REFERENCES

Aboshosha, B., Dessouky, M., Ramadan, R., & El-Sayed, A. (2019). LCA- Lightweight cryptographic algorithm for IoT constraint resources. In *International Conference on Electronic Engineering* (pp. 374–380). https://doi.org/10.21608/mjeer.2019.67379

Adams, C. M. (1997). Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes, and Cryptography*, *12*, 283–316. https://doi.org/10.1023/A:1008229029587

Al-Dabbagh, S. S. M. (2017). Design 32-bit lightweight block cipher algorithm (DLBCA). *International Journal of Computer Applications*, *166*(8), 17–20. https://doi.org/10.5120/ijca2017914088

Al-Dabbagh, S. S. M., Al Shaikhli, I. F. T., & Alahmad, M. A. (2014). HISEC: A new lightweight block cipher algorithm. In *International Conference on Security of Information and Networks* (pp. 151–156). https://doi.org/10.1145/2659651.2659662

Al-Dabbagh, S. S. M., & Shaikhli, I. F. T. Al. (2013). Improving the security of LBlock lightweight algorithm using bit permutation. In *International Conference on Advanced Computer Science Applications and Technologies* (pp. 296–299). IEEE. https://doi.org/10.1109/ACSAT.2013.65

Al-Dabbagh, S. S. M., & Shaikhli, I. F. T. Al. (2014). OLBCA: A new lightweight block cipher algorithm. In *International Conference on Advanced Computer Science Applications and Technologies* (pp. 15–20). IEEE. https://doi.org/10.1109/ACSAT.2014.10

Al-Dabbagh, S. S. M., Sulaiman, A. G., Al Shaikhli, I. F. T., Al-Enezi, K. A., & Alenezi, A. Y. (2018). Improving the cost factor of DLBCA lightweight block cipher algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(2), 786–791. https://doi.org/10.11591/ijeecs.v10.i2.pp786-791

Al-Rahman, S. Q. A., Sagheer, A. M., & Dawood, O. A. (2018). NVLC: New variant lightweight cryptography algorithm for internet of things. In *Annual International Conference on Information and Sciences* (pp. 176–181). IEEE. https://doi.org/10.1109/AiCIS.2018.00042

Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, *78*(23), 32633–32657. https://doi.org/10.1007/s11042-018-6801-z

Albrecht, M. R., Driessen, B., Kavun, E. B., Leander, G., Paar, C., & Yalçin, T. (2014). Block ciphers - Focus on the linear layer (feat. PRIDE). In *Annual Cryptology Conference* (pp. 57–76). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44371-2_4

Ariffin, S., Mahmod, R., Jaafar, A., & Ariffin, M. R. K. (2011). Immune systems approaches for cryptographic algorithm. *6th International Conference on Bio-Inspired Computing: Theories and Applications*, 231–235. https://doi.org/10.1109/BIC-TA.2011.33

Astuti, N. R. D. P., Arfiani, I., & Aribowo, E. (2019). Analysis of the security level of modified CBC algorithm cryptography using avalanche effect. In *IOP Conference Series: Materials Science and Engineering* (pp. 1–8). https://doi.org/10.1088/1757-899X/674/1/012056

Bajan, P.-M., Kiennert, C., & Debar, H. (2018). A new approach of network simulation for data generation in evaluating security products. In *International Conference on Internet Monitoring and Protection* (pp. 35–41).

Baker, S. A., & Nori, A. S. (2022). A comparison of the randomness analysis of the modified RECTANGLE block cipher and original algorithm. *NTU Journal of Pure Sciences*, *1*(2), 10–21.

Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2015). Midori: A block cipher for low energy. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 411–436). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48800-3_17

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2017). GIFT: A small present towards reaching the limit of lightweight encryption. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 321–345). https://doi.org/10.1007/978-3-319-66787-4_16

Bansod, G., Sutar, S., Patil, A., & Patil, J. (2018). NUX: A lightweight block cipher for security at wireless sensor node level. *International Journal of Bioengineering and Life Sciences*, *5*(1), 1–8.

Bansod, Gaurav. (2016). A new ultra lightweight encryption design for security at node level. *International Journal of Security and Its Applications*, *10*(12), 111–128. https://doi.org/10.14257/ijsia.2016.10.12.10

Bansod, Gaurav, Patil, A., Sutar, S., & Pisharoty, N. (2016). ANU: an ultra lightweight cipher design for security in IoT. *Security and Communication Networks*, *9*(18), 5238–5251. https://doi.org/10.1002/sec.1692

Bansod, Gaurav, Pisharoty, N., & Patil, A. (2016). PICO: An ultra lightweight and low power encryption design for ubiquitous computing. *Defence Science Journal*, *66*(3), 259–265. https://doi.org/10.14429/dsj.66.9276

Bansod, Gaurav, Pisharoty, N., & Patil, A. (2017). BORON: An ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology and Electronic Engineering*, *18*(3), 317–331. https://doi.org/10.1631/FITEE.1500415

Bansod, Gaurav, Pisharoty, N., & Patil, A. (2018a). GRANULE: An ultra lightweight cipher design for embedded security. *IACR Cryptology EPrint Archive*, 1–12.

