Evaluating Lightweight Cryptographic Standards for IoT: Design, Metrics, and Security Insights

Adarsh Jiju David
Dept. of Information Technology
Toc H Institute of Science & Technology
Ernakulam, India

Alan James Robert
Dept. of Information Technology
Toc H Institute of Science & Technology
Ernakulam, India

Aswin Mammen
Dept. of Information Technology
Toc H Institute of Science & Technology
Ernakulam, India

Eldhose Babichan
Dept. of Information Technology
Toc H Institute of Science & Technology
Ernakulam, India

Sandhya C.P.
Dept. of Information Technology
Toc H Institute of Science & Technology
Ernakulam, India

ABSTRACT

The rapid growth of Internet of Things (IoT) applications in domains such as healthcare, industrial systems, smart environments, and defence requires secure communication for devices, even when they operate with very low power, limited storage, or slow processors. Traditional cryptographic algorithms such as AES, although secure, demand significant processing power and hardware resources, making them unsuitable for constrained platforms. This challenge motivates the adoption of lightweight cryptography, which is specifically designed to deliver strong protection with minimal resource usage. This paper presents a survey of lightweight cryptographic algorithms tailored for IoT and embedded environments, analyzing their characteristics based on parameters such as block size, key size, number of rounds, throughput, and gate equivalents. Drawing on recent benchmarking studies and comparative evaluations, it highlights design trade-offs, security considerations, and implementation challenges. From this analysis, it is observed that lightweight algorithms achieve a more favorable balance of efficiency, robustness, and scalability, offering valuable guidance for selecting optimal cryptographic solutions in resource-constrained IoT deployments.

General Terms

IoT, Lightweight block ciphers, PRESENT, TEA, LED, ASCON, SPECK, SIMON, KATAN, LEA

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has helped in a new era of penetrating the smart devices, varying from low-power sensors and RFID tags to embedded microcontrollers in applications such as smart homes, healthcare, industrial automation, and environmental monitoring. A major limitation of IoT devices is resource-constrained. These constraints create challenges for implementing a strong cryptographic security. Hence, to provide tamper resistant software and hardware security functions in the resource constrained embedded systems like RFIDs, sensor networks and IoT devices, lightweight ciphers were introduced [22][24].

The lightweight cryptography plays an important role to resolve this critical gap. The primary goal of these algorithms is to balance security with low cost like power consumption and performance such as latency, throughput etc. and security. It enables confidentiality, integrity and authentication in the limited platforms [2][21]. It enables deployment in ultra resource-constraints through compact S-boxes, reduced round counts and simplified key schedules.

Lightweight cryptography is a specialized branch of cryptographic technique made for resource-constrained devices such as IoT, embedded systems, RFID tags and wireless sensor networks. For the standard ciphers like AES, they need more memory, power and computing power whereas, in lightweight block ciphers they are optimized for with fewer resources. Lightweight block ciphers play a vital role in meeting core security requirements such as confidentiality, data integrity, and authentication without overwhelming constrained devices and also reduce the power use and delay [21]. They use specialized architectures like Substitution-Permutation Networks (SPN), Feistel networks, Generalized Feistel networks (GFN), Hybrid models. This helped to obtain good cryptographic properties such as nonlinearity, balanced output, and prevent from differential and linear attacks. Lightweight ciphers are symmetric ciphers and can be classified as block ciphers and stream ciphers.

This paper presents a focused survey of selected lightweight cryptographic algorithms, critically analyzing their performance in the context of IoT and resource-constrained applications. It provides a unified framework for comparing key characteristics—including implementation metrics, hardware/software efficiency, and attack resistance—drawing upon recent benchmarking efforts and comparative studies [20][23]. Through this review, the study aims to elucidate current design trends, highlight practical challenges, and offer guidance for selecting optimal solutions in emerging IoT environments.

This paper is a survey of selected Lightweight cryptographic algorithms, analyse each algorithm through parameters like Key size, block size, throughput etc. based on some recent benchmarking studies. and identify its practical challenges and choose suitable algorithms for IoT.

