Mathematical Modeling and Algorithm Application
ISSN: 3006-0842 | Vol. 10, No. 1, 2026

Research on Lightweight Data Encryption Technology for Resource-Constrained Devices

Shuo Yang*

Shaanxi University of Science & Technology, Computer Science and Technology, Weiyang University Park, Weiyang District, Xi'an City, Shaanxi Province, 710021, China.

* **Corresponding author**: Shuo Yang (Email: 2246856721@qq.com)

Abstract: With the advancement of technology, an increasing number of intelligent devices have entered the online world, generating a huge demand for data exchange. Due to the limited storage space and computing power of some intelligent devices, traditional data encryption technologies are difficult to be effectively deployed, leading to increasingly serious privacy leakage problems. This paper conducts a systematic review of lightweight data encryption technologies for resource-constrained devices. This research systematically reviews lightweight encryption technologies suitable for resource-constrained devices, covering block ciphers, hash functions, authentication key negotiation, encryption strategies, and application scenario analysis. It focuses on how to strike a balance between low power consumption and high security. The research shows that future studies should not merely focus on the lightweighting of algorithms, but rather should concentrate on designing authentication encryption primitives that can dynamically adapt to resource fluctuations. Especially when facing physical threats such as side-channel attacks, how to maintain a high level of security margin and low latency response speed while operating under extremely limited power budgets will be the key to breaking through the current bottleneck in IoT security and coping with increasingly complex network environments.

Keywords: Blockcipher; Resource-constrained environment; Lightweight encryption technology; Authentication; Low power consumption.

1. Introduction

1.1. Research Background

With the deep integration of 5G and artificial intelligence technologies, the process of interconnection of all things is accelerating, and a large number of intelligent devices are widely applied in various fields. [1-4] However, these devices often have constraints such as weak computing power and small storage space, making it difficult to run traditional, computationally-intensive encryption algorithms, resulting in serious security risks of data leakage. At the same time, increasingly diverse network attack methods and constantly upgraded privacy protection regulations have raised higher requirements for the confidentiality, integrity, and availability of data throughout the entire cycle of collection, transmission, and storage [2,5]. Therefore, under the premise of ensuring necessary security strength, designing lightweight encryption algorithms, identity authentication protocols, and key management mechanisms with low power consumption, low latency, and low storage overhead has become a key issue that urgently needed to be solved in the current field of cybersecurity, and is also a key technical support for promoting the higher-level application of the Internet of Things and edge computing.

1.2. Current Research Status at Home

Research on lightweight data encryption technology for resource-constrained devices has already gained certain research foundation in China. At the algorithm level, Chen Ziqian designed lightweight block ciphers FONA32, FERX64 based on pure logical operations, and the SPOR algorithm based on high-performance S-box, and on this basis, proposed the lightweight hash function FAS, effectively reducing the hardware implementation area [5]; Guo Zichao designed a lightweight identity authentication scheme based on pre-shared keys and elliptic curve key agreement, and improved the ChaCha20-Poly1305 encryption algorithm [3]. Li Xiangning et al. conducted a systematic comparative analysis of typical lightweight cryptographic algorithms such as PRESENT, GIFT, and ASCON [2]. At the application architecture level, Huang Xiaoping proposed an adaptive lightweight data encryption model for cloud-edge-end collaborative scenarios [4]; Guo Xian et al. combined homomorphic encryption and distributed key generation technology to propose an anti-collusion federated learning privacy protection scheme [6]; Yang Huifeng et al. proposed an anti-eavesdropping semantic communication method based on feature obfuscation for power IoT terminals [7]; Gao Mengzhou proposed a selective and random encryption strategy from the perspective of control system security [8]; Li Zhenwei proposed a lightweight intrusion detection strategy based on data packet sampling and heuristic learning [9]; Zhang Xiaqin et al. designed a lightweight privacy protection scheme for cloud auditing [10]; Liu Feng et al. systematically reviewed the privacy protection cryptographic technologies in blockchain [1]. Overall, the existing research has made certain progress in block cipher algorithms, identity authentication and key negotiation, etc., but the balance of security, lightness and real-time performance remains a core issue that needs to be urgently addressed.

