DAFTAR PUSTAKA

[1] L. Chen *et al.*, "Report on Post-Quantum Cryptography," Apr. 2016. doi: 10.6028/NIST.IR.8105.

[2] D. Soni, K. Basu, M. Nabeel, N. Aaraj, M. Manzano, and R. Karri, "Chapter 1 - Introduction," in *Hardware Architectures for Post-Quantum Digital Signature Schemes*, Cham: Springer International Publishing, 2021, pp. 1–12.

[3] "Call for Proposals - Post-Quantum Cryptography - CSRC," *CSRC - NIST*. Jan. 2017, [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals.

[4] J. Bos *et al.*, "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," in *Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018*, Apr. 2018, pp. 353–367, doi: 10.1109/EuroSP.2018.00032.

[5] L. Ducas *et al.*, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, pp. 238–268, Feb. 2018, doi: 10.13154/tches.v2018.i1.238-268.

[6] P. . Fouque *et al.*, "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU." https://falcon-sign.info/ (accessed Jan. 23, 2024).

[7] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ Signature Framework." 2019, Accessed: Jan. 23, 2024. [Online]. Available: https://eprint.iacr.org/2019/1086.

[8] G. Alagic *et al.*, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," *NIST*, Jul. 2022, Accessed: Jan. 23, 2024. [Online]. Available: https://www.nist.gov/publications/status-report-third-round-nist-post-quantum-cryptography-standardization-process.

[9] D. Stebila and M. Mosca, "Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10532 LNCS, pp. 14–37, doi: 10.1007/978-3-319-69453-5_2.

[10] "liboqs," *Open Quantum Safe*. Accessed: Jan. 23, 2024. [Online]. Available: https://openquantumsafe.org/liboqs/.

[11] E. Lella *et al.*, "Cryptography in the Quantum Era," in *2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE)*, Jun. 2022, pp. 1–4, doi: 10.1109/WOLTE55422.2022.9882585.

[12] W. Stallings, *Cryptography and Network Security: Principles and Practice, 8th Edition*, 8th ed. Pearson, 2022.

[13] A. W. Mohsen, A. M. Bahaa-Eldin, and M. A. Sobh, "Lattice-based cryptography," in *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, Dec. 2017, pp. 462–467, doi: 10.1109/ICCES.2017.8275352.

[14] "SPHINCS+ Stateless hash-based signatures." https://sphincs.org/ (accessed Jan. 23, 2024).

[15] "CRYSTALS Cryptographic Suite for Algebraic Lattices." https://pq-crystals.org/ (accessed Jan. 23, 2024).

[16] "Kyber." https://pq-crystals.org/kyber/ (accessed Jan. 23, 2024).

[17] E. Crockett, C. Paquin, and D. Stebila, "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH," 2019, Accessed: Jan. 25, 2024. [Online]. Available: https://eprint.iacr.org/2019/858.

[18] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek, "On Feasibility of Post-Quantum Cryptography on Small Devices," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 462–467, 2018, doi: 10.1016/j.ifacol.2018.07.104.

[19] N. Chikouche and A. Ghadbane, "Performance evaluation of post-quantum public-key cryptography in smart mobile Devices," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in*

Bioinformatics), vol. 11195 LNCS, S. A. Al-Sharhan, A. C. Simintiras, Y. K. Dwivedi, M. Janssen, M. Mäntymäki, L. Tahat, I. Moughrabi, T. M. Ali, and N. P. Rana, Eds. Cham: Springer International Publishing, 2018, pp. 67–80.

[20] L. Ribeiro *et al.*, "Saber Post-Quantum Key Encapsulation Mechanism (KEM): Evaluating Performance in Mobile Devices and Suggesting Some Improvements," 2021, [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/ribeiro-saber-pq-key-pqc2021.pdf.

[21] J. A. Septien-Hernandez, M. Arellano-Vazquez, M. A. Contreras-Cruz, and J. P. Ramirez-Paredes, "A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications," *Sensors*, vol. 22, no. 2, p. 489, Jan. 2022, doi: 10.3390/s22020489.

[22] J. N. Ortiz, F. Carvalho Rodrigues, D. Gazzoni Filho, C. Teixeira, J. López, and R. Dahab, "Evaluation of CRYSTALS-Kyber and Saber on the ARMv8 architecture," in *Anais Do Simpósio Brasileiro de Segurança Da Informação e de Sistemas Computacionais (SBSeg)*, Sep. 2022, pp. 372–377, doi: 10.5753/sbseg.2022.224450.

[23] "Valgrind." https://valgrind.org/ (accessed Jan. 28, 2024).