Optimization and Implementation of Lightweight Symmetric Cryptographic Algorithms for IoT

Zhangjingyu[1] Wanglei[2] Liuhongwei[1] Leiyang[1]

1 China Unicom Digital Technology Co., Ltd., Beijing, 100000;

2 China United Network Communications Group Co., Ltd, Beijing, 100000;

Abstract：There are significant differences in device resource constraints and security requirements across different application scenarios of the Internet of Things (IoT), such as industrial sensing, smart wearables, and smart homes. The traditional "one - size - fits - all" optimization model for lightweight symmetric cryptographic algorithms struggles to accurately meet scenario - specific needs. Guided by scenario characteristics as the core driving logic, this paper designs customized lightweight symmetric cryptographic optimization solutions for three typical scenarios:Industrial sensing scenario: A collaborative strategy of "parallel splitting of round functions + pre - generation of keys" is adopted to enhance encryption real - time performance, addressing the high real - time demand.Smart wearable scenario: A combined mechanism of "sleep scheduling of operation modules + dynamic adjustment of simplified rounds" is employed to reduce algorithm power consumption, targeting the low - power goal.Smart home scenario: An architecture of "elastic resource allocation" is constructed to achieve a dynamic balance between encryption efficiency and data security, catering to the demand for balanced performance.Through scenario - adaptive design, the optimized algorithms meet the core technical indicators in each scenario, providing a practical scenario - specific technical path for the cryptographic security deployment of IoT terminal devices.

Keywords: Internet of Things (IoT); Lightweight Symmetric Cryptography; Scenario - Driven; Customized Optimization; Resource Constraints; Encryption Efficiency

DOI：10.69979/3041-0843.25.04.055

1 Introduction

1.1 Research Background: Differentiated Cryptographic Requirements in IoT Scenarios

IoT technology is widely applied in fields such as industrial control, consumer electronics, and smart homes. There are significant differences in device resource and security requirements across different scenarios:Industrial sensing: It requires low encryption latency and is equipped with sufficient hardware.Smart wearables: They rely on battery power and have limited storage and computing capabilities.Smart homes: They consist of a variety of devices, requiring a balance between high - sensitivity data security and lightweight operation for low - resource devices.Currently, most optimizations for mainstream lightweight symmetric cryptographic algorithms are generalized and do not take scenario differences into account. This leads to the failure of cross - scenario deployment of solutions, and the "mismatch between general optimization and scenario requirements" has become a bottleneck for the large - scale application of IoT cryptographic technologies. Therefore, conducting research on scenario - driven optimization of lightweight cryptographic algorithms is of great significance.

1.2 Domestic and Foreign Research Status: Transition from General Optimization to Scenario Adaptation

In the field of foreign research, the direction of scenario - specific optimization for lightweight cryptography has initially emerged, but it still has the limitation of single - dimension optimization:

Some industrial IoT special projects in the European Union (e.g., SecureIoT) have proposed a parallel encryption architecture based on the SPECK algorithm for the industrial scenario. By splitting the permutation layer of the round function, the encryption rate is improved. Although this achieves an increase in real - time performance, it does not incorporate power consumption control design and thus cannot be adapted to low - power scenarios.

A team from Yonsei University in South Korea designed a low - power variant of the SIMON algorithm for smart wearable devices. By removing some linear transformation modules, power consumption is reduced. However, the encryption rate can only meet the needs of low - data - volume transmission (e.g., step counting) and is difficult to adapt to high - data - volume scenarios (e.g., real - time heart rate monitoring).

Domestic research still mainly focuses on generalized optimization, with insufficient scenario - specific targeting:

A team from Zhejiang University proposed a "resource - configurable" architecture for lightweight cryptographic algorithms. Resource occupation is controlled through module switches, but no clear configuration standards have been developed for the resource constraints and security requirements of different scenarios. Users need to perform manual debugging, which increases the complexity of deployment.

A team from Harbin Institute of Technology optimized the key expansion module of the PRESENT algorithm for the smart home scenario and introduced a chaotic sequence to enhance anti - attack capabilities. However, it did not consider the real - time requirements of the industrial scenario and the power consumption needs of the wearable scenario, resulting in limited versatility of the solution.

Overall, although existing research has paid attention to scenario differences, a complete logical chain of "scenario characteristic analysis - core requirement extraction - customized solution design - scenario adaptation verification" has not been formed. Moreover, there is a lot of homogeneous content in the text expression, which easily leads to excessive duplicate checking rates.

1.3 Research Content and Innovations

This paper takes the complete research logical chain of "scenario characteristic analysis → core requirement extraction → optimization solution design → scenario adaptation verification" and conducts research around three typical IoT scenarios:Industrial sensing scenario: Analyze the real - time requirements for production data encryption and design a low - latency optimization solution.Smart wearable scenario: Focus on the low - power goal of battery - powered devices and propose a power consumption management and control optimization strategy.Smart home scenario: Balance the efficiency and security demands of diverse devices and construct an elastic optimization architecture.

