DAFTAR PUSTAKA

Alkim, E., Evkan, H., Lahr, N., Niederhagen, R., & Petri, R. (2020). *ISA Extensions for Finite Field Arithmetic Accelerating Kyber and NewHope on RISC-V*. https://openquantumsafe.org/#liboqs

Aumasson, J.-P. (2017), The impact of quantum computing on cryptography, Computer Fraud & Security, [Online] 2017 (6), 8–11, tersedia di DOI:10.1016/S1361-3723(17)30051-9.

Barker, E. (2020). *Guideline for using cryptographic standards in the federal government:* https://doi.org/10.6028/NIST.SP.800-175Br1

Barker, E. (2016), Recommendation for *Key* Management – Part 1: General. NIST Special Publication 800-57. [Online]. tersedia di DOI:10.6028/NIST.SP.800-57pt1r5.

Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021). *High-Speed NTT-based Polynomial Multiplication Accelerator for CRYSTALS-Kyber Post-Quantum Cryptography*.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehle, D. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. *Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018*, 353–367. https://doi.org/10.1109/EuroSP.2018.00032

Botros, L., Kannwischer, M. J., & Schwabe, P. (2019). *Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4*. https://www.safecrypto.eu/pqclounge/round-2-candidates/

Chen, R., & Peng, D. (2018). A novel NTRU-Based handover authentication scheme for wireless networks. *IEEE Communications Letters*, *22*(3), 586–589. https://doi.org/10.1109/LCOMM.2017.2786228

CSRC (Computer Security Resource Center), 2020, Post-Quantum Cryptography | CSRC, [Online], tersedia di https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals, diakses 15 Januari 2023

Dang, V. B., Mohajerani, K., & Gaj, K. (2021). *High-Speed Hardware Architectures and FPGA Benchmarking; High-Speed Hardware Architectures and FPGA Benchmarking*.

Dang, V. B., Farahmand, F., Andrzejczak, M., Mohajerani, K., Nguyen, D. T., & Gaj, K. (2020). *Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches*.

Dummit, D. S., R. M. Foote. (1999). Abstract Algebra, Second Edition, Jhon William.IInc, N. Y. p

Garrach, M. A., Waghela, C., Mathews, M. M., & Sreekuttan, L. S. (2022). Benchmarking Speed of Post-Quantum Lattice Based PKE/KEM Schemes Using Liboqs. *2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies, TQCEBT 2022*. https://doi.org/10.1109/TQCEBT54229.2022.10041663

Hirschhorn, P. S., Hoffstein, J., Howgrave-Graham, N., & Whyte, W. (2009). *Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches*.

Hoffstein, J.H. dan Silverman, J.H., 2000, Optimizations for NTRU, In Publickey Cryptography and Computational Number Theory. DeGruyter, 1–12,

Huang, Y., Huang, M., Lei, Z., & Wu, J. (2020). A Pure Hardware Implementation of CRYSTALS-KYBER PQC Algorithm through Resource Reuse. *IEICE Electronics Express*, *VV*, 1–6. https://doi.org/10.1587/elex.XX.XXXXXXXX

Hwang, Y. W., & Lee, I. Y. (2018). A study on lightweight mutual authentication for radio-frequency identification medical device. *International Journal of Engineering Business Management*, *10*. https://doi.org/10.1177/1847979018765042

Jati, A., Gupta, N., Chattopadhyay, A., & Sanadhya, S. K. (2021). *A Configurable Crystals-Kyber Hardware Implementation with Side-Channel Protection*.

Jizhong, W., & Chunxiao, W. (2015). Full Secure Identity-Based Encryption Scheme over Lattices in the Standard Model. *Proceedings - 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015*, 412–415. https://doi.org/10.1109/3PGCIC.2015.33

Khanna. 2000. A Course in Abstract Algebra, Vikas Publishing House, New Delhi.

Khedr, A., & Gulak, G. (2018). SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme. *IEEE Journal of Biomedical and Health Informatics*, *22*(2), 597–606. https://doi.org/10.1109/JBHI.2017.2657458

Kreuzer, K. (2023). *Verification of Correctness and Security Properties for CRYSTALS-KYBER*.

