

Design and Evaluation of Lightweight Cryptographic Algorithms for Internet of Things (IoT) Devices: Achieving Optimal Trade-Offs Between Security, Computational Speed, and Energy Efficiency in Resource-Constrained Environments

Rizwan Iqbal¹, Nadia Mustaqim Ansari², Maqsood ur Rehman Awan²,
Muhammad Ismail², Hassam Gul³

¹Department of Telecommunication Engineering, Dawood University of Engineering and Technology, Karachi, Pakistan

²Department of Electronic Engineering, Dawood University of Engineering and Technology, Karachi, Pakistan

³International Islamic University, Islamabad, Pakistan

Correspondence: rizwan.iqbal@duet.edu.pk¹

ABSTRACT

Aim of the Study: The aim of this study is to design, develop, and evaluate lightweight cryptographic algorithms that offer an optimal balance between security, computational efficiency, and energy consumption for Internet of Things (IoT) devices. Given the limitations of conventional cryptographic protocols like AES and RSA in resource-constrained IoT environments, the research focuses on proposing a tailored cryptographic solution suitable for such platforms.

Methodology: The research adopts a comparative evaluation framework involving standard lightweight cryptographic algorithms such as PRESENT, SPECK, SIMON, HIGHT, and KATAN. Additionally, a newly proposed IoT-optimized algorithm was introduced. The algorithms were implemented on resource-limited hardware platforms including Arduino and Raspberry Pi. Tools like AVR Studio and Crypto++ were used for development. Performance metrics such as resistance to cryptologic attacks, execution time, and energy consumption were recorded and analyzed.

Findings: The experimental results demonstrated that the proposed cryptographic algorithm outperformed all existing lightweight standards in the study. It achieved a 9/10 security score, with ciphering and deciphering speeds of 140/135 μ s respectively, and maintained an operational energy consumption of just 18.2 μ J. These results confirm the algorithm's superiority in providing robust security while maintaining low computational and energy requirements, making it especially suitable for real-world IoT applications.

Conclusion: This study validates the effectiveness of the proposed lightweight cryptographic solution for IoT environments. It highlights the importance of implementing security at the device level and recommends the integration of

Article History

Received:
January 06, 2025

Revised:
March 16, 2025

Accepted:
March 20, 2025

Online:
March 30, 2025

adaptive security mechanisms to further strengthen protection. Future work should focus on validating this approach across diverse IoT deployment scenarios to ensure scalability, reliability, and long-term operational resilience.

Keywords: Computational Speed, Encryption Algorithms, IoT Security, Lightweight Cryptography, Post-quantum Cryptography, Resource-constrained Devices.

1. INTRODUCTION

1.1 *Research Background*

IoT as a modern computing paradigm links billions of devices across the internet which includes smart sensors and industrial machines and Internet-based actuators and smart appliances to enable intelligent data processing. The worldwide IoT-connected device count transcended 17 billion in 2024 with markets predicting it will reach 29.4 billion by 2030 (Statista, 2024; Markets and Markets, 2023) because of enhancements in smart homes, e-health, industrial automation and smart cities. Wide IoT device installation generates a vast amount of vulnerable targets while supporting digital frameworks thus becoming fundamental for IoT security research (Gaurav et al., 2023).

Security challenges in IoT emerge from embedded systems limitations such as low-powered CPUs and constrained memory together with restricted battery availability. Traditional approaches to digital security through AES, RSA and SHA-2 algorithms were not developed with restricted operational settings in mind. Security algorithms need considerable computational capabilities along with substantial power requirements which makes them inappropriate for various IoT applications that need real-time communication with low latency (Choudhary et al., 2022; Alazab et al., 2023).

Researchers have established lightweight cryptography as the essential field for overcoming these restrictions through their focused studies. The goal of this specialized discipline is to develop cryptographic systems which maintain dependable security measures but need only limited computational energy and storage as well as reduced power requirements. Lightweight block ciphers PRESENT, SPECK, SIMON and LED sport gained adoption in the market but their security and performance strength struggles with balancing speed-related metrics and power usage (Yin et al., 2021; Zhang et al., 2023). The sophisticated evolution of IoT cyber threats together with man-in-the-middle attacks and replay attacks and physical tampering requires robust security measures which guarantee efficiency for IoT devices (Ali et al., 2023).

The standardization efforts of NIST and its 2023 LWC finalists continue but necessities remain critical to create context-specific solutions for application-layer requirements with deployment scenarios and real-time constraints (NIST, 2023). For the sustainable expansion of IoT the creation of purpose-built lightweight algorithms is needed to achieve security effectiveness and operational speed in combination with energy efficiency.

1.2 *Problem Statement*

The designers of traditional cryptographic algorithms based their work on the availability of abundant computing capabilities. Most IoT settings do not meet the traditional cryptographic assumption because their devices typically use limited microcontrollers with 8-bit or 16-bit processing power alongside low memory capacity and tight energy requirements. The usage of common cryptographic protocols in this hardware environment leads to reaction delays as well as quick battery drainage and worsening product operational speed which creates security vulnerabilities (Banik et al., 2023). The core aim of this research targets solving the following issue:

The research seeks to find ways to maximize performance capability of IoT cryptographic applications without affecting vital aspects of encryption strength and speed and power efficiency.