2. LIGHTWEIGHT BLOCK CIPHERS

2.1 PRESENT

PRESENT is a standardized lightweight block cipher designed for resource-constrained environments such as IoT devices, RFID tags, and embedded systems. It operates on block of 64-bit with key sizes either of 80 or 128 bits. The cipher follows a Substitution–Permutation Network (SPN) structure consisting of 31 rounds, each including AddRoundKey, Substitution, and Permutation steps. Compared to AES, PRESENT is optimized for low power, low memory usage, and minimal logic gates, making it highly suitable for lightweight applications. Due to these features, PRESENT is widely regarded as a benchmark lightweight cipher for secure hardware in constrained environments [12][13][14].

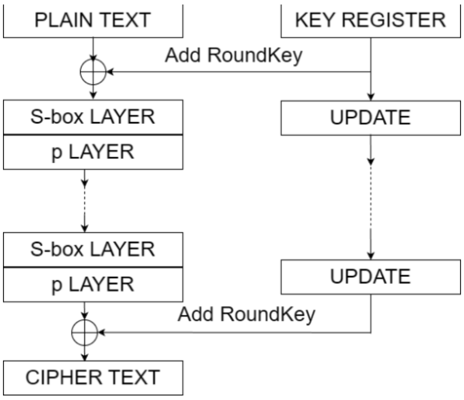

Fig 1 Block Diagram of the PRESENT cipher

2.2 TEA

The Tiny Encryption Algorithm is a lightweight block cipher which can be implemented within a 1500GE and designed for compact size and efficiency. It is suitable for resource-constrained devices like IoT, RFID tags and embedded systems. TEA operates on a 64-bit block size, a 128-bit key size, and it has Feistel structure. Where each round involves modular addition, XOR and shifts. The algorithm has the drawback of vulnerability to related-key attacks, which reduces its long-term security strength. To mitigate these limitations, improved TEA variants exist [3][4][5].

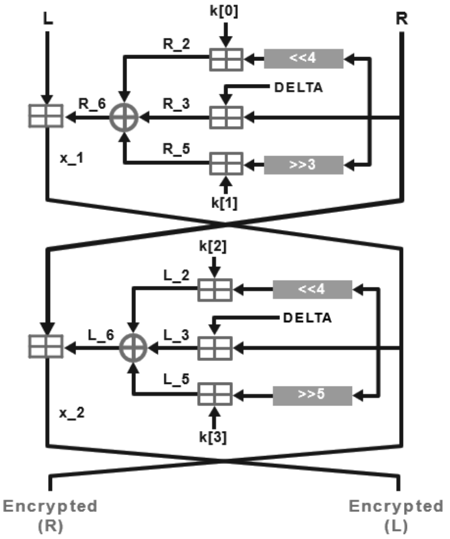

Fig 2 Encryption process of TEA cipher

2.3 LED

The Light Encryption Device (LED) is designed as a 64-bit block cipher tailored for platforms with limited resources, such as RFID tags. It supports key lengths of 64 and 128 bits, and employs a substitution-permutation network that features a 4×4 nibble matrix. The encryption process consists of multiple steps, with four rounds: AddConstants, Sub Cells, Shift Rows, and MixColumnsSerial. LED-64 operates with 32 rounds, while LED-128 functions with 48 rounds. Its straightforward key schedule reuses portions of the key along with round constants, thereby minimizing circuit complexity. Security evaluations show it has a robust defense against differential, linear, and related-key cryptanalysis. Hardware performance tests demonstrate its small gate equivalent footprint, making it ideal for ultra-lightweight encryption [8][9].

