DAFTAR PUSTAKA

[1] National Institute of Standards and Technology. (2023). *Status report on the final round of the NIST lightweight cryptography standardization process* (NIST IR 8454). https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8454.pdf

[2] Turan, M. S., McKay, K., Kang, J., Kelsey, J., & Chang, D. (2025). *Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions* (NIST SP 800-232). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf

[3] Fúster-Sabater, A., & Pazo-Robles, M. E. (2024). Security analysis of the symmetric cryptosystem TinyJambu. *Symmetry, 16*(4), 440. https://doi.org/10.3390/sym16040440

[4] Salam, I., Alawatugoda, J., & Madushan, H. (2024). Statistical fault analysis of TinyJAMBU. *Discover Applied Sciences, 6*, 55. https://doi.org/10.1007/s42452-024-05701-y

[5] Wu, H., et al. (2021). *TinyJAMBU v2 Specification*. NIST LWC finalist updated spec. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf

[6] Hell, M., et al. (2021). *Grain-128AEADv2 Specification*. NIST LWC finalist updated spec. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/grain-128aead-spec-final.pdf

[7] Saini, A., Tsokanos, A., & Kirner, R. (2022). Quantum randomness in cryptography, A survey of cryptosystems, RNG-based ciphers, and QRNGs. Information, 13, 358. https://doi.org/10.3390/info13080358

[8] Fúster-Sabater, A., & Pazo-Robles, M. E. (2024). Security analysis of the symmetric cryptosystem TinyJambu. Symmetry, 16(4), 440. https://doi.org/10.3390/sym16040440

[9] Hell, M., Johansson, T., Meier, W., Sönnerup, J., & Yoshida, H. (2021). Grain-128AEAD—A lightweight AEAD stream cipher (Round-2 specification). NIST LWC submission. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/grain-128aead-spec-final.pdf

[10] Das, M., & Mazumdar, B. (2024). Security analysis of ASCON cipher under persistent faults. https://eprint.iacr.org/2024/2030.pdf

[11] Description, Implementation and Performance/Security Analysis of ASCON128 V1.2. (2023, November-Desember). International Journal for Multidisciplinary Research (IJFMR), 5(6). https://www.ijfmr.com/papers/2023/6/10225.pdf

[12] Exact Security Analysis of ASCON. (2023). [Makalah presentasi]. Lightweight Cryptography Workshop 2023, National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/Events/2023/lightweight-cryptography-workshop-2023/documents/accepted-papers/10-exact-security-analysis-of-ascon.pdf

[13] Improved differential fault analysis of Grain-128AEAD. (2024, Maret). Journal of Surveillance, Security and Safety. OAE Publishing Inc. https://www.oaepublish.com/articles/jsss.2023.42

[14] Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. J. Cyber Secur. Risk Audit, 2025(2), 12-26. https://jcsra.thestap.com/articles/v-2025-i-2-p-2.pdf

[15] Rana, M., Mamun, Q., & Islam, R. (2024). Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. Electronics, 13(21), 4325. https://doi.org/10.3390/electronics13214325

[16] Aziz, S., Shoukat, I. A., Iftikhar, M., Murtaza, M., Alenezi, A. M., Lee, C.-C., & Taj, I. (2024). Next-Generation Block Ciphers: Achieving Superior Memory Efficiency and Cryptographic Robustness for IoT Devices. Cryptography, 8(4), 47. https://doi.org/10.3390/cryptography8040047

[17] Fang, T.; Salam, I.; Yau, W. C. Improved differential fault analysis of Grain-128AEAD. J. Surveill. Secur. Saf. 2024, 5, 62-79. http://dx.doi.org/10.20517/jsss.2023.42

[18] Patel, D. B., & Avadia, S. A. (2025). Comparison of Stream and Block Ciphers in Lightweight Cryptography for IoT Devices: A Systematic Literature Review. Available at SSRN 5360240. https://download.ssrn.com/2025/7/21/5360240.pdf

[19] Kaiser, A. M., & Hoiness, G. W. Throughput of ASCON Compared with Popular IoT Encryption Algorithms. Military Cyber Affairs, 8(1), 3. https://digitalcommons.usf.edu/mca/vol8/iss1/3/

[20] Salam, I., Alawatugoda, J., & Madushan, H. (2024). Discover Applied Sciences. Discover, 6, 419. http://dx.doi.org/10.1007/s42452-024-05701-y

[21] Luengo, E. A., Olivares, B. A., Villalba, L. J. G., & Hernandez-Castro, J. (2023). Further analysis of the statistical independence of the NIST SP 800-22 randomness tests. Applied Mathematics and Computation, 459, 128222. https://doi.org/10.1016/j.amc.2023.128222

[22] Lightweight cryptography for IoT: A comprehensive survey of algorithms, implementations, and standardization," World Journal of Advanced Engineering Technology and Sciences, 2024. [Online]. Available: https://journalwjaets.com/content/lightweight-cryptography-iot-comprehensive-survey-algorithms-implementations-and

[23] A Novel Diffusion-Based Cryptographic Method for Cyber Security," 2025. [Online]. Available: https://iasj.rdd.edu.iq/journals/uploads/2025/09/09/658d04edd41e7f76e6cb134bed207294.pdf

[24] F. Rastoceanu, R. V. Rughinis, and D.-C. Trancă, "Lightweight cryptographic secure random number generator for IoT devices," in 2023 24th International Conference on Control Systems and Computer Science (CSCS), 2023, pp. 180–185. [Online]. Available: https://www.semanticscholar.org/paper/b92c5300c2cd386412fa26162b1a3656b42ab2cc

[25] Zinabu, N. G., & Asferaw, S. (2022). Enhanced Security of Advanced Encryption Standard (ES-AES) Algorithm. *American Journal of Computer Science and Technology*, *5*(2), 41-48. https://doi.org/10.11648/j.ajcst.20220502.13

[26] Sivagurunathan, S., & Rajakumari, K. (2024). A Survey on the Advanced Encryption Standard (AES) Algorithm. *International Journal of Engineering Research & Technology (IJERT)*, *13*(04), 18-24. https://doi.org/10.47760/ijcsmc.2024.v13i04.008