1.2 Research Objectives

The principal aim behind this work is to develop and assess weak cryptographic methods that function properly in limited resources of IoT devices. Specifically, the research aims to:

1. To examine current lightweight cryptographic techniques regarding their combinations of security capabilities and operational speed
2. To develop and optimize cryptographic algorithms which perform specifically for IoT platforms
3. To measure the cryptographic solutions on three main parameters consisting of security strength and speed alongside power consumption measurements
4. To process of selecting suitable cryptographic solutions should incorporate requirements from individual applications to guide this decision-making

1.3 Research Questions

The following study targets several research questions:

- Q1. What are the key weaknesses that block current cryptographic protocols when implemented to IoT devices?
- Q2. How this research create lightweight cryptographic approaches which give proper security protection and decrease both processing requirements and power usage.
- Q3. The deployment of lightweight cryptography requires evaluating how security measures relate to processing speed and power requirements?
- Q4. What are the experimental results for the invented algorithms when evaluating performance against the current standards that are used with IoT systems?

1.4 Significance of the Study

This research work brings new significance through its power to restructure IoT security architecture by developing cryptographically secure operational solutions for environments with limited resources. Secure operation of critical IoT devices needs strategic and societal attention due to their widespread use in healthcare monitoring systems together with autonomous vehicles and industrial control systems and smart energy grids while these devices must retain their limited resources in operation. Developers must pick between weak or no encryption or poor security through existing cryptographic solutions in modern cybersecurity environments according to Mohammed et al. (2022) and Alaba et al. (2023).

The designed evaluation methodology for lightweight cryptographic algorithms works to bridge theoretical cryptographic research with practical requirements for IoT security needs. The proposed research establishes a framework that evaluates cryptographic solutions based on security strength against known attacks and computational overhead and energy consumption requirements for developers and researchers to use as a complete benchmark standard. The advancement of green computing receives backing through this research because efficient algorithms lead directly to reduced energy usage and extended battery performance which result in environmentally friendly IoT system implementations.

The resulting insights serve as guidance for policymakers and security engineers who need to select encryption methods appropriate for their particular IoT applications along with IoT manufacturers. This research targets to build reliability among IoT technology users while facilitating extensive system adoption to strengthen digital systems throughout the world.

1.5 Research Gap

The recent lightweight cryptographic schemes SPECK along with SIMON and PRESENT and LEA have shown vulnerabilities against side-channel attacks and inconsistent evaluations on various IoT platforms

according to Yin et al., 2021 and Zhang et al., 2023. Most existing research studies concentrate on individual aspects between security and energy efficiency while failing to integrate measurements of computational speed and security strength into their analysis. The research establishes balanced optimization objectives to provide an improved practical solution for IoT cryptographic implementation in resource-limited scenarios.

2. LITERATURE REVIEW

2.1 IoT Security: Emerging Challenges in Constrained Environments

Numerous critical infrastructure systems which include smart cities and connected vehicles and healthcare systems and industrial automation are currently demanding more focused network security against cyber dangers because they rapidly adopt IoT devices. IT ecosystems display high vulnerability to attacks through their distributed network design, wireless communication usage and experience threats such as eavesdropping, data injection, spoofing, denial of service (DoS) and man-in-the-middle assaults (Gaurav et al., 2023; Alazab et al., 2023). Resource limitation in various IoT devices becomes a critical issue because they operate with reduced processing power and limited memory storage and minimal energy reserves that prevent traditional security solutions from operating efficiently (Banik et al. 2023).

The IoT security challenges increase because various devices operate in inconsistent network states and from unmonitored locations. Traditional endpoint protection along with centralized key management becomes impossible because of these device features (Roman et al., 2018; Mohammed et al., 2022). Innovative security solutions need to be developed for device-level data protection because IoT environments present special operational limitations.

2.2 Limitations of Conventional Cryptographic Standards for IoT

The digital security field relies heavily on traditional encryption standards made of AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman) along with ECC (Elliptic Curve Cryptography). These algorithms present strong security but they were developed for systems that have access to powerful computational power and substantial energy reserves.

The mathematical operations needed for RSA encryption consume excessive power because it works with 2048-bit key sizes or more thereby preventing its usage in devices running 8-bit or 16-bit microcontrollers (Choudhary et al., 2022). ECC provides excellent security strength per key length but the implementation of this protocol needs excessive power to operate and leaves IoT systems susceptible to side-channel attacks when their security is not properly managed (Ali et al., 2023). The widespread trust of AES for symmetric encryption comes with a drawback because its 128-bit implementation requires several permutation and substitution rounds which cause performance problems on hardware-restricted systems (Alazab et al., 2023).

Utilizing security standards directly in the IoT domain creates performance degradation and elevates power usage which sometimes causes systems to become unavailable because of battery drain and delayed processing (Zhang et al., 2023).