1.3. The Main Content

This paper focuses on lightweight encryption technologies in resource-constrained environments and systematically reviews and summarizes the existing research. Firstly, it introduces lightweight block cipher algorithms and analyzes their design principles of reducing computational resource

requirements through the symmetric encryption mechanism (Section 2); Secondly, it elaborates on the structural characteristics of Hash functions and their application in data integrity verification (Section 3); Thirdly, it summarizes the research progress of authentication and key negotiation protocols (Section 4); Fourthly, it summarizes the protection mechanisms of selective encryption and random encryption strategies (Section 5); Finally, it analyzes the privacy protection schemes and their effectiveness in different application scenarios (Section 6). Based on this, this paper further refines the key challenges currently faced in this field and points out that designing authentication encryption algorithms that balance low power consumption and high security is an important trend for future development.

2. Principles of Design for Lightweight Block Cipher Algorithms

2.1. Definition and Research Status

Lightweight block ciphers are one of the core technologies for data encryption on resource-constrained devices. Their design goal is to ensure the necessary security strength while minimizing the hardware implementation area, power consumption, and computational latency. Li Xiangning et al. [7] conducted a systematic comparative analysis of typical lightweight block cipher algorithms such as PRESENT, GIFT, and ASCON. They summarized the design characteristics and application scenarios of each algorithm from three dimensions: algorithm structure, hardware performance, and software performance. Chen Ziqian [1] further explored the technical path for minimizing hardware area based on pure logical operations by systematically elaborating the basic concepts of lightweight block ciphers and proposing the FONA32 and FERX64 algorithms.

2.2. Typical Structures

The design of lightweight block ciphers usually relies on three structures: Feistel structure, SPN structure, and ARX structure [1,7]. These three structures have different focuses in terms of hardware efficiency and software performance.

The Feistel structure divides the plaintext data into two parts and gradually completes encryption through multiple rounds of the round function. Its main advantage lies in the highly similar encryption process, which can be implemented on hardware with lower power consumption, but achieving the same level of security requires more rounds [1]. Chen Ziqian [1] designed FONA32 with a dual-branch Feistel structure, and FERX64 with a four-branch Feistel structure. Both introduce XOR operations in the round functions to enhance diffusion and nonlinearity.

The SPN structure consists of reversible nonlinear permutation layers (S-boxes) and reversible linear diffusion layers (P-permutations), and has a fast data diffusion speed, making it suitable for parallel implementation [1]. PRESENT is a representative algorithm of this structure and is recognized as the first ultra-lightweight block cipher, using a 31-round SPN structure, with a 4-bit S-box in the nonlinear layer and only bit permutation operations in the diffusion layer, with a hardware implementation area of approximately 1560 GE [7].

The ARX structure only uses modulo addition, modular addition, rotation, and XOR operations and circular shift operations to provide nonlinearity, with lower hardware and software implementation costs, but requires more iterations to ensure security [1,7]. Representative algorithms such as SIMON and SPECK use simple operation combinations in their round functions to achieve good diffusion and confusion effects, with good implementation efficiency in both software and hardware [7].

2.3. Security Analysis

The security assessment of lightweight block ciphers typically involves key space analysis and strict avalanche effect tests. If the key space exceeds 2^100, it can be considered to be able to resist brute-force attacks [1]. Chen Ziqian [1] pointed out that FONA32 and FERX64 adopt dynamic iterative rounds (adjusting based on the high 8 bits of the plaintext), which increases the difficulty of static analysis; the key space of the SPOR algorithm is approximately 2^128 × 24 computations, much greater than 2^100. The avalanche effect test shows that both FONA32 and FERX64 meet the strict avalanche standard, that is, a single bit change in the plaintext or key approximately causes 50% of the ciphertext bits to change [1].

