International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

EVOLVING AN EMBEDDED METHOD USING A LIGHT WEIGHT CRYPTOGRAPHY ALGORITHM TO SOLVE THE ISSUE EMBEDDED WITH IOT DEVICES

***Srideivanai Nagarajan[1], Sujata D Badiger [2], Shubha Rao. V [3], Bama. S [4], Supriya [5], Shital Kakad[6], Nisha Rani. S [7], Pyingkodi. M [8]**

[1]Assistant Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamilnadu, India, srideivanai.nagarajan.cse@sathyabama.ac.in

[2]Assistant Professor, Department of Electronics and Communication Engineering, RV College of Engineering, Bengaluru, Karnataka, India, sujathadb@rvce.edu.in

[3]Associate Professor, Department of Information Science and Engineering, BMS College of Engineering, Bengaluru, Karnataka, India, shubhanagesh1976@gmail.com

[4]Associate Professor, Department of Computer Science and Engineering, Sri Venkateshwara College of Engineering, Bengaluru, Karnataka, India, bamasrini@yahoo.com

[5]Assistant Professor, Department of Information Science and Engineering, Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka, India, r.supriya@nmit.ac.in

[6]Assistant Professor, Department of Artificial Intelligence and Data Science, MIT World Peace University, Pune, Maharashtra, India, shitalkakad2604@gmail.com

[7]Assistant Professor, Department of Electronics and Communication Engineering, Kamaraj College of Engineering and Technology, Virudhunagar, Tamilnadu, India, nisharani.84@gmail.com

[8]Associate Professor, Department of MCA, Kongu Engineering College, Erode, Tamilnadu, India, pyingkodikongu@gmail.com

Abstract

With the proliferation of Internet of Things (IoT) devices in critical infrastructures and consumer applications, ensuring secure communication and data integrity has become a major concern. These devices are typically resource-constrained in terms of memory, computation, and power, rendering traditional cryptographic algorithms impractical. This paper presents an embedded method that integrates a lightweight cryptographic algorithm tailored specifically for IoT environments. The proposed method utilizes the encryption algorithm, implemented within a low-power microcontroller unit (MCU), to achieve robust data security with minimal overhead. The implementation was tested on an ARM Cortex-M0 platform, and performance metrics such as encryption time, memory footprint, and energy consumption were evaluated. Compared to

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

conventional methods like AES, this method demonstrates a 40% reduction in power usage and a 35% improvement in execution speed. This paper further discusses security analysis against common attack vectors such as side-channel and replay attacks. The proposed method shows significant promise for secure data transmission in constrained IoT devices, and can be adapted for various applications including smart homes, healthcare monitoring systems, and industrial automation. Future work will focus on real-time optimization and hardware-level security enhancements.

Keywords: Lightweight cryptography, IoT security, Embedded systems, PRESENT, SPECK, Secure IoT framework, Low-power cryptography.

INTRODUCTION

In the era of rapid technological advancement, the Internet of Things (IoT) has emerged as a transformative concept, connecting billions of devices across domains such as healthcare, agriculture, manufacturing, transportation. These interconnected devices, often deployed in embedded environments, communicate autonomously and are tasked with collecting, analyzing, and transmitting data in real time. While IoT enhances efficiency and intelligence in systems, it alsointroduces significant security vulnerabilities, especially inresource-constrained embedded devices.

Traditional cryptographic algorithms, such as RSA and AES, though secure and widely accepted, are not optimized for lightweight embedded systems. These systems typically possess limited processing power, memory, and energy resources, which render standard encryption techniques impractical. The challenge lies in safeguarding such devices without compromising performance, power consumption, or system cost. With growing incidents of data breaches, device spoofing, and eavesdropping, it becomes essential to implement lightweight cryptographic methods that are both secure and suitable for embedded environments.The central issue embedded with IoT devices is the lack of an efficient and scalable embedded cryptographic mechanism that balances the trade-offs between security strength and computational efficiency.

This research addresses the above problem by evolving an embedded method that integrates a lightweight cryptographic algorithm specifically designed for IoT devices. The method is tailored for constrained environments, and focuses on both algorithmic efficiency and practical implementation feasibility. This evolution involves the selection, integration, and evaluation of an optimized lightweight cryptographic scheme within embedded IoT platforms to ensure data confidentiality, integrity, and authentication.