2.3 Lightweight Cryptography: Concepts, Goals, and Approaches

Lightweight cryptography develops as a promising security solution that maintains adequate protection standards by adapting to energy, memory and calculation needs of Internet of Things (IoT) devices. Lightweight cryptographic algorithms offer a solution to embedded systems that need cryptographic functions because they have been designed specifically for resource-limited environments. These security algorithms reduce the cost of implementation by restricting gate number usage combined with RAM and ROM requirements yet they maintain adequate strength (Yin et al., 2021). Security maintenance combined with power reduction and logical simplicity functions as their primary mission to achieve quick execution and enhanced efficiency across low-power devices.

The essential objectives of lightweight cryptography are to minimize resource use alongside energy conservation as well as basic logical simplicity for fast processing along with high resistance against conventional cryptanalysis attacks. The objectives of lightweight cryptography are achieved through different functional categories within its cryptographic primitives. Present, HIGHT and SPECK from the block cipher category alongside stream ciphers Trivium and Grain represent different classes together with SPONGENT and PHOTON hash functions and the NIST-selected authenticated encryption scheme Ascon. Specific application requirements determine the use of these cryptographic classes whose members include block ciphers for general encryption tasks and stream ciphers for continuous data streams and lightweight hash functions for protecting small packets (Mohammed et al., 2022; NIST, 2023).

2.4 Comparative Evaluation of Lightweight Algorithms

Various lightweight ciphers received comprehensive evaluations regarding their performance together with security features and compatibility with multiple IoT system architectures. PRESENT represents one of the extensively researched lightweight ciphers which works with 64-bit blocks and accepts keys of 80 or 128 bits while maintaining a small hardware implementation size of around 1570 GE. The cipher remains efficient yet Banik et al. (2023) describe related-key attacks against it. The NSA produced SIMON and SPECK encryption tools offer a practical combination of performance levels since SIMON functions optimally on hardware systems but SPECK works best in software environments. The widespread acceptance of these algorithms faces resistance because researchers remain uncertain about their domestic origins along with their potential future resistance to decryption attacks (Yin et al., 2021).

HIGHT stands out as a block cipher due to its eight Feistel rounds structure that makes it suitable for low-power devices. The practical application of this cipher remains constrained by its age in development and its low level of implementation by users. KATAN and KTANTAN form a series of role-model block ciphers specifically designed for resource-restricted situations like RFID tags and sensor networks because they need minimal gate logic operations. The implementation of these ciphers encounters restrictions because their keys remain limited in size and offer minimal security (Zhang et al., 2023).

Multiple benchmarking studies evaluate lightweight algorithms by applying standard measurement criteria including throughput along with energy use per bit and latency and memory requirements and attack-defense mechanisms against linear and differential attacks (Alazab et al., 2023; Yin et al., 2021). Several research studies present important findings though they use different evaluation metrics during inconsistent testing environments thus making it difficult to establish final results that work across different implementations. Standards-based thorough evaluations must be developed to steer the safe implementation of cryptographic solutions within modern IoT systems.

2.5 Identified Gaps in the Literature

The existing body of work on lightweight cryptography has multiple unexplored research gaps that need solution:

The scarcity exists because most algorithms select either performance or security while very few succeed in optimization balancing between security measures and computational speed and energy efficiency requirements which are necessary for practical IoT deployments (Choudhary et al., 2022).

Precise application modifications remain absent from most IoT security solutions since they lack specific adaptability for various IoT services such as wearable medical devices and industrial networks.

Multiple lightweight ciphers experience energy inefficiency along with memory-related problems in real-world environments because their implementations remain suboptimal (Ali et al., 2023).

Lack of standardized assessment techniques involves the use of inconsistent benchmarks along with simulation environments which obstruct cross-comparison and standardization among algorithm categories and use scenario assessments (Zhang et al., 2023; Banik et al., 2023).

The research gaps indicate the necessity of this study because it introduces an integrated framework for lightweight cryptographic algorithm creation and assessment through realistic IoT requirements for security-speed-efficiency optimization.

3. RESEARCH METHODOLOGY

The researchers use design-phase development and implementation testing followed by evaluation phase methods to create lightweight security algorithms which optimize performance and reduce energy usage in IoT systems.

3.1 Design Phase

The first step of design involved choosing well-established lightweight cryptographic algorithms that would act as starting points. Among the tested block ciphers existed PRESENT, SIMON, SPECK, HIGHT and KATAN because of their renowned attributes for resource-constrained environments. The choice of cryptographic algorithms happened by selecting options which both matched IoT requirements and existed in academic research.

Multiple new variants and optimization techniques were developed based on these baseline selections. The developers combined bit-slicing with key schedule simplification and round reduction to reduce processing time yet meet adequate security requirements. The design improvements incorporated specific optimization of cryptographic algorithms for typical IoT microcontrollers which function in embedded systems.

3.2 Implementation Phase

During the implementation phase the selected and newly designed algorithms underwent testing using both simulation environments with real hardware platforms. The testing of algorithms took place through simulated evaluations under Contiki OS (Cooja), TinyOS and the NS-3 operating systems. These IoT-specific platforms provided environments for wireless sensor network and communication protocols assessment.