3. Lightweight Hash Functions

3.1. Definition and Research Status

Hash functions are one of the fundamental tools in cryptography, capable of receiving messages of any length and outputting fixed-length message digests, mainly applied in scenarios such as data integrity verification, digital signatures, and identity authentication. To address the issue that they cannot operate normally on resource-constrained devices, lightweight Hash functions optimize the iterative structure and internal permutations to significantly reduce the hardware implementation area and power consumption while maintaining the necessary security strength [1]. Chen Ziqian [1] systematically expounded the design principles of lightweight Hash functions. In terms of the iterative structure, existing schemes mainly adopt two frameworks: the Sponge structure and the MD-like (Merkle-Damgård) structure. Among them, the Sponge structure, due to its flexibility and provable security, has become the preferred choice for most lightweight Hash function designs. This structure is divided into two stages: the absorption stage groups the padded message according to the digest rate and performs an XOR operation with the internal state, which is then processed by a permutation function and enters the next round; the compression stage generates the required-length message digest through multiple permutations and truncation operations [1].

3.2. Typical Structure

Lightweight Hash functions typically employ the Sponge structure [1]. This structure divides the internal state into digest rate and capacity sections, and the whole process is divided into two stages: absorption and compression. The absorption stage successively mixes the message groups with the internal state and processes them through permutation functions; the compression stage outputs the required-length message digest through multiple permutations and truncation operations [1]. Compared with traditional structures, the Sponge structure is more resistant to length extension attacks [1]. The typical algorithm Ascon-Hash adopts the Sponge structure, with an internal state of 320 bits, and the round function consists of three steps: round constant addition, S-box substitution, and linear diffusion [1,7]. Chen Ziqian [1]

designed FAS, which is also based on the Sponge structure, but made adjustments in parameter selection and S-box size, further optimizing the hardware area.

3.3. Security Analysis

The security of lightweight Hash functions is mainly evaluated from three aspects: collision resistance, preimage resistance, and second-preimage resistance. For the Sponge structure, its security is determined jointly by the capacity c and the output length n [1]. The FAS algorithm designed by Chen Ziqian [1] has an output length of 256 bits, a capacity of 256 bits, and a digest length of 64 bits. Therefore, its collision resistance is 2^128, preimage resistance is 2^192, and second-preimage resistance is 2^128, which can meet the security requirements of most IoT application scenarios. In addition, the avalanche effect test shows that the internal permutation of FAS has good diffusion characteristics. A small change in the input can trigger a significant change in the output, further enhancing the algorithm's ability to resist cryptographic attacks such as differential analysis [1].

4. Authentication and Key Agreement Protocol

4.1. Definition and Research Status

Identity verification and key negotiation are two core security mechanisms that ensure the security of IoT device access and the confidentiality of subsequent communications. Identity verification is used to confirm the true identities of the communicating parties and prevent illegal devices from accessing the system; key negotiation enables the communicating parties to establish a shared session key over an insecure public channel, providing key materials for subsequent symmetric encryption transmission [4]. In resource-constrained IoT environments, the traditional identity authentication method based on digital certificates is difficult to apply due to excessive computational and storage costs [4]. Guo Zichao [4] systematically analyzed the shortcomings of existing lightweight authentication schemes, pointing out that the existing schemes mainly have two types of problems: one is that the authentication methods based on static pre-shared keys (PSK) or passwords are lightweight, but they cannot ensure forward security. Once the key is leaked, all historical communication content will be cracked; the other is that protocols such as AugPAKE avoid certificate costs, but the registration codes used in the authentication process must remain unchanged, which also has forward security problems and lacks mechanisms such as timestamps, making it vulnerable to replay attacks [4].

4.2. Typical Scheme

In response to the above issues, Guo Zichao [4] proposed a lightweight two-way identity authentication scheme that combines pre-shared key (PSK) and temporary elliptic curve key agreement (ECDHE). The innovation of this scheme lies in using the static PSK representing the device identity and the dynamically generated temporary key each session by the ECDHE algorithm to perform an XOR operation, generating a one-time key for the session, and then using this session key to complete the challenge-response two-way authentication [4].

The specific authentication process is divided into five stages [4]:

The first stage (client preparation): The client sends the identity identifier and elliptic curve parameters (including the temporary public key) to the server.