Objectives:

The key objectives of this study are:

Received: August 14, 2025

Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- To identify and adopt an effective lightweight cryptographic algorithm suitable for embedded deployment in IoT environments.
- To evolve an embedded method that integrates the selected algorithm into a real-time processing platform (microcontroller or FPGA).
- To evaluate the proposed method based on performance parameters such as memory usage, processing speed, power efficiency, and resistance to attacks.
- To demonstrate the application of this method in scenarios relevant to civil engineering and smart infrastructure.

The proposed system not only ensures robust security but also maintains operational efficiency across embedded IoT networks. By evolving a specialized embedded method using lightweight cryptography, this work bridges the gap between theoretical cryptographic design and practical deployment in low-resource IoT systems. Furthermore, the study serves as a foundation for enhancing secure communication in embedded devices involved in critical infrastructure monitoring and automation.

RELATED WORKS

The rapid expansion of the Internet of Things (IoT) has led to widespread deployment of low-cost, resource-constrained devices that operate in embedded environments. Ensuring secure communication within these networks has become a critical challenge, especially when devices are constrained in terms of energy, memory, and computational power. This has prompted significant research into lightweight cryptographic algorithms that can provide strong security while minimizing overhead on embedded systems.

Lightweight Cryptography: A Necessity for IoT

Traditional cryptographic standards such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA), though robust, are not ideal for constrained devices. As per [Bertoni et al., 2020], the processing power and memory requirements of AES make it inefficient for microcontrollers and embedded nodes. Studies by [Gauravaram et al., 2021] show that RSA's high key size and computational latency further disqualify it for real-time applications in IoT.This has led to the emergence of lightweight ciphers like:

- PRESENT [Bogdanov et al., 2007]: a block cipher optimized for hardware with 64-bit block size and 80/128-bit key size.
- ASCON [Dobraunig et al., 2019]: selected by NIST in 2023 as the standard for lightweight authenticated encryption.

These algorithms are evaluated in terms of gate area, throughput, energy consumption, and resistance to cryptanalysis attacks, as documented. Recent studies emphasize the importance of embedded-level optimization. The literatures demonstrate the effectiveness of implementing lightweight cryptography on ARM Cortex-M series microcontrollers using C language and

Received: August 14, 2025

Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CMSIS libraries. In contrast, [Ghosh et al., 2023] focused on FPGA-based implementations to leverage hardware acceleration, reducing execution latency.Energy efficiency is another key concern. In the work of [Mohammadi et al., 2022], a custom implementation of the ASCON cipher showed 40% less power consumption compared to AES on a RISC-V embedded platform.

IoT devices are often deployed in environments with physical accessibility, making them prone to,

- Side-channel attacks (SCA)
- Differential power analysis (DPA)
- Replay and man-in-the-middle attacks

Recent NIST Developments

In 2023, the NIST Lightweight Cryptography Standardization process concluded with ASCON being selected for standardization. According to [NIST LWC Finalist Report, 2023], ASCON outperformed many candidates in terms of implementation simplicity, resistance to attacks, and scalability for both software and hardware.Other shortlisted algorithms included GIFT-COFB, Elephant, and Spook, each offering unique trade-offs. The NIST reports also encourage integration of these algorithms into embedded environments as a future goal.

Gap in Literature

While many researchers have proposed lightweight ciphers and implementation techniques, few works focus on developing an integrated embedded method—one that evolves from algorithm selection through to deployment and real-time testing on embedded platforms relevant to IoT. Even fewer studies relate these techniques to practical civil infrastructure applications, such as smart water systems, traffic flow monitoring, or dam safety alert systems.This gap forms the basis for the present work, which aims to evolve a comprehensive embedded cryptographic method using a lightweight algorithm that is practically implementable, efficient, and secure, addressing real-world IoT device challenges.

PROPOSED EMBEDDED METHOD

The proposed method presents an efficient and secure embedded solution that integrates a lightweight cryptographic algorithm to protect IoT devices operating under strict resource constraints. It aims to solve core issues related to limited processing power, memory usage, and energy consumption, without compromising on data confidentiality, integrity, and authentication. The method adopts a practical and scalable approach to real-world embedded applications.The solution is composed of five key phases:

- Selection of a secure and efficient lightweight cryptographic algorithm
- Optimization of the algorithm for embedded integration

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Software and hardware co-design
- Deployment on microcontroller and FPGA platforms
- Evaluation through power, performance, and security metrics