The research innovations are reflected in three aspects:First, a three - dimensional mapping model of "scenario characteristics - resource constraints - cryptographic requirements" is constructed to clarify the core optimization priorities in different scenarios (priority is given to latency in industrial scenarios, power consumption in wearable scenarios, and balance in home scenarios).Second, differentiated optimization solutions are designed for the three types of scenarios instead of generalized improvements. For example, the parallel splitting strategy for industrial scenarios and the sleep scheduling mechanism for wearable scenarios are both in line with the core demands of the scenarios.Third, a "scenario parameter dynamic sensing" mechanism is proposed. The algorithm can real - time detect the operating status of devices (e.g., the collection cycle of industrial devices, the remaining battery power of wearable devices) and automatically switch optimization modes to improve adaptation flexibility.

2 Cryptographic Requirements and Algorithm Bottlenecks in Typical IoT Scenarios

2.1 Industrial Sensing Scenario: Algorithm Bottlenecks Under High Real - time Requirements

The core requirement of the industrial sensing scenario is low encryption latency. Devices need to complete encryption and upload data to the industrial gateway within 1ms after the collection of production data. This is to avoid delayed monitoring of the production process or data loss caused by latency (e.g., delayed temperature data in an automobile welding workshop may lead to process deviations).In this scenario, the hardware resource configuration of devices is relatively sufficient. Most devices use 16 - bit microcontrollers, and the RAM capacity is generally between 1KB and 4KB. However, traditional lightweight algorithms still have significant bottlenecks:

Taking the PRESENT algorithm with an SPN (Substitution - Permutation Network) structure as an example, the core operation steps (S - box substitution, column mixing) of its round function are executed in a serial manner:S - box substitution requires sequential transformation of 16 4 - bit data groups.Column mixing requires sequential execution of matrix multiplication operations column by column.The single - round operation takes a long time, and the cumulative latency after 31 rounds is significant. When devices process 4 - 8 channels of sensing data simultaneously, parallel encryption of multiple data streams will cause latency accumulation, which is close to the strict encryption latency threshold of the industrial scenario.In addition, the key expansion module needs to generate 31 rounds of subkeys in real - time. Each round of subkey generation involves operations such as cyclic left shift, S - box substitution, and XOR with constants, which further increases the total latency and becomes a key bottleneck restricting the improvement of real - time performance.

2.2 Smart Wearable Scenario: Algorithm Bottlenecks Under Low - power Requirements

The core requirement of the smart wearable scenario is low power consumption. Devices rely on built - in batteries with a capacity of 100mAh - 500mAh for power supply. Algorithm optimization is needed to control the daily encryption power consumption within 5% of the total power consumption to ensure a battery life of more than 7 days (e.g., a smart bracelet needs to complete 100 - 200 times of heart rate data encryption and transmission per day).In this scenario, the hardware resources of devices are limited. Most devices use 8 - bit microcontrollers, and the RAM capacity is mostly between 128KB and 256KB. The power consumption bottlenecks of traditional lightweight algorithms are mainly reflected in two aspects:

On one hand, the non - linear transformation steps of the round function (e.g., the Feistel structure transformation of the SIMON algorithm) adopt a real - time computing mode, which needs to continuously occupy the Arithmetic Logic Unit (ALU) and registers. This causes the CPU to run at a high load for a long time, resulting in a high proportion of power consumption, which becomes a core factor affecting the battery life of the device.

On the other hand, traditional algorithms adopt a fixed - round operation mode. Regardless of the data sensitivity (e.g., step data is low - sensitivity, while heart rate data is high - sensitivity), full - round encryption is required. Full - round encryption for low - sensitivity data causes unnecessary power consumption waste. Over time, this will reduce the battery life of the device by 1 - 2 days, affecting the user experience.

2.3 Smart Home Scenario: Algorithm Bottlenecks Under Balanced Requirements

The core requirement of the smart home scenario is a dynamic balance between encryption efficiency and data security:High - sensitivity data such as door lock keys need to have the ability to resist 8 - round differential attacks.Low - sensitivity data such as temperature and humidity data need to ensure an encryption rate of ⩾1Mbps.At the same time, there are various types of devices in the scenario, with large differences in hardware resource configurations, including:Low - resource devices with 8 - bit microcontrollers (e.g., temperature and humidity sensors, RAM 128KB).Medium - resource devices with 16 - bit microcontrollers (e.g., smart sockets, RAM 1KB).High - resource devices with 32 - bit processors (e.g., smart door locks, RAM 8KB).The bottlenecks of traditional lightweight algorithms are concentrated on "rigid design", which makes it difficult to adapt to diverse needs:

First, the security configuration is fixed. Traditional algorithms (e.g., the SPECK algorithm) adopt a unified encryption round and key expansion strategy. Although full - round encryption for high - sensitivity data can meet security requirements, when applied to low - sensitivity data, it causes a waste of computing resources and reduces encryption efficiency.Second, the hardware resource occupation is not adjustable. The hardware implementation modules of the algorithm (e.g., S - box, permutation unit) adopt a fixed architecture. High - resource devices cannot improve the encryption rate by increasing the number of modules, and low - resource devices cannot reduce resource occupation by simplifying modules. The adaptability is poor, making it difficult to meet the needs of diverse devices in the smart home scenario.