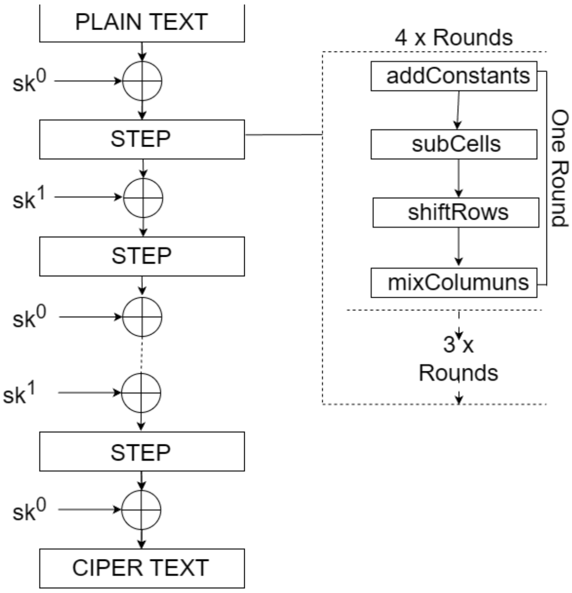

Fig 3 Encryption process of LED block cipher

2.4 KATAN

KATAN ciphers are simple encryption methods for devices with low computing power. They work with 32, 48, or 64 bits of blocks using an 80-bit key over 254 rounds. The Conditional Differential Analysis leveraging Deep Learning (CDDL) method improves the cryptanalysis by utilizing multi-differential neural distinguishers and deep residual networks to find out the subtle differential characteristics. This method, which incorporates condition-based filtering and a Bayesian key search, has resulted in successful key recovery attacks on as many as 97 rounds of KATAN32, KATAN48 with 82 rounds, and KATAN64 with 70 rounds [6][7].

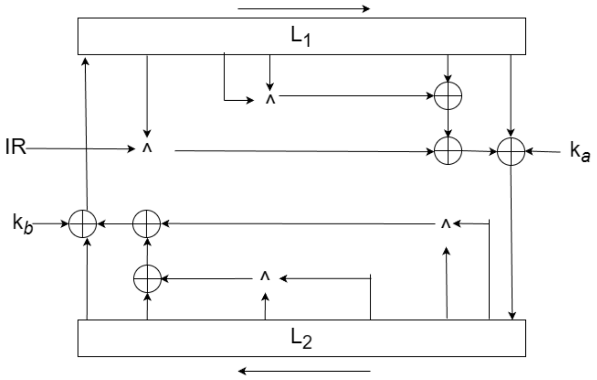

Fig 4 KATAN cipher structure

2.5 ASCON

The ASCON applies substitution permutation (SPN) operations across multiple rounds to achieve confusion and diffusion and its based on sponge construction. Ascon-128 is used to balance the efficiency and security, Ascon-128a is used to provide higher throughput and Ascon-80pq strengthens protection in post-quantum contexts. ASCON supports key sizes of 160 bits and 128 bits, where 12-bit nonce and up to 128-bit security. Even though the decryption uses slightly more memory, the encryption and decryption performance remains consistent across file sizes. ASCON's design in highly effective for short message encryption and authenticated encryption with associated data (AEAD), which is necessary for IoT and control system applications. ASCON is resistant to linear, differential and side-channel attacks. It is faster and more lightweight than AES in both hardware and software implementations. The major drawback of ASCON is that it is relatively new and has undergone less long-term scrutiny than already established ciphers. Delete the author and affiliation lines for the extra authors [19].

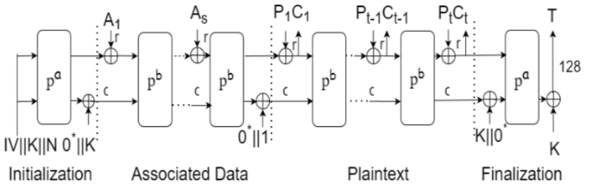

Fig 5 Encryption process of ASCON

2.6 LEA

LEA is a block cipher utilizing a 128-bit structure based on the SPN framework. This design uses simple mixing operations Addition, Rotation, XOR to protect information. This works with 128, 192, or 256 bit keys. These key sizes use 24, 28, or 32 rounds respectively. Its simple design makes it quick performance in both computer hardware, software. It handles a lot of data, requires few resources, and low memory. Security assessments show that LEA holds up well against traditional cryptanalysis. well-suited for resource-limited settings like IoT and sensor networks [10][11].

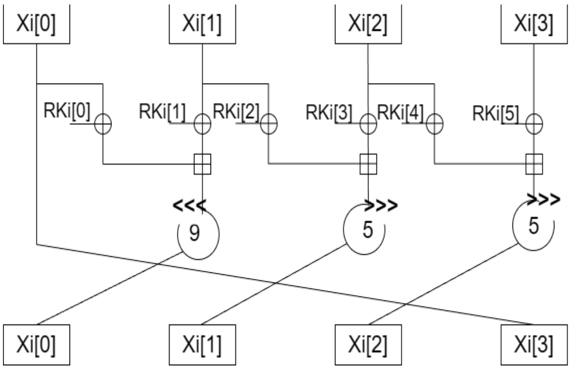

Fig 6 Encryption process of LEA

2.7 SPECK

SPECK is designed for efficient software implementation on resource-constrained IoT devices. It is a lightweight block cipher which is introduced by the NSA alongside SIMON. It offers high throughput with low memory and code size. The SPECK provides strong performance across diverse IoT platforms due to the adaptability of SPECK. It is well-suited for securing the data transmission in low-resource IoT systems [17][18].

