

Lightweight Cryptographic Algorithms in IoT Communication: A Comprehensive Review

Kaiwen Wang

Department of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, 710000, China
1816562828@qq.com

ABSTRACT

This review describes the lighting description language used for lightweight cryptographic algorithms. This paper focuses on a simple problem. How can small IoT devices protect data when power, memory and computing power are low? In the story, the meaning and main types of lightweight cryptography are explained. In addition, it also introduces the common usage in RFID system, wireless sensor networks and smart grids. This review compares LED, PRESENT and KTANTAN. These algorithm will reduce the cost and energy consumption, but there are still attack problems such as fault attacks and side-channel attacks. The paper also discusses the reuse of hardware, the design of composite field, the simplification of software and parallel processing. The last part is 5G, edge computing, attribute-based encryption and hybrid encryption. The main results are clear. Although Lightweight cryptography contributes to the security of IoT, every design needs to be fully tested and continuously improved.

Keywords: Lightweight Cryptographic Algorithm; Internet Of Things; Security Analysis; Performance Optimization; RFID Communication.

1. INTRODUCTION

IoT devices are now used everywhere every day. Appears in tags, sensors, power systems, smart homes, industrial devices, etc. These devices collect and send data. This data includes identity information, system status and users' private records. Security is important because attackers may read, change or copy this information.

Traditional cryptographic algorithms will protect us very strongly. The problem is that many IoT devices are not easy to move these. A small tag or sensor may require less battery, storage and processing speed. A heavy algorithm may protect data, but it will slow down the device or eliminate battery as soon as possible. So lightweight cryptography becomes important.

This review checks lightweight cryptographic algorithms in IoT communication. I want to talk about three things. The first is the basic idea and classification of lightweight algorithms. The second method is used in RFID, wireless sensor networks and smart grids. The third is the balance between security and resource cost. The review will also discuss future directions, including 5G communication and edge computing ^[1-3].

This review uses the method of "structured literature review". Relevant research has been collected from famous academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, CNKI and Google Scholar. I searched around the papers from 2009 to 2025. The keyword used for retrieval are "lightweight cryptography", "lightweight cipher", "internet of things", "RFID security" and "wireless sensor networks", "lightweight authentication", "IoT communication security".

When I first searched, I found more than 120 publication. In addition to not researching lightweight cryptographic techniques for IoT environment with insufficient resources, 23 representative study were selected for detailed investigation. The selected literature involves algorithm design, performance evaluation, practical application of IoT, security analysis and future development trend. This review process aims to balance today's lightweight cryptographic solutions and whether they can be used in various IoT environments.

2. LITERATURE REVIEW AND THEORETICAL FOUNDATIONS

2.1 Definition and Characteristics of Lightweight Cryptography

Lightweight cryptography is designed for devices with few resources. Try to keep data safe without using too much memory, energy or computing power. Starting from this goal, there will be the usual trade-offs. A design that is made very small may become faster. But if the margin of safety is too small, the power of guarding will be slightly weakened.

Previous studies have clearly demonstrated this trade-off. Wang and Wei proposed a nonlinear cipher for RFID data transmission. Their design uses shift computation, which reduces the cost of calculation. After that, Wang and Wei re-examined the lightweight ciphers for RFID devices. They discussed the number of cryptographic rounds, the key length and the cost of implementation. Other researches include low-power hardware, optimized block ciphers and attribute-based encryption for IoT. These studies all show the same problem. The security of IoT should not only conform to the theory, but also to the equipment ^[1,4-7].

2.2 Lightweight Cryptographic Primitives

Lightweight Cryptographic Primitives is a basic component for protecting security on IoT devices with few resources. According to the characteristics of work, it is usually divided into three types. stream ciphers, block ciphers and hash functions.

2.2.1 Stream Cipher Algorithms.

Stream ciphers encrypt data into a continuous stream. They are useful when devices need faster processing speed and less memory. The original review wrote that RC4 has better performance in execution efficiency, security strength and hardware burden compared with ECC and PRESENT. This point should be treated as a result from the cited comparison, not as a universal rule for all IoT systems ^[2].

Hash functions also matter in this field. They support data integrity and digital signatures. Gong explains that conventional hash functions may create heavy costs for small devices. This is why lightweight hash functions are studied for limited hardware environments ^[8].

2.2.2 Block Cipher Algorithms.

Block ciphers encrypt fixed-size blocks of data. Many lightweight block ciphers have been studied for RFID tags and sensor networks. Wang proposed a self-reflection structure to reduce hardware cost. Li, Li, Cao, and Le compared LED, TWINE, and GOST. Their results in the original review suggest that these ciphers can be efficient when plaintext size is below 2 KB. Zhong, Gu, and Cao also organized lightweight block ciphers into categories and compared hardware and software features ^[9-11].