Bansod, Gaurav, Pisharoty, N., & Patil, A. (2018b). MANTRA: An ultra lightweight cipher design for ubiquitous computing. *International Journal of Ad Hoc and Ubiquitous Computing*, *28*(1), 13–26. https://doi.org/10.1504/IJAHUC.2018.091568

Barreto, P. S. L. M., & Rijmen, V. (2000). The Khazad legacy-level block cipher.

Baysal, A., & Şahin, S. (2015). RoadRunneR: A small and fast bitslice block cipher for low cost 8-bit processors. In *Lightweight Cryptography for Security and Privacy* (pp. 58–76). Springer, Cham. https://doi.org/10.1007/978-3-319-29078-2_4

Beaulieu, R., Shors, D., Smith, J., & Treatman-clark, S. (2013). The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptology EPrint Archive*, 404–449.

Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S. M. (2016). The SKINNY family of block ciphers and its low-latency variant MANTIS. In *Annual International Cryptology Conference* (pp. 123–153). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-53008-5_5

Beierle, C., Leander, G., Moradi, A., & Rasoolzadeh, S. (2019). CRAFT: Lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Transactions on Symmetric Cryptology*, *1*, 5–45. https://doi.org/10.13154/tosc.v2019.i1.5-45

Berger, T. P., Francq, J., & Minier, M. (2015). CUBE cipher: A family of quasi-involutive block ciphers easy to mask. In *International Conference on Codes, Cryptology, and Information Security* (pp. 89–105). Springer, Cham. https://doi.org/10.1007/978-3-319-18681-8_8

Berger, T. P., Francq, J., Minier, M., & Thomas, G. (2015). Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: LILLIPUT. *IEEE Transactions on Computers*, *65*(7), 2074–2208. https://doi.org/10.1109/TC.2015.2468218

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, *4*(1), 3–72. https://doi.org/10.1007/BF00630563

Biham, E., & Shamir, A. (1993). *Differential cryptanalysis of the Data Encryption Standard*. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag.

Biswas, A., Majumdar, A., Nath, S., Dutta, A., & Baishnab, K. L. (2020). LRBC: A lightweight block cipher design for resource constrained IoT devices. *Journal of Ambient Intelligence and Humanized Computing*, 1–15. https://doi.org/10.1007/s12652-020-01694-9

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 450–466). Springer-Verlag.

Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., Yalçin, T. (2012). PRINCE - A low-latency block cipher for pervasive computing applications. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 208–225). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_14

Boura, C., Canteaut, A., & Coggia, D. (2019). A general proof framework for recent AES distinguishers. *IACR Transactions on Symmetric Cryptology*, 170–191. https://doi.org/10.13154/tosc.v2019.i1.170-191

Buja, A. G. (2018). *Security analysis techniques using differential relationships for block ciphers*. Ph.D Thesis. Universiti Teknikal Malaysia Melaka.

Caelli, W., Dawson, E., Nielsen, L., & Gustafson, H. (1992). *CRYPT–X statistical package manual, measuring the strength of stream and block ciphers*. Queensland University of Technology.

Cazorla, M., Marquet, K., & Minier, M. (2013). Survey and benchmark of lightweight block ciphers for wireless sensor networks. In *International Conference on Security and Cryptography* (pp. 1–6). IEEE. https://doi.org/10.5220/0004530905430548

Chen, B. W., Xia, X., Liang, Q. M., & Zhong, W. D. (2021). Lightweight design of SM4 algorithm and realization of threshold scheme. In *Journal of Physics: Conference Series* (pp. 1–14). https://doi.org/10.1088/1742-6596/1871/1/012124

Chen, Z., Chen, J., Meng, W., Teh, J. Sen, Li, P., & Ren, B. (2020). Analysis of differential distribution of lightweight block cipher based on parallel processing on GPU. *Journal of Information Security and Applications*, *55*, 1–10. https://doi.org/10.1016/j.jisa.2020.102565

Cheng, H., Heys, H. M., & Wang, C. (2008). PUFFIN: A novel compact block cipher targeted to embedded digital systems. In *EUROMICRO Conference on Digital System Design Architectures, Methods and Tools* (pp. 383–390). IEEE. https://doi.org/10.1109/DSD.2008.34

CSM. (2021). MySEAL - National Trusted Cryptographic Algorithm List. Retrieved August 9, 2021, from https://myseal.cybersecurity.my/en/index.html

Cui, T., & Jin, C. (2017). Classification of SPN structures from the viewpoint of structural cryptanalysis. *IEEE Access*, *6*, 9733–9739. https://doi.org/10.1109/ACCESS.2017.2784543

D'souza, F. J., & Panchal, D. (2018). Design and implementation of AES using hybrid approach. In *International Conference on Power Energy, Environment and Intelligent Control* (pp. 517–521). IEEE. https://doi.org/10.1109/PEEIC.2018.8665586

Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-The Advanced Encryption Standard*. *Springer Science & Business Media*.

