[30] Jithendra, K. B. and Shahana, T.K. New Results in Related Key Impossible Differential Cryptanalysis on Reduced Round AES-192. International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, India; 2018. p. 1-5.

[31] Pammu, A. A., Chong, K. -S., Ho, W.-G., and Gwee, B. -H. Interceptive side channel attack on AES-128 wireless communications for IoT applications. In: IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Jeju, Korea (South); 2016. p. 650-653.

[32] Zhu, L., Wang, Y., and Li, R. Efficient differential fault analysis attacks to AES decryption for low ost sensors in IoTs. In: IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada; 2016. p. 554-557.

[33] Reyhani-masoleh, A., Taha, M., and Ashmawy, D. New Area Record for the AES Combined S-box / Inverse S-box. In: IEEE 25th Symposium on Computer Arithmetic (ARITH), Amherst, MA, USA; 2018. p. 145-152.

[34] Shah, T., Haq, T. U., Farooq, G. Serpent Algorithm: An improvement by 4 × 4 S - box from finite Chain ring. In: International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan; 2018. p. 1-6.

[35] Parikh, P., and Narkhede, S. High performance implementation of mixing of column and inv-mixing of column for AES on FPGA. In: International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), Melmaruvathur, India; 2016. p. 174-179.

[36] Li, H., and Friggstad, Z. An efficient architecture for the AES mix columns operation. In: IEEE International Symposium on Circuits and Systems (ISCAS), Kobe; 2005. vol 5. p. 4637-4640.

[37] Banik, S., Bogdanov, A., and Regazzoni, F. Exploring Energy Efficiency of Lightweight Block Ciphers. In: Dunkelman, O., Keliher, L. (eds) Selected Areas in Cryptography – SAC, Lecture Notes in Computer Science, Springer; 2015. vol 9566.

[38] Zhao, W., Ha, Y., and Alioto, M. AES architectures for minimum energy operation and silicon demonstration in 65nm with lowest energy encryption. In: IEEE International Symposium on Circuits and Systems (ISCAS), Lisbon, Portugal; 2015. p. 2349-2352.

[39] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: Biryukov, A. (eds) Fast Software Encryption. FSE Lecture Notes in Computer Science, Springer, Berlin, Heidelberg; 2007. vol 4593.

[40] Kim, B., Cho, J., Choi, B., Park, J., Seo, H. Compact Implementations of HIGHT Block Cipher on IoT Platforms. Security and Communication Networks. 2019; 5323578: 1-10.

[41] Leander, G., Paar, C., Poschmann, A., Schramm, K. New Lightweight DES Variants. In: Biryukov, A. (eds) Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg; 2007. vol 4593. p. 196-210.

[42] Bogdanov. A., Knudsen, L.R., Leander, G., Paar, C., Poschmann. A., Robshaw, M.J.B., Seurin, Y., and Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds) Cryptographic Hardware and Embedded Systems - CHES. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg; 2007.

[43] Majhi, S., and Mitra, P. Lightweight Cryptographic Techniques in 5G Software-Defined Internet of Things Networking. Lightweight Cryptographic Techniques and Cybersecurity Approaches. 2022. IntechOpen.

[44] Moradi., A. Pushing the Limits: A Very Compact and a Threshold Implementation of AES. In: Advances in Cryptology – EUROCRYPT, Lecture Notes in Computer Science, Springer; 2011. 6632. p. 69-88.

[45] Surendran, S., Nassef, A., & Beheshti, B. D. A survey of cryptographic algorithms for IoT devices. In: IEEE Long Island Systems, Applications and Technology Conference (LISAT); 2018. p. 1-8.

[46] Zhang, X.; Tang, S.; Li, T.; Li, X.; Wang, C. GFRX: A New Lightweight Block Cipher for Resource-Constrained IoT Nodes. Electronics. 2023; 12: 405.

[47] Biswas, A., Majumdar, A., Nath, S. *et al.* LRBC: a lightweight block cipher design for resource constrained IoT devices. J Ambient Intell Human Comput. 2023; 14: 5773–5787.

[48] Roy, S., Roy, S., Biswas, A., Baishnab, K. L. LCB: Light Cipher Block An Ultrafast Lightweight Block Cipher For Resource Constrained IOT Security Applications. KSII Transactions on Internet and Information Systems. 2021; 15(11): 4122-4144.

[49] Rana, M., Mamun, Q., and Islam, R. A block cipher for resource-constrained IoT devices. World Academy of Science, Engineering and Technology. 2023; 17(3): 266-271.

[50] Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., and Wingers, L. The SIMON and SPECK lightweight block ciphers. In: 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA; 2015. p. 1-6.

[51] Rashidi, B. Lightweight Cryptographic S-Boxes Based on Efficient Hardware Structures for Block Ciphers, ISeCure, 2023; 15(1): 137-151.

[52] Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E. Twine: a lightweight, versatile block cipher. In: ECRYPT workshop on lightweight cryptography; 2011, p. 146–169.

[53] Agwa, S., Yahya, E., and Ismail, Y. Power efficient AES core for IoT constrained devices implemented in 130nm CMOS. In: IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA; 2017. p. 1-4.

[54] Bui, D. -H., Puschini, D., Bacles-Min, S., Beigné, E., and Tran, X. -T. AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2017; 25(12): 3281-3290.

[55] Ibrahim, N, and Agbinya, J. Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices. Applied Science. 2023; 13(7): 4398.

[56] Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H., Alkhzaimi, H.A. Cryptography Algorithms for Enhancing IoT Security. Internet of Things. 2023; 22: 100759.