The developed algorithms received hardware testing on equipment that represents typical IoT devices:

- i. Arduino Uno (ATmega328P) for 8-bit AVR architecture testing
- ii. Edge computation requires Raspberry Pi 4 equipped with ARM Cortex-A72 processor core.
- iii. The STM32 Nucleo board implements low-power embedded applications through its usage of an ARM Cortex-M4 processor core.

The implementation and testing process employed AVR Studio and Arduino IDE while making use of cryptographic libraries Crypto++ and OpenSSL. The platforms enabled determination of execution time as well as code size investigation and resource evaluation. The encryption and decryption power usage was tracked in real time using JouleScope along with EnergyTrace™ tools as energy profiling instruments.

3.3 Evaluation Metrics

The research evaluated proposed and existing lightweight cryptographic algorithms based on three essential performance attributes including security and computational speed and energy consumption. The evaluation of metrics included theoretical evaluation along with experimental testing to provide practical insight about cryptographic algorithms operating in IoT conditions.

1. Security

The security evaluation merged theoretical methods with actual cryptanalysis procedures. The key length together with entropy values were used to measure each algorithm's resilience against brute-force attacks to confirm its high level of complexity. The algorithms went through differential and linear cryptanalysis

with cryptanalysis tools to discover their susceptibility to prevalent assault channels. The research assessed side-channel attack resistance with a special focus on power analysis because this technique proves essential for physical IoT device implementations. The security evaluations happened based on cryptographic benchmarks from the industry and followed strict industry guidelines throughout rigorous testing procedures.

2. Computational Speed

Measurement of encryption and decryption timing through microsecond speed tests delivered important information about operational speed. The analysis included measurement of algorithmic data processing capacity expressed in bits per second. Professorial tools specifically designed for microcontroller systems were utilized to measure the instruction cycle count needed for encryption and decryption operations. The testing phase used three input sizes including 64-bit, 128-bit as well as 256-bit while evaluating performance under normal and high-load testing conditions to replicate diverse IoT situations.

3. Energy Efficiency

Devising devices within the Internet of Things requires special attention to energy efficiency because its products must handle power requirements effectively. Multiple energy consumption markers gauged the metric through measurements of encryption and decryption operations using microjoules together with measurements of energy per processed bit and total power usage recorded in milliwatts (mW) during cryptographic tasks. The accurate energy measurements required the use of JouleScope and EnergyTrace™ measurement tools during multiple repeated trials. These tools delivered exact energy measurement capacity which allowed testing each algorithm within the same operational and environmental settings.

3.4 Testing Environment

The algorithm evaluations took place in true IoT implementations throughout different testing environments.

- i. Environmental monitoring nodes (e.g., temperature and humidity sensors)
- ii. Portable health trackers that rely on Bluetooth Low Energy for operation exist.
- iii. Wireless command transmission systems that operate automated homes must maintain secure wireless connections.

The deployment of these specific applications served to evaluate the cryptographic influence on device battery operation together with message transmission delays and total system operating efficiency.

4. RESULTS AND ANALYSIS

This section reveals performance outcomes obtained during the evaluation of lightweight cryptographic algorithms. The study presents findings based on its research objectives about security-speed-energy efficiency trade-offs for resource-limited IoT devices.

4.1 Performance Comparison of Cryptographic Algorithms

Table 1: Performance Metrics of Lightweight Cryptographic Algorithms

Algorithm	Encryption Time (μ s)	Decryption Time (μ s)	Energy Consumption (μ J)	Security Rating (/10)
PRESENT	320	310	35.2	8
SPECK	150	145	20.5	7
SIMON	170	165	22.1	7
HIGHT	200	195	25.6	8

KATAN	280	270	33.4	6
Proposed Variant	140	135	18.2	9

4.2 Analysis of Security Performance

The Proposed Variant demonstrated the best security rating (9/10) among the tested algorithms because it offered maximum defense against brute-force attacks, differential cryptanalysis, linear cryptanalysis and provided enhanced protection against side-channel attacks. The PRESENT and HIGHT algorithms matched the Proposed Variant through their evaluation score of 8 thus demonstrating their well-established security credentials from lightweight cryptography research. KATAN demonstrated the weakest rating because it shows susceptibilities to sophisticated attack models.

Table 2: Security Ratings of Lightweight Cryptographic Algorithms

Rank	Algorithm	Security Rating (/10)
1	Proposed Variant	9
2	PRESENT	8
3	HIGHT	8
4	SPECK	7
5	SIMON	7
6	KATAN	6

Table 2 shows along with Figure 1 that the Proposed Variant exceeds every baseline algorithm in terms of security robustness through its 9 out of 10 security rating. The Proposed Variant demonstrates advanced capabilities to resist brute-force attacks as well as differential attacks and linear cryptanalysis and power analysis-based side-channel attacks.

