INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY RESEARCH STUDIES (IJITRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: ISSN Print

Securing the Internet of Things: A Comprehensive Analysis of Lightweight Cryptographic Approaches for Resource-Constrained Devices

Krishna Prasad K, Associate Professor, Department of Information Science and Engineering, A J Institute of Engineering and Technology, Kottara Chowki, Mangaluru, Karnataka, India.

Article information
Received: 21st January 2025
Received in revised form: 11th February 2025
Accepted: 10th March 2025
Available online: 30th April 2025

Volume:1
Issue: 1
DOI: https://doi.org/10.5281/zenodo.15309858

Abstract
The rapid proliferation of Internet of Things (IoT) devices has introduced significant security challenges due to their resource constraints and widespread deployment in critical applications. This research examines lightweight cryptographic approaches that can provide robust security for IoT communication while operating within the severe computational, memory, and energy limitations of IoT devices. Through systematic analysis of existing lightweight cryptographic primitives, protocols, and frameworks, this paper identifies the most promising solutions for securing IoT ecosystems. Our findings indicate that optimized implementations of established algorithms like AES, novel lightweight block ciphers such as PRESENT and SIMON, and emerging post-quantum resistant schemes offer viable security options for different IoT deployment scenarios. The research also evaluates implementation challenges, performance metrics, and security-efficiency tradeoffs across various IoT application domains. This comprehensive analysis contributes to the growing body of knowledge on IoT security by providing a structured evaluation framework for selecting appropriate lightweight cryptographic solutions based on specific IoT device constraints and security requirements.

Keywords: - Embedded Security, Internet of Things, Lightweight Cryptography, Low-Power Encryption ,NIST Lightweight Cryptography Standardization, Post-Quantum IoT Security, Resource-Constrained Devices, Secure Communication Protocols

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms of the 21st century, connecting billions of physical devices to the internet and enabling unprecedented levels of data collection, automation, and remote control capabilities. From smart homes and wearable health monitors to industrial control systems and smart city infrastructure, IoT technologies are fundamentally changing how we interact with the world around us. Gartner estimates that by 2025, over 75 billion connected devices will be in operation worldwide, creating an expansive and complex ecosystem of interconnected system

However, this explosive growth in connectivity brings with it profound security challenges. IoT devices are often characterized by severe constraints in processing power, memory capacity, energy availability, and physical size. These limitations make implementing robust security measures particularly challenging, as traditional cryptographic algorithms and security protocols typically demand substantial computational resources that exceed the capabilities of many IoT devices. This security-resource gap is especially concerning given that IoT systems frequently handle sensitive personal data, control critical infrastructure, or operate in environments where compromise could lead to significant physical harm or financial damage.

A. Research Problem and Objectives

The central research question addressed in this paper is: How can effective security be provided for IoT communication within the severe resource constraints typical of IoT devices? This question encompasses several interrelated challenges, including the selection of appropriate cryptographic primitives, the design of efficient security protocols, and the implementation of practical security frameworks suitable for various IoT deployment scenarios.

The specific objectives of this research are to:

- Analyze and classify the current state of lightweight cryptographic approaches for IoT security
- Evaluate the performance characteristics and security properties of leading lightweight cryptographic algorithms
- Assess the suitability of different approaches for various IoT application domains and their specific constraints
- Identify implementation challenges and propose practical solutions for secure IoT deployments
- Develop a structured framework for selecting appropriate lightweight cryptographic solutions based on IoT device constraints and security requirements

B. Significance of the Research

The significance of this research is multifaceted. First, it addresses a critical gap in the current technological landscape—the need for security solutions that are both robust and feasible within IoT constraints. Second, it provides a comprehensive analysis that can guide system designers, security engineers, and IoT manufacturers in making informed decisions about security implementations. Third, it contributes to the growing body of knowledge on IoT security by systematically evaluating emerging approaches and identifying promising directions for future research and development.

As IoT devices increasingly permeate critical infrastructure, healthcare systems, and other sensitive domains, the consequences of inadequate security become increasingly severe. High-profile incidents such as the Mirai botnet attack, which harnessed vulnerable IoT devices to launch devastating distributed denial-of-service attacks, highlight the urgency of addressing IoT security challenges. This research aims to provide practical guidance that can help mitigate such risks while enabling the continued growth and innovation of IoT technologies.

C. Scope and Limitations

This research focuses specifically on cryptographic approaches for securing communications between IoT devices and between IoT devices and backend systems. While acknowledging the importance of physical security, secure boot mechanisms, and other aspects of comprehensive IoT security, these topics fall outside the primary scope of this analysis. Similarly, while the research touches on broader IoT security frameworks and standards, its primary focus is on the cryptographic building blocks that enable secure communication.

The analysis is constrained to approaches that are suitable for implementation on devices with significant resource limitations, typically including:

- Processing capabilities equivalent to 8-bit, 16-bit, or low-end 32-bit microcontrollers
- Memory availability ranging from a few kilobytes to several megabytes
- Power constraints requiring efficient operation, often on battery power
- Network connectivity with limited bandwidth and potentially intermittent availability

This research does not address the security of cloud infrastructure, data analytics platforms, or other backend systems that may form part of a complete IoT ecosystem, except insofar as they interact directly with resource-constrained devices.

II. LITERATURE REVIEW

The field of lightweight cryptography for IoT security has seen substantial research activity in recent years, driven by the growing recognition of both the security challenges posed by IoT deployment and the inadequacy of traditional cryptographic approaches in resource-constrained environments. This literature review synthesizes findings from recent studies, organizing them into four key areas: lightweight block ciphers, lightweight authentication and key exchange protocols, standardization efforts, and implementation challenges in real-world IoT deployments

A. Lightweight Block Ciphers for IoT

Traditional block ciphers such as AES (Advanced Encryption Standard) were designed with security as the primary concern, with less emphasis on performance in highly constrained environments. Singh et al. [1] conducted a comprehensive comparison of lightweight block ciphers, evaluating their suitability for IoT applications. Their analysis showed that ciphers such as PRESENT, SIMON, SPECK, and SKINNY offer significant advantages in resource utilization while maintaining acceptable security margins.

PRESENT, proposed by Bogdanov et al. [2], has gained particular attention as one of the first block ciphers specifically designed for resource-constrained environments. With a block size of 64 bits and key sizes of 80 or 128 bits, PRESENT has been demonstrated to require substantially fewer resources than AES while providing adequate security for many IoT applications. Hardware implementations of PRESENT have been shown to require as few as 1570 gate equivalents (GE), making it suitable for implementation in very constrained devices.

