

## DAFTAR PUSTAKA

- Albrecht, M. *et al.* (2019) ‘NTS-KEM Second round submission’. Available at: <https://nts-kem.io/>.
- Androulaki, E. *et al.* (2018) ‘Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains’, *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018-Janua. doi: 10.1145/3190508.3190538.
- Avanzi, R. *et al.* (2020) ‘CRYSTALS-KYBER Algorithm Specifications And Supporting Documentation (version 3.0)’. Available at: <https://pq-crystals.org/kyber/resources.shtml>.
- Baumhof, A. (2019) *Breaking RSA Encryption - an Update on the State-of-the-Art*. Available at: <https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/> (Accessed: 16 June 2021).
- Call for Proposals* (2020). Available at: <https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals> (Accessed: 17 April 2020).
- Cryptology ePrint Archive: Report 2017/634* (2017). Available at: <https://eprint.iacr.org/2017/634> (Accessed: 1 December 2020).
- Explore With Uniform Sampling* (no date). Available at: <https://openmole.org/Uniform+Sampling.html> (Accessed: 17 June 2021).
- Gerjuoy, E. (2004) ‘Shor’s factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers’, *American Journal of Physics*, 73(6), pp. 521–540. doi: 10.1119/1.1891170.
- Hyperledger Caliper* (2020). Available at: [https://www.hyperledger.org/use/caliper#:~:text=Hyperledger Caliper is a blockchain,set of predefined use cases.](https://www.hyperledger.org/use/caliper#:~:text=Hyperledger%20Caliper%20is%20a%20blockchain,set%20of%20predefined%20use%20cases.) (Accessed: 25 April 2021).
- Hyperledger Fabric 1.4 Documentation (2020) *Welcome to Hyperledger Fabric*. Available at: <https://hyperledger-fabric.readthedocs.io/en/release/> (Accessed: 18 April 2020).
- Kelsey, J., Change, S. and Perlner, R. (2016) ‘NIST Special Publication 800-185 - SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash’, *NIST Special Publication*. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-185.pdf>.
- Nasir, Q. *et al.* (2018) ‘Performance analysis of hyperledger fabric platforms’, *Security and Communication Networks*, 2018. doi: 10.1155/2018/3976093.
- Patil, P. and Bansode, R. (2020) ‘Performance Evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text & Images’, pp. 3773–3778.

Philips, W. (2021) *IMPLEMENTASI HYPERLEDGER FABRIC UNTUK APLIKASI AUTENTIKASI PRODUK*. Universitas Multimedia Nusantara.

*PQC Standardization Process: Third Round Candidate Announcement* (2020). Available at: <https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement> (Accessed: 1 December 2020).

Rosencrance, L. (2018) *Authentication*. Available at: <https://searchsecurity.techtarget.com/definition/authentication>.

SEJPM (2015) *Easy explanation of "IND-" security notions?* Available at: <https://crypto.stackexchange.com/a/26738> (Accessed: 5 January 2021).

Sprenkels, D. (2020) *The Kyber/Dilithium NTT*. Available at: <https://dsprenkels.com/ntt.html> (Accessed: 16 June 2021).

Tutoveanu, A. (2021) 'Active Implementation of End-to-End Post Quantum Encryption'. Available at: <https://eprint.iacr.org/2021/356.pdf>.

Zeng, P., Chen, S. and Choo, K. K. R. (2019) 'An IND-CCA2 secure post-quantum encryption scheme and a secure cloud storage use case', *Human-centric Computing and Information Sciences*, 9(1). doi: 10.1186/s13673-019-0193-6.