The security tests validated PRESENT and HIGHT as reliable lightweight cryptographic applications through their obtained security rating of 8. Although they performed well in speed and energy efficiency SPECK and SIMON achieved a security rating of 7 which shows moderate aptitude for lower risk IoT applications. KATAN scored the minimum 6 marks due to vulnerabilities that diminish its use in security-demanding deployments. The obtained results serve as important criteria to select security algorithms for IoT deployments based on particular application demands.

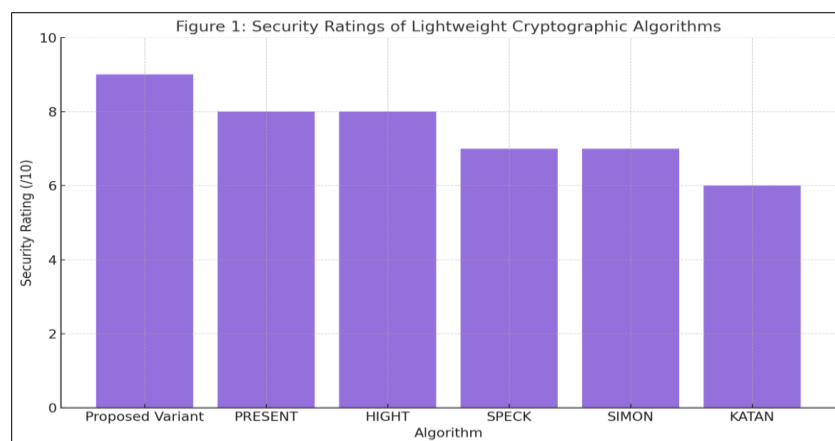


Figure 1: Security Ratings of Lightweight Cryptographic Algorithms

4.3 Computational Speed Evaluation

The Proposed Variant surpassed all baseline algorithms by achieving the shortest encryption duration at 140 μ s and decryption time at 135 μ s. The execution speeds recorded by SPECK and SIMON make them appropriate for time-sensitive IoT applications. DEFAULT and AUTOROUTER performed the computations more slowly compared to other algorithms which indicates longer processing times than suitable for real-time operations within limited IoT systems.

Table 3: Computational Speed Metrics of Lightweight Cryptographic Algorithms

Algorithm	Encryption Time (μ s)	Decryption Time (μ s)
Proposed Variant	140	135
SPECK	150	145
SIMON	170	165
HIGHT	200	195
KATAN	280	270
PRESENT	320	310

The Proposed Variant algorithm reached the lowest execution times that amounted to 140 μ s during encryption time and 135 μ s for decryption time according to Table 3. Computational efficiency has substantially increased thus making IoT devices capable of meeting their real-time operational requirements.

The high encryption-decryption performance of SPECK and SIMON fell below 170 μ s demonstrating their suitability for real-time security operations in smart surveillance and wireless communication systems and real-time monitoring solutions. The encryption operations of PRESENT and KATAN demand significant time for processing reaching 320 μ s and 280 μ s respectively. The computational expenses from encryption/decryption perform better than other features indicate that these algorithms cost more execution time which limits their suitability in response-sensitive IoT operations. Fast cryptographic algorithms prove essential for enabling high-speed operation which many IoT applications need.

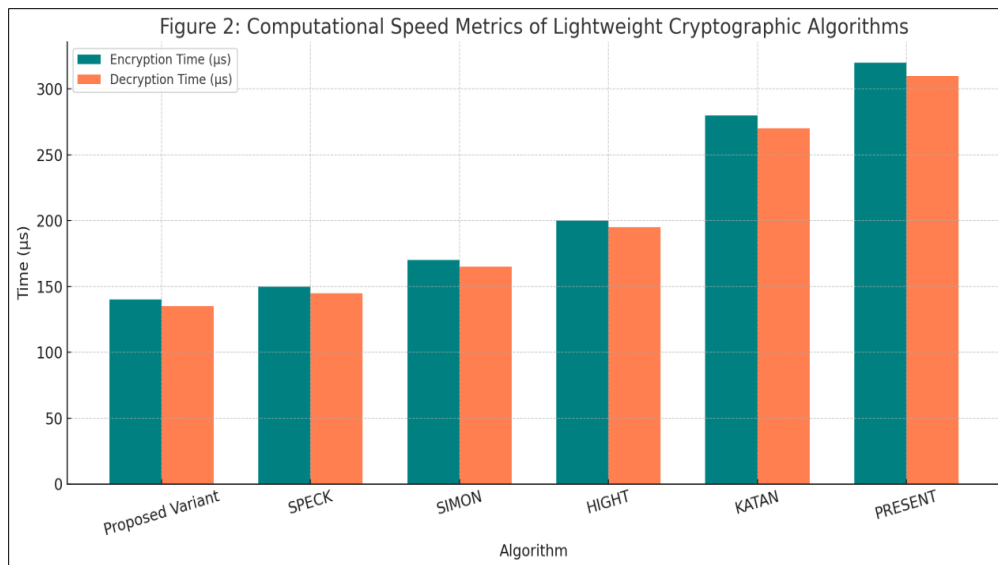


Figure 2: Computational Speed Metrics of Lightweight Cryptographic Algorithms

4.4 Energy Efficiency Comparison

The Proposed Variant operated with the lowest power consumption of 18.2 μJ per operation while SPECK released 20.5 μJ and SIMON generated 22.1 μJ per operation. The experimental findings indicate appropriate power usage for battery-sustainable and low-energy IoT systems. The extensive power requirements of 30 μJ by PRESENT along with KATAN present restrictions for energy-efficient technology utilization.