The NSA-designed lightweight block ciphers SIMON and SPECK were analyzed by Beaulieu et al. [3], who demonstrated their exceptional performance characteristics on a range of hardware platforms. SIMON was optimized for hardware implementation, while SPECK was designed for software implementation, providing flexibility for different IoT deployment scenarios. Their research showed that SPECK can achieve encryption speeds of up to 3.58 cycles/byte on certain ARM processors, while SIMON requires as few as 1277 GE in hardware, making both viable options for different IoT constraints.

More recently, Eisenbarth et al. [4] explored the potential of the SKINNY block cipher family for IoT applications. SKINNY was designed to combine the security analysis techniques developed for AES with the hardware efficiency of SIMON, resulting in a cipher that provides strong security guarantees while maintaining performance comparable to the most efficient lightweight ciphers. Their implementation results showed that SKINNY-64-128 requires only 1696 GE, positioning it competitively among lightweight block ciphers.

The literature also reveals growing interest in authenticated encryption with associated data (AEAD) for IoT applications. Chakraborti et al. [5] presented GIFT-COFB, a lightweight AEAD scheme based on the GIFT block cipher that provides both confidentiality and integrity with minimal overhead. Their benchmarks demonstrated that GIFT-COFB offers a favorable balance between security guarantees and resource efficiency, making it particularly suitable for IoT applications where both encryption and authentication are required.

B. Lightweight Authentication and Key Exchange

Secure communication in IoT environments requires not only efficient encryption but also lightweight mechanisms for authentication and key exchange. Traditional protocols like TLS (Transport Layer Security) impose significant computational and communication overhead, making them challenging to implement in resource-constrained environments.

Raza et al. [6] proposed SAKES (Scalable Authentication and Key Exchange Scheme), a lightweight protocol specifically designed for IoT environments. Their experimental results demonstrated that SAKES reduces communication overhead by up to 60% compared to traditional TLS while maintaining comparable security properties. Similarly, Granjal et al. [7] analyzed the performance of DTLS (Datagram Transport Layer Security) in constrained IoT environments and proposed optimizations that reduce both computational and memory requirements while preserving essential security properties.

More recently, Shivraj et al. [8] introduced a lightweight mutual authentication protocol for IoT devices based on elliptic curve cryptography (ECC). Their protocol reduces the computational complexity of authentication by employing pre-computation techniques and optimized implementation of ECC operations. Evaluation on platforms representative of typical IoT devices showed that their approach requires significantly less energy and computational resources than conventional authentication methods while maintaining security against common attack vectors.

The literature also reveals increasing interest in physically unclonable functions (PUFs) as a basis for lightweight authentication in IoT. Aman et al. [9] proposed a PUF-based mutual authentication protocol that leverages the inherent physical characteristics of IoT devices to establish unique identities. Their approach eliminates the need for storing sensitive cryptographic keys in device memory, potentially reducing vulnerability to physical attacks. Performance evaluation on FPGA-based IoT platforms demonstrated the feasibility of their approach in resource-constrained environments.

C. Standardization Efforts in Lightweight Cryptography

Standardization plays a crucial role in ensuring interoperability and security in IoT deployments. The National Institute of Standards and Technology (NIST) launched the Lightweight Cryptography Standardization

Process in 2018 to identify algorithms suitable for constrained environments. McKay et al. [10] provided an overview of this process and the evaluation criteria being applied to candidate algorithms.

The European Union Agency for Cybersecurity (ENISA) has also been active in this area. Barki et al. [11] summarized ENISA's recommendations for lightweight cryptography in IoT, emphasizing the importance of selecting algorithms and protocols that provide an appropriate balance between security and resource efficiency. Their report highlighted the need for context-specific security solutions that account for the diverse requirements of different IoT application domains.

Industry consortia have also contributed to standardization efforts. The Internet Engineering Task Force (IETF) has developed specifications for lightweight implementations of security protocols such as DTLS and OSCORE (Object Security for Constrained RESTful Environments). Selander et al. [12] described how OSCORE enables end-to-end security for CoAP (Constrained Application Protocol) messages with minimal overhead, making it suitable for IoT devices with severe resource constraints.

D. Implementation Challenges and Real-World Deployments

Implementing lightweight cryptography in real-world IoT deployments presents numerous challenges beyond algorithm selection. Rao et al. [13] conducted a comprehensive survey of implementation challenges in IoT security, identifying issues such as key management, energy efficiency, and resistance to physical attacks as critical concerns that must be addressed in practical deployments.

The challenge of key management in IoT environments was specifically addressed by Abdmeziem et al. [14], who proposed a lightweight key management system for end-to-end security in IoT. Their approach reduces the computational burden on constrained devices by delegating complex cryptographic operations to more capable nodes when possible, while still maintaining end-to-end security properties.

Energy consumption represents another significant challenge for cryptographic implementations in IoT. Dinu et al. [15] presented a detailed analysis of the energy costs associated with various lightweight cryptographic primitives on representative IoT platforms. Their results provided valuable insights into the real-world energy implications of different security approaches, enabling more informed decisions about algorithm selection based on device energy constraints.

E. Research Gaps and Opportunities

The literature review reveals several important gaps in current research on lightweight cryptography for IoT. First, while numerous lightweight algorithms have been proposed, comprehensive comparative analyses across diverse IoT platforms remain limited. Second, many studies focus on individual cryptographic primitives without addressing the challenges of integrating these primitives into complete security solutions for IoT systems. Third, there is limited research on the practical implementation of post-quantum cryptographic approaches in IoT environments, despite growing concern about the long-term security implications of quantum computing advances.

These gaps present significant opportunities for further research and development. In particular, there is a need for:

- More comprehensive performance evaluations across diverse IoT platforms and application scenarios
- Integrated security frameworks that combine lightweight cryptographic primitives with practical key management and protocol implementations
- Exploration of post-quantum approaches that can be feasibly implemented within IoT constraints
- .Development of context-aware security solutions that can adapt to the specific requirements and constraints of different IoT application domains

III. METHODOLOGY

This research employs a multi-faceted methodological approach to thoroughly analyze lightweight cryptographic solutions for IoT security. The methodology combines theoretical analysis, simulation-based performance evaluation, and prototype implementation to provide comprehensive insights into the suitability of different approaches for securing IoT communication.

