International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195935

Lightweight Cryptography Algorithms for IoT and Embedded Systems

Dharmi Patel[1], Twinkle More[2], Trusha Maurya[3]

[1]DS student, faculty of computer application[1], Sigma University (Vadodara)

[2]IT student, faculty of computer application[2], Sigma University (Vadodara)

[3]MCA student, faculty of computer application[3], Sigma University (Vadodara)

Abstract

The proliferation of Internet of Things (IoT) devices and embedded systems has introduced new security challenges due to their constrained computational, memory, and power resources. Traditional cryptographic algorithms such as AES and RSA often impose prohibitive overhead, necessitating the development of lightweight cryptography (LWC). This paper reviews major lightweight cryptographic algorithms, compares their performance in constrained environments, highlights standardization efforts such as NIST's Lightweight Cryptography Project, and discusses open challenges and future research directions. The findings show that lightweight block ciphers such as SPECK, SIMON, PRESENT, and GIFT, and authenticated ciphers like ASCON provide strong security with minimal resource usage, making them suitable for diverse IoT applications.

Article Information

Received: 25th October 2025

Acceptance: 25th December 2025

Available Online: 9th January 2026

Keywords: Chlorophytum comosum, Fusarium oxysporum, C. albicans, Bacillus subtilis, E.coli, nanoparticles.

1. Introduction

Billions of IoT devices—including wearables, medical sensors, smart meters, and industrial controllers—operate with limited CPU capabilities, restricted RAM, and battery constraints. Ensuring confidentiality, integrity, and authentication in such devices requires cryptographic algorithms that minimize energy consumption while maintaining strong security guarantees.

Traditional cryptographic standards such as AES-128 and RSA-2048 are designed for high-performance computing environments and often exceed the resource capacities of low-power

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195935

microcontrollers. Lightweight cryptography (LWC) addresses this gap by optimizing algorithm structure, key size, and round functions to reduce computational complexity.

This paper presents a comprehensive survey and comparative analysis of lightweight cryptography algorithms suited for IoT and embedded systems.

2. Background and Motivation

2.1 IoT and Embedded System Constraints

IoT devices typically suffer from:

- Limited memory (often < 32 KB RAM)
- Low CPU clock speeds (8–100 MHz)
- Power constraints (battery or energy harvesting)
- Limited communication bandwidth

These constraints create a need for specialized cryptographic solutions with:

- low latency
- low energy consumption
- small code size
- minimal hardware footprint

2.2 Limitations of Traditional Cryptography

- **RSA** requires large key sizes (2048–4096 bits), which is computationally expensive.
- **ECC** is faster than RSA but still heavy for ultra-low-power sensors.
- **AES** is secure and widely used but can be inefficient on 8-bit microcontrollers without hardware acceleration.

Hence, lightweight cryptographic schemes are essential for secure IoT deployment.

3. Lightweight Cryptography Principles

Lightweight algorithms aim to reduce:

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195935

- **Gate complexity** (for hardware)
- **Code size** (for firmware)

 RAM/ROM usage **Energy per operation**

Design strategies include:

- simple substitution–permutation networks (SPN)
- Feistel structures
- reduced number of rounds
- small S-boxes
- ARX operations (Add–Rotate–XOR)

4. Types of Lightweight Cryptography

4.1 Lightweight Block Ciphers

4.1.1 PRESENT

- 64-bit block size
- 80- or 128-bit keys
- Known for extremely small hardware footprint (< 2000 GE)
- Suitable for RFID tags, smart cards

4.1.2 GIFT

- Improvement over PRESENT
- Offers better security margins
- Used as part of several authenticated encryption schemes

4.1.3 SIMON and SPECK (ARX-based by NSA)

- SIMON (hardware optimized)
- SPECK (software optimized)

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195935

- Very lightweight with high speed
- Some concerns due to authorship, but cryptanalytically robust

4.2 Lightweight Stream Ciphers

Grain Family (Grain v1, Grain-128a)

