**REFERENCES**

[1] L. Lamport, “Password authentication with insecure communication,” Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.

[2] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, “A generic framework for three-factor authentication: Preserving security and privacy in distributed systems,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[3] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, “Robust multifactor authentication for fragile communications,” IEEE Trans. Dependable Secure Comput., vol. 11, no. 6, pp. 568–581,Nov./Dec. 2014.

[4] D. He, S. Zeadally, N. Kumar, and J. Lee, “Anonymous authentication for wireless body area networks with provable security,” IEEE Syst. J., vol. 22, pp. 1–12, 2016.

[5] L. Li, L. Lin, and M. Hwang, “A remote password authentication scheme for multiserver architecture using neural networks,” IEEE Trans. Neural Netw., vol. 12, no. 6, pp. 1498–1504, Nov. 2001.

[6] W. Juang, “Efficient multi-server password authenticated key agreement using smart cards,” IEEE Trans. Consumer Electron., vol. 50, no. 1, pp. 251–255, Feb. 2004.

[7] C. C. Chang and J. S. Lee, “An efficient and secure multi-server password authentication scheme using smart cards,” in Proc. Int. Conf. Cyberworlds, 2004, pp. 417–422.

[8] J.-L. Tsai, “Efficient multi-server authentication scheme based on one-way hash function without verification table,” Comput. Secur., vol. 27, no. 3C4, pp. 115–121, 2008.

[9] W. Tsaur, J. Li, and W. Lee, “An efficient and secure multi-server authentication scheme with key agreement,” J. Syst. Softw., vol. 85, no. 4, pp. 876–882, 2012.

[10] Y. Liao and C. Hsiao, “A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients,” Future Generation Comput. Syst., vol. 29, no. 3, pp. 886–900, 2013.

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, May 2002.

[12] D. Wang and P. Wang, Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards. New York, NY, USA: Springer International Publishing, 2015.

[13] J. K. Lee, S. R. Ryu, and K. Y. Yoo, “Fingerprint-based remote user authentication scheme using smart cards,” Electron. Lett., vol. 38, no. 12, pp. 554–555, 2002.

[14] C. Lin and Y. Lai, “A flexible biometrics remote user authentication scheme,” Comput. Standards Interfaces, vol. 27, no. 1, pp. 19–23, 2004.

[15] C. Chang and I. Lin, “Remarks on fingerprint-based remote user authentication scheme using smart cards,” Operating Syst. Rev., vol. 38, no. 4, pp. 91–96, 2004.

[16] H. Kim, S. Lee, and K. Yoo, “Id-based password authentication scheme using smart cards and fingerprints,” Operating Syst. Rev., vol. 37, no. 4, pp. 32–41, 2003.

[17] M. Scott, “Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints,” Operating Syst. Rev., vol. 38, no. 2, pp. 73–75, 2004.

[18] M. K. Khan and J. Zhang, “Improving the security of ’a flexible biometrics remote user authentication scheme’,” Comput. Standards Interfaces, vol. 29, no. 1, pp. 82–85, 2007.

[19] E. Yoon and K. Yoo, “Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem,” J. Supercomputing, vol. 63, no. 1, pp. 235–255, 2013.

[20] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, “Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme,” in Proc. Int. Conf. Comput. Sci. Appl., 2012, pp. 391–406.

[21] D. He and D. Wang, “Robust biometrics-based authentication scheme for multiserver environment,” IEEE Syst. J., vol. 9, no. 3, pp. 816–823, Sep. 2015.

[22] V. Odelu, A. K. Das, and A. Goswami, “A secure biometrics-based multi-server authentication protocol using smart cards,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[23] A. G. Reddy, E. J. Yoon, A. K. Das, V. Odelu, and K. Y. Yoo, “Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment,” IEEE Access, vol. 5, pp. 3622–3639, Feb. 2017.

[24] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic id-based remote user authentication scheme,” IEEE Trans. Consumer Electron., vol. 50, no. 2, pp. 629–631, May 2004.

[25] Y. Wang, J. Liu, F. Xiao, and J. Dan, “A more efficient and secure dynamic id-based remote user authentication scheme,” Comput. Commun., vol. 32, no. 4, pp. 583–585, 2009.

[26] K. Yeh, C. Su, N. Lo, Y. Li, and Y. Hung, “Two robust remote user authentication protocols using smart cards,” J. Syst. Softw., vol. 83, no. 12, pp. 2556–2565, 2010.

[27] F. Wen and X. Li, “An improved dynamic id-based remote user authentication with key agreement scheme,” Comput. Electr. Eng., vol. 38, no. 2, pp. 381–387, 2012.

[28] D. He, S. Zeadally, N. Kumar, and W. Wu, “Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 9, pp. 2052–2064, Sep. 2016.

[29] D. He, “Security flaws in a biometrics-based multi-server authentication with key agreement scheme,” IACR Cryptology Eprint Archive, vol. 2011, p. 365, 2011.

[30] M. H. Afifi, L. Zhou, S. Chakrabartty, and R. Jian, “Dynamic authentication protocol using self-powered timers for passive internet of things,” IEEE Internet Things J., vol. 5, no. 4, pp. 2927–2935,Aug. 2018.

[31] A. Dua, N. Kumar, A. K. Das, and W. Susilo, “Secure message communication protocol among vehicles in smart city,” IEEE Trans. Veh. Technol., vol. 67, no. 5, pp. 4359–4373, May 2018.

[32] P. Xie, J. Feng, Z. Cao, and J. Wang, “Genewave: Fast authentication and key agreement on commodity mobile devices,” IEEE/ACM Trans. Netw., vol. 26, no. 4, pp. 1688–1700, Aug. 2018.

[33] L. Wu, J. Wang, K.-K. R. Choo, and D. He, “Secure key agreement and key protection for mobile device user authentication,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 2, pp. 319–330, Feb. 2019.

[34] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. D. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.

[35] C. P. Schnorr, Efficient Identification and Signatures for Smart Cards. Berlin, Germany: Springer, 1989.

[36] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in Proc. Int. Conf. Theory Appl. Cryptographic Tech., 1996, pp. 387–398.

[37] N. Fleischhacker, T. Jager, and D. Schr€oder, “On tight security proofs for schnorr signatures,” in Proc. Int. Conf. Theory Appl. Cryptology Inf. Secur., 2014, pp. 512–531.

[38] Y. Tseng, S. Huang, T. Tsai, and J. Ke, “List-free id-based mutual authentication and key agreement protocol for multiserver architectures,” IEEE Trans. Emerging Top. Comput., vol. 4, no. 1, pp. 102–112, Jan. 2016.

[39] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, “Id-based authenticated key agreement for low-power mobile devices,” in Proc. 10th Australasian Conf. Inf. Secur. Privacy, 2005, pp. 494–505.

[40] J. C. Cha and J. H. Cheon, “An identity-based signature from gap diffie-hellman groups,” in Proc. 6th Int. Workshop Theory Practice Public Key Cryptography: Public Key Cryptography, 2003, pp. 18–30.

[41] H. H. Kilinc and T. Yanik, “A survey of sip authentication and key agreement schemes,” IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 1005–1023, Apr.-Jun. 2014.