Dahiphale, V., Bansod, G., & Patil, J. (2018). ANU-II: A fast and efficient lightweight encryption design for security in IoT. In *2017 International Conference on Big Data, IoT and Data Science, BID 2017* (pp. 130–137). IEEE. https://doi.org/10.1109/BID.2017.8336586

Dahiphale, V., Raut, H., & Bansod, G. (2019). Design and implementation of novel datapath designs of lightweight cipher RECTANGLE for resource constrained environment. *Multimedia Tools and Applications*, *78*(16), 23659–23688. https://doi.org/10.1007/s11042-019-7587-3

Dai, X., Huang, Y., Chen, L., Lu, T., & Su, F. (2015). VH: A lightweight block cipher based on dual pseudo-random transformation. In *International Conference on Cloud Computing and Security* (pp. 3–13). Springer, Cham. https://doi.org/10.1007/978-3-319-27051-7_1

Das, S. (2014). Halka: A lightweight, software friendly block cipher using ultra-lightweight 8-bit S-box. *IACR Cryptology EPrint Archive*, 1–16.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society*, *19*(1), 161–180.

De Cannière, C., Dunkelman, O., & Knežević, M. (2009). KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 272–288). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04138-9_20

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. *Wireless Personal Communications*, *112*, 1947–1980. https://doi.org/10.1007/s11277-020-07134-3

Dinu, D. D. (2017). *Efficient and secure implementations of lightweight symmetric cryptographic primitives*. Ph.D Thesis. University of Luxembourg.

Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., & Biryukov, A. (2016). Design strategies for ARX with provable bounds: Sparx and LAX (Full Version)⋆. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 484–513). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-53887-6_18

Do Nascimento, E. M., & Xexeo, J. A. M. (2017). A flexible authenticated lightweight cipher using Even-Mansour construction. In *IEEE International Conference on Communications* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2017.7996734

Dobraunig, C., Rotella, Y., & Schoone, J. (2020). Algebraic and higher-order differential cryptanalysis of Pyjamask-96. *IACR Transactions on Symmetric Cryptology*, *1*, 289–312. https://doi.org/10.13154/tosc.v2020.i1.289-312

Encarnacion, P. C., Gerardo, B. D., & Hernandez, A. A. (2020). Modified round function of SIMECK 32/64 block cipher. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1), 258–266.

Engels, D., Fan, X., Gong, G., Hu, H., & Smith, E. M. (2010). Hummingbird: Ultra-lightweight cryptography for resource-constrained devices. In *International Conference on Financial Cryptography and Data Security* (pp. 3–18). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14992-4_2

Engels, D., Saarinen, M.-J. O., Schweitzer, P., & Smith, E. M. (2011). The Hummingbird-2 lightweight authenticated encryption algorithm. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (pp. 19–31). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25286-0_2

ETSI. (2014). *Universal mobile telecommunications system (UMTS); LTE; 3G security; specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi specification (3GPP TS 35.202 version 12.0.0 Release 12).*

Feizi, S., Nemati, A., Ahmadi, A., & Makki, V. A. (2015). A high-speed FPGA implementation of a bit-slice ultra-lightweight block cipher, RECTANGLE. In *5th International Conference on Computer and Knowledge Engineering* (pp. 206–211). IEEE.

Girija, M., Manickam, P., & Ramaswami, M. (2020). PriPresent: An embedded prime lightweight block cipher for smart devices. *Peer-to-Peer Networking and Applications*, *14*, 1–11. https://doi.org/10.1007/s12083-020-00992-5

Gong, Z., Nikova, S., & Law, Y. W. (2011). KLEIN: A new family of lightweight block ciphers. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (pp. 1–18). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25286-0_1

Guo, J., Peyrin, T., & Poschmann, A. (2011). The PHOTON Family of Lightweight Hash Functions. In *Advances in Cryptology - CRYPTO 2011* (pp. 222–239). Springer. https://doi.org/10.1007/978-3-642-22792-9_13

Guo, J., Peyrin, T., Poschmann, A., & Robshaw, M. (2011). The LED block cipher*. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 326–341). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_22

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, *8*(2), 141–184. https://doi.org/10.1007/s13389-017-0160-y

Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*, *26*(3), 189–221. https://doi.org/10.1080/0161-110291890885

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S. (2006). HIGHT: A new block cipher suitable for low-resource device. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 46–59). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_4

Imdad, M., Ramli, S. N., & Mahdin, H. (2022). An enhanced key schedule algorithm of PRESENT-128 block cipher for random and non-random secret keys. *Symmetry*, *14*, 1–22.