- Suitable for ultra-low hardware environments
- High throughput in hardware

Trivium

- Hardware-efficient
- Used in many LWC benchmarking studies

4.3 Lightweight Hash Functions

PHOTON & SPONGENT

- Sponge-based
- Designed for constrained hardware environments

4.4 Lightweight Authenticated Encryption (AEAD)

AEAD is essential for IoT to ensure confidentiality + integrity in one operation. **ASCON (Winner of NIST LWC Competition, 2023)**

- Selected as the standard for lightweight cryptography
- Includes ASCON-128, ASCON-128a, and ASCON-80pq
- Very strong resistance to differential and linear attacks
- Efficient on both 8-bit and 32-bit microcontrollers

International Journal of Recent Trends in Science Technology & Management(IJRTSTM)
©2023 (IJRTSTM) | Volume 4 | Issue 3 | ISSN: 2584-0894
October-December 2025 | DOI: https://doi.org/10.5281/zenodo.18195935

ACORN & AEGIS

- High-speed authenticated encryption
- ACORN is extremely lightweight for hardware
- AEGIS provides high speed but with higher resource usage

5. Performance Comparison

Algorithm	Type	RAM/ROM Usage	Energy Efficiency	Security Level	Ideal Use Case
PRESENT	Block Cipher	Very Low	High	Moderate	RFID, sensors
GIFT	Block Cipher	Low	High	High	Smart cards, IoT nodes

SPECK	Block Cipher	Low	Very High	High	Constrained MCUs
Trivium	Stream Cipher	Very Low	High	Moderate	Embedded systems
ASCON	AEAD	Moderate	Very High	Very High	General IoT security

Most studies show ASCON and GIFT-COFB as top performers for balanced security and efficiency.

6. NIST Lightweight Cryptography Standardization

In 2023, NIST announced **ASCON** as the official standard for lightweight authenticated encryption. Criteria included:

- security robustness
- resistance to attacks
- software/hardware performance
- small implementation size

As a result, ASCON is expected to become the dominant LWC primitive in the IoT ecosystem.

7. Applications of Lightweight Cryptography

- Smart Home Systems
- Healthcare IoT (wearable sensors, implants)
- Industrial IoT (IIoT)
- Automotive ECUs
- Smart Agriculture
- Wireless Sensor Networks (WSN)

- Low-power RFID and NFC devices

8. Challenges and Future Research Directions

8.1 Post-Quantum Lightweight Cryptography

Most lightweight schemes are not quantum-resistant. Designing lightweight PQC is a major open challenge.

8.2 Secure Implementation Against Side-Channel Attacks

Lightweight algorithms often have small S-boxes and simple operations, making them vulnerable to:

- power analysis
- timing attacks
- electromagnetic leakage

8.3 Standardization and Interoperability

More unified global standards are needed to ensure interoperability across IoT platforms.

8.4 Balancing Ultra-Low Power and Strong Security

Many ultra-lightweight ciphers compromise security margins. Further research is required to optimize energy efficiency without reducing security.

9. Conclusion

Lightweight cryptography is fundamental for securing IoT and embedded systems.
Algorithms such as PRESENT, GIFT, Trivium, and especially the NIST-selected ASCON provide robust security with minimal resource consumption. As IoT ecosystems expand, future research must focus on quantum-resistant designs, implementation security, and unified standards. Lightweight cryptography will continue to play a crucial role in enabling secure, scalable, and energy-efficient IoT deployments.

10. References

1. A. Bogdanov, L.R. Knudsen, G. Leander, et al., “PRESENT: An Ultra-Lightweight Block Cipher,” CHES 2007, LNCS 4727, pp. 450–466, Springer, 2007.

2. A. Dinur, L. Goubin, S. Gueron, “The SIMON and SPECK Families of Lightweight Block Ciphers,” IACR Cryptology ePrint Archive, 2013/404.

3. T. Peyrin, L. Wang, “GIFT: A Small PRESENT,” CHES 2017, LNCS 10529, pp. 321– 345, Springer.

4. C. De Cannière, O. Dunkelman, M. Knežević, “KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers,” CHES 2009, LNCS 5747, pp. 272–288.