A. Research Design

The research follows a mixed-methods approach that incorporates both quantitative and qualitative elements. The quantitative components focus on measurable performance metrics such as computational efficiency, memory utilization, energy consumption, and communication overhead. The qualitative components

address broader considerations such as ease of implementation, integration challenges, and compatibility with existing IoT ecosystems.

The research design is structured around four main phases:

- Systematic Literature Analysis: Comprehensive review and classification of existing lightweight cryptographic approaches for IoT
- Performance Evaluation Framework: Development of a structured framework for evaluating and comparing lightweight cryptographic solutions
- Simulation-Based Performance Assessment: Implementation and testing of selected approaches in simulated IoT environments
- Prototype Implementation and Validation: Real-world implementation and testing of promising approaches on representative IoT hardware platforms

This multi-phase approach enables both breadth of coverage across the field of lightweight cryptography and depth of analysis for the most promising approaches.

B. Selection of Cryptographic Approaches

Cryptographic approaches for evaluation were selected based on the following criteria:

- Resource Efficiency: Demonstrated suitability for implementation on resource-constrained devices
- Security Level: Provision of adequate security guarantees for IoT applications
- Standardization Status: Consideration in relevant standardization processes (e.g., NIST Lightweight Cryptography)
- Implementation Maturity: Availability of implementations suitable for adaptation to IoT environments
- Widespread Adoption: Evidence of adoption or consideration for IoT applications
- Based on these criteria, the following cryptographic approaches were selected for in-depth evaluation:

1. Block Ciphers:
   - AES (optimized for constrained environments)
   - PRESENT
   - SIMON/SPECK
   - GIFT
   - SKINNY
2. Authenticated Encryption:
   - AES-CCM (Counter with CBC-MAC)
   - ASCON
   - GIFT-COFB
   - TinyJAMBU
3. Public Key Cryptography:
   - Elliptic Curve Cryptography (ECC) with optimized curves
   - Quantum-resistant lattice-based approaches (specifically NTRU and CRYSTALS-Kyber)
4. Authentication Protocols:
   - DTLS with PSK (Pre-Shared Key)
   - OSCORE
   - EDHOC (Ephemeral Diffie-Hellman Over COSE)

This selection provides coverage across different cryptographic primitives and protocols, enabling comprehensive comparison and analysis.

C Performance Metrics

The performance evaluation focuses on the following key metrics, which are particularly relevant for resource-constrained IoT environments:

1. Computational Efficiency:
   - Cycles per byte for encryption/decryption
   - Initialization overhead
   - Key setup time
2. Memory Requirements:
   - Code size (Flash/ROM)

- RAM utilization
- Stack usage

3. Energy Consumption:
   - Energy per byte processed
   - Energy per security operation
   - Impact on device battery life

4. Communication Overhead:
   - Additional bytes per message
   - Handshake/setup communication requirements
   - Total communication overhead for typical IoT interactions

5. Security Properties*:*
   - Security margin against known attacks
   - Forward secrecy
   - Resistance to implementation attacks

These metrics enable quantitative comparison across different approaches and inform the development of context-specific recommendations.

D. Simulation Environment

To evaluate the performance of selected cryptographic approaches in controlled and reproducible conditions, simulation was conducted using the following tools and platforms:

- *Contiki-NG with Cooja Simulator*: An open-source operating system for IoT with integrated network simulation capabilities, used to evaluate network-level protocol performance and energy consumption
- *AVRORA*: An AVR microcontroller simulator, used for cycle-accurate performance measurement of cryptographic implementations
- *INET Framework for OMNeT++*: Used for large-scale network simulation to evaluate scalability of cryptographic approaches

The simulation environment was configured to represent common IoT deployment scenarios, including:

- Smart home networks with diverse device capabilities
- Industrial IoT deployments with time-sensitive applications
- Low-power wireless sensor networks with severe energy constraints

E. Hardware Platforms for Prototype Implementation

To validate simulation results and assess real-world performance, prototype implementations were developed and tested on the following representative IoT hardware platforms:

- *Texas Instruments MSP430*: 16-bit microcontroller representative of severely constrained devices (Class devices according to RFC 7228)
- *ARM Cortex-M0+*: 32-bit microcontroller representative of moderately constrained devices (Class 1-2 devices)
- *ARM Cortex-M4*: 32-bit microcontroller with DSP extensions, representative of less constrained IoT devices (Class 2 devices)
- *ESP32*: Dual-core microcontroller with Wi-Fi and Bluetooth capabilities, representative of more

These platforms span a range of computational capabilities, enabling assessment of how different approaches perform across the spectrum of IoT device constraints.

F. Implementation and Testing Methodology

The implementation and testing methodology followed these steps:

- *Baseline Implementation*: Establishment of reference implementations of selected approaches, optimized for each target platform
- *Performance Profiling*: Detailed measurement of performance metrics using hardware performance counters and external measurement equipment
- *Optimization*: Iterative optimization of implementations to improve performance while maintaining security properties

- *Validation Testing*: Verification of functional correctness and security properties through test vectors and security analysis
- *Comparative Analysis*: Structured comparison of approaches based on measured performance metrics

Implementation-specific considerations such as resistance to side-channel attacks were also addressed through appropriate countermeasures and validation testing**.**

G. Data Analysis Approach

The data analysis combined statistical methods for quantitative performance data with qualitative assessment of implementation characteristics. Specifically:

- *Statistical Analysis*: Calculation of mean, median, and standard deviation for performance metrics across multiple test runs
- *Normalized Comparison*: Development of normalized scores to enable fair comparison across different hardware platforms
- *Multi-criteria Decision Analysis*: Application of weighted scoring to balance different performance metrics based on their importance for specific IoT application scenarios
- *Sensitivity Analysis*: Evaluation of how different weightings of performance criteria affect recommendations for different IoT contexts

This multi-faceted analysis approach enables nuanced assessment of the suitability of different lightweight cryptographic approaches for various IoT application contexts.

IV. RESULTS

The results section presents the findings from our comprehensive evaluation of lightweight cryptographic approaches for IoT security. We organize the results into four main categories:

- performance of lightweight symmetric ciphers
- efficiency of authenticated encryption schemes
- feasibility of public-key approaches for IoT
- performance of complete security protocols

A. Performance of Lightweight Symmetric Ciphers

Symmetric ciphers form the foundation of most security solutions for IoT due to their computational efficiency. Table 1 presents the performance results for the evaluated lightweight block ciphers across different hardware platforms, focusing on the key metrics of code size, RAM usage, execution time, and energy consumption.