The second stage (server challenge): After the server verifies the validity of the identity identifier, it generates its own temporary key pair and returns the challenge text and temporary public key to the client.

The third stage (client response): The client calculates the temporary key SK = dc × Qs using the ECDHE algorithm, and then derives the session key K = SK ⊕ PSK. It encrypts the challenge text sent by the server and its own generated challenge text using K, and returns the ciphertext along with the client's temporary public key to the server.

The fourth stage (server verification and response): The server calculates the session key K in the same way, decrypts the client's response to obtain the challenge text, and verifies whether the sent challenge text is consistent. If the verification is successful, it encrypts the client's challenge text using K and returns it.

The fifth stage (authentication completion): The client decrypts and verifies the challenge text returned by the server. Both parties confirm the legitimacy of the identity and complete the negotiation of the session key [4].

Guo Zichao's [4] experiments show that this scheme is superior in resource consumption to the certificate-based scheme and is basically on par with similar lightweight schemes in performance.

4.3. Security Analysis

In terms of security, Guo Zichao [4] provided a systematic proof for this scheme:

Mutual authentication: Both communicating parties participate in the generation of the session key through the pre-shared key. The attacker cannot correctly decrypt or encrypt the challenge text because they cannot obtain the PSK, and thus cannot forge an identity to pass the verification [4].

Anti-man-in-the-middle attack: If the attacker pretends to be one of the communicating parties, they cannot generate the correct session key for the challenge-response due to the inability to obtain the PSK, and thus cannot complete the two-way authentication process [4].

Anti-replay attack: The authentication message carries a timestamp. The communicating party identifies the replayed message by checking whether the message arrives within a reasonable time delay. Messages exceeding the time limit will be rejected [4].

5. Selective and Randomized Encryption Strategies

5.1. Definitions and Research Status

In resource-constrained systems, encryption protection brings additional time delays, computational resource consumption, and energy consumption, which may affect the real-time performance and stability of the system. To strike a balance between security and resource efficiency, researchers have proposed two strategic encryption methods: selective encryption and random encryption [2].

Selective encryption is a method that only encrypts a portion of the critical data, effectively reducing the cost of encryption operations [2]. Gao Mengzhou [2] pointed out that the traditional "full encryption" approach is difficult to be directly deployed in scenarios with limited resources and high real-time requirements, and needs to dynamically adjust the encryption strength based on the importance of the data and

the current state of the system.

Random encryption refers to randomly performing encryption operations with a certain probability, rather than encrypting all data completely, thereby reducing the average resource consumption [2]. Gao Mengzhou [2] stated that when the system is not under attack, random encryption can significantly reduce unnecessary encryption computations; when the system is under attack, appropriately increasing the encryption probability can still ensure the random stability of the system.

5.2. Typical Scheme

In typical resource-constrained scenarios, selective encryption and random encryption are two representative lightweight protection strategies. The core of selective encryption lies in encrypting only a portion of the critical data, aiming to strike an optimal balance between security gain and computational overhead. Gao Mengzhou [2] modeled this problem as a security optimization problem and solved it by combining the particle swarm optimization algorithm and the stability boundary traversal method. The simulation results show that the optimal encryption strategy will dynamically transition from full encryption to no encryption as the security weight changes, thereby achieving differentiated protection configurations. Complementary to this, random encryption emphasizes randomly performing encryption operations with a certain probability, thereby reducing the average resource consumption statistically. Gao Mengzhou [2] proved the stability conditions of the system under random zero-value attacks based on LMI theory and pointed out that there is an optimal range for the encryption probability. An excessively high probability may even disrupt the system stability. Additionally, Yang Huifeng et al. [8] implemented anti-eavesdropping in semantic communication using a feature confusion method based on random permutation, with a CPU occupancy rate of approximately 25%. This further validates the feasibility and lightness of randomization processing on resource-constrained terminals. The two strategies approach the problem from two dimensions: "selecting the protected objects" and "controlling the protection frequency", providing complementary ideas for encryption design in resource-constrained environments.