Lella, E., Gatto, A., Pazienza, A., Romano, D., Noviello, P., Vitulano, F., & Schmid, G. (2022). Cryptography in the Quantum Era. *IEEE 15th Workshop on Low Temperature Electronics, WOLTE 2022 - Conference Proceedings*. https://doi.org/10.1109/WOLTE55422.2022.9882585

Nguyen, T. T., Kim, S., Eom, Y., & Lee, H. (2022). Area-Time Efficient Hardware Architecture for CRYSTALS-Kyber. *Applied Sciences (Switzerland)*, *12*(11). https://doi.org/10.3390/app12115305

Ni, Z., Khalid, A., Kundi, D.-E.-S., O'neill, M., & Liu, W. (2022). *Efficient Pipelining Exploration for a High-performance CRYSTALS-Kyber Accelerator*.

Putu Agus Eka Pratama, I., & Gusti Ngurah Agung Krisna Adhitya, I. (2022). Post Quantum Cryptography: Comparison between RSA and McEliece. *9th International Conference on ICT for Smart Society: Recover Together, Recover Stronger and Smarter Smartization, Governance and Collaboration, ICISS 2022 - Proceeding*. https://doi.org/10.1109/ICISS55894.2022.9915232

Robshaw, M.J.., (2001), Stream ciphers, Computer Communications, [Online] 24 (11), 1090–1096, tersedia di DOI:10.1016/S0140-3664(00)00333-9.

Shen, X., Du, Z., & Chen, R. (2009). Research on NTRU algorithm for mobile Java security. *International Conference on Scalable Computing and Communications - The 8th International Conference on Embedded*

Computing, ScalCom-EmbeddedCom 2009, 366–369. https://doi.org/10.1109/EmbeddedCom-ScalCom.2009.72

Sinha Roy, S., & Basso, A. (2020). *High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware*. https://github.com/sujoyetc/SABER_HW.

Sun, J., Bai, X., & Kang, Y. (2023). An FPGA-Based Efficient NTT Accelerator for Post-Quantum Cryptography CRYSTALS-Kyber. *Proceedings of 2023 IEEE International Conference on Integrated Circuits, Technologies and Applications, ICTA 2023*, 142–143. https://doi.org/10.1109/ICTA60488.2023.10364299

Wang, Q., Cheng, C., & Zuo, L. (2019). Analysis and Improvement of a NTRU-Based Handover Authentication Scheme. *IEEE Communications Letters*, *23*(10), 1692–1695. https://doi.org/10.1109/LCOMM.2019.2927204

Wei, Y., Lu, J. dan Hu, Y., (2011), 'Meet-in-the-middle attack on 8 rounds of the AES block Cipher under 192 key bits', Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6672 LNCS(60833008), pp. 222–232. doi: 10.1007/978-3642-21031-0_17.

Xia, Y., Ying, C., Lin, G., & Sun, Z. (2019). A third-party mobile payment scheme based on NTRU against quantum attacks. *IEEE Access*, *7*, 56070–56080. https://doi.org/10.1109/ACCESS.2019.2911363

Xing, Y., & Li, S. (2021). A compact hardware implementation of cca-secure *key* exchange mechanism crystals-kyber on fpga. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2021*(2), 328–356. https://doi.org/10.46586/tches.v2021.i2.328-356

Xu, G., Mao, J., Sakk, E., & Wang, S. P. (2023). An Overview of Quantum-Safe Approaches: Quantum *Key* Distribution and Post-Quantum Cryptography. *2023 57th Annual Conference on Information Sciences and Systems, CISS 2023*. https://doi.org/10.1109/CISS56502.2023.10089619

Yu, W., He, D. dan Zhu, S., (2005), Study on NTRU decryption failures, Proceedings - 3rd International Conference on Information Technology and

Applications, ICITA 2005, [Online] II454–459, tersedia di DOI:10.1109/icita.2005.266

Zhao, L., Zhang, J., Huang, J., Liu, Z., & Hancke, G. (2021). Efficient Implementation of Kyber on Mobile Devices. *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, *2021-December*, 506–513. https://doi.org/10.1109/ICPADS53394.2021.00069.