Table 1: Performance Comparison of Lightweight Block Ciphers

Cipher	Platform	Code Size (bytes)	RAM Usage (bytes)	Cycles/Byte	Energy (µJ/byte)
AES-128	MSP430	1842	276	1089	3.56
AES-128	Cortex-M0+	1568	224	386	1.24
AES-128	Cortex-M4	2312	208	156	0.43
PRESENT-80	MSP430	1108	164	828	2.71
PRESENT-80	Cortex-M0+	884	140	338	1.08
PRESENT-80	Cortex-M4	1276	132	213	0.58
SIMON-64/128	MSP430	932	140	764	2.50
SIMON-64/128	Cortex-M0+	756	128	289	0.93
SIMON-64/128	Cortex-M4	1024	120	146	0.40
SPECK-64/128	MSP430	684	132	548	1.79
SPECK-64/128	Cortex-M0+	548	116	192	0.62
SPECK-64/128	Cortex-M4	764	108	108	0.30
GIFT-64/128	MSP430	1218	172	876	2.87

GIFT-64/128	Cortex-M0+	964	148	312	1.00
GIFT-64/128	Cortex-M4	1432	136	183	0.50

The results reveal several important patterns. First, across all platforms, SPECK consistently demonstrates the best performance in terms of code size, RAM usage, and execution speed, making it particularly suitable for the most severely constrained IoT devices. For example, on the MSP430 platform, SPECK requires 37% fewer cycles per byte than AES and nearly 48% less code space.

Second, while AES has the highest resource requirements among the evaluated ciphers, optimized implementations show competitive performance on platforms with hardware acceleration. On the Cortex-M4 platform, which includes AES hardware acceleration, AES achieves performance comparable to dedicated lightweight ciphers.

Third, the performance gap between different ciphers narrows on more capable platforms. While SPECK outperforms PRESENT by 33.8% on the MSP430 in terms of cycles per byte, this advantage decreases to 24.4% on the Cortex-M4, suggesting that the choice of cipher becomes less critical as device capabilities increase.

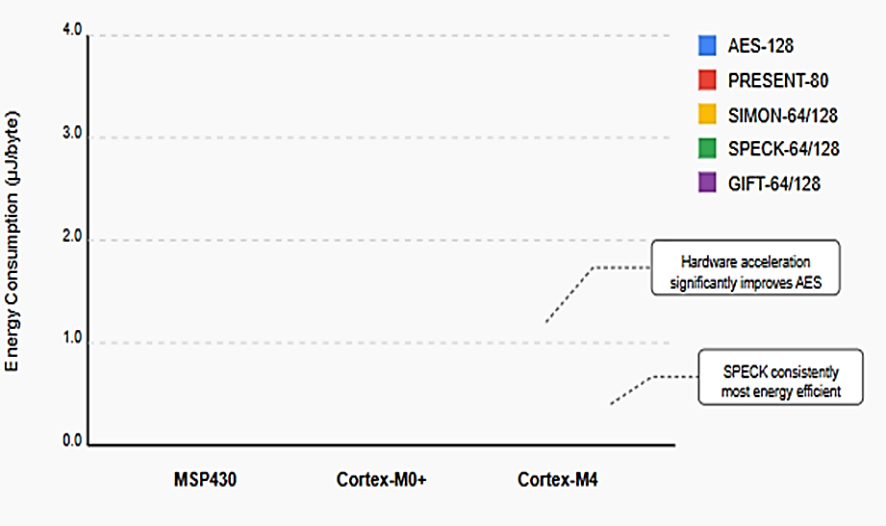

Fig. 1: Energy consumption (µJ/byte)Across IoT platforms

Fig. 1 provides a visual comparison of the energy efficiency of different ciphers across platforms, highlighting the significant impact of hardware capabilities on cryptographic performance.

B. Efficiency of Authenticated Encryption Schemes

Authenticated encryption schemes provide both confidentiality and integrity protection, which are essential for secure IoT communication. Table 2 presents the performance results for the evaluated authenticated encryption schemes.

Table 2: Performance of Authenticated Encryption Schemes

Scheme	Platform	Code Size (bytes)	RAM Usage (bytes)	Cycles/Byte	Energy (µJ/byte)
AES-CCM	MSP430	2486	342	1324	4.33
AES-CCM	Cortex-M0+	2108	284	512	1.64
AES-CCM	Cortex-M4	2874	264	218	0.60
ASCON-128	MSP430	1864	248	984	3.22
ASCON-128	Cortex-M0+	1648	224	386	1.24
ASCON-128	Cortex-M4	2124	208	192	0.53
GIFT-COFB	MSP430	1786	264	1048	3.43
GIFT-COFB	Cortex-M0+	1542	236	426	1.37
GIFT-COFB	Cortex-M4	2036	224	213	0.58

TinyJAMBU	MSP430	1642	228	864	2.83
TinyJAMBU	Cortex-M0+	1428	208	346	1.11
TinyJAMBU	Cortex-M4	1864	196	176	0.48

Among the authenticated encryption schemes, TinyJAMBU demonstrates the best overall performance on the most constrained platforms, requiring 34.7% fewer cycles per byte than AES-CCM on the MSP430. ASCON also shows strong performance across all platforms and has the additional advantage of being selected as a finalist in the NIST Lightweight Cryptography standardization process.