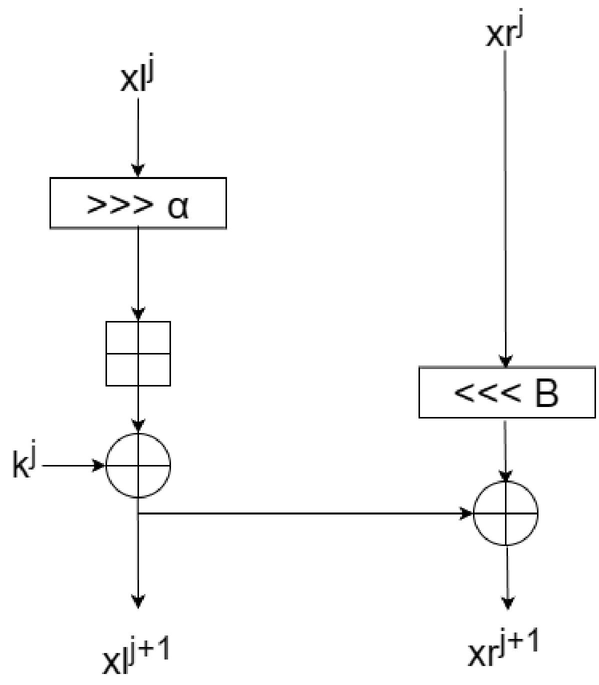

Fig 7 Representation for the general round of SPECK cipher

2.8 SIMON

SIMON represents a group of simple encryption methods created by the NSA. It functions well in sRFID tags, wireless sensors, and Internet of Things (IoT) devices. This cipher uses a Feistel network, working with blocks sizes of 32 to 128 bits and key size ranging from 64 to 256 bits. SIMON uses simple bitwise operations to reduce gate count and power consumption, thereby achieving high hardware efficiency. Although vulnerabilities exist under differential and related-key attacks, SIMON continues to serve as a benchmark in both academic and industrial cryptography research [15][16].

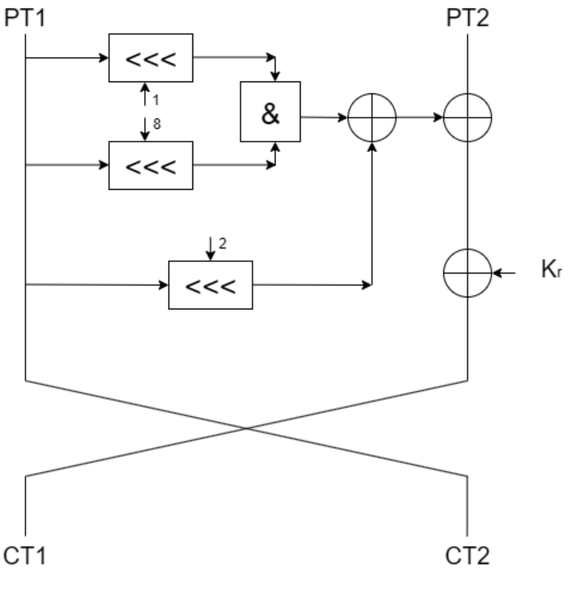

Fig 8 Round function process of SIMON cipher

3. COMPARISON

The Table 1 below shows the differences in key size, block size, structure, rounds, gate equivalent, throughput, security level [1][24][25] .

TABLE 1. Comparison Between Lightweight Block Ciphers

Algorithm	Block Size	Key Size	Structure	Rounds	Gate Equivalents	Throughput	Security Level
TEA	64 bits	128 bits	Feistel Network	64	~1500	Moderate	Adequate for constrained Iot nodes
SIMON	32-128 bits	64-256 bits	Feistel Network	32-72	1440-2200	High	Strong differential resistance
PRESENT	64 bits	80/128 bits	SPN	31	~2200	Low	High-speed software-oriented
SPECK	32-128 bits	64-256 bits	ARX	22-34	1380-2100	High	Excellent resistance large footprint
LEA	128 bits	128/192/256 bits	Substitution–Permutation framework using ARX	24/28/32 bits	~2400–3000	High	Resistant to basic cryptanalysis
LED	64 bits	64/128 bits	SPN	32	~3600	Low	Strong authenticated encryption
KATAN	32/48/ 64 bits	80 bits	Substitution–Permutation	254	~1300	Very Low	Good for small code size
ASCON	64/128 bits	128/256 bits	FSR-based	12/6	~2000	High	High security heavier resource use

Fig 9 illustrates the gate equivalents required by various lightweight cryptographic algorithms, highlighting significant differences in hardware implementation cost among them, with LED and LEA demanding the highest resources and KATAN and ASCON requiring the least.