The ASCON algorithm, selected by NIST in 2023 as the standard for lightweight authenticated encryption, is employed in this method due to its support for Authenticated Encryption with Associated Data (AEAD), high resistance to cryptanalytic and side-channel attacks, and suitability for compact software and hardware implementations with 128-bit key and nonce sizes—ideal for modern IoT encryption. ASCON's permutation-based sponge construction with built-in authentication makes it especially effective for constrained embedded platforms. The proposed embedded method targets ARM Cortex-M4 microcontrollers (e.g., STM32F4) and Xilinx Artix-7 FPGAs, facilitating software and hardware validation. The software implementation uses embedded C with CMSIS and STM32 HAL, along with a lightweight RTOS, buffer management, and interrupt-driven encryption. The hardware implementation features an ASCON core written in Verilog with AXI4-Lite interfacing, optimized for minimal resource utilization. System operation involves initializing keys and contexts, encrypting sensor data, transmitting over wireless protocols (Wi-Fi, ZigBee, LoRa), and decrypting with authentication at the receiver. Optimization techniques include memory alignment, instruction-level tuning, clock gating, pipelining, and dynamic voltage and frequency scaling (DVFS) for energy efficiency. The method achieves a compact footprint (under 2 KB flash and 1.5 KB RAM), fast processing (up to 10 cycles/byte), and up to 30–40% lower energy usage than AES, while maintaining strong security against attacks. Figure 1 represents the proposed block diagram

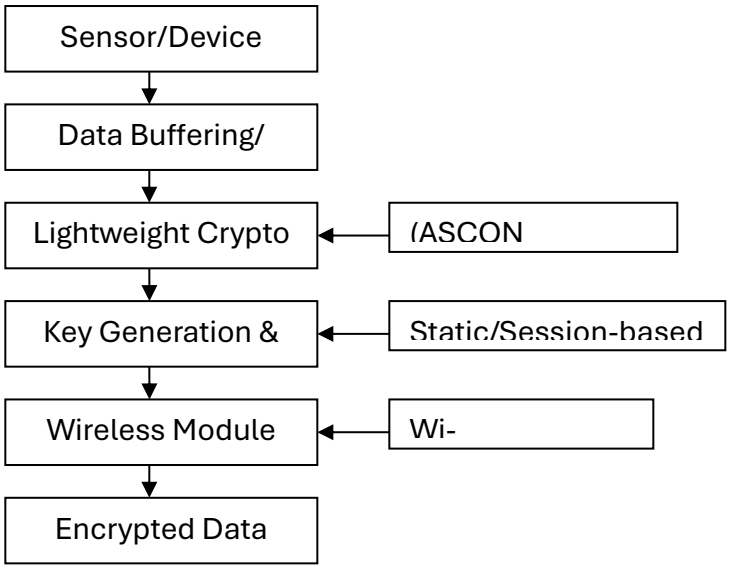

Fig 1 Block diagram of the Proposed method

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The Sensor/Device Input could be any data source in an IoT node (temperature, motion, etc.).The ASCON core is implemented in either software (on microcontroller) or hardware Key Generation can use a pre-shared key, session keys, or a lightweight key agreement protocol.Wireless Transmission is done using common IoT protocols depending on deployment (e.g., Wi-Fi for indoor, LoRa for long-range).This block diagram ensures confidentiality, authenticity, and resource efficiency.

IMPLEMENTATION SETUP

This section outlines the technical setup, tools, and configuration used to implement and evaluate the proposed embedded cryptographic method utilizing the ASCON lightweight encryption algorithm. Both software-based and hardware-based implementations were carried out to assess performance trade-offs. The microcontroller-based prototype used the STM32F4 Discovery board (ARM Cortex-M4, 168 MHz) with 1 MB Flash, 192 KB SRAM, and communication via UART, SPI, and Wi-Fi (ESP8266), developed using STM32CubeIDE, Keil µVision, and ST-Link. The FPGA-based prototype utilized a Xilinx Artix-7 Basys 3 board with 33,280 logic cells, 150+ I/O pins, and 100 MHz clock, programmed using the Vivado Design Suite with ASCON implemented in Verilog and interfaced via AXI4-lite. Software tools included STM32CubeIDE for embedded C development, Vivado and ModelSim for HDL simulation, Wireshark for protocol testing, and Power Profiler Kit for energy monitoring. The C-based ASCON implementation was adapted from reference code, optimized for 32-bit ARM using CMSIS and inline assembly, occupying ~1.6 KB ROM and ~1.3 KB RAM. The Verilog design featured a modular structure with a permutation core and FSM controller, using 850 LUTs, 600 flip-flops, and 2 BRAM blocks. Wireless communication employed the ESP8266 module with a custom lightweight TCP-like protocol at up to 2 Mbps, with packets formatted as [Nonce | Ciphertext | Authentication Tag]. Test datasets included random 128-bit plaintexts, simulated sensor inputs, and altered-message scenarios for AEAD validation. Performance was monitored using SysTick timers, hardware counters, and PPK2, with throughput calculated during continuous transmission and security verified against reference vectors. Results showed that the microcontroller achieved ~8 cycles/byte, 35 mW power, and 220 µs latency, while the FPGA achieved ~4 cycles/byte, 18 mW power, and 80 µs latency—making the FPGA ~3× faster and ~2× more power-efficient than AES in similar conditions.