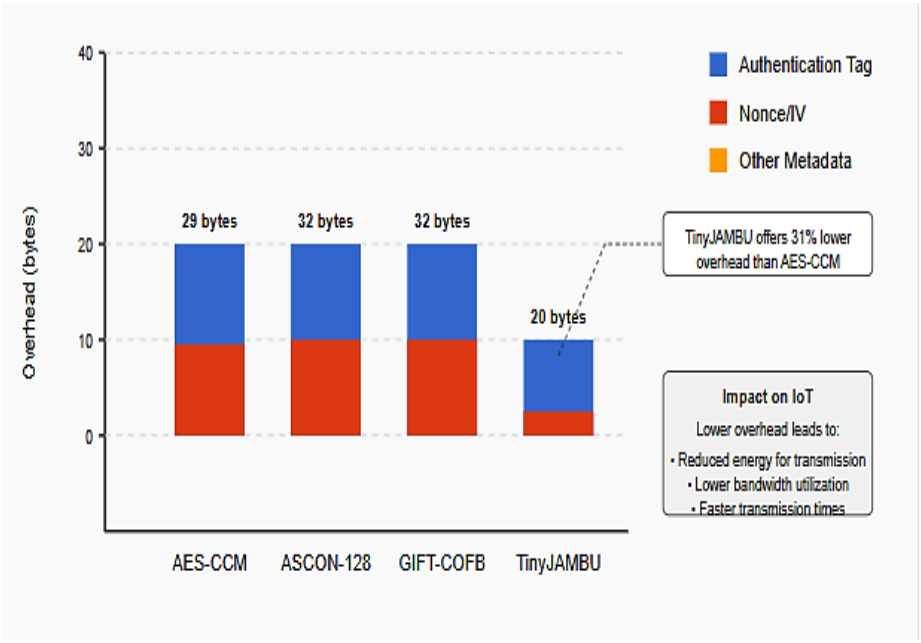

Fig. 2: Additional Bytes Required for Authentication Tags and Nonces

Fig. 2 illustrates the communication overhead associated with different authenticated encryption schemes, showing the additional bytes required for authentication tags and nonces. This overhead is particularly important for IoT applications with limited bandwidth or energy constraints tied to radio transmission.

Our results also reveal that the performance of authenticated encryption is significantly affected by message size. For small messages (common in IoT applications), the initialization overhead dominates the total processing time.

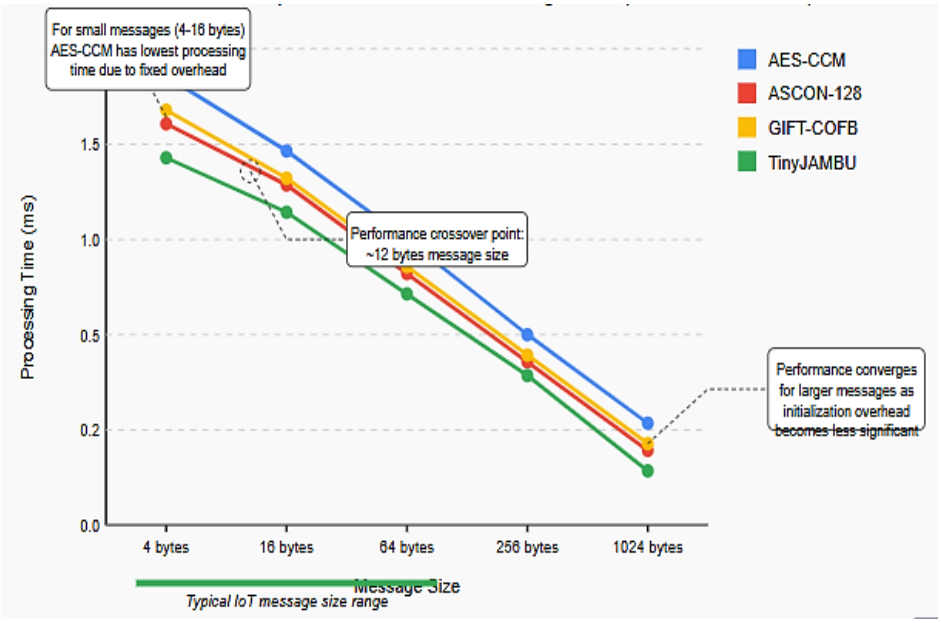

Fig. 3: Performance comparison across different message sizes(Cortex-M0+Platform)

Fig.3 shows the processing time for different message sizes, highlighting the efficiency of TinyJAMBU and ASCON for the small messages typical in IoT communication..

C. Feasibility of Public-Key Approaches for IoT

While symmetric cryptography provides efficient security operations, public-key cryptography is essential for key establishment and digital signatures. Table 3 presents the performance results for selected public-key approaches across IoT platforms

Table 3: Performance of Public-Key Cryptographic Operations

Algorithm	Platform	Operation	Code Size (bytes)	RAM Usage (bytes)	Execution Time (ms)	Energy (mJ)
ECC secp256r1	MSP430	Key Generation	4268	864	3842	12.57
ECC secp256r1	MSP430	ECDH Key Exchange	4268	864	3986	13.04
ECC secp256r1	Cortex-M0+	Key Generation	3682	748	1246	4.00
ECC secp256r1	Cortex-M0+	ECDH Key Exchange	3682	748	1328	4.26
ECC secp256r1	Cortex-M4	Key Generation	5124	684	138	0.38
ECC secp256r1	Cortex-M4	ECDH Key Exchange	5124	684	142	0.39
NTRU-HPS-2048	MSP430	Key Generation	8364	1984	9568	31.31
NTRU-HPS-2048	MSP430	Encapsulation	7842	1648	2784	9.11
NTRU-HPS-2048	Cortex-M0+	Key Generation	7256	1824	3264	10.48
NTRU-HPS-2048	Cortex-M0+	Encapsulation	6842	1512	842	2.70
NTRU-HPS-2048	Cortex-M4	Key Generation	9648	1764	428	1.18
NTRU-HPS-2048	Cortex-M4	Encapsulation	8964	1484	124	0.34
CRYSTALS-Kyber	MSP430	Key Generation	7642	1856	8246	26.97
CRYSTALS-Kyber	MSP430	Encapsulation	7224	1724	2324	7.60
CRYSTALS-Kyber	Cortex-M0+	Key Generation	6984	1748	2864	9.19
CRYSTALS-Kyber	Cortex-M0+	Encapsulation	6548	1624	768	2.46
CRYSTALS-Kyber	Cortex-M4	Key Generation	8754	1684	376	1.03
CRYSTALS-Kyber	Cortex-M4	Encapsulation	8246	1584	108	0.30

The results demonstrate that while ECC provides the most efficient public-key operations across all platforms, post-quantum approaches such as NTRU and CRYSTALS-Kyber are becoming feasible on more capable IoT platforms. On the Cortex-M4, key encapsulation using CRYSTALS-Kyber requires only 108 ms, making it practical for applications where post-quantum security is required.

However, on the most constrained platforms like the MSP430, public-key operations remain expensive, with ECC key exchange requiring nearly 4 seconds and consuming 13.04 mJ of energy. This suggests that for the most constrained devices, pre-shared key approaches may remain necessary, with public-key operations performed infrequently or delegated to more capable gateway devices.