2.2.3 Hash Functions.

Hash functions help check whether data has been changed. This function is important in IoT communication because data may pass through weak networks. Gong studied lightweight hash functions for devices with limited hardware. Li explored low-power hash implementation using magnetic tunnel junction technology. Jiang and Yu combined elliptic curves and hash functions to build a lower-overhead secure communication method. These studies show that hashing is not only a separate tool. It can also become part of a larger authentication system ^[5,8,12].

2.3 Application Requirements in IoT

IoT applications need security, but they also need low cost. RFID systems may have very small tags. Wireless sensor nodes may run on batteries. Smart grid terminals may need fast and stable communication. Because of this, an algorithm cannot be judged only by its theoretical strength. It must also be judged by power use, memory use, running time, and communication cost.

The original review gives one useful smart grid example. Wang designed a verifiable encryption algorithm for smart grid communication data. The reported CPU use did not exceed 12 percent. The reported memory use did not exceed 6500 bytes. These numbers show why lightweight design matters in real systems ^[13]. To provide a systematic comparison of lightweight cryptographic algorithms, the following sections evaluate representative schemes from four dimensions: memory consumption, energy efficiency, computational latency, and security level.

3. APPLICATION STATUS IN IOT COMMUNICATION

3.1 Application Cases

3.1.1 RFID Systems.

RFID systems are a major use case for lightweight cryptography. RFID tags often have small chips and limited power. They need authentication and encryption, but they cannot afford heavy computation. Wang and Wei proposed a nonlinear cipher for RFID communication. Wang later studied lightweight authentication and encryption for IoT. Luo proposed an ultra-lightweight authentication protocol for RFID systems. These works all focus on reducing cost while protecting privacy [4,14,15].

3.1.2 Wireless Sensor Networks.

Wireless sensor networks also need lightweight security. Sensor nodes may monitor temperature, motion, energy use, or other physical conditions. These nodes often work for long periods with limited battery power. Authentication and access control are important because a false node can send wrong data. Luo studied lightweight security protocols and key technologies for resource-constrained IoT nodes. This research supports the need for simple but reliable protection in sensor networks [16].

3.1.3 Smart Grids.

Smart grids are more demanding than simple RFID systems. They need security, speed, and reliability at the same time. Communication data in a smart grid may affect power monitoring and control. Wang designed a verifiable encryption algorithm for this setting. Kang and coauthors studied lightweight 5G key technologies for power IoT. Their work connects terminal cost, energy use, and security requirements [3,13].

3.2 Existing Problems and Challenges

The main problem is not whether lightweight cryptography is useful. The problem is how to balance security and cost. A lighter algorithm may run faster and use less power. At the same time, it may face new risks if the design removes too much complexity. The original review identifies several risks. These include side-channel attacks, fault attacks, hardware limits, and performance bottlenecks [1,10,11].

Power use creates another challenge. Li discussed low-power lightweight cryptography and MTJ technology. This direction is important because some IoT systems must run in extreme power conditions. But the review does not provide enough evidence to claim that one low-power method is best for all devices. A careful conclusion is safer. Different IoT devices need different choices [5].

4. DESIGN AND PERFORMANCE ANALYSIS

4.1 Design Principles

A lightweight cryptographic design usually follows two basic goals. It should reduce resource use, and it should keep enough security. These goals are connected, but they often conflict. Fewer rounds may improve speed. A smaller circuit may reduce cost. But either change may also reduce protection if attackers can use the simpler structure.

Several studies address this design problem. Wang used a self-reflection structure to reduce implementation scale. Lu and coauthors compared ECC, RC4, and PRESENT to show different trade-offs. Li used MTJ technology for low-power security. Zhong, Gu, and Cao provided a wider classification of lightweight block ciphers. These studies show that lightweight design is not one method. It is a set of choices based on the device and the threat model [2,5,9,11].

4.2 Performance Analysis of Typical Algorithms

4.2.1 LED Algorithm.

LED is a lightweight block cipher used in IoT research. The original review reports that LED can offer a good balance between hardware overhead and performance. It also reports that LED has a security weakness under differential fault analysis. Li, Gu, Zhao, Liu, and Liu found that 64-bit and 128-bit keys could be recovered with only a small number of faulty ciphertexts. This does not mean LED is useless. It means implementation must include protection against fault attacks [2,17].