5.3. Safety Analysis

The security guarantee mechanisms of selective encryption and random encryption strategies exhibit fundamental differences. The security of the selective encryption strategy is evaluated by constructing a comprehensive quantitative index from three dimensions: integrity, confidentiality, and availability [2]. Gao Mengzhou [2] constructed the integrity/confidentiality index based on attack losses and the availability index based on system stability. Through weighted combination, a unified quantitative security measurement was formed. The essence of its security is the dynamic balance between encryption strength and system stability - simulation results show that when the security weight is high, full encryption is the optimal choice. However, when the availability weight is high, excessive encryption may cause delay and potentially destabilize the system. In this case, not encrypting may be better [2]. This means that the security of selective encryption depends on the accurate classification of data importance and the precise perception of system stability margin. In contrast, the security of the random encryption strategy is analyzed based on the random stability theory [2]. Gao Mengzhou [2] proved the stability conditions of the system under random zero-value attacks using LMI theory, revealing an unexpected phenomenon: there is an optimal interval for the encryption probability - too small a probability cannot effectively resist attacks, and too large a probability will cause delay accumulation and damage system stability [2]. In response to the situation where integrity attacks may damage encrypted data, this research further designed a security compensation controller to expand the system stability domain [2]. The essence of the security of random encryption lies in exchanging average resource consumption reduction for probabilistic protection, while maintaining the random stability of the system through controllable protection probability at critical attack moments. The logical differences in the security logic of the two strategies can be summarized as follows: selective encryption ensures data security in the worst-case scenario through "directional protection" in the spatial domain, and its security depends on the precise identification of the protected objects; while random encryption guarantees system security in a statistical sense through "probability protection" in the temporal domain, and its security depends on the precise matching between the protection frequency and the system stability margin. The two strategies approach from the data dimension and the time dimension respectively, providing two different theoretical paradigms and practical paths for security design in resource-constrained environments.

6. Privacy protection solutions in different application scenarios

6.1. Cloud-edge-end Collaboration Scenario

The cloud-edge-end collaboration architecture consists of three layers: the terminal device layer, the edge service layer, and the cloud service layer. Terminal devices have limited resources, edge nodes have limited computing capabilities, and the cloud has abundant computing power but has higher communication latency. Huang Xiaoping [5] proposed an adaptive lightweight data encryption model for this scenario. This model reduces computing and transmission costs at the source through data cleaning and adopts an adaptive encryption algorithm AEA that intelligently selects three lightweight encryption algorithms (AES, Blowfish, enyo) based on the user's password and runs them in parallel [5]. Experiments show that the AEA algorithm has an encryption delay that can be as low as one-tenth of that of the RSA algorithm, and it only occupies 15.39 GE of resources, making it suitable for small-scale applications where computing capacity is the bottleneck [5].

6.2. Industrial Control System Scenario

Industrial control systems have extremely high requirements for real-time performance and reliability, and the computing capabilities of on-site equipment are limited, making it difficult to deploy traditional encryption protection schemes. Gao Mengzhou [2] from the perspective of cybernetics analyzed the impact of encryption protection on the system's timing and stability, and proposed a selective encryption strategy based on security optimality and a random encryption strategy based on random stability. In the selective encryption, by constructing quantitative indicators for integrity/confidentiality based on attack losses and availability quantitative indicators based on stability, the selection of encryption schemes is modeled as a security

optimization problem [2]. In the random encryption, by performing encryption operations with a certain probability, while ensuring the random stability of the system, the consumption of resources and energy due to encryption is significantly reduced [2].

6.3. Power Internet of Things Scenario

Power Internet of Things terminals are widely distributed, have limited resources, and their wireless communications are vulnerable to eavesdropping attacks. Yang Huifeng et al. [6] proposed a semantic communication architecture based on the Machine Learning as a Service platform for this scenario. They offloaded the task of semantic model training to the cloud, and the terminals only performed inference, effectively reducing the computing burden. To prevent the leakage of model parameters in the Machine Learning as a Service platform and thus prevent eavesdropping, this research designed a feature confusion technology based on random permutation of rows, columns, and channels [6]. Experimental results show that the CPU usage of the feature confusion module remains at around 25%, the memory usage is approximately 120MB, and the average delay for the terminal to restore the image is within 33ms. It can effectively prevent eavesdroppers from restoring the original image on resource-constrained terminals [6].