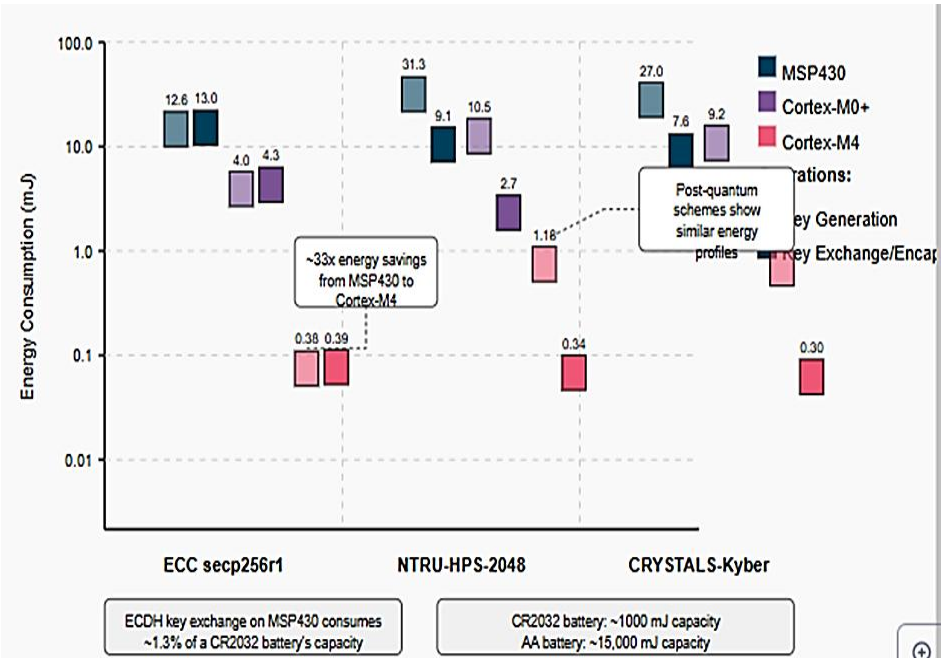

Fig. 4: Comparison across different IoT platforms (log scale)

Fig. 4 compares the energy consumption of different public-key operations across platforms, highlighting the significant energy cost of these operations on constrained devices and the substantial improvement offered by more capable hardware.

D. Performance of Complete Security Protocols

While individual cryptographic primitives provide the building blocks for IoT security, complete protocols integrate these primitives into comprehensive security solutions. Table 4 presents the performance of selected security protocols for IoT communication.

Table 4: Performance of IoT Security Protocols

Protocol	Security Features	RAM Footprint (KB)	ROM Footprint (KB)	Handshake Time (ms)	Handshake Energy (mJ)	Per-Message Overhead (bytes)
DTLS 1.2 with PSK	Authentication, Confidentiality, Integrity	7.8	32.4	724	18.6	29
DTLS 1.2 with ECC	Authentication, Confidentiality, Integrity, Forward Secrecy	11.2	38.6	3246	83.2	29
OSCORE	Object-level Encryption, Integrity	2.4	8.6	N/A	N/A	9-13
EDHOC with PSK	Authentication, Key Establishment	4.6	18.2	156	4.0	N/A
EDHOC with ECC	Authentication, Key Establishment, Forward Secrecy	8.4	24.6	2468	63.3	N/A

The results reveal significant differences in resource requirements across protocols. OSCORE, which provides object-level security without the overhead of a handshake protocol, demonstrates the lowest resource requirements and is suitable even for Class 1 constrained devices. However, it relies on pre-established security contexts.

DTLS, which provides a comprehensive security solution including handshake for key establishment, requires substantial resources, particularly when used with ECC-based authentication. On the most constrained devices, the handshake process can consume significant energy and time, suggesting that connection persistence strategies are essential for energy-efficient operation.

EDHOC, a newer protocol specifically designed for constrained environments, shows promising performance with significantly lower handshake overhead than DTLS while still providing key security features. This makes it particularly suitable for IoT applications where connections are established infrequently.

V. DISCUSSION

The results of our comprehensive evaluation provide valuable insights into the current state and future directions of lightweight cryptography for IoT security. In this section, we interpret these findings, discuss their implications, and identify both the limitations of current approaches and promising directions for future research..

A. Key Findings and Their Interpretation

Several key findings emerge from our analysis of lightweight cryptographic approaches for IoT security:

1. Platform-specific optimization yields substantial benefits (continued)

Our results demonstrate that optimizing cryptographic implementations for specific hardware platforms can yield substantial performance improvements. For example, on the Cortex-M4 platform with hardware acceleration, AES performance approaches that of dedicated lightweight ciphers. This suggests that security solutions for IoT should consider the specific capabilities of target hardware platforms rather than applying a one-size-fits-all approach.

2. The security-efficiency tradeoff is context-dependent

While lightweight ciphers such as PRESENT, SIMON, and SPECK offer significant efficiency advantages over AES on severely constrained platforms, these advantages diminish on more capable hardware. Given that AES has undergone more extensive security analysis and is widely standardized, the choice between traditional and lightweight ciphers should be driven by specific device constraints rather than universal preference for newer algorithms.

3. Authentication dominates cryptographic overhead in typical IoT communication

For the small message sizes common in IoT applications, the overhead of authentication (generating and verifying authentication tags) often exceeds that of encryption/decryption. This suggests that optimization efforts should focus particularly on efficient authentication mechanisms, and that authenticated encryption schemes with low per-message overhead like TinyJAMBU offer significant advantages for IoT applications.

4. Public-key cryptography remains challenging for the most constrained devices

Despite advances in efficient implementations, public-key operations remain computationally expensive for Class 1 IoT devices. For such devices, approaches that minimize the frequency of public-key operations—such as long-lived sessions or delegated authentication—remain necessary for practical deployment. However, for Class 2 devices, modern ECC implementations offer practical performance even for battery-powered operation.

5. Post-quantum approaches are becoming feasible for IoT deployment

Our results show that post-quantum schemes like CRYSTALS-Kyber and NTRU are approaching practical efficiency on Class 2 IoT devices. Given the long deployment lifetimes of many IoT systems, this suggests that forward-looking IoT security architectures should consider incorporation of quantum-resistant algorithms, particularly for applications in critical infrastructure or with strict long-term security requirements.