Isa, H., & Z'aba, M. R. (2012). Randomness analysis on LED block ciphers. In *5th International Conference on Security of Information and Networks* (pp. 60–66). https://doi.org/10.1145/2388576.2388584

Izadi, M., Sadeghiyan, B., Sadeghian, S. S., & Khanooki, H. A. (2009). MIBS: A new lightweight block cipher. In *International Conference on Cryptology and Network Security* (pp. 334–348). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-10433-6_22

Jallouli, O., El Assad, S., & Chetto, M. (2016). Robust chaos-based stream-cipher for secure public communication channels. In *11th International Conference for Internet Technology and Secured Transactions* (pp. 23–26). IEEE. https://doi.org/10.1109/ICITST.2016.7856658

Javeed, A., Shah, T., & Ullah, A. (2020). Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group. *Wireless Personal Communications*, 1–14. https://doi.org/10.1007/s11277-020-07052-4

Jha, P., Zorkta, H. Y., Allawi, D., & Al-Nakkar, M. R. (2020). Improved lightweight encryption algorithm (ILEA). In *International Conference for Emerging Technology* (pp. 1–4). IEEE. https://doi.org/10.1109/INCET49848.2020.9154170

Jithendra, K. B., & Kassim, S. T. (2020). ACT: An ultra-light weight block cipher for internet of things. *International Journal of Computing and Digital Systems*, *9*(5), 921–929. https://doi.org/10.12785/ijcds/090512

John, J. (2014). BEST-1: A light weight block cipher. *IOSR Journal of Computer Engineering*, *16*(2), 91–95. https://doi.org/10.9790/0661-162129195

Kanjo, E., Kuss, D. J., & Ang, C. S. (2017). NotiMind: Utilizing responses to smart phone notifications as affective sensors. *IEEE Access*, *5*, 22023–22035. https://doi.org/10.1109/ACCESS.2017.2755661

Knudsen, L., Leander, G., Poschmann, A., & Robshaw, M. J. B. (2010). PRINTcipher: A block cipher for IC-printing. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 16–32). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-15031-9_2

Knuth, D. E. (1998). *The art of computer programming. Volume 2: Seminumerical algorithms.* Addison-Wesley, Reading, Massachusetts.

Kolay, S., & Mukhopadhyay, D. (2014). Khudra: A new lightweight block cipher for FPGAs. In *International Conference on Security, Privacy, and Applied Cryptography Engineering* (pp. 126–145). Springer, Cham.

Koo, B., Roh, D., Kim, H., Jung, Y., Lee, D. G., & Kwon, D. (2017). CHAM: A family of lightweight block ciphers for resource-constrained devices. In *International Conference on Information Security and Cryptology* (pp. 3–25). Springer, Cham. https://doi.org/10.1007/978-3-319-78556-1_1

Kosuge, H., Tanaka, H., Iwai, K., & Kurokawa, T. (2016). Integral attack on reduced-round RECTANGLE. In *2nd IEEE International Conference on Cyber Security and Cloud Computing* (pp. 68–73). https://doi.org/10.1109/CSCloud.2015.15

Krishna, B. M., Anusha, K., Kiran, C. K., Rajyalaxmi, K. P., Rao, S. H., Sujith, S. J., & Rishi, S. (2018). FPGA implementation of asymmetric cryptography techniques. *International Journal of Pure and Applied Mathematics, 119*(7), 489–504.

Kubba, Z. M. J., & Hoomod, H. K. (2019). A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system. In *International Conference of Computer and Applied Sciences* (pp. 199–203). IEEE. https://doi.org/10.1109/CAS47993.2019.9075488

Kulah, Y., Dincer, B., Yilmaz, C., & Savas, E. (2019). SpyDetector: An approach for detecting side-channel attacks at runtime. *International Journal of Information Security*, *18*(4), 393–422. https://doi.org/10.1007/s10207-018-0411-7

Kumar, M., Pal, S., & Panigrahi, A. (2019). FeW: A lightweight block cipher. *Turkish Journal of Mathematics and Computer Science, 11*(2), 58–73. https://doi.org/10.13140/2.1.3035.7126

Lai, X., & Massey, J. L. (1991). A proposal for a new block encryption standard. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 389–404). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-46877-3_35

Leander, G., Paar, C., Poschmann, A., & Schramm, K. (2007). New lightweight DES variants. In *International Workshop on Fast Software Encryption* (pp. 196–210). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_13

Lerman, L., Nakahara, J., & Veshchikov, N. (2013). Improving block cipher design by rearranging internal operations. In *International Conference on Security and Cryptography* (pp. 1–12). IEEE. https://doi.org/10.5220/0004498200270038

Li, L., Liu, B., & Wang, H. (2016). QTL: A new ultra-lightweight block cipher. *Microprocessors and Microsystems*, *45*, 45–55. https://doi.org/10.1016/j.micpro.2016.03.011

Li, L., Liu, B., Zhou, Y., & Zou, Y. (2018). SFN: A new lightweight block cipher. *Microprocessors and Microsystems*, *60*, 138–150. https://doi.org/10.1016/j.micpro.2018.04.009