4.2.2 PRESENT Algorithm.

PRESENT is another common lightweight cipher. It is often discussed because it can be implemented in constrained environments. Lu and coauthors tested PRESENT on microprocessors. Jiang studied meet-in-the-middle attacks on related lightweight ciphers. Li, Li, Cao, and Le compared PRESENT-like algorithms with other lightweight designs. The evidence in the original review suggests that PRESENT is practical, but it still needs security review as new attacks appear [2,10,18].

4.2.3 KTANTAN Algorithm.

KTANTAN is designed for highly constrained devices. Its simple hardware design is useful for small systems. But the original review also notes possible weaknesses. Jiang studied meet-in-the-middle attacks and indirect partial matching. Li, Gu, Zhao, Liu, and Liu reported that three faulty ciphertexts could be enough to recover a 64-bit key in their fault model. This finding shows why a small design must still include careful attack resistance [17,18].

4.3 Performance Evaluation Methods and Tools

Performance evaluation should not rely on one number. A complete test should look at memory, power, speed, hardware area, and security. The original review mentions Atmega-32 microcontroller simulation, MTJ-based low-power implementation, and benchmark comparisons. Li, Li, Cao, and Le provide performance indicators for LED, TWINE, and GOST. Zhong, Gu, and Cao compare software and hardware platforms. These methods help researchers choose suitable algorithms for different IoT devices [10,11].

5. SECURITY ANALYSIS

5.1 Security Evaluation Standards and Methods

Security evaluation should include both mathematical attacks and physical attacks. Mathematical attacks study the structure of the algorithm. Physical attacks use information leaked during implementation. A device may leak power patterns, timing data, or electromagnetic signals. For IoT devices, physical attacks are important because many devices are cheap and exposed.

The original review discusses several defense ideas. Wang and Wei used nonlinear design ideas. Wang and Wei also discussed side-channel threats in RFID. Li studied MTJ-based low-power protection. Li proposed revocable attribute-based encryption with outsourced computation. Jiang and Yu combined physical unclonable functions, elliptic curves, and hash functions for authentication. These methods show that IoT security often needs both algorithm design and system-level protection [1,4,5,7,12].

5.2 Typical Attack Methods and Defense Strategies

5.2.1 Differential Fault Attack.

A differential fault attack tries to disturb a device during encryption. The attacker then studies the wrong output. If the design is weak, a few faulty outputs may reveal secret keys. Li, Gu, Zhao, Liu, and Liu used a random nibble fault model in their LED analysis. The original review states that only a few faulty ciphertexts were enough in that model. Possible defenses include redundant computation and fault detection circuits [8,17].

5.2.2 Side-Channel Attack.

A side-channel attack does not always break the mathematics of the cipher. Instead, it uses physical leakage. Power use and electromagnetic emissions are common examples. Wang and Wei suggested that their RFID cipher had some built-in resistance. But the original review also shows that lightweight ciphers still need special countermeasures. Masking and hiding are common defense methods [1,4,17].

5.2.3 Meet-in-the-Middle Attack.

A meet-in-the-middle attack splits encryption into parts. The attacker then tries to match intermediate values. Jiang studied this type of attack on KTANTAN-related designs. Wang proposed design ideas to improve the avalanche effect. A stronger avalanche effect makes small input changes spread more widely through the output. This can make some attacks harder, but it does not remove the need for formal testing [9,18].

5.3 Practical Cases of Security Analysis

The reviewed studies show that lightweight cryptography can work in practical IoT settings. RFID encryption, MTJ-based low-power implementation, and comparative tests all support this point. LED, TWINE, and GOST appear in performance studies. Ultra-lightweight RFID authentication also appears as a practical direction. But these cases also show a limit. A working lightweight design still needs repeated testing because IoT threats change over time [2,4,5,10,15].

6. OPTIMIZATION AND IMPROVEMENT

6.1 Hardware Optimization Techniques

6.1.1 Resource Reuse Technology.

Resource reuse reduces chip area and power use. The original review gives the example of a lightweight SM4 architecture. Zhu and coauthors reused core circuits for subkey expansion and the round function. This design avoided storing 32 round subkeys. Jiang and Yu also reduced authentication transmission overhead. These examples show that optimization can happen inside the circuit and inside the protocol [12,19].

6.1.2 Composite Field Technology.

Composite field technology can improve S-box implementation. The S-box is often one of the expensive parts of a block cipher. Wang used self-reflection structure with composite field methods to improve efficiency. Zhu and coauthors also discussed composite field use in lightweight SM4 implementation. The original review treats this method as useful under hardware limits [9,11,19].