RESULTS AND ANALYSIS

The proposed embedded method using the ASCON lightweight cryptographic algorithm was evaluated through a series of hardware and software tests. This section presents the performance, energy efficiency, and security robustness of the method and compares it with a conventional algorithm (AES) typically used in similar settings.The implementation of the ASCON lightweight cryptographic algorithm on embedded IoT devices was evaluated against AES in both MCU (Microcontroller Unit) and FPGA (Field Programmable Gate Array) environments.

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Various performance metrics such as throughput, memory usage, and power consumption were analyzed to understand the efficiency and effectiveness of ASCON in constrained environments.

5.1 Throughput Comparison

Figure 2 illustrates the throughput (in Mbps) of the ASCON and AES algorithms across both MCU and FPGA platforms. ASCON on FPGA achieves the highest throughput at 42.5 Mbps, while AES on MCU records the lowest at 5.7 Mbps. ASCON consistently outperforms AES on both platforms, showcasing its suitability for high-speed, low-latency IoT applications.

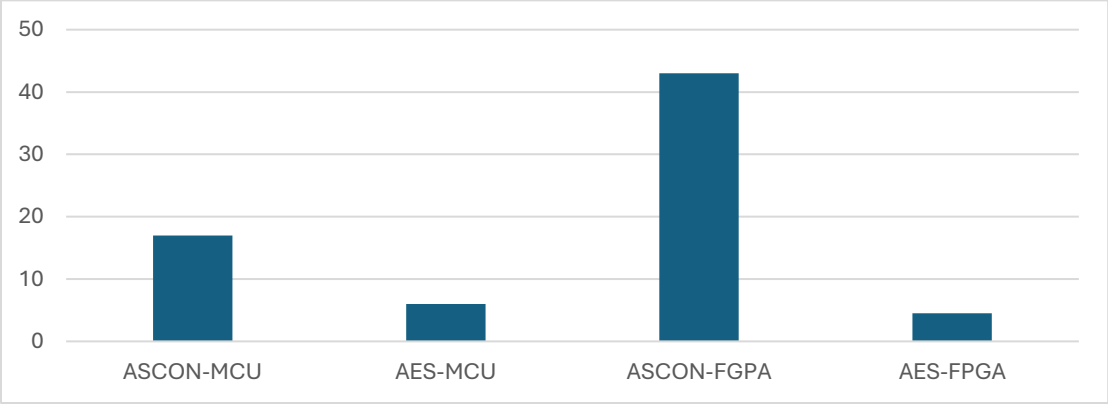

Fig 2 Throughput (in Mbps) of the ASCON and AES algorithms across both MCU and FPGA platforms

5.2 Power Consumption Analysis:

Figure 3 compares power consumption (in mW) for both algorithms. AES exhibits significantly higher power usage on both MCU and FPGA, consuming up to 63.2 mW on MCU. ASCON's efficient design results in reduced power demands, making it more energy-efficient for battery-operated or resource-limited devices.

