References

[1] ANSI X9.17. American National Standard Institute. Financial Institution Key Management (Wholesale). ASC X9 Secretariat, American Bankers Association, 1986.

[2] I. Biehl, J. Buchmann, S. Hamdy, and A. Meyer. A signature scheme based on the intractability of computing roots. *Designs, Codes and Cryptography,* 25(3):223–236, 2002.

[3] E. Biham. Cryptanalysis of multiple modes of operation. *Journal of Cryptology,* 11(1):45–58, 1998.

[4] E. Biham. Cryptanalysis of triple modes of operation. *Journal of Cryptology,* 12(3):161–184, 1999.

[5] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In A. Menezes and S. Vanstone, editors, *Advances in Cryptology - CRYPTO'90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990. Proceedings,* volume 537 of *Lecture Notes in Computer Science,* pages 2–21. Springer-Verlag, 1990.

[6] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In B. Kaliski, editor, *Advances in Cryptology - CRYPTO'97: 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1997. Proceedings,* volume 1294 of *Lecture Notes in Computer Science,* pages 513–525. Springer-Verlag, 1997.

[7] Bluetooth$^{\mathrm{TM}}$. *Bluetooth Specifications, version 1.2,* 2003. Available on `https://www.bluetooth.org`.

[8] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *MOBICOM 2001, Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July 16–21, 2001, Rome, Italy,* pages 180–189. ACM Press, 2001.

[9] J. L. Camenisch, J.-M. Piveteau, and M. A. Stadler. Blind signatures based on the discrete logarithm problem. In A. DeSantis, editor, *Advances in Cryptology*

– EUROCRYPT *'94: Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 1994. Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 428–434. Springer-Verlag, 1994.

[10] B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux. Password interception in a SSL/TLS channel. In D. Boneh, editor, *Advances in Cryptology* – CRYPTO *2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 583–599. Springer-Verlag, 2003.

[11] D. Catalano, R. Gennaro, N. Howgrave-Graham, and P. Q. Nguyen. Paillier's cryptosystem revisited. In *Proceedings of the 8th ACM conference on Computer and Communications Security, Philadelphia, PA, U.S.A.*, pages 206–214. ACM Press, 2001.

[12] D. Catalano, P. Q. Nguyen, and J. Stern. The hardness of Hensel lifting: The case of RSA and discrete logarithm. In Y. Zheng, editor, *Advances in Cryptology* - ASIACRYPT *'02: 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*, pages 299–310. Springer-Verlag, 2002.

[13] J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer-Verlag, 2002.

[14] D. W. Davies. Some regular properties of the DES. In A. Gersho, editor, *Advances in Cryptology: a report on CRYPTO'81, IEEE Workshop on Communication Security, Santa Barbara, August 24–26, 1981. U.C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-84*, page 41, 1982.

[15] J. M. DeLaurentis. Weakness in common modulus protocol for the RSA. *Cryptologia*, 8(3):253–259, 1984.

[16] S. Dreyfus. *Underground.* Random House Australia, 1997. Available on `http://www.underground-book.com`.

[17] P. Flagolet and A. Odlyzko. Random mappings statistics. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology* - EUROCRYPT *'89: Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, April 1989. Proceedings*, volume 434 of *Lecture Notes in Computer Science*, pages 329–354. Springer-Verlag, 1990.

[18] P.-A. Fouque and G. Poupard. On the security of RDSA. In E. Biham, editor, *Advances in Cryptology* – EUROCRYPT *'03: International Conference on the Theory and Application of Cryptographic Techniques, Warsaw, Poland, May 2003. Proceedings*, volume 2656 of *Lecture Notes in Computer Science*, pages 462–476. Springer-Verlag, 2003.

[19] H. Gilbert, D. Gupta, A Odlyzko, and J.-J. Quisquater. Attacks on Shamir's "RSA for paranoids". *Information Processing Letters*, 68(4):197–199, 1998.

[20] D. Hong, J Sung, S. Hong, W. Lee, S. Lee, J. Lim, and O. Yi. Known-IV attacks on triple modes of operation of block ciphers. In C. Boyd, editor, *Advances in*

Cryptology - ASIACRYPT*'01: 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 208–221. Springer-Verlag, 2001.

[21] I. Ingemarsson, D. T. Tang, and C. K. Wong. A conference key distribution system. In *IEEE Trans. on Information Theory*, volume IT-28, pages 714–720, September 1982.

[22] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Number 84 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 1990.

[23] A. Joux. Multicollisions in iterated hash functions. Application to cascaded constructions. In M. Franklin, editor, *Advances in Cryptology* – CRYPTO *2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 306–316. Springer-Verlag, 2004.

[24] L. Knudsen. The security of Feistel ciphers with six rounds or less. *Journal of Cryptology*, 15(3):207–222, 2002.

[25] A. Lenstra, X. Wang, and B. de Weger. Colliding X.509 certificates. Cryptology ePrint Archive, Report 2005/067, 2005. `http://eprint.iacr.org/`.

[26] J. Massey. SAFER-K: a byte-oriented block-ciphering algorithm. In R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop, Cambridge, UK, December 9-11, 1993. Proceedings*, volume 809 of *Lecture Notes in Computer Science*, pages 1–17. Springer-Verlag, 1994.

[27] Mathworld. `http://mathworld.wolfram.com`.

[28] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology* – EUROCRYPT*'93: Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 1993. Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1993.

[29] A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of applied cryptography.* The CRC Press series on discrete mathematics and its applications. CRC-Press, 1997.

