BIBLIOGRAPHY

[1] R. Arshad and N. Ikram. Cryptanalysis of a non-interactive deniable authentication protocol based on factoring. *International Journal of Network Security*, 14, 03 2012.

[2] B. Bhushan, G. Sahoo, and A. kumar Rai. Man-in-the-middle attack in wireless and computer networking — a review. *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, pages 1–6, 2017.

[3] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, and G. Stephanides. Two types of key-compromise impersonation attacks against one-pass key establishment protocols. volume 23, pages 227–238, 01 2009. ISBN 978-3-540-88652-5. doi: 10.1007/ 978-3-540-88653-2 17.

[4] G. Couteau. *Zero-Knowledge Proofs for Secure Computation*. PhD thesis, 11 2017.

[5] Q. Dang. Secure hash standard (shs), 2012-03-06 2012.

[6] X. Deng, C. Lee, and H. Zhu. Deniable authentication protocols. *Computers and Digital Techniques, IEE Proceedings -*, 148:101 – 104, 04 2001. doi: 10.1049/ip-cdt: 20010207.

[7] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. doi: 10.1109/TIT.1976.1055638.

[8] C. Dwork, M. Naor, and A. Sahai. Concurrent zero-knowledge. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, page 409–418, New York, NY, USA, 1998. Association for Computing Machinery. ISBN 0897919629. doi: 10.1145/276698.276853. URL https://doi.org/10.1145/276698.276853.

[9] M. Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 2015.

[10] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theor.*, 31(4):469–472, sep 2006. ISSN 0018-9448. doi: 10.1109/TIT.1985.1057074. URL https://doi.org/10.1109/TIT.1985.1057074.

[11] M. P. G. Bertoni, J. Daemen and G. V. Assche. Keccak sponge function family main document. 2009.

[12] F. Hao. Schnorr non-interactive zero-knowledge proof. *RFC*, 8235:1–13, 2017.

[13] M. K. Ibrahem. Modification of diffie-hellman key exchange algorithm for zero knowledge proof. pages 147–152, 04 2012. ISBN 978-1-4673-0261-6. doi: 10.1109/ICFCN. 2012.6206859.

[14] J. Kar and B. Majhi. A secure deniable authentication protocol based on bilinear diffie-hellman algorithm. Cryptology ePrint Archive, Report 2010/340, 2010. https://eprint.iacr.org/2010/340.

[15] F. Li and T. Takagi. Cryptanalysis and improvement of robust deniable authentication protocol. *Wireless Personal Communications*, 69(4):1391–1398, Apr. 2013. ISSN 0929-6212. doi: 10.1007/s11277-012-0640-4.

[16] M.-H. Lim, S. Lee, and H. Lee. Cryptanalysis on improved chou et al.'s id-based deniable authentication protocol. In *Proceedings of the 2008 International Conference on Information Science and Security*, ICISS '08, page 87–93, USA, 2008. IEEE Computer Society. ISBN 076953080X. doi: 10.1109/ICISS.2008.7. URL https://doi.org/10.1109/ICISS.2008.7.

[17] C.-Y. Liu, C.-C. Lee, and T.-C. Lin. Cryptanalysis of an efficient deniable authentication protocol based on generalized elgamal signature scheme. *Int. J. Netw. Secur.*, 12:58–60, 2011.

[18] A. Mallik, A. Ahsan, M. Shahadat, and J.-C. Tsou. Man-in-the-middle-attack: Understanding in simple words. 3:77–92, 01 2019. doi: 10.5267/j.ijdns.2019.1.001.

[19] A. Rama, G. Rao, P. Lakshmi, and R. S. Nowpada. Cryptanalysis of a deniable authentication protocol based on bilinear pairing using single sender and group sender. *International Journal of Computer Applications*, 41:10–13, 03 2012. doi: 10.5120/5520-7551.

[20] M. Sadeghpour. Cryptanalysis of an improvement of a robust deniable authentication protocol. 09 2016.

[21] B. Schneier. *Applied Cryptography (2nd Ed.): Protocols, Algorithms, and Source Code in C*. John Wiley amp; Sons, Inc., USA, 1995. ISBN 0471117099.

[22] J. Shao, Z. Cao, and R. Lu. An improved deniable authentication protocol. *Networks*, 48:179–181, 12 2006. doi: 10.1002/net.20130.

[23] M. Yilmaz and H. Arslan. Impersonation attack identification for secure communication. pages 1275–1279, 12 2013. ISBN 978-1-4799-2851-4. doi: 10.1109/GLOCOMW.2013.6825169.

[24] E.-J. Yoon, K.-Y. Yoo, S.-S. Yeo, and C. Lee. Robust deniable authentication protocol. *Wirel. Pers. Commun.*, 55(1):81–90, sep 2010. ISSN 0929-6212. doi: 10.1007/s11277-009-9787-z. URL https://doi.org/10.1007/s11277-009-9787-z.