Section VI: References

Alani, M. M. (2012). Neuro-cryptanalysis of DES and triple-DES. In T. Huang, Z. Zeng, C. Li, & C. S. Leung

    (Eds.), *Neural Information Processing* (Vol. 7667, pp. 637–646). Springer Berlin Heidelberg.

    https://doi.org/10.1007/978-3-642-34500-5_75

Benamira, A., Gerault, D., Peyrin, T., & Tan, Q. Q. (2021). A deeper look at machine learning-based

    cryptanalysis. In A. Canteaut & F.-X. Standaert (Eds.), *Advances in Cryptology – EUROCRYPT 2021*

    (Vol. 12696, pp. 805–835). Springer International Publishing.

    https://doi.org/10.1007/978-3-030-77870-5_28

Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. In A. Boldyreva &

    D. Micciancio (Eds.), *Advances in Cryptology – CRYPTO 2019* (Vol. 11693, pp. 150–179). Springer

    International Publishing. https://doi.org/10.1007/978-3-030-26951-7_6

Goncharov, S. V. (2019). *Using fuzzy bits and neural networks to partially invert few rounds of some*

    cryptographic hash functions. arXiv. https://doi.org/10.48550/ARXIV.1901.02438

Greydanus, S. (2017). *Learning the Enigma with recurrent neural networks* (arXiv:1708.07576). arXiv.

    http://arxiv.org/abs/1708.07576

Liu, G., Lu, J., Li, H., Tang, P., & Qiu, W. (2021). Preimage attacks against lightweight scheme Xoodyak

    based on deep learning. In K. Arai (Ed.), *Advances in Information and Communication* (Vol. 1364,

    pp. 637–648). Springer International Publishing. https://doi.org/10.1007/978-3-030-73103-8_45

Rivest, R. L. (1993). Cryptography and machine learning. In H. Imai, R. L. Rivest, & T. Matsumoto (Eds.),

    Advances in Cryptology—ASIACRYPT '91 (Vol. 739, pp. 427–439). Springer Berlin Heidelberg.

    https://doi.org/10.1007/3-540-57332-1_36

Sharma, N., & Bhatt, R. (2018). Privacy preservation in WSN for healthcare application. *Procedia*

    Computer Science, *132*, 1243–1252. https://doi.org/10.1016/j.procs.2018.05.040

So, J. (2020). Deep learning-based cryptanalysis of lightweight block ciphers. *Security and*