6.4. Cloud Audit Scenario

After users outsource their data to the cloud server, they lose direct control over the data and need a verifiable auditing mechanism to ensure data integrity. Zhang Xiaqin et al. [6] designed a lightweight privacy protection scheme for cloud auditing, drawing on the scrambling idea in image encryption, using a pseudo-random function to scramble the order of data blocks within the file without incurring additional storage costs. This scheme outsources the calculation task of verifying the labels to the cloud server, significantly reducing the computational costs of users, the cloud server, and third-party auditors [6].

6.5. Federated Learning Scenario

Federated learning enables multiple users to collaboratively train models without revealing their local data. However, collusion attacks between the server and users may pose a threat to privacy security. Guo Xian et al. [3] combined homomorphic encryption and distributed key generation technology to propose an anti-collusion verifiable privacy-preserving federated learning scheme. Through the distributed key generation protocol, the key is collaboratively generated and decrypted, eliminating the reliance on a trusted third party; through bilinear aggregation signatures, users can independently verify the correctness of the server's aggregation results [3]. Experimental results show that this scheme performs well in terms of model convergence speed and prediction accuracy, and the time for users to verify the aggregated results does not increase with the increase in the number of users [3].

6.6. Blockchain Scenarios

The public and transparent nature of blockchain is inherently in conflict with the need for user privacy protection. Liu Feng et al. [10] systematically reviewed the cryptographic privacy protection technologies in blockchain. At the basic element level, it covered methods such as one-time addresses, mixing technology, oracle privacy processing, and smart contract security governance; at the cryptographic primitive level, it analyzed the privacy protection principles and applicable scenarios of technologies such as ring signatures, blind signatures, aggregated signatures, attribute-based encryption, homomorphic encryption, secure multi-party computation, and zero-knowledge proofs [10]. This review also envisioned the application prospects of post-quantum cryptography technologies such as lattice cryptography and fully homomorphic encryption in blockchain privacy protection [10].

6.7. Summary of This Chapter

Overall, the requirements for privacy protection technologies vary across different application scenarios: the cloud-edge-end collaboration scenario focuses on the joint optimization of computing offloading and encryption, the industrial control system scenario emphasizes the guarantee of real-time performance and stability, the power Internet of Things scenario focuses on lightweight anti-eavesdropping, the cloud auditing scenario emphasizes verifiability and low overhead, federated learning focuses on anti-collusion and verifiable aggregation, and blockchain focuses on anonymity and the deep integration of cryptographic primitives. These differentiated requirements collectively drive the lightweight cryptographic technology towards a more scenario-specific and customized direction.

7. Summary and Outlook

7.1. Summary of the Entire Paper

This paper focuses on lightweight data encryption technologies in resource-constrained environments. It systematically reviews and summarizes the existing research from five aspects: lightweight block cipher algorithms, lightweight Hash functions, authentication and key negotiation protocols, selective and random encryption strategies, and privacy protection schemes in typical application scenarios.

First, in the field of lightweight block cipher algorithms, this paper analyzes the differences in hardware efficiency and software performance among three typical structures: Feistel, SPN, and ARX. PRESENT, as the first ultra-lightweight block cipher, adopts a 31-round SPN structure and has a hardware implementation area of approximately 1560 GE; its improved version GIFT further reduces the area to approximately 1345 GE [2]. Chen Ziqian [5] designed the FONA32 and FERX64 algorithms based on pure logical operations, using a dual-branch and four-branch Feistel structure, introducing the XOR operation in the round function to enhance diffusion, achieving encryption rates of 374.6 Mb/s and 328.1 Mb/s respectively, exploring the technical path for minimizing hardware area. Security analysis indicates that a key space of 2^100 or more can resist brute-force attacks, and both FONA32 and FERX64 meet the strict avalanche standard [5].