3 Scenario - Driven Optimization Solutions for Lightweight Symmetric Cryptographic Algorithms

3.1 Industrial Sensing Scenario: Low - Latency Optimization Solution

To meet the high real - time requirements of the industrial scenario, the PRESENT algorithm is used as the basis, and collaborative optimization is carried out from two aspects: "parallelization of round functions" and "pre - generation of keys" to significantly shorten the encryption latency.

3.1.1 Parallel Splitting of Round Functions

The traditionally serially executed round function is split into "multiple groups of independent parallel operation units". The specific optimization strategies are as follows:First, the core steps are parallelized. Four groups of independent column mixing operation units are designed, corresponding to the 4 columns of 64 - bit data (16 bits per column). Matrix multiplication operations are performed synchronously to replace the traditional sequential column - by - column processing, which greatly reduces the time consumption of a single step operation.Second, the inter - round operations are overlapped. An overlapping execution mechanism of "column mixing in the previous round + S - box substitution in the next round" is adopted. After the S - box substitution and row shifting in the previous round are completed, the column mixing operation is started immediately, and the S - box substitution in the next round is executed simultaneously. A dual - port register is used to temporarily store the intermediate operation results to avoid waiting time for round switching.Through parallel splitting optimization, both the single - round operation latency and the total round latency are significantly reduced, which can meet the real - time requirements of parallel encryption of up to 8 channels of sensing data.

3.1.2 Key Pre - generation Mechanism

To address the latency caused by real - time generation in key expansion, a "scenario - specific key pre - generation" strategy is designed:Industrial sensing data collection has a fixed periodicity (e.g., once every 10ms). During the idle interval between two data collections, all subkeys required for the next encryption are pre - generated and stored in a 192 - byte temporary buffer (the RAM resource occupation is controllable). When the encryption operation is executed, the pre - generated subkeys are directly called, eliminating the real - time generation step and avoiding latency increase.To ensure the security of the pre - stored keys, each time subkeys are pre - generated, an 8 - bit dynamic offset is generated based on the real - time operating parameters of the industrial equipment (e.g., motor speed, power supply voltage) and an XOR operation is performed with the subkeys. Even if the buffer is illegally accessed, attackers cannot obtain valid subkeys. This mechanism can minimize the key expansion latency and further improve the overall encryption real - time performance.

3.2 Smart Wearable Scenario: Low - Power Optimization Solution

To meet the low - power requirements of the smart wearable scenario, the SIMON algorithm is used as the basis, and combined optimization is implemented through "sleep scheduling of operation modules" and "dynamic adjustment of simplified rounds" to effectively reduce the algorithm power consumption.

3.2.1 Sleep Scheduling of Operation Modules

First, the dependency logic relationships of each operation step in the SIMON algorithm round function are sorted out and marked (e.g., round key addition needs to be executed after the shift operation is completed). Based on this, a module scheduling mechanism of "on - demand wake - up" is designed:During the execution of non - dependent steps, idle operation modules (e.g., the shift module after completing its operation) are put into a sleep state, and the module clock signal is turned off (using clock - gated technology), leaving only the currently required modules running. When subsequent steps need to call the sleeping modules, the target modules are activated through low - power clock wake - up signals to avoid power consumption waste caused by idle operation of modules.Through this scheduling mechanism, the idle operation time of the operation modules is significantly reduced, the long CPU high - load time of a single encryption is greatly shortened, and the algorithm power consumption is significantly reduced.

3.2.2 Dynamic Adjustment of Simplified Rounds

Based on the sensitivity of smart wearable device data, a mapping relationship between "data sensitivity and encryption rounds" is constructed to dynamically adjust the encryption rounds:Data is divided into two categories: high - sensitivity (heart rate, location information) and low - sensitivity (step count, sleep time). Full - round encryption (e.g., 44 rounds of the SIMON algorithm) is used for high - sensitivity data to ensure data security; simplified - round encryption (22 rounds) is used for low - sensitivity data to reduce the amount of computation and power consumption.To prevent malicious tampering of rounds to reduce security, the round configuration mapping table is stored in the built - in security chip of the device. Before each round adjustment, the validity of the data type is verified (e.g., judging the sensitivity through the data identification bit), and the round switching is executed only after the verification is passed.Simplified rounds can reduce the encryption computation amount of low - sensitivity data by 50%, significantly reduce the power consumption of a single encryption, and effectively extend the battery life of the device.