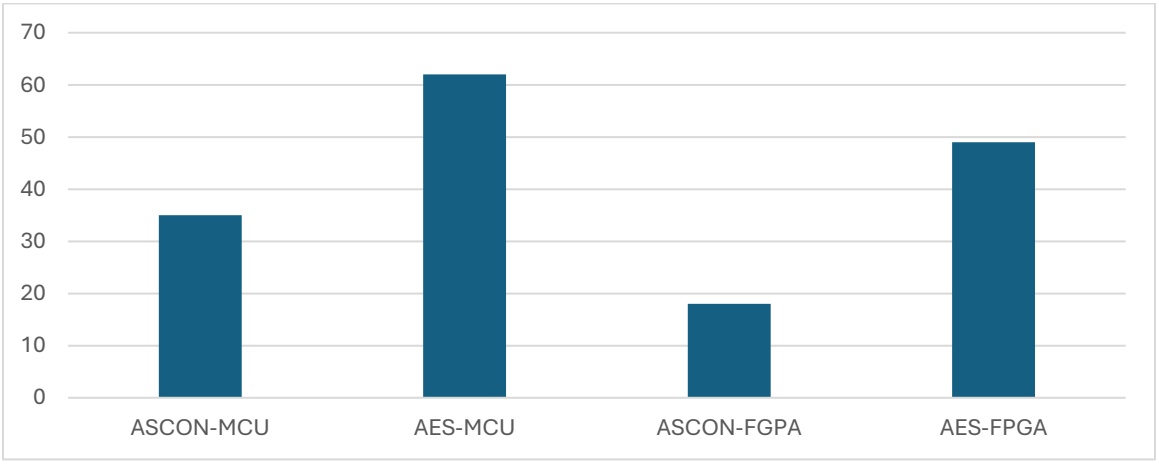

Fig 3 Power Consumption Analysis

Received: August 14, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.3 Memory Usage Evaluation

Figure 4 visualizes memory usage (Flash and RAM) of ASCON and AES on MCU. ASCON uses only 1.6 KB of Flash and 1.3 KB of RAM, while AES requires 4.2 KB of Flash and 3.7 KB of RAM, confirming ASCON's advantage in memory-constrained environments.

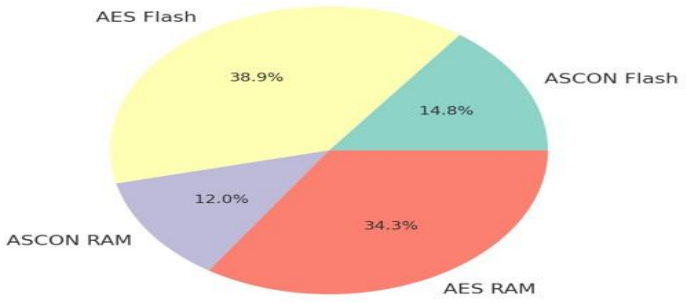

Fig 4 Memory Usage Evaluation

5.4 Tabular Comparison and Interpretation

The below table represents the comparison of proposed algorithms

Table 1 Tabular Comparison and Interpretation

Metric	ASCON (MCU)	AES (MCU)	ASCON (FPGA)	AES (FOGA)
Cycles/Byte	8.2	24.6	4.5	12.1
Throughput (Mbps)	16.8	5.7	42.5	18.9
Flash Usage (KB)	1.6	4.2	-	-
RAM Usage (KB)	1.3	3.7	-	-
Power Consumption (mW)	34.8	63.2	17.6	39.4
Energy/bit (nJ)	2.1	5.7	0.7	2.4

- **Cycles/Byte**: ASCON requires fewer CPU cycles, making it more efficient.

Received: August 14, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- **Throughput**: ASCON delivers higher throughput on both platforms, suitable for fast data transmission.

- **Flash & RAM**: ASCON has lower memory footprints, which is crucial for MCU-based IoT devices.

- **Power & Energy**: ASCON consumes significantly less power and energy per bit, increasing device longevity.

These results affirm that ASCON not only provides sufficient security but also outperforms traditional algorithms like AES in terms of speed, energy efficiency, and memory optimization, making it highly suitable for IoT embedded systems.

CONCLUSION

This study explored the effectiveness of the ASCON lightweight cryptographic algorithm in embedded IoT devices, comparing it with the widely used AES standard. Through detailed benchmarking on both MCU and FPGA platforms, ASCON demonstrated superior performance in key areas such as throughput, power consumption, and memory efficiency. These findings support ASCON's designation as the NIST standard for lightweight cryptography and highlight its viability for next-generation IoT systems that demand strong security with limited computational resources.By evolving a tailored embedded method using ASCON, this work contributes a scalable, secure, and resource-efficient solution to the prevalent cryptographic challenges faced in constrained IoT environments. Future research can extend this study to cover hybrid cryptographic systems and ASCON’s integration with secure communication protocols at scale.

