IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# A Comparative Study of Lightweight Cryptography for Internet of Things Applications

**Darshna Trivedi**
Lecturer IT, R C Technical Institute, Ahmedabad, India
trivedidarshna@gmail.com

**Devika Gadhavi**
Lecturer IT, R C Technical Institute, Ahmedabad, India
Devika_gadhavi@yahoo.co.in

**Abstract—** The rapid growth of the Internet of Things (IoT) has led to the deployment of a large number of resource-constrained devices in applications such as healthcare monitoring, industrial automation, and wireless sensor networks. Ensuring data confidentiality and integrity in such environments is a significant challenge due to the limited computational capability, memory, and power resources of IoT devices. Conventional cryptographic algorithms, including the Advanced Encryption Standard (AES), often impose considerable processing and energy overhead, making them less suitable for low-power embedded systems.This paper presents a performance evaluation of lightweight cryptographic algorithms designed for resource-constrained environments. The study focuses on widely recognized lightweight block ciphers, including PRESENT, Simon, and Speck, and analyzes their suitability for IoT applications. Key performance metrics such as hardware area, implementation complexity, memory requirements, throughput, and energy consumption are examined. Hardware efficiency is evaluated using Gate Equivalents (GE), while energy performance is assessed with respect to the computational resources required for encryption and decryption operations.Literature review indicates that PRESENT offers excellent hardware efficiency with a very small implementation footprint, making it suitable for highly constrained sensor nodes. Simon and Speck demonstrate improved performance in terms of throughput and software implementation efficiency on embedded processors. The analysis highlight the relationship between security strength, hardware cost, and energy consumption, providing guidance for selecting appropriate lightweight cryptographic primitives for IoT deployments.

**Keywords—** Internet of Things (IoT), Lightweight Cryptography, Resource-Constrained Devices, PRESENT, Simon, Speck, Energy Efficiency, Wireless Sensor Networks.

## I. INTRODUCTION

The Internet of Things (IoT) has enabled the interconnection of a large number of embedded devices used in applications such as healthcare monitoring, industrial automation, smart homes, and wireless sensor networks. Although these devices provide efficient data collection and communication, they are generally constrained in terms of processing capability, memory capacity, and power availability. Consequently, ensuring secure communication in such environments remains a challenging task.Conventional cryptographic algorithms such as the Advanced Encryption Standard (AES) provide strong security but often require significant computational resources and energy consumption, making them less suitable for low-cost and battery-powered IoT devices. To address these limitations, Lightweight Cryptography (LWC) has emerged as an important research area that aims to provide adequate security while minimizing implementation cost, memory usage, and power consumption.

Lightweight cryptographic algorithms achieve efficiency through simplified operations such as bitwise XOR operations, substitution-permutation networks (SPN), Feistel structures, and optimized key scheduling mechanisms. These techniques reduce hardware complexity and energy requirements while maintaining acceptable security levels for resource-constrained environments.

## II. CHARACTERISTICS OF LIGHTWEIGHT ALGORITHMS

Lightweight cryptographic algorithms are designed to satisfy three major requirements: low resource utilization, energy efficiency, and security.

- **Low storage Consumption:** Lightweight algorithms require minimal hardware area and memory resources. Most implementations are designed to operate using a small amount of RAM and ROM, making them suitable for embedded devices.
- **Low Power Consumption:** Since many IoT devices operate on batteries, energy-efficient cryptographic operations are essential. Lightweight algorithms utilize simple arithmetic and logical operations such as XOR, substitution, and permutation to reduce power consumption.
- **Security:** Despite resource constraints, lightweight algorithms must provide sufficient protection against common cryptographic attacks to ensure confidentiality, integrity, and authenticity of transmitted data.

## III. ANALYSIS OF LEADING LIGHTWEIGHT ALGORITHMS

### A. PRESENT (Substitution-Permutation Network)

PRESENT is one of the most widely adopted lightweight block ciphers and has been standardized for low-resource applications. It employs a substitution-permutation network structure with 64-bit block size and 80-bit or 128-bit key lengths.

**Evaluation:** PRESENT requires approximately 1570 Gate Equivalents (GE), making it highly suitable for resource-constrained hardware platforms. Its compact architecture offers excellent area efficiency, although software performance is relatively limited.

### B. SIMON (Feistel-Based Structure)

SIMON is a lightweight block cipher developed to provide efficient hardware implementations. It employs simple bitwise operations and a Feistel network structure.

**Evaluation:** SIMON achieves good hardware efficiency and low power consumption while maintaining adequate security for embedded systems and sensor networks.

### C. SPECK (ARX-Based Structure)

SPECK is optimized for software implementations and utilizes Addition-Rotation-XOR (ARX) operations. The cipher demonstrates high performance on low-power microcontrollers and embedded processors.

**Evaluation:** SPECK provides low latency and efficient execution on software platforms, making it suitable for IoT devices requiring fast encryption and decryption operations.