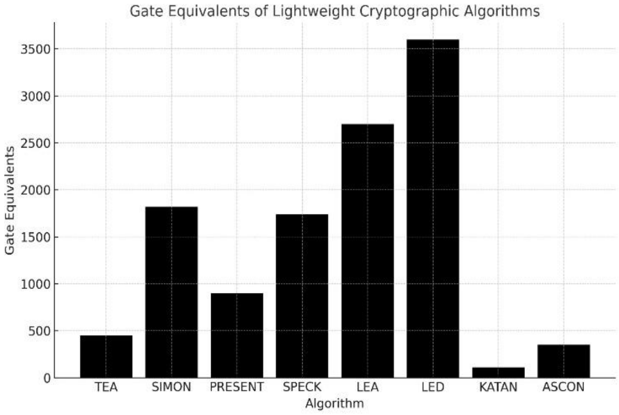

Fig 9 Gate Equivalents Required by various lightweight cryptographic algorithms

4. CONCLUSION

Lightweight cryptographic algorithms can vary for the suitability for IoT devices, depending on factors such as computational cost, Performance and Security. TEA works well with PRESENT because they each have unique benefits. TEA's Feistel-based design relies only on simple arithmetic and logical operations, resulting in minimal memory usage, low computational overhead, and reduced energy consumption, making it a good fit for software-driven and resource-constrained platforms. On the other hand, PRESENT provides a compact substitution–permutation structure and requires only ~2200 gate equivalents, therefore it makes for hardware implementation while it protects against differential attacks, particularly in its 128-bit key variant. Some other lightweight algorithms offer certain advantages, and disadvantages. AES gives high security but demands high processing power and memory. SIMON and SPECK are fast but raise cryptanalytic and trust concerns. LED consumes more hardware area than PRESENT without clear additional benefits. KATAN has low throughput and vulnerability to algebraic attacks, whereas ASCON, although secure and versatile, requires more memory and state management than ultra-constrained IoT nodes can accommodate.

TEA works efficiently when power use is limited in software environments, however PRESENT sets a benchmark for lightweight hardware encryption. These working of two algorithms together offers simplicity, compactness, and reliable security and it makes them superior to other existing lightweight cryptographic alternatives.

5. ACKNOWLEDGMENTS

The authors gratefully acknowledge the support and guidance provided by the Department Faculties.

6. REFERENCES

[1] M. A. Philip and Vaithiyanathan, "A survey on lightweight ciphers for IoT devices," *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)*, Kollam, India, 2017, pp. 1-4, doi:10.1109/TAPENERGY.2017.8397271.

[2] Al-Nofaie SM, Sharaf S, Molla R. Design Trends and Comparative Analysis of Lightweight Block Ciphers for IoTs. Applied Sciences. 2025; 15(14):7740. https://doi.org/10.3390/app15147740

[3] B. S, K. Jain and P. Krishnan, "Securing IoT Devices with Enhanced Tiny Encryption Algorithm," 2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2024, pp. 700-705, doi:10.1109/ICACRS62842.2024.10841704.

[4] Wheeler, D.J., Needham, R.M. (1995). TEA, a tiny encryption algorithm. In: Preneel, B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, vol 1008. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-60590-8_29.

[5] P. E. A. Adriaanse, M. Ayşen, and Z. Erkin, "A Comparative Study of the TEA, XTEA, PRESENT and Simon lightweight cryptographic schemes," Delft University of Technology, Cyber Security Group, Dept. of Intelligent Systems, 2021.

[6] De Cannière, C., Dunkelman, O., Knežević, M. (2009). KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds) Cryptographic Hardware and Embedded Systems - CHES 2009. CHES 2009. Lecture Notes in Computer Science, vol 5747. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04138-9_20

[7] D. Lin, M. Li, Z. Hou, and S. Chen, "Conditional differential analysis on the KATAN ciphers based on deep learning," IET Signal Processing, vol. 16, no. 8, pp. 981–989, Nov. 2022, doi: 10.1049/ise2.12099.