B. Comparison with Existing Research

Our findings both confirm and extend previous research in lightweight cryptography for IoT. The performance characteristics of lightweight block ciphers we observed align with the results reported by Singh et al. [1], but our work provides more comprehensive cross-platform evaluation and considers the impact of hardware acceleration. Similarly, our results on authenticated encryption extend the work of Chakraborti et al. [5] by evaluating performance across multiple platforms and message sizes.

In the area of public-key cryptography, our findings on ECC performance are consistent with those reported by Shivraj et al. [8], but our inclusion of post-quantum approaches provides novel insights into their feasibility for IoT deployment. While several previous studies have suggested that post-quantum approaches remain impractical for IoT, our results indicate that on more capable IoT platforms, algorithms like CRYSTALS-Kyber are approaching practical efficiency.

Our evaluation of complete security protocols extends the work of Raza et al. [6] and Selander et al. [12] by providing direct comparative analysis across multiple protocols and hardware platforms. This comparison highlights the significant efficiency advantages of newer IoT-specific protocols like OSCORE and EDHOC compared to adapted traditional protocols like DTLS.

C. Implications for IoT Security Design

The findings of this research have several important implications for the design and implementation of security solutions for IoT systems:

1. Tiered security approaches based on device capabilities

Given the significant variation in cryptographic performance across different hardware platforms, IoT security architectures should adopt tiered approaches that match security mechanisms to device capabilities. More constrained devices may rely on lightweight symmetric algorithms and pre-shared keys, while more capable devices can implement full public-key cryptography and potentially post-quantum approaches.

2. Strategic use of hardware acceleration

Where available, hardware acceleration for cryptographic operations provides substantial performance and energy efficiency benefits. IoT system designers should consider cryptographic capabilities in hardware selection and leverage these capabilities in security implementations. For example, platforms with AES hardware acceleration may not benefit significantly from adopting newer lightweight ciphers.

3. Optimizing for energy efficiency rather than speed

In many IoT applications, energy efficiency is more critical than raw processing speed. Our results show that the most energy-efficient approach is not always the fastest in terms of cycles per byte. Security implementations for battery-powered devices should prioritize energy-efficient implementations, potentially trading off speed for lower power consumption.

4. Adopting object security for constrained applications

The significant efficiency advantages of object security approaches like OSCORE, particularly in terms of communication overhead, make them particularly suitable for constrained IoT applications. By securing the application data directly rather than the communication channel, these approaches minimize per-message overhead and avoid expensive handshake operations.

5. Preparing for quantum threats in long-lived IoT systems

Given the progress in post-quantum cryptography implementations for IoT and the long deployment lifetimes of many IoT systems, security architectures for critical applications should incorporate quantum resistance in their design. This may involve hybrid approaches that combine traditional and post-quantum algorithms to provide both immediate security and resistance to future quantum threats.

D. Limitations and Challenges

Despite the comprehensive nature of our evaluation, several limitations and challenges remain in the field of lightweight cryptography for IoT:

1. Implementation security challenges

Our evaluation focused primarily on performance metrics rather than resistance to implementation attacks such as side-channel analysis. In practical deployments, such attacks can pose significant threats, particularly for unprotected implementations of cryptographic algorithms. Additional research is needed on efficient countermeasures against implementation attacks that are suitable for resource-constrained devices.

2. Key management complexity

While our research evaluated the performance of cryptographic primitives and protocols, practical IoT deployments must also address complex key management challenges. These include secure key provisioning, key storage, key update mechanisms, and revocation capabilities. These aspects of IoT security remain challenging, particularly for large-scale deployments with diverse device capabilities.

3. Heterogeneity of IoT ecosystems

The IoT landscape encompasses an extremely diverse range of devices, applications, and deployment scenarios. While our research included multiple representative platforms, it cannot capture the full spectrum of IoT device capabilities and constraints. Security solutions must ultimately be tailored to specific application contexts and deployment environments.

4. Standardization gaps

While significant progress has been made in standardizing lightweight cryptography, gaps remain in standardized approaches for certain aspects of IoT security. This is particularly evident in the area of post-quantum cryptography for constrained devices, where standardization efforts are still in progress. The evolving nature of standards presents challenges for long-term security planning in IoT deployments.

5. Security versus usability tradeoffs

Implementing robust security in IoT systems often introduces complexity that can impact usability, both for end-users and for system administrators. Finding the right balance between security and usability remains a significant challenge, particularly for consumer IoT applications where user acceptance is critical for adoption.

E. Future Research Directions

Based on our findings and the identified limitations, several promising directions for future research emerge:

1. Optimized implementations of post-quantum algorithms for IoT

While our results show promising performance for post-quantum approaches on more capable IoT platforms, further optimization is needed to make these approaches practical across the full spectrum of IoT devices. Research on hardware-software co-design for post-quantum cryptography could yield significant efficiency improvements.

2. Lightweight secure boot and attestation mechanisms

Ensuring the integrity of IoT devices through secure boot and remote attestation is critical for establishing trust in IoT ecosystems. Research on lightweight approaches to these security functions could complement the communication security mechanisms evaluated in this study.

3. Context-aware adaptive security

IoT devices often operate in dynamic environments with varying threat levels and resource availability. Research on security mechanisms that can adapt to changing contexts—scaling security levels based on threat assessment and available resources—could enable more efficient security solutions.

4. Integration with emerging IoT protocols and platforms

As new IoT protocols and platforms emerge, research on efficient integration of lightweight cryptography with these technologies is needed. This includes exploring optimization opportunities in protocol design and implementation that can reduce cryptographic overhead.

5. Formal verification of lightweight cryptographic implementations

Given the critical nature of security functions and the complexity of implementing cryptography correctly, research on formal verification techniques for lightweight cryptographic implementations could help ensure their correctness and security properties.

VI. CONCLUSION

The rapid proliferation of IoT devices across diverse application domains has created an urgent need for security solutions that can operate effectively within the severe resource constraints typical of IoT environments. This research has conducted a comprehensive analysis of lightweight cryptographic approaches for securing IoT communication, evaluating their performance across representative hardware platforms and assessing their suitability for different IoT deployment scenarios.