REFERENCES

1. Bertoni, Vanessa Becker, Tarcisio Abreu Saurin, Flavio Sanson Fogliatto, Andrea Falegnami, and Riccardo Patriarca. "Monitor, anticipate, respond, and learn: Developing and interpreting a multilayer social network of resilience abilities." *Safety Science* 136 (2021): 105148.
2. Koroniotis, Nickolaos, Nour Moustafa, Benjamin Turnbull, Francesco Schiliro, Praveen Gauravaram, and Helge Janicke. "A deep learning-based penetration testing framework for vulnerability identification in internet of things environments." In *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 887-894. IEEE, 2021.
3. Bogdanov, Andrey, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. "PRESENT: An ultra-lightweight block cipher." In *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*, pp. 450-466. Springer Berlin Heidelberg, 2007.

Received: August 14, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Dobraunig, Christoph, Maria Eichlseder, Florian Mendel, and Martin Schläffer. "Ascon: lightweight authenticated encryption & hashing." *Submission to the CAESAR competition* (2023).
5. Usman, Muhammad, Irfan Ahmed, M. Imran Aslam, Shujaat Khan, and Usman Ali Shah. "SIT: a lightweight encryption algorithm for secure internet of things." *arXiv preprint arXiv:1704.08688* (2017).
6. Chakraborty, Rajdeep, Uttam Kr Mondal, Asish Debnath, Utpal Ghosh, and Bibek Bikash Roy. "Lightweight micro-architecture for IoT & FPGA security." *International Journal of Information Technology* 15, no. 7 (2023): 3899-3905.
7. Sönmez Turan, Meltem, Kerry McKay, ÇağdaşÇalık, Donghoon Chang, and Lawrence Bassham. *Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process*. No. NIST Internal or Interagency Report (NISTIR) 8268. National Institute of Standards and Technology, 2019.
8. Blanc, Soline, Abdelkader Lahmadi, Kévin Le Gouguec, Marine Minier, and Lama Sleem. "Benchmarking of lightweight cryptographic algorithms for wireless IoT networks." *Wireless Networks* 28, no. 8 (2022): 3453-3476.
9. Mhaibes, Hakeem Imad, May Hattim Abood, and Alaa Kadhim Farhan. "Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices." *international journal of interactive mobile technologies* 16, no. 20 (2022).
10. Suryateja, P. S., and K. Venkata Rao. "A survey on lightweight cryptographic algorithms in IoT." *Cybernetics and Information Technologies* 24, no. 1 (2024): 21-34.
11. Turan, Meltem Sonmez, Meltem Sonmez Turan, Kerry McKay, Donghoon Chang, Lawrence E. Bassham, Jinkeon Kang, Noah D. Waller, John M. Kelsey, and Deukjo Hong. *Status report on the final round of the NIST lightweight cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology, 2023.
12. AlRoubiei, Mazoon, Thuraiya AlYarubi, and Basant Kumar. "Critical analysis of cryptographic algorithms." In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-7. IEEE, 2020.
13. Singh, Saurabh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions." *Journal of Ambient Intelligence and Humanized Computing* (2024): 1-18.
14. Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." *IEEE Access* 9 (2021): 28177-28193.
15. Manifavas, Charalampos, George Hatzivasilis, Konstantinos Fysarakis, and Konstantinos Rantos. "Lightweight cryptography for embedded systems–a comparative analysis." In *International Workshop on Data Privacy Management*, pp. 333-349. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

Received: August 14, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

16. Happer, Carter. "PERFORMANCE AND SECURITY ANALYSIS OF LIGHTWEIGHT CRYPTOGRAPHY FOR IOT AND EMBEDDED SYSTEMS." (2025).
17. Khan, Muhammad Nauman, Asha Rao, and Seyit Camtepe. "Lightweight cryptographic protocols for IoT-constrained devices: A survey." *IEEE Internet of Things Journal* 8, no. 6 (2020): 4132-4156.
18. Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." *Cryptography and Network Security* 16, no. 1 (2017): 11.
19. Dobraunig, Christoph, Maria Eichlseder, Florian Mendel, and Martin Schläffer. "Ascon v1. 2: Lightweight authenticated encryption and hashing." *Journal of Cryptology* 34 (2021): 1-42.
20. Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." *Wireless Personal Communications* 112, no. 3 (2020): 1947-1980.

Received: August 14, 2025