[8] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M. (2011). The LED Block Cipher. In: Preneel, B., Takagi, T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23951-9_22

[9] Mendel, F., Rijmen, V., Toz, D., Varıcı, K. (2012). Differential Analysis of the LED Block Cipher. In: Wang, X., Sako, K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_13

[10] Lee D, Kim D-C, Kwon D, Kim H. Efficient Hardware Implementation of the Lightweight Block Encryption Algorithm LEA. Sensors. 2014; 14(1):975-994. https://doi.org/10.3390/s140100975

[11] H. M. S. El Hennawy, A. E. A. Omar, and S. M. A. Kholaif, "LEA: Link encryption algorithm proposed stream cipher algorithm," Ain Shams Eng. J., vol. 6, no. 4, pp. 1339–1346, Dec. 2015, doi: 10.1016/j.asej.2014.08.001.

[12] Z. Haider, K. Javeed, M. Song and X. Wang, "A Low-Cost Self-Test Architecture Integrated With PRESENT Cipher Core," in IEEE Access, vol. 7, pp. 46045-46058, 2019, doi: 10.1109/ACCESS.2019.2907717.

[13] R. Chatterjee and R. Chakraborty, "A Modified Lightweight PRESENT Cipher For IoT Security," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 2020, pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132950.

[14] C. A. Lara-Nino, A. Diaz-Perez and M. Morales-Sandoval, "Lightweight Hardware Architectures for the Present Cipher in FPGA," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 64, no. 9, pp. 2544-2555, Sept. 2017, doi: 10.1109/TCSI.2017.2686783.

[15] Biryukov, A., Roy, A., Velichkov, V. (2015). Differential Analysis of Block Ciphers SIMON and SPECK. In: Cid, C., Rechberger, C. (eds) Fast Software Encryption. FSE 2014. Lecture Notes in Computer Science(), vol 8540. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46706-0_28

[16] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in Proc. 52nd Annu. Design Autom. Conf. (DAC), San Francisco, CA, USA, Jun. 2015, pp. 1–6, doi: 10.1145/2744769.2747946.

[17] Radhakrishnan I, Jadon S, Honnavalli PB. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors. 2024; 24(12):4008. https://doi.org/10.3390/s24124008

[18] D. Indrajati and W. M. Ashari, "Evaluation of the effectiveness of lightweight encryption algorithms on data performance and security on IoT devices," J. Appl. Inform. Comput., vol. 9, no. 3, pp. 642–650, Jun. 2025.

[19] G. Cagua, V. Gauthier-Umaña and C. Lozano-Garzon, "Implementation and Performance of Lightweight Authentication Encryption ASCON on IoT Devices," in IEEE Access, vol. 13, pp. 16671-16682, 2025, doi: 10.1109/ACCESS.2025.3529757.

[20] Prasanthi, B.V. & Reddy, P. (2024). Advances in Cyber Security and Digital Forensics e-ISBN: 978-93-6252-987-9 iip series frontiers in secure software defined networking: a research perspective frontiers in secure software defined networking: a research perspective iip series frontiers in secure software defined networking: a research perspective. 10.58532/nbennurch259.

[21] P. S. Suryateja and K. V. Rao, "A Survey on Lightweight Cryptographic Algorithms in IoT", Dept. of CS&SE, AUCOE, Andhra University, India, Published Online: Mar. 23, 2024, pp. 21–34, received Oct. 23, 2023, accepted Jan. 15, 2024, doi: 10.2478/cait-2024-0002.

[22] V. Panchami and M. M. Mathews, "A Substitution Box for Lightweight Ciphers to Secure Internet of Things," J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 9, pp. 10491–10504, Sep. 2023, doi: 10.1016/j.jksuci.2023.03.004.

[23] J. Kaur, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, "A comprehensive survey on the implementations, attacks,

and countermeasures of the current NIST lightweight cryptography standard," arXiv preprint arXiv:2304.06222, Apr. 2023, doi: 10.48550/arXiv.2304.06222.

[24] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access*, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[25] El-hajj, M.; Mousawi, H.; Fadlallah, A. Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. *Future Internet* 2023, *15*, 54. https://doi.org/10.3390/fi15020054