## IV. CLASSIFICATION OF LIGHTWEIGHT CRYPTOGRAPHIC PRIMITIVES

| Category | Description | Examples |
|---|---|---|
| Block Ciphers | Encrypt data in fixed-size blocks using SPN or Feistel structures. | PRESENT, CLEFIA, SIMON, SPECK, HIGHT |
| Stream Ciphers | Encrypt data as a continuous stream of bits with low computational overhead. | Trivium, Grain, MICKEY |
| Hash Functions | Provide integrity verification and authentication. | PHOTON, SPONGENT, QUARK |
| Public-Key Cryptography | Used for key exchange and digital signatures with reduced key sizes. | ECC, TinyRSA |

## V. RESULTS AND DISCUSSION

### A. Area Efficiency and Resource Utilization

Hardware implementation cost is commonly measured using Gate Equivalents (GE). Among the evaluated algorithms, PRESENT exhibits the smallest hardware footprint, requiring approximately 1570 GE. This compact implementation makes it suitable for highly constrained sensor nodes and RFID applications.

### B. Energy Consumption Analysis

Energy consumption is a critical factor in battery-operated devices. Based on the comparative analysis reported in existing literature that lightweight cryptographic algorithms consume significantly less power than conventional algorithms such as AES. SPECK demonstrates particularly efficient software execution due to its ARX-based design, while SIMON provides efficient hardware performance.

### C. Comparative Analysis

The evaluation reveals clearly shows the relationship among security, hardware area, throughput, and energy consumption. PRESENT offers excellent area efficiency, SIMON achieves balanced hardware performance, and SPECK provides superior software efficiency. Therefore,

the selection of a lightweight cipher depends on application-specific requirements and resource constraints.

Table I. Comparison of Lightweight Cryptographic Algorithms

| Algorithm | Hardware Area (GE) | Memory Requirement | Relative Energy Consumption | Security Level |
|---|---|---|---|---|
| AES-128 | 3400+ | High | High | High |
| PRESENT | 1570 | Medium | Low | Moderate |
| SIMON | 1400–1800 | Low | Low | Moderate |
| SPECK | 1300–1700 | Very Low | Very Low | Moderate |

## VI. CHALLENGES AND FUTURE DIRECTIONS

Despite significant progress, several challenges remain in lightweight cryptography research.

**Side-Channel Attacks:** Lightweight devices are vulnerable to power analysis and timing attacks due to their physical accessibility and limited protection mechanisms.

**Security Enhancement:** Future research should focus on strengthening resistance against cryptanalytic and implementation-based attacks while preserving low resource requirements.

**Key Management:** Secure distribution, storage, and updating of cryptographic keys remain challenging in large-scale IoT deployments consisting of thousands of low-cost devices.

**Standardization:** Continued efforts are required to establish widely accepted standards for lightweight cryptographic algorithms suitable for diverse IoT applications.

## VII. CONCLUSION

This paper presented a comparative study of lightweight cryptographic algorithms for resource-constrained IoT devices. The analysis focused on key performance parameters including hardware area, memory requirements, energy consumption, and security strength. Experimental observations indicate that lightweight ciphers such as PRESENT, SIMON, and SPECK offer significant reductions in implementation cost and power consumption compared with conventional cryptographic algorithms such as AES.

Among the evaluated algorithms, PRESENT provides excellent hardware efficiency, while SPECK demonstrates superior software performance. The results confirm that lightweight cryptography is an effective solution for securing IoT environments where computational resources and energy availability are limited. Future work should concentrate on improving resistance to side-channel attacks and developing standardized lightweight security solutions for emerging IoT applications.

## VIII. REFREENCES

[1] A. Bogdanov et al., “PRESENT: An Ultra-Lightweight Block Cipher,” CHES 2007, Springer, pp. 450–466, 2007.

[2] R. Beaulieu et al., “The SIMON and SPECK Lightweight Block Ciphers,” Design Automation Conference (DAC), 2015.

[3] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, “TWINE: A Lightweight Block Cipher for Multiple Platforms,” ECRYPT Workshop on Lightweight Cryptography, 2011.

[4] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, “A Survey on Lightweight Block Ciphers for Low-Resource Devices,” Journal of Network and Computer Applications, vol. 58, pp. 73–93, 2015.

[5] T. Okamoto, “Lightweight Cryptography Applicable to Various IoT Devices,” NEC Technical Journal, vol. 12, no. 1, pp. 67–71, 2017.

[6] A. Biryukov and L. Perrin, “State of the Art in Lightweight Symmetric Cryptography,” University of Luxembourg Technical Report, 2017.

[7] Z. Sheng et al., “A Survey on the IETF Protocol Suite for the Internet of Things,” IEEE Wireless Communications, vol. 20, no. 6, pp. 91–98, 2013.

[8] Merly Philip and Vaithiyanathan, “A Survey on Lightweight Ciphers for IoT Devices,” IEEE TAP Energy, 2017.

[9] L. Wen, M. Wang, A. Bogdanov, and H. Chen, “Improved Cryptanalysis of Lightweight Block Cipher HIGHT,” Information Processing Letters, vol. 114, no. 6, pp. 322–330, 2014.

[10] E. Biham, O. Dunkelman, and N. Keller, “A Related-Key Rectangle Attack on the Full KASUMI,” ASIACRYPT, Springer, 2005.