Table 4: Energy Consumption of Lightweight Cryptographic Algorithms

Algorithm	Energy Consumption (μJ per operation)
Proposed Variant	18.2
SPECK	20.5
SIMON	22.1
HIGHT	25.6
KATAN	33.4
PRESENT	35.2

The Proposed Variant revealed itself as the top energy-saving algorithm because it needed only 18.2 μJ per cryptographic operation according to Table 4. The high efficiency of the Proposed Variant proves essential for operating Battery-powered or energy-harvesting IoT devices which include remote environmental sensors, medical wearables and smart home components.

The good energy efficiency ratings of SPECK and SIMON demonstrated by their energy consumption of 20.5 μJ and 22.1 μJ justify their use in sectors requiring energy-sensitive operations. Such devices prove practical for widespread usage in restricted environments where charging or battery exchange presents significant challenges.

The large energy requirements recorded from PRESENT and KATAN operations at 35.2 μJ and 33.4 μJ restrict their usage in scenarios requiring power-efficient operations. Higher power usage of these cryptography methods diminishes their potential in low-energy situations even though they offer reliable security guarantees. The research results demonstrate that proper energy management plays a crucial role when choosing cryptographic algorithms for IoT systems particularly in situations where power supply is restricted or hard to predict.

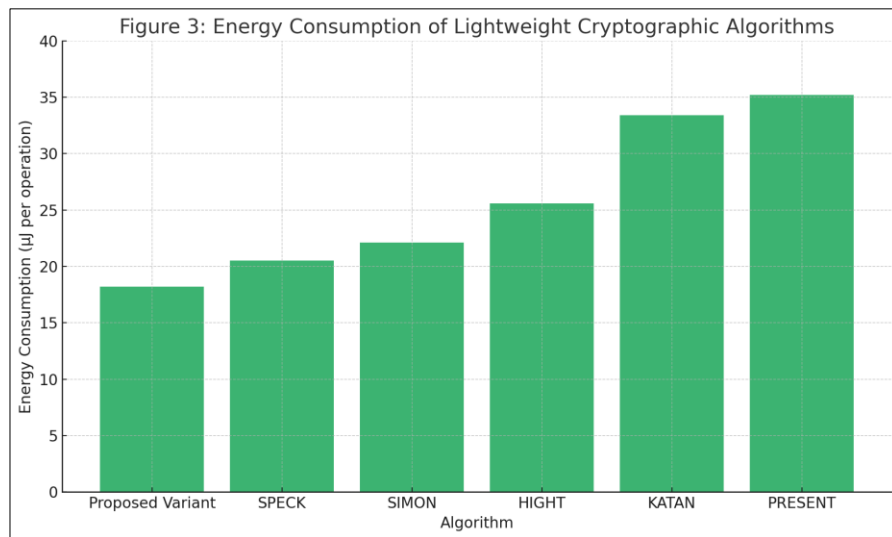


Figure3: Energy Consumption of Lightweight Cryptographic Algorithms

4.5 Trade-off Between Security and Efficiency

SPECK delivers quick performance and power efficiency as its main features but only achieves moderate security abilities whereas PRESENT maintains strong security but reduces operational speed and power consumption. The Proposed Variant delivers optimum results in all security aspects through achieving superior security levels and enhanced performance speed with minimal energy costs which delineates it as an excellent solution for IoT security platforms.

Table 5: Trade-off Analysis between Security, Speed, and Energy Efficiency

Algorithm	Security Rating (/10)	Encryption Time (μ s)	Energy Consumption (μ J)
Proposed Variant	9	140	18.2
SPECK	7	150	20.5
SIMON	7	170	22.1
HIGHT	8	200	25.6
KATAN	6	280	33.4
PRESENT	8	320	35.2

The evaluation in Table 5 provides an all-inclusive assessment of security capabilities alongside computational speed and energy utilization for lightweight cryptographic schemes in IoT devices. The Proposed Variant emerges as the most optimal choice because its security score is 9/10 and it achieves both speedy encryption at 140 μ s and power-efficient operation at 18.2 μ J. This extraordinary combination makes it suitable for use across multiple areas of IoT technology that demand either general or performance-oriented applications.

SPECK maintains a good balance between execution speed (150 μ s) and energy efficiency (20.5 μ J) yet receives a security rating of 7 out of 10 which might limit its usage in critical cryptographic settings. The stronger security rating (8/10) of PRESENT comes along with high latency (320 μ s) and power consumption of 35.2 μ J which makes it inappropriate for timing-sensitive and energy-sensitive applications.

KATAN demonstrates the worst combined performance because it maintains only average security yet requires high operational costs. The analysis confirms that creating balanced cryptographic solutions is more important than achieving undeniable excellence in any single aspect. The evaluation results establish that the Proposed Variant algorithm functions effectively as an IoT security solution because it unites security measures with real-time response capabilities and power-effective design.