Li, P., Zhou, S., Ren, B., Tang, S., Li, T., Xu, C., & Chen, J. (2019). Efficient implementation of lightweight block ciphers on volta and pascal architecture. *Journal of Information Security and Applications*, *47*, 235–245. https://doi.org/10.1016/j.jisa.2019.04.006

Lim, C. H., & Korkishko, T. (2005). mCrypton - A lightweight block cipher for security of low-cost RFID tags and sensors. In *International Workshop on Information Security Applications* (pp. 243–258). Springer Berlin Heidelberg. https://doi.org/10.1007/11604938_19

Liu, B. T., Li, L., Wu, R. X., Xie, M. M., & Li, Q. P. (2019). Loong: A family of involutional lightweight block cipher based on SPN structure. *IEEE Access*, *7*, 136023–136035. https://doi.org/10.1109/ACCESS.2019.2940330

Liu, J., Li, W., & Bai, G. (2018). An improved s-box of lightweight block cipher Roadrunner for hardware optimization. In *China Semiconductor Technology International Conference* (pp. 1–4). IEEE. https://doi.org/10.1109/CSTIC.2018.8369335

Liu, X., Zhang, W. Y., Liu, X. Z., & Liu, F. (2014). Eight-sided fortress: A lightweight block cipher. *Journal of China Universities of Posts and Telecommunications*, *21*(1), 104–128. https://doi.org/10.1016/S1005-8885(14)60275-2

Mala, H. (2014). Unified byte permutations for the block cipher 3D. *Journal of Computing and Security*, *1*(1), 15–22.

Malutan, S. B., Dragomir, I. R., Lazar, M., & Vitan, D. (2019). HERMES, a proposed lightweight block cipher used for limited resource devices. In *International Conference on Speech Technology and Human-Computer Dialogue* (pp. 1–6). IEEE. https://doi.org/10.1109/SPED.2019.8906563

Marsaglia, G. (1995). The Marsaglia random number CDROM including the Diehard battery of tests of randomness. Retrieved from http://www.stat.fsu.edu/pub/diehard

Massey, J. L. (1993). SAFER K-64: A byte-oriented block-ciphering algorithm. In *International Workshop on Fast Software Encryption* (pp. 1–17). Springer, Berlin, Heidelberg.

Matsui, M. (1993). Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 386–397). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48285-7_33

Matsui, M. (1997). New block encryption algorithm MISTY. In *International Workshop on Fast Software Encryption* (pp. 54–68). Springer, Berlin, Heidelberg. https://doi.org/10.1007/bfb0052334

McKay, K. A., Bassham, L., Turan, M. S., & Mouha, N. (2017). *Report on lightweight cryptography*. NIST Internal or Interagency Report (NISTIR) 8369. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf

Modi, P., Singh, P., & Acharya, B. (2021). Multiplexer-based high-speed S-box architecture for PRESENT cipher in FPGA. In *Lecture Notes in Electrical Engineering* (pp. 643–652). https://doi.org/10.1007/978-981-15-7486-3_55

Mushtaq, M. F., Jamel, S., Megat, S. R. B., Akram, U., & Deris, M. M. (2019). Key schedule algorithm using 3-dimensional hybrid cubes for block cipher. *International Journal of Advanced Computer Science and Applications*, *10*(8), 427–442. https://doi.org/10.14569/ijacsa.2019.0100857

Nakahara, J. (2008). 3D: A three-dimensional block cipher. In *International Conference on Cryptology and Network Security* (pp. 252–267). Springer, Berlin, Heidelberg.

Nascimento, E. M. do, & Xexéo, J. A. M. (2019). FlexAEAD v1.1 -A lightweight AEAD cipher with integrated authentication. *Journal of Information Security and Cryptography (Enigma)*, *6*(1), 15–24. https://doi.org/10.17648/jisc.v6i1.74

Naser, N. M., & Naif, J. R. (2022). A systematic review of ultra-lightweight encryption algorithms. *International Journal of Nonlinear Analysis and Applications*, *13*(1), 3825–3851.

Nayancy, Dutta, S., & Chakraborty, S. (2020). A survey on implementation of lightweight block ciphers for resource constraints devices. *Journal of Discrete Mathematical Sciences and Cryptography*, 1–22. https://doi.org/10.1080/09720502.2020.1766764

NSA. (1998). Skipjack and KEA Algorithm Specifications.

O'Dea, S. (2021). Forecast number of mobile users worldwide 2020-2025. Retrieved March 15, 2022, from https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/

Omrani, T., Becheikh, R., Mannai, O., Rhouma, R., & Belghith, S. (2018). RARE: A robust algorithm for rapid encryption. In *International Conference for Internet Technology and Secured Transactions* (pp. 23–28). IEEE. https://doi.org/10.23919/ICITST.2017.8356339

Omrani, T., Rhouma, R., & Becheikh, R. (2019). LICID: A lightweight image cryptosystem for IoT devices. *Cryptologia*, *43*(4), 313–343. https://doi.org/10.1080/01611194.2018.1563009

Omrani, T., Rhouma, R., & Sliman, L. (2018). Lightweight cryptography for resource-constrained devices: A comparative study and rectangle cryptanalysis. In *International Conference on Digital Economy* (pp. 107–118).