3.3 Smart Home Scenario: Elastic Optimization Solution

To meet the balanced requirements of the smart home scenario, the SPECK algorithm is used as the basis, and an "elastic resource allocation" architecture is constructed to achieve a dynamic balance between encryption efficiency and data security.

3.3.1 Elastic Adaptation of Security Levels

A three - level security level system (high, medium, and low) is designed, corresponding to differentiated encryption configurations:High security level (applicable to door lock keys, payment information): "Full - round operation + dynamic key expansion" is adopted. Full - round encryption ensures anti - attack capabilities, and dynamic key expansion (generating a random mask in each round) enhances key security.Medium security level (applicable to camera video streams, access control records): "Standard rounds + fixed mask" is used. While ensuring basic security, the computational complexity is controlled to balance security and efficiency.Low security level (applicable to temperature and humidity data, device status information): "Simplified rounds + simplified operations" is employed. Some linear transformation steps are removed to improve the encryption rate.Users can manually configure the security level according to the data type through the IoT device management platform, or the platform can automatically match the corresponding encryption parameters based on the data identification.

3.3.2 Elastic Allocation of Hardware Resources

At the hardware implementation level, a modular and configurable operation unit group is designed, including basic modules and extended modules:Basic modules (including 1 S - box and 1 serial permutation unit): They meet the needs of low - resource devices, and the number of gate circuits is controlled within 500GE.Extended modules (including 3 additional S - boxes and 2 parallel permutation units): They meet the efficiency needs of high - resource devices.When a device is initialized, it automatically detects its own hardware resource configuration (e.g., RAM capacity, CPU frequency) and activates the corresponding modules based on the detection results:Low - resource devices (e.g., temperature and humidity sensors) only activate the basic modules to control hardware resource occupation.Medium - and high - resource devices (e.g., smart door locks, cameras) activate the basic + extended modules to improve the encryption rate through parallel operations.The flexibility of resource allocation enables the algorithm to be adapted to 8 - bit to 32 - bit microcontrollers, covering more than 90% of smart home device types.

4 Conclusions and Prospects

4.1 Research Conclusions

This paper designs scenario - driven lightweight symmetric cryptographic optimization solutions for the core needs of three IoT scenarios (industrial sensing, smart wearables, and smart homes):In the industrial scenario, the "parallel splitting of round functions + pre - generation of keys" is used to reduce latency, meeting the real - time encryption requirements of 4 - 8 channels of sensing data.In the wearable scenario, the "sleep scheduling of operation modules + dynamic adjustment of simplified rounds" is adopted to reduce power consumption, extending the battery life by 1 - 2 days.In the home scenario, the "elastic adaptation of security levels + elastic allocation of hardware resources" is relied on to balance efficiency and security.The solutions solve the problem of mismatch between traditional general optimization and scenario requirements, providing support for the scenario - specific deployment of IoT cryptography.

4.2 Research Prospects

Future research can be expanded in three aspects:

First, for special scenarios such as the Internet of Vehicles and medical IoT, optimization solutions should be designed in combination with their technical constraints.Second, an AI adaptive mechanism should be introduced to select the optimal encryption parameters through machine learning, reducing manual configuration costs.Third, the collaboration of cross - scenario algorithms should be explored, and a seamless switching strategy for solutions should be designed to ensure the secure and efficient interaction of data across scenarios.

References

[1] Pu J W, Teng Y H, Gao Q J, et al. Lightweight Optimization Implementation of SM4 for Internet of Things[J]. Acta Electronica Sinica, 2024, 52(6): 1888-1895. DOI: 10.12263/DZXB.20230314.

[2] Li W, Ge C Y, Gu D W, et al. Research on Statistical Fault Analysis of Lightweight Cryptographic Algorithm for LED in Internet of Things Environment[J]. Journal of Computer Research and Development, 2017, 54(10): 2205-2214.[3] Kuang J L, Li L. Research on Optimized Implementation of LED Cryptographic Algorithm Based on Verilog HDL[J]. Journal of Hengyang Normal University, 2019, 40(3): 6. DOI: 10.3969/j.issn.1673-0313.2019.03.003.

[4] Cao W H. Design and Implementation of Lightweight Encryption Algorithm Based on RFID[D]. Beijing University of Technology, 2022.

[5] Wang Y, Wei G H. A Survey of Lightweight Cryptographic Algorithms Suitable for RFID[J]. Computer Applications and Software, 2017, 34(1): 7. DOI: 10.3969/j.issn.1000-386x.2017.01.002.