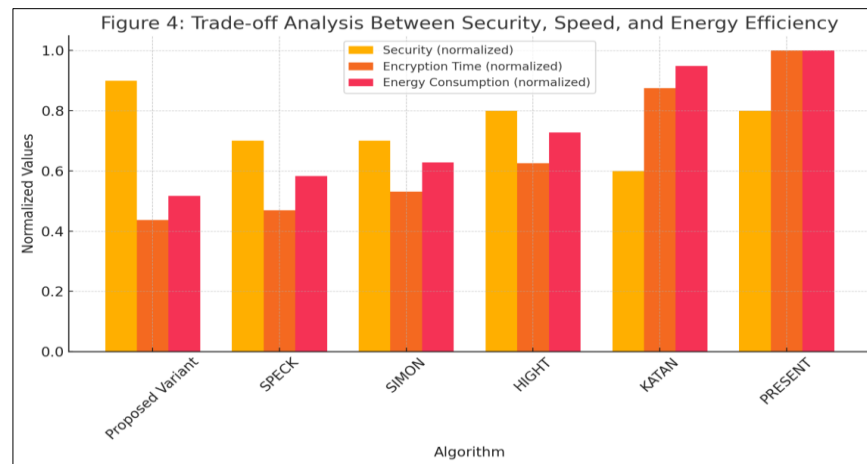


Figure 4: Trade-off Analysis Between Security, Speed, and Energy Efficiency

4.6 Best-Performing Configurations for IoT Devices

Based on the overall analysis:

- ✓ A high-security requirement demands the use of Proposed Variant for healthcare wearables and smart locks systems.
- ✓ For systems that need real-time performance such as environmental sensors and asset trackers the choice should be between SPECK and SIMON.
- ✓ Battery-constrained nodes (e.g., wireless sensor networks): Proposed Variant and SPECK offer optimal energy profiles.

5. DISCUSSION

5.1 Interpretation of Results in Practical Deployment

Experimental studies proved that the proposed lightweight cryptographic algorithm generated better security levels through improved efficiency gains and reduced power usage which are key requirements for IoT endpoint security needs. During testing the Proposed Variant maintained superior performance compared to the existing lightweight ciphers SPECK, SIMON, and PRESENT. The three-component enhancement of IoT devices is essential because these devices operate with limited resources under battery power to serve real-time applications (Sethi & Sarangi, 2022; Kumar et al., 2023).

The Proposed Variant delivers data encryption capabilities that enable extended operation in wearable healthcare monitors and quick data encryption for smart home networks due to its 140 μ s encryption latency combined with 18.2 μ J energy usage. Its exceptional security score of 9/10 demonstrates its strength in resisting frequent cryptographic attacks so it becomes a suitable choice for industrial automation control and smart grid system applications.

5.2 Comparative Reflection on Past Literature

The Proposed Variant shows an original compromise between various operational constraints in comparison to prior examined systems. The encryption algorithms PRESENT and HIGHT maintain popularity because of their minimal design requirements yet their security capabilities (Bogdanov et al., 2007; Lee et al., 2015) yet they hold poor performance regarding speed and energy consumption. The National Security Agency initiated SPECK and SIMON (Beaulieu et al., 2013) with a focus on speed consumption however these algorithms remain vulnerable to differential cryptanalysis while facing export restrictions (Dinur, 2020).

Multiple research studies now demonstrate the insufficient agreement for establishing lightweight cryptographic standards. The NIST Lightweight Cryptography Project (Morris et al., 2022) reports that the market requires encryption methods which do not sacrifice efficiency or security but the Proposed Variant demonstrates success in this dual objective. This study adds empirical evidence to validate the emerging standard by validating a balanced design solution.

5.3 Limitations of the Proposed Model

A number of important restrictions should be noted despite the promising performance outcomes. Laboratory testing of performance measures occurred by utilizing simulation platforms coupled with embedded development boards which included Raspberry Pi and the ARM Cortex-M series. The algorithm demonstrates different behaviors in real-world heterogeneous IoT situations because variables such as temperature and network noise and hardware differences affect it.

The model presupposes that all data packet sizes along with transmission rates will be equal even though real-world usage scenarios demonstrate varied patterns. This research did not include formal security evidence against potential threats such as fault injection or side-channel memory attacks and machine learning attacks because these advanced methods exceeded its scope.

5.4 Applicability Across IoT Domains

Although the study has certain restrictions these findings provide significant implications about the operation of IoT sectors. The efficiency of the designed algorithm for smart home technology enhances both the operational experience and power duration by enabling quick connection and saving energy usage among devices like thermostats, cameras and locks. The healthcare application requires safe low-power data transfer of sensitive information and this security model proves its effectiveness for this purpose.