5. M. Hell, T. Johansson, W. Meier, “Grain: A Stream Cipher for Hardware-Constrained Environments,” IJWMC, vol. 2, no. 1, pp. 86–93, 2007.

6. C. De Cannière, B. Preneel, “Trivium Specifications,” eSTREAM Project, Report 2005/018.

7. B. Authenticated Encryption and NIST Lightweight Cryptography

8. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, “The Sponge and Duplex Constructions,” NIST Workshop on Hash Functions, 2011.

9. C. Dobraunig, M. Eichlseder, F. Mendel, et al., “Ascon v1.2: Lightweight Authenticated Encryption and Hashing,” IACR Transactions on Symmetric Cryptology, 2016(2), pp. 1–35.

10. National Institute of Standards and Technology (NIST), “Lightweight Cryptography: Finalist Algorithms and Reports,” NISTIR 8369, 2023.

11. National Institute of Standards and Technology (NIST), “NIST Announces ASCON as the Lightweight Cryptography Standard,” Official Press Release, 2023.

12. W. Beullens, “NIST Lightweight Cryptography: Security Overview,” IACR ePrint, 2022/1583.

13. A. Chakraborti, S. Sarkar, “A Complete Evaluation of NIST LWC Finalist Ciphers on Embedded Platforms,” ACM TECS, 2022.

14. C. IoT Security Constraints and Lightweight Cryptography Deployments

15. H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” RFC 2104, 1997.

16. M. Ambrose, C. Paar, “Low-Energy Cryptographic Hardware for IoT Devices: A Survey,” IEEE Transactions on Circuits and Systems, 2018.

17. S. Ravi, A. Raghunathan, P. Kocher, S. Hattangady, “Security Challenges in Embedded System Design,” DAC 2004, pp. 129–135.

18. A. Juels, “RFID Security and Privacy: A Research Survey,” IEEE Journal on Selected Areas in Communications, 24(2), pp. 381–394, 2006.

19. D. Halperin et al., “Security and Privacy for Implanted Medical Devices,” IEEE Pervasive Computing, 7(1), pp. 30–39, 2008.

20. D. Benchmarking and Performance Evaluation Studies

21. T. Eisenbarth, S. Kumar, C. Paar, “A Survey of Lightweight Cryptography Implementations,” IEEE Design & Test of Computers, 2007.

22. M. Feldhofer, J. Wolkerstorfer, “AES Implementation on a Smart Card and Performance Comparison to PRESENT,” IEEE ISCAS 2007.

23. A. Poschmann, “Lightweight Cryptography: Cryptographic Engineering for a Pervasive World,” IEEE Transactions on Computers, 2009.

24. S. Huang, B. Yang, “Energy-Efficient Hardware Architectures for Lightweight Ciphers,” IEEE Transactions on VLSI Systems, 2021.

25. S. Tillich, P. Großschädl, “Power Analysis Resistance of Lightweight Ciphers,” CHES 2008, LNCS 5154, pp. 230–245.

26. E. Side-Channel Attacks on Lightweight Ciphers

27. E. B. Kavun, T. Yalçin, “Side-Channel Attacks on PRESENT and Hardware Countermeasures,” IET Information Security, 2011.

28. A. Moradi, O. Mischke, C. Paar, “Practical Evaluation of DPA Countermeasures on Lightweight Cryptography,” ISCAS 2011.

29. J. Großschädl et al., “Energy-Efficient Implementation Attacks and Countermeasures,” IEEE Transactions on Computers, 2016.

30. F. Surveys and Comprehensive Overviews

31. M. Abomhara, G. Køien, “Security and Privacy in the Internet of Things: Current Status and Open Issues,” IEEE ISCC, 2014.

32. A. Raza, T. Voigt, V. Jutvik, “Lightweight Cryptography for the Internet of Things: A Survey,” IEEE IoT Journal, 2020.

33. B. Schneier, “Applied Cryptography (2nd Ed.),” Wiley, 1996. (Classic reference)

34. P. Schwabe, S. Kölbl, “Lightweight Cryptography for Embedded Security—Current Landscape and Future Directions,” ACM Computing Surveys, 2022.