REFERENCES

[1] A. Hülsing, J. Rijneveld, and F. Song, "Mitigating Multi-Target Attacks in Hash-based Signatures," Springer, Berlin, Heidelberg, Feb. 2016, pp. 387–416. doi: https://doi.org/10.1007/978-3-662-49384-7_15.

[2] F. Shahid and A. Khan, "Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers," *Future Generation Computer Systems*, vol. 111, pp. 241–253, Oct. 2020, doi: 10.1016/j.future.2020.04.042.

[3] L. Li, X. Lu, and K. Wang, "Hash-based signature revisited," Jul. 01, 2022, *Springer Science and Business Media B.V.* doi: http://dx.doi.org/10.1186/s42400-022-00117-w.

[4] P. Lafrance, "Digital Signature Schemes Based on Hash Functions," Thesis, University of Waterloo, Waterloo,Ontario, 2017.

[5] L. Reyzin and N. Reyzin, "Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying," Jan. 2002. [Online]. Available: http://www.cs.bu.edu/˜reyzin

[6] D. J. Bernstein *et al.*, "SPHINCS: practical stateless hash-based signatures," Springer, Berlin, Heidelberg, Apr. 2015, pp. 368–397. doi: https://doi.org/10.1007/978-3-662-46800-5_15.

[7] J. Lee and Y. Park, "HORSIC+: An efficient post-quantum few-time signature scheme," *Applied Sciences (Switzerland)*, vol. 11, no. 16, Aug. 2021, doi: 10.3390/app11167350.

[8] R. Hu, "Visual Blockchain Using Merkle Tree," Thesis, 2019. Accessed: Sep. 16, 2024. [Online]. Available: https://hdl.handle.net/10292/12529

[9] W. Wirachantika, A. M Barmawi, and B. A. Wahyudi, "Memperkuat Fawkescoin Melawan Serangan Pembelanjaan Ganda Menggunakan Merkle Tree," pp. 49–54, Jan. 2019, doi: https://doi.org/10.1145/3309074.3309105.

[10] J. P. Aumasson and G. Endignoux, "Improving stateless hash-based signatures," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2018, pp. 219–242. doi: 10.1007/978-3-319-76953-0_12.

[11] A. V Sills, "COMPOSITIONS, PARTITIONS, AND FIBONACCI NUMBERS," *https://www.researchgate.net/publication/259105764_Compositions_Partitions_and_Fibonacci_Numbers*, vol. 49, Dec. 2013.

[12] N. Kishore, "Study the Effects of Parallel Hashing Algorithms and the Use of Digital Footprints for Security and Fast Digital Forensic Investigations View project," 2016. [Online]. Available: https://www.researchgate.net/publication/307415004

[13] J. Lee, S. Kim, Y. Cho, Y. Chung, and Y. Park, "HORSIC: An efficient one-time signature scheme for wireless sensor networks," *Inf Process Lett*, vol. 112, no. 20, pp. 783–787, Oct. 2012, doi: 10.1016/j.ipl.2012.07.007.

[14] M. Massierer, J. Franklin, and R. Buckland, "Provably Secure Cryptographic Hash Functions," Thesis, School of Mathematics, The University of New South Wales., 2006.

[15] J.-P. Aumasson and G. Endignoux, "Clarifying the subset-resilience problem," *https://ia.cr/2017/909*, Sep. 2017, Accessed: Sep. 10, 2024. [Online]. Available: https://eprint.iacr.org/2017/909

[16] J. Pieprzyk, H. Wang, and C. Xing, "LNCS 3006 - Multiple-Time Signature Schemes against Adaptive Chosen Message Attacks," 2004.

[17] M. Yehia, R. Altawy, and T. A. Gulliver, “Hash-based Signatures Revisited: A Dynamic FORS with Adaptive Chosen Message Security,” A. Nitaj and A. Youssef, Eds., Springer International Publishing, Jul. 2020, pp. 239–257. doi: https://doi.org/10.1007/978-3-030-51938-4_12.

[18] E. Andreeva *et al.*, “New Second-Preimage Attacks on Hash Functions,” *Journal of Cryptology*, vol. 29, no. 4, pp. 657–696, 2016, doi: 10.1007/s00145-015-9206-4ï.

[19] E. Dahmen, K. Okeya, T. Takagi, and C. Vuillaume, “Digital Signatures Out of Second-Preimage Resistant Hash Functions,” B. Johannes and D. Jintai, Eds., Berlin,Heidelberg: Springer, Berlin, Heidelberg, 2008, pp. 109–123. doi: https://doi.org/10.1007/978-3-540-88403-3_8.

[20] M. Matsumoto and T. Nishimura, “Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator,” *ACM Trans. Model. Comput. Simul.*, vol. 8, no. 1, pp. 3–30, Jan. 1998, doi: 10.1145/272991.272995.