6.2 Software Optimization Techniques

6.2.1 Algorithm Simplification.

Algorithm simplification reduces computing work. But simplification must be controlled. A design should not remove so much structure that security becomes weak. Wang and Wei showed a nonlinear shift-based approach. Li explored MTJ-based low-power design. Lu and coauthors compared ECC, RC4, and PRESENT. Jiang and Yu reduced authentication information size. These studies show that simplification is useful when the security effect is tested [2,4,5,12].

6.2.2 Parallel Processing.

Parallel processing can improve throughput. This matters when a system must handle many messages quickly. The original review connects this idea with high-speed transmission, microprocessor testing, MTJ-based design, and hybrid encryption. Jiang and Yu used hybrid encryption to support authentication and encryption with lower total delay. This point is promising, but the exact gain depends on the device and implementation [2,4,5,12].

6.3 Comprehensive Optimization Strategies

A strong IoT security design usually combines several methods. It may use a smaller algorithm, shared hardware, lower communication cost, and a safer protocol. Wang and Wei summarized important design problems. Lu and coauthors provided comparative benchmarks. Jiang discussed security and performance trade-offs. Li and Gong studied low-power encryption and hash design. Han studied challenge-response authentication with SM9 and AES. Ma and coauthors proposed a lightweight trusted IoT communication protocol. These works show that cross-layer design is often necessary [1,2,5,8,18,20,21].

7. FUTURE DEVELOPMENT DIRECTIONS

7.1 Impact of Emerging Technologies

7.1.1 5G Communication Technology.

5g communication will change the demand of IoT security. 5G will support more device, reduce latency and be used in a wider industry. Kang studied the key technologies of lightweight 5G for power IoT. Their goal is to simplify terminals, reduce energy consumption and improve security. Jiang and Yu also studied hybrid encryption in the 5G IoT. Hu, Xu and Du proposed a lightweight symmetric-key solution for the security of perception-layer. It can be seen from these studies that 5G pushes lightweight cryptography to a faster and more freely used protocol [3, 12, 22].

7.1.2 Edge Computing.

Edge computing moves computing near IoT devices. Because data doesn't always have to go to a remote server, it can reduce the delay. Lightweight cryptography fits this scenario. Because the resources of edge nodes may be very small. Wang and Wei put forward the basic idea of RFID password. Li is studying the low-power algorithm. Jiang and Yu are reducing the communication burden through mixed passwords. The original review thought that combining lightweight cryptography with edge computing might improve real-time security. This is a good research direction, but the actual result depends on the design of the system [4, 5, 12].

7.2 Key Areas for Future Research

7.2.1 Lightweight Attribute-Based Encryption.

Attribute-based encryption can support fine-grained access control. This means a system can decide access based on user attributes instead of only one identity. Li proposed a revocable attribute-based encryption scheme for IoT. The scheme supports key traceability and attribute revocation. Liu, Liao, and Wei designed a lightweight key management system based on symmetric keys. These studies show that future IoT security may need better access control, not only faster encryption [7,23].

7.2.2 Lightweight Hybrid Encryption Algorithms.

Hybrid encryption combines symmetric and asymmetric methods. Symmetric encryption is usually fast. Asymmetric encryption can support key exchange and identity functions. Jiang and Yu combined elliptic curves and hash functions to reduce IoT overhead. Zhu and coauthors implemented a resource-reusable SM4 architecture. Gong studied lightweight hash functions. These works suggest that hybrid structures may become more common in IoT systems [8,12,19].

7.3 Challenges and Countermeasures

Future research still faces several problems. Attack methods continue to develop. IoT devices have different hardware limits. Standards are not always unified across applications. Some algorithms also show weaknesses under specific attacks. Jiang reported vulnerabilities in KTANTAN-related analysis. Wang and Wei, Lu and coauthors, and Li and coauthors discussed risks from side-channel and fault attacks. Possible responses include better protection implementation, ultra-lightweight authentication and formal security verification. In the original review, post-quantum lightweight cryptography was also listed as the future direction. This should be considered as the direction of research, not as a complete solution [1, 2, 15, 17, 18].

8. CONCLUSION

Lightweight cryptographic algorithms are still indispensable to protect IoT devices with less resources. The existing methods, such as LED, PRESENT and KTANTAN, show that it can be very safe even if the amount of calculation, memory and energy is reduced. Therefore, they are suitable for RFID systems, wireless sensor networks, smart grids and edge-enabled IOT environments.