[30] D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli. Can DSA be improved? Complexity trade-offs with the digital signature standard. In A. De Santis, editor, *Advances in Cryptology* - EUROCRYPT*'94: Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 1994. Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 77–85. Springer-Verlag, 1995.

[31] D. Naccache and J. Stern. A new public-key cryptosystem based on higher residues. In *Proceedings of the 5th ACM conference on Computer and Communications Security, San Francisco, California, U.S.A.*, pages 59–66. ACM Press, 1998.

[32] J. Nakahara, P. Barreto, B. Preneel, J. Vandewalle, and Y. Kim. Square attacks on reduced-round PES and IDEA block ciphers. In B. Macq and J.-J. Quisquater, editors, *Proceedings of 23rd Symposium on Information Theory in the Benelux, Louvain-la-Neuve, Belgium, May 29-31, 2002*, pages 187–195, 2002.

[33] National Institute of Standards and Technology, U. S. Department of Commerce. *Advanced Encryption Standard (AES) - FIPS 197*, 26 November 2001.

[34] U. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In K. Nyberg, editor, *Advances in Cryptology* - EUROCRYPT *'98: International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May/June 1998. Proceedings*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318. Springer-Verlag, 1998.

[35] H. Ong, C. P. Schnorr, and A. Shamir. An efficient signature scheme based on quadratic equations. In R. DeMillo, editor, *Proceedings of the sixteenth annual ACM symposium on Theory of computing, Washington D.C., U.S.A.*, pages 208–216. ACM Press, 1984.

[36] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In J. Stern, editor, *Advances in Cryptology* - EUROCRYPT *'99: International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 1999. Proceedings*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 1999.

[37] T. Peyrin. Bluetooth security. Diploma Project, CPE Lyon, September 2004.

[38] T. Peyrin and S. Vaudenay. The pairing problem with user interaction. In Security and Privacy in the Age of Ubiquitous Computing IFIP TC11 20th International Information Security Conference (SEC'05), Chiba, Japan, 2005.

[39] J. M. Pollard and C. P. Schnorr. An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$. *IEEE Transactions on Information Theory*, IT-33(5):702–709, 1987.

[40] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, MIT, 1979.

[41] R. L. Rivest. Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem. *Cryptologia*, 2(1):62–65, 1978.

[42] R. L. Rivest and A. Shamir. PayWord and MicroMint: two simple micropayment schemes. In M. Lomas, editor, *Proceedings of 1996 International Workshop on Security Protocols*, number 1189 in Lecture Notes in Computer Science, pages 69–87, 1997.

[43] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM*, 21(2):120–126, 1978.

[44] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *Advances in Cryptology* - ASIACRYPT *'01: 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold*

Coast, Australia, December 2001, Proceedings, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer-Verlag, 2001.

[45] R. L. Rivest and R. Silverman. Are "strong" primes needed for RSA. Cryptology ePrint Archive, Report 2001/007, 2001. `http://eprint.iacr.org/`.

[46] T. Satoh, M. Haga, and K. Kurosawa. Towards secure and fast hash functions. In *IEICE Trans.*, volume E82-A, 1999.

[47] C. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In A. De Santis, editor, *Advances in Cryptology* – EUROCRYPT *'94: Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 1994. Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 47–57. Springer-Verlag, 1995.

[48] A. Shamir. RSA for paranoids. *Cryptobytes*, 1(3):1–4, 1995.

[49] G. J. Simmons. A "weak" privacy protocol using the RSA crypto algorithm. *Cryptologia*, 7(2):180–182, 1983.

[50] G. J. Simmons and M. J. Norris. Preliminary comments on the M.I.T public-key cryptosystem. *Cryptologia*, 1(4):406–414, 1977.

[51] S. Singh. *The Code Book: The secret history of codes and code-breaking.* Fourth Estate Ltd., 2000.

[52] J. Stern and S. Vaudenay. CS-Cipher. In S. Vaudenay, editor, *Fast Software Encryption, 5th International Workshop, FSE'98, Paris, France, March 23-25, 1998. Proceedings*, volume 1372 of *Lecture Notes in Computer Science*, pages 189–205. Springer-Verlag, 1998.

[53] S. Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. In B. Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994. Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 286–297. Springer-Verlag, 1995.

[54] S. Vaudenay. On the Lai-Massey scheme. In K. Lam , T. Okamoto, and C. Xing, editors, *Advances in Cryptology* – ASIACRYPT *'99: International Conference on the Theory and Application of Cryptology and Information Security, Singapore, November 14-18, 1999. Proceedings*, volume 1716 of *Lecture Notes in Computer Science*, pages 8–19. Springer-Verlag, 2000.

[55] S. Vaudenay. Decorrelation: a theory for block cipher security. *Journal of Cryptology*, 16(4):249–286, 2003.

[56] S. Vaudenay. *A Classical Introduction to Cryptography: Applications for Communications Security.* Springer-Verlag, 2005.

[57] D. Wagner. Cryptanalysis of the Yi-Lam hash. In T. Okamoto, editor, *Advances in Cryptology* – ASIACRYPT *2000: 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000. Proceedings*, volume 1976 of *Lecture Notes in Computer Science*, pages 483–488. Springer-Verlag, 2000.

[58] W. Xiaoyun and Y. Hongbo. How to break MD5 and other hash functions. In R. Cramer, editor, *Advances in Cryptology* – EUROCRYPT*'05: International Conference on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 2005. Proceedings*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer-Verlag, 2005.