Patil, A., Bansod, G., & Pisharoty, N. (2015). Hybrid lightweight and robust encryption design for security in IoT. *International Journal of Security and Its Applications*, *9*(12), 85–98. https://doi.org/10.14257/ijsia.2015.9.12.10

Patil, J., Bansod, G., & Kant, K. S. (2017). LiCi: A new ultra-lightweight block cipher. In *International Conference on Emerging Trends and Innovation in ICT* (pp. 40–45). IEEE. https://doi.org/10.1109/ETIICT.2017.7977007

Patil, J., Bansod, G., & Kant, K. S. (2019). DoT: A new ultra-lightweight SP network encryption design for resource-constrained environment. In *International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing* (pp. 249–257). Springer, Singapore. https://doi.org/10.1007/978-981-13-1610-4_26

Pawar, S. V, & Pattanshetti, T. R. (2018). Lightweight cryptography: A survey. *International Research Journal of Engineering and Technology*, *5*(5), 3911–3915.

Pehlivanoğlu, M. K., Sakalli, M. T., Akleylek, S., & Duru, N. (2017). On the design strategies of diffusion layers and key schedule in lightweight block ciphers. In *International Conference on Computer Science and Engineering* (pp. 456–461). IEEE. https://doi.org/10.1109/UBMK.2017.8093436

Poschmann, A., Ling, S., & Wang, H. (2010). 256 bit standardized crypto for 650 GE - GOST revisited. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 219–233). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15031-9_15

Preneel, B. (2002). New European schemes for signature, integrity and encryption (NESSIE): A status report. In *International Workshop on Public Key Cryptography* (pp. 297–309). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45664-3_21

Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2018). Cryptography methods for software-defined wireless sensor networks. In *IEEE 27th International Symposium on Industrial Electronics* (pp. 1257–1262). https://doi.org/10.1109/ISIE.2018.8433630

Rahim, N., Ahmad, J., Muhammad, K., Sangaiah, A. K., & Baik, S. W. (2018). Privacy-preserving image retrieval for mobile devices with deep features on the cloud. *Computer Communications*, *127*, 75–85. https://doi.org/10.1016/j.comcom.2018.06.001

Ramadan, R. A., Aboshosha, B. W., Yadav, K., Alseadoon, I. M., Kashout, M. J., & Elhoseny, M. (2021). LBC-IoT: Lightweight block cipher for IoT constraint devices. *Computers, Materials and Continua*, *67*(3), 3563–3579. https://doi.org/10.32604/cmc.2021.015519

Ramudu, S., & Shanthi, G. (2015). Implementation of an ultra-lightweight block cipher. *International Journal & Magazine of Engineering, Technology, Management and Research*, *2*(2), 233–243.

Rivest, R. L. (1994). The RC5 encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 86–96). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-60590-8_7

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. *NIST Special Publication 800-22 Revision 1a*. Retrieved from http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Sahasrabuddhe, A., & Laiphrakpam, D. S. (2021). Multiple images encryption based on 3D scrambling and hyper-chaotic system. *Information Sciences*, *550*, 252–267. https://doi.org/10.1016/j.ins.2020.10.031

Sakamoto, K., Minematsu, K., Shibata, N., Shigeri, M., Kubo, H., Funabiki, Y., Bogdanov, A., Morioka, S., Isobe, T. (2020). Tweakable TWINE: Building a tweakable block cipher on generalized Feistel structure. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *103*(12), 1629–1639. https://doi.org/10.1587/transfun.2019EAP1141

Salam, A., Setiadi, D. R. I. M., Rachmawanto, E. H., & Sari, C. A. (2019). ShiftMod cipher: A symmetrical cryptosystem scheme. In *International Seminar on Application for Technology of Information and Communication* (pp. 1–5). IEEE. https://doi.org/10.1109/ISEMANTIC.2019.8884321

Sallam, A. I., Faragallah, O. S., & El-Rabaie, E. S. M. (2017). HEVC selective encryption using RC6 block cipher technique. *IEEE Transactions on Multimedia*, *20*(7), 1636–1644. https://doi.org/10.1109/TMM.2017.2777470

Salunke, R., Bansod, G., & Naidu, P. (2019). Design and implementation of a lightweight encryption scheme for wireless sensor nodes. In *Advances in Intelligent Systems and Computing* (pp. 566–581). Springer, Cham. https://doi.org/10.1007/978-3-030-22868-2_41

Santos, R. J., Vieira, M., & Bernardino, J. (2016). XSX: Lightweight encryption for data warehousing environments. In *International Conference on Big Data Analytics and Knowledge Discovery* (pp. 281–295). Springer, Cham. https://doi.org/10.1007/978-3-319-43946-4_19

Schneier, B. (1993). Description of a new variable-length key, 64-bit block cipher (Blowfish). In *International Workshop on Fast Software Encryption* (pp. 191–204). Springer, Berlin, Heidelberg.

