introduction to number theory, Prentice-Hall, 2nd Ed.

Sinkov, A. (1996), Elementary cryptanalysis: A mathematical approach, Math Assn Amer.

Stallings, W., (2003), Cryptography and Network Security, Prentice Hall.

Stinson, D. (2002), Cryptography, Theory and Practice, Chapman & Hall/ CRC.

Trappe, W. & Washington, L. (2002), Introduction to cryptography with coding theory, Prentice-Hall.

Tsudik, G. (1992). "Message Authentication with One-Way Hash Functions", Computer Communication Review 22(5): 29–38.

van der Lubbe, J., (1998), Basic Methods of Cryptography, Cambridge University Press.

Webster, A. & Tavares, S. (1986). “On the Design of S-Boxes”, CRYPTO 85, Vol. LNCS 403 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 21-25, pp. 523–534.

Yuval, G. (1979). “How to swindle Rabin”, Cryptologia, v.3. n.3, pp. 187-190.

Zheng, Y., Matsumoto, T., Imai, H. (1990). “On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses”, CRYPTO 89, Vol. LNCS 435 of Advances in Cryptology, Springer-Verlag, Santa Barbara, California, USA, August 20-24, pp. 461–480.

Γκετζ, Ν. (1999). Το Θεώρημα του Παπαγάλου, ΠΟΛΙΣ.

Πάγκαλος, Γ. & Μαυρίδης, Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Ανικούλα.

Singh, S. (2001), Κώδικες και Μυστικά, Π. ΤΡΑΥΛΟΣ.