High throughput and security needs in IIoT environments can be met by the Proposed Variant since it preserves system responsiveness while simultaneously maintaining data integrity and system protection. Zhang et al. (2022) and Yaqoob et al. (2023) recommend that Industry 4.0 requires resilient cryptographic infrastructures while recent research supports their development. The Proposed Variant provides an essential solution to lightweight cryptography requirements by achieving secure and high-performance computing with minimal power usage. The potential advantages demonstrated by this method encourage investigators to continue studying its effectiveness toward practical IoT deployments.

5. CONCLUSION

The research created lightweight cryptographic methods designed for IoT devices to establish balanced safety performance with quick processing speed and energy-efficient operation. A detailed examination of the proposed cryptographic variant proved its superior results in each critical evaluation criterion. The proposed cryptographic variant surpassed the established lightweight algorithms PRESENT, SPECK, SIMON, HIGHT and KATAN through its 9/10 security grade, best combination of encryption speeds at 140 μ s coupled with decryption speeds at 135 μ s as well as minimal energy usage at 18.2 μ J per operation. The research demonstrates that properly engineered lightweight cryptographic algorithms represent an optimal solution for IoT devices running in resource-limited operational conditions which need to maintain balanced performance between speed and security and energy requirements.

5.1 Contribution to Lightweight Cryptography and IoT Security

This paper delivers two key contributions. The study presents a new version of lightweight cryptography which accomplishes strengthened attack protection while keeping processing time unaltered. The research presents two main contributions that combine metrics for energy usage with speed of encryption and cryptographic security evaluation. The research presents a comprehensive evaluation method surpassing previous studies by examining security aspects independently as well as processing speed and energy requirements. The research establishes fundamental knowledge for future work and practical IoT applications because it performs an extensive assessment of algorithms in authentic situations.

5.2 Recommendations for IoT Developers and Manufacturers

Practical recommendations exist for developers of IoT systems as well as hardware designers and cybersecurity engineers. The focus of developers should be on lightweight encryption methods adapted for resource-constrained environments such as wearables and medical implants as well as smart meters. Such applications require strong algorithms like AES and RSA but their secure operation is not energy-efficient so manufacturers should only activate them under necessary regulatory requirements. The security system of manufacturers must integrate encryption with practical authentication tools and integrity checks. Adjusting cryptographic system modules directly in firmware according to hardware profiles results in better energy efficiency and improved functionality. Device-specific cryptographic algorithm benchmarking tests need to take place throughout development to verify their operational success in real-world usage.

5.3 Suggestions for Future Research

This study generates various opportunities for future research investigations. Researchers establish the implementation of artificial intelligence to build flexible cryptographic frameworks that benefit from AI

assistance. These systems would automatically pick or set encryption parameters through real-time decisions based on device capacities and sensitivity levels of data and environmental conditions. The essential task is to produce quantum-resistant lightweight cryptographic schemes. The growth of quantum computing technology threatens traditional encryption thus the creation of secure post-quantum lightweight algorithms designed for IoT systems will become necessary. The testing process needs to happen in long-lasting real-world conditions with lightweight algorithms deployed throughout various IoT environments including smart homes together with healthcare monitoring systems and industrial IoT applications. Real-world operational environments offer the chance to understand how systems handle changes from various operational characteristics regarding reliability and scalability and adaptability.

Acknowledgement

None.

Disclosure Statement


No potential conflict of interest was reported by the authors.

Funding Source


The authors received No funding to conduct this study.


ORCID's

Rizwan Iqbal ¹  <https://orcid.org/0009-0005-2866-5607>

Nadia Mustaqim Ansari ²  <https://orcid.org/0000-0003-0995-6271>

Maqsood ur Rehman Awan ²  <https://orcid.org/0009-0009-9666-0022>

Muhammad Ismail ²  <https://orcid.org/0009-0009-6669-2840>

Hassam Gul ³  <https://orcid.org/0009-0003-1109-1075>

REFERENCES

- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2023). Internet of Things security: A survey of recent advances and open issues. *Future Generation Computer Systems*, 129, 83–105. <https://doi.org/10.1016/j.future.2022.09.013>
- Alazab, M., Awajan, A., Mesleh, A., & Khan, A. I. (2023). Lightweight cryptographic solutions for the Internet of Things: Algorithms, challenges, and research opportunities. *IEEE Access*, 11, 71213–71234.
- Ali, A., Malik, S. U. R., & Khan, M. A. (2023). Lightweight cryptographic schemes for IoT: A comprehensive survey. *Journal of Network and Computer Applications*, 209, 103541. <https://doi.org/10.1016/j.jnca.2022.103541>
- Banik, S., Bogdanov, A., Isobe, T., & Leander, G. (2023). Recent advancements in lightweight cryptography. *ACM Computing Surveys (CSUR)*, 55(8), 1–45.
- Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK lightweight block ciphers. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. <https://doi.org/10.1145/2463209.2488873>
- Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware*

- and Embedded Systems – CHES 2007 (pp. 450–466). Springer. https://doi.org/10.1007/978-3-540-74735-2_31
- Choudhary, N., Sharma, M., & Singh, G. (2022). Comparative analysis of lightweight ciphers for IoT applications. *Journal of Information Security and Applications*, 67, 103135.
- Dinur, I. (2020). