References

1. Anderson, R., 1996. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

2. Aumasson, J.P., & Bernstein, D.J. (2012). SipHash: a fast short-input PRF. International Conference on Cryptology in India, 489-508.

3. Bamford, J., 1982. The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization. Penguin.

4. Bernhard, M., Pereira, O., & Warinschi, B., 2020. Post-Quantum Zero-Knowledge Proofs for Accumulators with Applications to Ring Confidential Transactions. In Advances in Cryptology – EUROCRYPT 2020.

5. Bernstein, D.J. & Lange, T., 2017. Post-Quantum Cryptography. Springer.

6. Bertoni, G., Daemen, J., Peeters, M. & Assche, G.V., 2011. Sponge functions. Ecrypt Hash Workshop 2011.

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

8. Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing, 32(3), 586-615.

9. Boyd, C., & Mathuria, A. (2003). Protocols for Authentication and Key Establishment. Springer.

10. Canetti, R. (2001). Universally Composable Security: A New Paradigm for Cryptographic Protocols. Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science.

11. Coppersmith, D. (1997). Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. Journal of Cryptology, 10(4), 233-260.

12. Daemen, J., & Rijmen, V. (2002). "The Design of Rijndael: AES - The Advanced Encryption Standard."

13. Damgård, I., 1989. A design principle for hash functions. Advances in Cryptology—CRYPTO’89 Proceedings, pp.416-427.

14. Denning, D. E., 2000. Encryption Policy. Encyclopedia of Computer Science, 4th ed.

15. Diffie, W. & Hellman, M.E., 1976. New directions in cryptography. IEEE Transactions on Information Theory, 22(6), pp.644-654.

16. Diffie, W., & Hellman, M. (1976). Multiuser cryptographic techniques. Proceedings of AFIPS National Computer Conference, 109-112.

17. FIPS. (1977). Data Encryption Standard. Federal Information Processing Standards Publication.

18. Goldreich, O., Goldwasser, S., & Micali, S. (1984). How to Construct Random Functions. Journal of the ACM, 33(4), 792-807.

19. Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM Journal on Computing, 17(2), 281-308.

20. Green, M. and Miers, I., 2017. Cryptographic Attacks on Bitcoin Wallet Privacy. Journal of Cryptographic Engineering, 7(2), pp.139-150.

21. Grover, L.K., 1996. A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.

22. Hellman, M. E. (1980). A Cryptanalytic Time-Memory Trade-Off. IEEE Transactions on Information Theory, 26(4), 401-406.

23. Hinsley, F. H., & Stripp, A. (eds.) (1993). Codebreakers: The Inside Story of Bletchley Park. Oxford University Press.

24. Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner.

25. Katz, J., & Lindell, Y. (2007). Introduction to Modern Cryptography. Chapman & Hall/CRC.

26. Kelsey, J., Schneier, B., Wagner, D., & Hall, C. (1997). Side Channel Cryptanalysis of Product Ciphers. Journal of Computer Security, 5(2, 3), 141-158.

27. Knudsen, L. R., & Robshaw, M. J. B. (2011). The Block Cipher Companion. Springer.

28. Koblitz, N. (1987). "Elliptic curve cryptosystems." Mathematics of computation, 48(177), 203-209.

29. Koops, B.J., 2010. Cryptography, Law, and Privacy. In: Encyclopedia of Cryptography and Security. Springer, pp. 324-327.

30. Krawczyk, H., Bellare, M., & Canetti, R. (1997). "HMAC: Keyed-Hashing for Message Authentication."

31. Lai, X., & Massey, J. L. (1991). A Proposal for a New Block Encryption Standard. Advances in Cryptology – EUROCRYPT 1990, 389-404.

32. Lenstra, A.K., & Verheul, E.R. (2000). Selecting cryptographic key sizes. Journal of Cryptology, 14(4), 255-293.

33. Lessig, L., 2006. Code: Version 2.0. Basic Books.

34. Liu, Z. & Wang, L., 2012. A Survey on Empirical Cryptographic Algorithm Evaluation Approaches. Computer Science and Information Technology, 4(1), pp.22-28.

35. Luby, M., & Rackoff, C. (1988). How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM Journal on Computing, 17(2), 373-386.

36. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.

37. Menezes, A., van Oorschot, P., & Vanstone, S. (1997). Handbook of Applied Cryptography. CRC Press.

38. Merkle, R. C. (1978). Secure Communications over Insecure Channels. Communications of the ACM, 21(4), 294-299.

39. Merkle, R.C., 1979. Secrecy, authentication, and public key systems. Stanford University.

40. Micali, S., & Reyzin, L. (2001). Physically Observable Cryptography. Proceedings of the 1st Theory of Cryptography Conference, 278-296.

41. Miller, V. (1986). "Use of elliptic curves in cryptography."

42. NIST (2015). FIPS PUB 180-4, "Secure Hash Standard (SHS)."

43. NIST, 2001. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197.

44. Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

45. National Institute of Standards and Technology, 2001. Security Requirements for Cryptographic Modules. FIPS PUB 140-2. U.S. Department of Commerce.

46. National Security Agency, 2001. Secure Hash Standard (SHS). Federal Information Processing Standards Publication, 180-1.

47. Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

48. Pfitzmann, B., & Waidner, M. (2001). Composition and Integrity Preservation of Secure Reactive Systems. Proceedings of the 7th ACM Conference on Computer and Communications Security, 245-254.

49. Rabin, M. O. (1979). Digitalized Signatures and Public-Key Functions as Intractable as Factorization. MIT Laboratory for Computer Science.

50. Rescorla, E., 2018. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446.

51. Rivest, R., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), pp.120-126.

52. Rogaway, P., & Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. FSE 2004, 371-388.

53. Rogaway, P., 2015. The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162.

54. Schneier, B. (1993). Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). Fast Software Encryption, Cambridge Security Workshop.

55. Shor, P.W., 1999. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review, 41(2), pp.303-332.

56. Sicari, S. et al., 2015. Security, Privacy, and Trust in the Internet of Things. Journal of Distributed Sensor Networks, 12(8).

57. Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor.

58. Stallings, W. (2014). Cryptography and Network Security: Principles and Practice. Pearson.

59. Stinson, D. R. (2005). Cryptography: Theory and Practice. CRC Press.

60. Sullivan, C., 2000. ATM Security Using Symmetric Cryptography. In: Symposium on Network and Distributed System Security (NDSS).

61. Wang, X. et al. (2004). Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. CRYPTO, 2004.

62. Yao, A. C. (1982). Protocols for Secure Computations. Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science, 160-164.

63. Zimmermann, P., 1995. The Official PGP User's Guide. MIT Press.

64. van Tilborg, H. C. A., & Jajodia, S. (2011). Encyclopedia of Cryptography and Security. Springer.