Sehrawat, D., & Gill, N. S. (2018). Lightweight block ciphers for IoT based applications: A review. *International Journal of Applied Engineering Research, 13*(5), 2258–2270.

Sehrawat, D., & Gill, N. S. (2019). BRIGHT: A small and fast lightweight block cipher for 32-bit processor. *International Journal of Engineering and Advanced Technology*, *8*(5), 1549–1556.

Sehrawat, D., & Gill, N. S. (2020). Ultra BRIGHT: A tiny and fast ultra lightweight block cipher for IoT. *International Journal of Scientific and Technology Research*, *9*(2), 1063–1068.

Selvam, R., Shanmugam, D., & Annadurai, S. (2014). Side channel attacks: Vulnerability analysis of PRINCE and RECTANGLE using DPA. *Cryptology EPrint Archive*, 1–15.

Selvam, Ravikumar, Shanmugam, D., & Annadurai, S. (2015). Vulnerability analysis of PRINCE and RECTANGLE using CPA. In *1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015* (pp. 81–87). https://doi.org/10.1145/2732198.2732207

Senol, A. (2017). *Improved differential attacks on RECTANGLE*. Master's Thesis. Middle East Technical University.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shantha, M. J. R., & Arockiam, L. (2018). SAT-Jo: An enhanced lightweight block cipher for the Internet of Things. In *International Conference on Intelligent Computing and Control Systems* (pp. 1146–1150). IEEE. https://doi.org/10.1109/ICCONS.2018.8663068

Shantha Mary Joshitta, R., & Arockiam, L. (2018). A novel block cipher for enhancing data security in healthcare internet of things. In *Journal of Physics: Conference Series* (pp. 1–11). https://doi.org/10.1088/1742-6596/1142/1/012002

Sherine, J. R., Sudhakar, R., & Karthikpriya, M. (2021). Design of compact S Box for resource constrained applications. In *Journal of Physics: Conference Series* (pp. 1–12). https://doi.org/10.1088/1742-6596/1767/1/012059

Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., & Shirai, T. (2011). Piccolo : An ultra-lightweight blockcipher. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 342–357). Springer, Berlin, Heidelberg.

Singh, P., Acharya, B., & Chaurasiya, R. K. (2019). A comparative survey on lightweight block ciphers for resource constrained applications. *International Journal of High Performance Systems Architecture*, *8*(4), 250–270. https://doi.org/10.1504/IJHPSA.2019.104953

Soto, J. (1999). *Randomness testing of the Advanced Encryption Standard candidate algorithms*. *NIST Internal or Interagency Report (NISTIR) 6390*. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151193

Standaert, François Xavier, Piret, G., Gershenfeld, N., & Quisquater, J. J. (2006). SEA: A scalable encryption algorithm for small embedded applications. In *International Conference on Smart Card Research and Advanced Applications* (pp. 222–236). Springer, Berlin, Heidelberg. https://doi.org/10.1007/11733447_16

Standaert, Francois Xavier, Piret, G., Rouvroy, G., Quisquater, J. J., & Legat, J. D. (2004). ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware. In *International Workshop on Fast Software Encryption* (pp. 279–298). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-25937-4_18

Suri, P. R., & Deora, S. S. (2011). 3D array block rotation cipher: An improvement using lateral shift. *Global Journal of Computer Science and Technology*, *11*(19), 17–23.

Suzaki, T., Minematsu, K., Morioka, S., & Kobayashi, E. (2011). Twine: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography* (pp. 146–169). Springer Berlin Heidelberg.

Tezcan, C. (2020). Analysis of Ascon, DryGASCON, and Shamash permutations. *International Journal of Information Security Science*, *9*(3), 172–187.

Tezcan, C., Okan, G. O., Senol, A., Dogan, E., Yucebas, F., & Baykal, N. (2016). Differential attacks on lightweight block ciphers PRESENT, PRIDE, and RECTANGLE revisited. In *International Workshop on Lightweight Cryptography for Security and Privacy* (pp. 18–32). Springer, Cham. https://doi.org/10.1007/978-3-319-55714-4

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*, *9*, 28177–28193. https://doi.org/10.1109/ACCESS.2021.3052867

Thorat, C., Inamdar, V., & Jadhav, B. (2020). TED: A lightweight block cipher for IoT devices with side-channel attack resistance. *International Journal on Information Technologies & Security*, *12*(2), 83–96.

Toprak, S., Akbulut, A., Aydın, M. A., & Zaim, A. H. (2020). LWE: An energy-efficient lightweight encryption algorithm for medical sensors and IoT devices. *Electrica*, *20*(1), 71–81.

