Bibliography

[1] J. Daemen and V. Rijmen, *The design of Rijndael: The wide trail strategy explained*. Springer, 2001.

[2] H. Delfs and H. Knebl, "Symmetric-key encryption", in *Introduction to Cryptography*, Springer, 2007, pp. 11–31.

[3] H. Bennett Ch and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing int", in *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, 1984, pp. 175–9.

[4] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] M. E. Hellman, "An overview of public key cryptography", *IEEE Communications Magazine*, vol. 40, no. 5, pp. 42–49, 2002.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] A. K. Lenstra, "Unbelievable security matching aes security using public key systems", in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2001, pp. 67–86.

[9] A. Shamir, "On the security of des", in *Advances in Cryptology*, Springer-Verlag, 1985, pp. 280–281.

[10] J. Jonsson and B. S. Kaliski, “On the security of rsa encryption in tls”, in *Annual International Cryptology Conference*, Springer, 2002, pp. 127–142.

[11] Y. Tsiounis and M. Yung, “On the security of elgamal based encryption”, in *International Workshop on Public Key Cryptography*, Springer, 1998, pp. 117–134.

[12] Y.-C. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data”, in *International Conference on Applied Cryptography and Network Security*, Springer, 2005, pp. 442–455.

[13] D. Boneh and B. Waters, “Conjunctive, subset, and range queries on encrypted data”, in *Theory of Cryptography Conference*, Springer, 2007, pp. 535–554.

[14] L. Wu, B. Chen, K.-K. R. Choo, and D. He, “Efficient and secure searchable encryption protocol for cloud-based internet of things”, *Journal of Parallel and Distributed Computing*, vol. 111, pp. 152–161, 2018.

[15] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions”, in *Annual International Cryptology Conference*, Springer, 2005, pp. 205–222.

[16] Y. Wang, J. Wang, and X. Chen, “Secure searchable encryption: A survey”, *Journal of Communications and Information Networks*, vol. 1, no. 4, pp. 52–65, 2016.

[17] E.-J. Goh *et al.*, “Secure indexes.”, *IACR Cryptology ePrint Archive*, vol. 2003, p. 216, 2003.

[18] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions”, *Journal of Computer Security*, vol. 19, no. 5, pp. 895–934, 2011.

[19] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search”, in *International conference on the theory and applications of cryptographic techniques*, Springer, 2004, pp. 506–522.

[20] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", *Journal of Computer Security*, vol. 19, no. 5, pp. 895–934, 2011.

[21] K. Bennett, C. Grothoff, T. Horozov, and I. Patrascu, "Efficient sharing of encrypted data", in *Australasian Conference on Information Security and Privacy*, Springer, 2002, pp. 107–120.

[22] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval", in *Foundations of Computer Science, 1995. Proceedings., 36th Annual Symposium on*, IEEE, 1995, pp. 41–50.

[23] C. Cachin, S. Micali, and M. Stadler, "Computationally private information retrieval with polylogarithmic communication", in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 1999, pp. 402–414.

[24] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data", in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, IEEE, 2000, pp. 44–55.

[25] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data", in *International Conference on Applied Cryptography and Network Security*, Springer, 2004, pp. 31–45.

[26] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation", in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, ACM, 1996, pp. 639–648.

[27] O. Goldreich, "Secure multi-party computation", *Manuscript. Preliminary version*, vol. 78, 1998.

[28] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms", *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[29] C. Gentry, “Fully homomorphic encryption using ideal lattices. proceedings of the 41st annual acm symposium on symposium on theory of computing-stoc’09. vol. 9”, 2009.

[30] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*, 09. Stanford University Stanford, 2009, vol. 20.

[31] C. Gentry, “Computing arbitrary functions of encrypted data”, *Communications of the ACM*, vol. 53, no. 3, pp. 97–105, 2010.

[32] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers”, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2010, pp. 24–43.

[33] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys”, in *Annual Cryptology Conference*, Springer, 2011, pp. 487–504.

[34] C. Gentry and S. Halevi, “Implementing gentry’s fully-homomorphic encryption scheme”, in *Annual international conference on the theory and applications of cryptographic techniques*, Springer, 2011, pp. 129–148.

[35] W. Ding, Z. Yan, and R. H. Deng, “Encrypted data processing with homomorphic re-encryption”, *Information Sciences*, vol. 409, pp. 35–55, 2017.

[36] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes”, in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 1999, pp. 223–238.

[37] R. Cramer and V. Shoup, “Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption”, in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2002, pp. 45–64.

[38] E. Bresson, D. Catalano, and D. Pointcheval, “A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications”, in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2003, pp. 37–54.

[39] G. Shafi and S. Micali, “Probabilistic encryption”, *Journal of computer and system sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[40] 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*, ACM, 1998, pp. 59–66.

[41] D. J. Bernstein, “Chacha, a variant of salsa20”, in *Workshop Record of SASC*, vol. 8, 2008, pp. 3–5.

[42] V. V. Bochkarev, A. V. Shevlyakova, and V. D. Solovyev, “The average word length dynamics as an indicator of cultural changes in society”, *Social Evolution & History*, vol. 14, no. 2, pp. 153–175, 2015.

[43] S. Goldwasser and M. Bellare, “Lecture notes on cryptography”, *Summer course Cryptography and computer security at MIT*, vol. 1999, p. 1999, 1996.

[44] G. Procter, “A security analysis of the composition of chacha20 and poly1305.”, *IACR Cryptology ePrint Archive*, vol. 2014, p. 613, 2014.

[45] A. Langley and Y. Nir, “Chacha20 and poly1305 for ietf protocols”, 2018.