Secondly, in the field of lightweight Hash functions, this paper discusses two iterative frameworks: the Sponge structure and the MD-like structure. Among them, the Sponge structure has become the mainstream choice due to its flexibility and provable security [5]. The typical algorithm Ascon-Hash, which won the NIST lightweight cryptography competition, adopts a Sponge structure with a 320-bit internal state. The round function includes round constants addition, a 5-bit S-box substitution layer, and a linear diffusion layer

[2,5]. The FAS algorithm proposed by Chen Ziqian [5] is also based on the Sponge structure. It generates a 256-bit message digest with a 64-bit digest rate and a 256-bit capacity, providing 2^128 collision-resistant attack resistance and 2^192 preimage resistance, and the hardware area is approximately 1998 GE less than Ascon-Hash.

Thirdly, in the aspect of identity verification and key negotiation protocols, this paper points out that the existing lightweight authentication schemes mainly have two types of problems: The methods based on static PSK or passwords cannot ensure forward security; protocols such as AugPAKE, although avoiding certificate overhead, still have forward security issues and are vulnerable to replay attacks [3]. Guo Zichao [3] proposed the PSK-ECDHE scheme, which achieves fourfold protection goals of two-way identity authentication, anti-man-in-the-middle attack, anti-replay attack and forward security by XORing the static PSK with the dynamic temporary key of ECDHE to generate a one-time session key. Experiments show that compared with the ECDHE-RSA scheme, the execution time decreases by 26.8%, the CPU usage rate decreases by 41.7%, and the bandwidth consumption decreases by 44.1% [3].

Fourth, in terms of selective and random encryption strategies, this paper analyzes two strategic protection methods aimed at optimizing resource consumption. Gao Mengzhou [9] proposed a selective encryption scheme that models the encryption selection as a security optimization problem. The optimal solution was solved using the particle swarm optimization algorithm and the stability boundary traversal method. Simulation results showed that the optimal solution dynamically changed from full encryption to no encryption. The random encryption scheme was based on LMI theory to prove the stability conditions of the system under random zero-value attacks. It was found that there exists an optimal protection probability interval [9]. Yang Huifeng et al. [6] proposed a feature confusion method that achieves anti-eavesdropping by randomly arranging images in semantic communication. The CPU usage was only approximately 25%, demonstrating the feasibility of the data confusion strategy on resource-constrained terminals [6].

Fifth, in terms of privacy protection in typical application scenarios, this paper summarizes the differentiated requirements and corresponding solutions for five types of scenarios: the cloud-edge-end collaboration scenario uses adaptive encryption AEA to reduce encryption latency to one-tenth of RSA [4]; the industrial control system scenario uses selective/random encryption to ensure the balance between real-time performance and stability [9]; the power Internet of Things scenario uses feature obfuscation to achieve lightweight anti-eavesdropping, with CPU usage being approximately 25% [6]; the cloud auditing scenario uses data block scrambling and label calculation outsourcing to reduce the cost of third-party computing [8]; the federated learning scenario uses homomorphic encryption and distributed key generation to achieve anti-collusion and verifiable aggregation [10]; the blockchain scenario uses cryptographic primitives such as ring signatures and zero-knowledge proofs to achieve anonymity protection [1].

7.2. Research Prospects

Although lightweight data encryption technology has made significant progress, it still faces several problems that need to be addressed urgently. Future research can delve deeper into the following directions

7.2.1. Further Optimization of Authenticated Encryption Algorithms

Most existing studies have designed encryption and authentication functions separately. However, the standardization of Ascon by NIST indicates that a certified encryption algorithm that integrates confidentiality, integrity, and identity authentication is an important trend [2]. How to further reduce the hardware area and power consumption while ensuring the security strength remains a core challenge.