However, lightweight design also has great problems. Fault attack, side-channel attack, meet-in-the-middle attack are very dangerous in practical use, and the types of IoT devices are increasing, so it is necessary to formulate common security rules. Therefore, to choose the right algorithm, we should not only look at the implementation efficiency, but also consider APP requirements, hardware limitations and thermal models.

In the future research, we will study the strength of not losing to attacks, Post-quantum lightweight cryptography, improvisational security mechanism, cross-layer optimization, and 5G communication, edge computing, lightweight encryption, which are very important for the new generation of IoT systems to keep a safe state even if it keeps growing.

AUTHORS' CONTRIBUTIONS

The conceptualization, literature review, analysis, writing and revision of this manuscript are entirely done by its author. The author confirmed and approved the final version of manuscript.

REFERENCES

- [1] Wang, Y., Wei, G. (2017) A survey of lightweight cryptographic algorithms for RFID. *Comput. Appl. Softw.*, 34(1): 1–7
- [2] Lu, A., Yang, J., Li, F., Zhang, B., Chen, C. (2014) Comparative study of several lightweight encryption algorithms. *Mod. Electron. Tech.*, 37(12): 28–32
- [3] Kang, S., Wang, X., Li, Z., Feng, X., Shao, Z., Li, S., Wang, X. (2024) Research on lightweight 5G communication key technologies for power IoT. *Electr. Power Sci. Eng.*, 40(4): 1–12
- [4] Wang, X., Wei, G. (2009) Research on cipher algorithm for data transmission in IoT RFID system. *J. Beijing Inf. Sci. Technol. Univ.*, 24(4): 1–5
- [5] Li, W. (2020) The study on application of low power secure lightweight cryptography algorithms. Harbin Institute of Technology, Harbin
- [6] Zhang, J. (2020) Design and analysis of lightweight block cipher to be used in IoT applications. University of Electronic Science and Technology of China, Chengdu
- [7] Li, H. (2023) Lightweight revocable attribute-based encryption research in the Internet of Things. University of Electronic Science and Technology of China, Chengdu
- [8] Gong, Z. (2016) Research on lightweight hash functions. *J. Cryptol.*, 3(1): 1–10
- [9] Wang, Y. (2013) Design and analysis of lightweight block ciphers. University of Electronic Science and Technology of China, Chengdu
- [10] Li, Y., Li, W., Cao, Y., Le, J. (2016) Performance analysis of several lightweight block ciphers. *Comput. Appl. Softw.*, 33(10): 1–6
- [11] Zhong, Y., Gu, J., Cao, H. (2023) A survey on lightweight block ciphers. *Comput. Sci.*, 50(9): 1–15
- [12] Jiang, Y., Yu, X. (2024) Low-overhead IoT secure communication method based on hybrid encryption algorithm. *Changjiang Inf. Commun.*, 37(11): 45–50
- [13] Wang, Z. (2025) Design of lightweight verifiable encryption algorithm for smart grid communication data. *Inf. Technol.*, 49(11): 1–8
- [14] Wang, Y. (2017) The study of lightweight authentication and encryption technology in Internet of Things. Nanjing University of Posts and Telecommunications, Nanjing
- [15] Luo, Y. (2023) The study of ultra-lightweight security authentication protocol of RFID systems in IoT environment. Xidian University, Xi an
- [16] Luo, H. (2019) A study on light security protocol and key technology of the Internet of Things. University of Electronic Science and Technology of China, Chengdu
- [17] Li, W., Gu, D., Zhao, C., Liu, Z., Liu, Y. (2012) Security analysis of LED lightweight cipher in IoT environment. *Chin. J. Comput.*, 35(3): 1–9.
- [18] Jiang, S. (2014) Analysis of lightweight block cipher algorithms. Donghua University, Shanghai
- [19] Zhu, K., Dai, Z., Zhang, L., Li, W., Zhu, W. (2016) Lightweight implementation of SM4 algorithm for IoT. *Appl. Electron. Tech.*, 42(12): 1–5
- [20] Han, J. (2021) Study of light-weight authentication system of IoT devices. Taiyuan University of Technology, Taiyuan
- [21] Ma, J., Liu, Z., Li, G., Yang, F., Dang, J. (2021) A lightweight trusted IoT communication protocol. *Telecommun. Sci.*, 37(11): 1–9
- [22] Hu, X., Xu, G., Du, L. (2013) Solution for establishing IoT perception layer information security based on lightweight encryption technology. *Netw. Secur. Technol. Appl.*, 14(3): 1–4
- [23] Liu, X., Liao, Z., Wei, Z. (2018) Design of lightweight key system for IoT information security protection. *Inf. Secur. Res.*, 4(9): 1–5