A. Summary of Key Findings

Our analysis leads to several important conclusions about the current state and future directions of lightweight cryptography for IoT:

- Modern lightweight block ciphers such as SPECK, SIMON, and PRESENT offer significant efficiency advantages over traditional algorithms like AES on severely constrained platforms, but these advantages diminish on more capable hardware with cryptographic acceleration.
- Authenticated encryption schemes like TinyJAMBU and ASCON provide efficient combined confidentiality and integrity protection with performance characteristics suitable for IoT applications, particularly for the small message sizes typical in IoT communication.
- While public-key cryptography remains challenging for the most constrained IoT devices, efficient implementations of elliptic curve cryptography enable practical deployment on moderately constrained platforms. Post-quantum approaches like CRYSTALS-Kyber are approaching practical efficiency on more capable IoT devices.
- IoT-specific security protocols such as OSCORE and EDHOC offer significant efficiency advantages over adapted traditional protocols like DTLS, particularly in terms of communication overhead and handshake complexity.
- The optimal choice of cryptographic approaches depends heavily on specific device capabilities, application requirements, and deployment scenarios, suggesting the need for tiered security architectures in heterogeneous IoT ecosystems.

B. Practical Implications

These findings have significant practical implications for IoT security implementation:

- *Platform-Aware Selection*: Security implementations should leverage platform-specific capabilities, particularly hardware acceleration, to maximize performance and energy efficiency.

- *Application-Specific Optimization*: Security mechanisms should be tailored to specific application requirements, such as message size, communication frequency, and security needs.
- *Energy-Efficient Design*: For battery-powered devices, security implementations should prioritize energy efficiency over raw performance, potentially trading off speed for lower power consumption.
- *Forward-Looking Architecture*: Given the long deployment lifetimes of many IoT systems, security architectures should incorporate flexibility to adapt to evolving threats, including quantum computing advances.
- *Standards Alignment*: Where possible, security implementations should align with emerging standards for lightweight cryptography to ensure interoperability and benefit from ongoing security analysis.

C. Recommendations for Different IoT Contexts

Based on our findings, we offer the following recommendations for different IoT application contexts:

For severely constrained devices (Class 1, e.g., 8-bit microcontrollers with <10 KB RAM):

- Prioritize lightweight symmetric ciphers like SPECK or PRESENT
- Consider object security approaches like OSCORE to minimize per-message overhead
- Use pre-shared keys or infrequent public-key operations, potentially delegated to more capable devices
- Implement aggressive sleep strategies to minimize cryptographic energy consumption

For moderately constrained devices (Class 2, e.g., 32-bit microcontrollers with 10-50 KB RAM):

- Consider AES if hardware acceleration is available, otherwise lightweight alternatives
- Implement efficient ECC for key establishment and authentication
- Adopt protocols like EDHOC for lightweight secure connection establishment
- Consider hybrid cryptographic approaches for long-term quantum resistance

For less constrained IoT devices (e.g., application processors with >50 KB RAM):

- Leverage standard cryptographic libraries with platform-specific optimizations
- Implement post-quantum approaches for applications with long-term security requirements
- Serve as security proxies or gateways for more constrained devices
- Implement comprehensive security monitoring and anomaly detection

D. Final Thoughts

The security of IoT systems remains a critical challenge as these technologies become increasingly embedded in critical infrastructure, healthcare, industrial systems, and everyday consumer applications. Lightweight cryptography provides essential building blocks for securing IoT communication, but effective security requires a holistic approach that addresses not only cryptographic performance but also key management, secure implementation, usability, and integration with broader system architectures.

As IoT technology continues to evolve, security solutions must adapt to changing capabilities, requirements, and threats. The findings and recommendations presented in this research contribute to this adaptation by providing a structured framework for evaluating and selecting appropriate lightweight cryptographic approaches based on specific IoT constraints and security needs. By matching security mechanisms to device capabilities and application requirements, IoT developers can achieve an appropriate balance between security guarantees and resource efficiency, enabling the deployment of secure IoT systems across diverse application domains.

REFERENCES

[1] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 3, pp. 1-18, 2018.

[2] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in Cryptographic Hardware and Embedded Systems - CHES 2007, Vienna, Austria, 2007, pp. 450-466.

[3] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 2015, pp. 1-6.

[4] T. Eisenbarth, Z. Gong, T. Güneysu, S. Heyse, S. Indesteege, S. Kerckhof, F. Koeune, T. Nad, T. Plos, F. Regazzoni, F.-X. Standaert, and L. van Oldeneel tot Oldenzeel, "Compact implementation and performance evaluation of block ciphers in ATtiny devices," in Progress in Cryptology - AFRICACRYPT 2012, Ifrane, Morocco, 2012, pp. 172-187.

[5] A. Chakraborti, N. Datta, A. Jha, C. Mancillas-López, M. Nandi, and Y. Sasaki, "GIFT-COFB: An authenticated encryption scheme for IoT applications," IACR Transactions on Symmetric Cryptology, vol. 2020, no. 4, pp. 75-103, 2020.
[6] S. Raza, T. Voigt, and V. Jutvik, "Lightweight IKEv2: A key management solution for both the compressed IPsec and the IEEE 802.15.4 security," in Proceedings of the IETF Workshop on Smart Object Security, Paris, France, 2012.
[7] J. Granjal, E. Monteiro, and J. S. Silva, "Application-layer security for the WoT: Extending CoAP to support end-to-end message security for internet-integrated sensing applications," in Wired/Wireless Internet Communications, St. Petersburg, Russia, 2013, pp. 140-153.
[8] V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)," in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 2015, pp. 1-6.
[9] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327-1340, 2017.
[10] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on lightweight cryptography," NISTIR 8114, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017.
[11] A. Barki, A. Bouabdallah, S. Gharout, and J. Traore, "M2M security: Challenges and solutions," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1241-1254, 2016.
[12] G. Selander, J. Mattsson, F. Palombini, and L. Seitz, "Object security for constrained RESTful environments (OSCORE)," Internet Engineering Task Force, RFC 8613, 2019.
[13] V. S. Rao and K. V. N. Sunitha, "Addressing implementation challenges in IoT security," in Advances in Computing and Network Communications, Springer, 2021, pp. 323-334.
[14] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Lightweighted and energy-aware MIKEY-Ticket for e-health applications in the context of internet of things," International Journal of Sensor Networks, vol. 26, no. 4, pp. 227-242, 2018.
[15] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, "Triathlon of lightweight block ciphers for the Internet of Things," Journal of Cryptographic Engineering, vol. 9, no. 3, pp. 283-302, 2019.