DAFTAR PUSTAKA

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., 2020a, *Guideline for using cryptographic standards in the federal government:* [Online]. tersedia di DOI:10.6028/NIST.SP.800-175Br1.

Barker, E., 2020b, *Recommendation for key management: Part 1 – General*. [Online]. tersedia di DOI:10.6028/NIST.SP.800-57pt1r5.

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.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. dan Smith-Tone, D., 2016, *Report on Post-Quantum Cryptography*. [Online]. tersedia di DOI:10.6028/NIST.IR.8105.

Chen, R. dan Peng, D., 2018, A novel NTRU-Based handover authentication scheme for wireless networks, *IEEE Communications Letters*, [Online] 22 (3), 586–589, tersedia di DOI: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 21 Mei 2021.

Galbraith, S.D., 2018, *Mathematics of Public Key Cryptography. Version 2.0*, 632,

Heasuk, J., Yunho, L., Mijin, K., Seungjoo, K. dan Dongho, W., 2009, Off-line password-guessing attack to Yang's and Huang's authentication schemes for session initiation protocol, *NCM 2009 - 5th International Joint Conference on INC, IMS, and IDC*, [Online] 618–621, tersedia di DOI:10.1109/NCM.2009.251.

Hirschhorn, P.S., Hoffstein, J., Howgrave-Graham, N. dan Whyte, W., 2009, Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches, *Lecture Notes in Computer Science (including*

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), [Online] 5536 LNCS437–455, tersedia di DOI:10.1007/978-3-642-01957-9_27.

Hoffstein, J., Pipher, J. dan Silverman, J.H., 1998, NTRU: A ring-based public key cryptosystem, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, [Online] 1423267–288, tersedia di DOI:10.1007/bfb0054868.

Hoffstein, J., Silverman, J.H. dan Whyte, W., 1999, Estimated breaking times for NTRU lattices, *http:. WWW. ntru. corn. 1999—03—09*, [Online] (012), tersedia di *http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:estimated+breaking+times+for+NTRU+lattices#0*.

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

Hwang, Y.-W. dan Lee, I.-Y., 2018, A study on lightweight mutual authentication for radio-frequency identification medical device, *International Journal of Engineering Business Management*, [Online] 10184797901876504, tersedia di DOI:10.1177/1847979018765042.

Jeong, S.H., Park, K.S. dan Park, Y.H., 2018, Quantum resistant NTRU-based key distribution scheme for SIP, *International Conference on Electronics, Information and Communication, ICEIC 2018*, [Online] 2018-Janua1–2, tersedia di DOI:10.23919/ELINFOCOM.2018.8330689.

Khedr, A. dan Gulak, G., 2018, SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme, *IEEE Journal of Biomedical and Health Informatics*, [Online] 22 (2), 597–606, tersedia di DOI:10.1109/JBHI.2017.2657458.

Lenstra, A.K., 2007, Key Length, *Brute Force*, [Online] 23–35, tersedia di DOI:10.1007/0-387-27160-0_4.

Loriya, H.T., Kulshreshta, A. dan Keraliya, D.R., 2017, *Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network*, [Online] 6 (2), tersedia di DOI:10.17148/IJARCCE.2017.6262.

Lv, X., Yang, B. dan Pei, C., 2005, Efficient traitor tracing scheme based on NTRU, *Parallel and Distributed Computing, Applications and Technologies, PDCAT Proceedings*, [Online] 2005 (60372046), 120–124, tersedia di DOI:10.1109/PDCAT.2005.130.

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

Sepulveda, J., Liu, S. dan Bermudo Mera, J.M., 2019, Post-Quantum Enabled Cyber Physical Systems, *IEEE Embedded Systems Letters*, [Online] 11 (4), 106–110, tersedia di DOI:10.1109/LES.2019.2895392.

Shen, X., Du, Z. dan 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*, [Online] 366–369, tersedia di DOI:10.1109/EmbeddedCom-ScalCom.2009.72.

Wang, Q., Cheng, C. dan Zuo, L., 2019, Analysis and Improvement of a NTRU-Based Handover Authentication Scheme, *IEEE Communications Letters*, [Online] 23 (10), 1692–1695, tersedia di DOI:10.1109/LCOMM.2019.2927204.

Xia, Y., Ying, C., Lin, G. dan Sun, Z., 2019, A third-party mobile payment scheme based on NTRU against quantum attacks, *IEEE Access*, [Online] 756070–56080, tersedia di DOI:10.1109/ACCESS.2019.2911363.

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.