Turan, M. S., McKay, K. A., Çalık, Ç., Chang, D., & Bassham, L. (2021). *Status report on the first round of the NIST lightweight cryptography standardization process. NIST Internal or Interagency Report (NISTIR) 8369*. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8268.pdf

Usman, M., Ahmed, I., Imran, M., Khan, S., & Ali, U. (2017). SIT: A lightweight encryption algorithm for secure Internet of Things. *International Journal of Advanced Computer Science and Applications*, *8*(1), 402–411. https://doi.org/10.14569/ijacsa.2017.080151

Verma, G., Liao, M., Lu, D., He, W., Peng, X., & Sinha, A. (2019). An optical asymmetric encryption scheme with biometric keys. *Optics and Lasers in Engineering*, *116*, 32–40. https://doi.org/10.1016/j.optlaseng.2018.12.010

Wang, C., & Heys, H. M. (2009). An ultra compact block cipher for serialized architecture implementations. In *Canadian Conference on Electrical and Computer Engineering* (pp. 1085–1090). IEEE. https://doi.org/10.1109/CCECE.2009.5090296

Wang, Q., & Jin, C. (2018). A non-alternate 3D structure and its practical security evaluation against differential and linear cryptanalysis. *Science China Information Sciences*, *61*(5), 1–3. https://doi.org/10.1007/s11432-017-9181-4

Wheeler, D. J., & Needham, R. M. (1994). TEA, a tiny encryption algorithm. In *International Workshop on Fast Software Encryption* (pp. 363–366). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-60590-8_29

Wu, W., & Zhang, L. (2011). LBlock : A lightweight block cipher. In *International Conference on Applied Cryptography and Network Security* (pp. 327–344). Springer, Berlin, Heidelberg.

Xiang, Z., Zeng, X., Lin, D., Bao, Z., & Zhang, S. (2020). Optimizing implementations of linear layers. *IACR Transactions on Symmetric Cryptology*, *2020*(2), 120–145. https://doi.org/10.13154/tosc.v2020.i2.120-145

Yan, H., Luo, Y., Chen, M., & Lai, X. (2019). New observation on the key schedule of RECTANGLE. *Science China Information Sciences*, *62*(3). https://doi.org/10.1007/s11432-018-9527-8

Yang, G., Zhu, B., Suder, V., Aagaard, M. D., & Gong, G. (2015). The Simeck family of lightweight block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 307–329). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48324-4_16

Yap, H., Khoo, K., Poschmann, A., & Henricksen, M. (2011). EPCBC - A block cipher suitable for electronic product code encryption. In *International Conference on Cryptology and Network Security* (pp. 76–97). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-25513-7_7

Yeoh, W. Z., Teh, J. Sen, & Sazali, M. I. S. B. M. (2020). µ2: A Lightweight block cipher. In *Computational Science and Technology* (pp. 281–290). Springer, Singapore. https://doi.org/10.1007/978-981-15-0058-9_27

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020a). Extended RECTANGLE algorithm using 3D bit rotation to propose a new lightweight block cipher for IoT. *IEEE Access*, *8*, 198646–198658. https://doi.org/10.1109/access.2020.3035375

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020b). Modifications of key schedule algorithm on RECTANGLE block cipher. In *International Conference on Advances in Cyber Security* (pp. 194–206). Springer, Singapore.

Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020*c*). Randomness analysis on RECTANGLE block cipher. In *Cryptology and Information Security Conference 2020* (pp. 133–142).

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, *58*(12), 1–15. https://doi.org/10.1007/s11432-015-5459-7

Zhang, W., Bao, Z., Rijmen, V., & Liu, M. (2015). A new classification of 4-bit optimal s-boxes and its application to PRESENT, RECTANGLE and SPONGENT. In *International Workshop on Fast Software Encryption* (pp. 494–515).

Zhou, C., Zhang, W., Ding, T., & Xiang, Z. (2019). Improving the MILP-based security evaluation algorithm against differential/linear cryptanalysis using a divide-and-conquer approach. *IACR Transactions on Symmetric Cryptology*, *4*, 438–469. https://doi.org/10.13154/tosc.v2019.i4.438-469

Zhou, L., Su, C., Wen, Y., Li, W., & Gong, Z. (2018). Towards practical white-box lightweight block cipher implementations for IoTs. *Future Generation Computer Systems*, *86*, 507–514. https://doi.org/10.1016/j.future.2018.04.011

Zhu, B., Dong, X., & Yu, H. (2019). MILP-based differential attack on round-reduced GIFT. In *Cryptographers' Track at the RSA Conference* (pp. 372–390). Springer, Cham. https://doi.org/10.1007/978-3-030-12612-4_19

Zhu, R., Zhang, X., Liu, X., Shu, W., Mao, T., & Jalaian, B. (2015). ERDT: Energy-efficient reliable decision transmission for intelligent cooperative spectrum sensing in industrial IoT. *IEEE Access*, *3*, 2366–2378. https://doi.org/10.1109/ACCESS.2015.2501644