7.2.2. Lightweight Post-Quantum Cryptography

With the rapid development of quantum computing technology, the existing cryptographic systems based on discrete logarithms and large integer factorization are under threat [1]. Although post-quantum schemes such as lattice cryptography and fully homomorphic encryption have shown potential, their computational complexity and key size still cannot meet the requirements of resource-constrained devices [1]. Designing lightweight post-quantum cryptographic solutions suitable for the Internet of Things is a key direction for the future.

7.2.3. Adaptive Protection Against Specific Attacks

Attack methods are becoming increasingly diverse, with emerging threats such as zero-day attacks and side-channel attacks [9]. The existing encryption strategies are mostly designed based on known attack models and lack adaptability to unknown attacks [9]. In the future, by combining artificial intelligence and reinforcement learning technologies, an adaptive encryption mechanism that can dynamically adjust the protection intensity according to the attack situation can be designed.

7.2.4. Standardization and Industrialization Promotion

The standardization work in the field of lightweight cryptography in China is still in its infancy [2]. Promoting the standardization process of domestic lightweight cryptographic algorithms and facilitating their large-scale application in scenarios such as the Internet of Things and industrial Internet is an important way to enhance China's ability for independent control of information security.

In conclusion, lightweight data encryption technology, as the cornerstone for ensuring the security of resource-constrained devices, is evolving from the single algorithm design to a multi-level and systematic approach of algorithm - protocol - strategy - application. Designing authentication encryption algorithms that balance low power consumption and high security, and promoting their standardization and industrialization implementation, is an important trend for the future development of this field.

References

[1] Chen, Z. (2025). Mianxiang wulianwang de qingliangji hash hanshu sheji yu yanjiu [Design and research of lightweight hash function for the internet of things] (Master's thesis). Zhongyuan University of Technology.

[2] Gao, M. (2017). Mianxiang ziyuan shouxian kongzhi xitong anquan de xuanze xing ji suijixing jiami celve yanjiu [Research on selective and stochastic encryption strategies for the resource-constrained control systems security] (Doctoral dissertation). Zhejiang University.

[3] Guo, X., Wang, D., Feng, T., Cheng, Y., & Jiang, Y. (2025). Jiyu tongtai jiami de keyanzheng yinsi baohu lianbang xuexi fangan [A verifiable privacy protection federated learning scheme based on homomorphic encryption]. Journal of Electronics & Information Technology, 47(4), 1113-1125.

[4] Guo, Z. (2023). Mianxiang shouxian wulianwang shebei qingliangji anquan fangan yanjiu yu shixian [Research and implementation of lightweight security solutions for constrained iot devices] (Master's thesis). Southeast University.

[5] Huang, X. (2024). Jiyu yunbian duan xietong de anquan gaoxiao xinxi chuanshu celve yanjiu [Research on secure and efficient information transmission strategy based on cloud-edge-device collaboration] (Master's thesis). Nanjing University of Posts and Telecommunications.

[6] Zhang, X., Yao, Y., & Wang, Y. (2024). Mianxiang yun shenji de qingliangji yinsi baohu fangan [Lightweight privacy protection scheme for cloud audit]. Journal of Chongqing University, 47(2), 75-83.

[7] Li, X., Zhang, S., Hu, P., & Deng, C. (2023). Qingliangji mima suanfa duibi fenxi ji yingyong [Comparative analysis and application of lightweight cryptography algorithm]. Communications Technology, 56(12), 1401-1410.

[8] Yang, H., Shang, L., Cui, J., Liu, H., Wang, J., & Lin, P. (2025). Mianxiang ziyuan shouxian dianli wulianwang zhongduan de yuyi anquan tongxin fangfa [A semantic secure communication approach for resource-constrained power IoT terminals]. Chinese Journal on Internet of Things, 9(2), 106-116.

[9] Li, Z. (2022). Bianyuan jisuan jiedian ziyuan shouxian de ruqin jiance celve yanjiu [Research on intrusion detection strategy with limited resource of edge computing nodes] (Master's thesis). Donghua University.

[10] Liu, F., Yang, J., & Qi, J. (2022). Qukuailian mima xue yinsi baohu jishu zongshu [Survey on blockchain privacy protection techniques in cryptography]. Journal of Cyber Security, 7(4), 1-19.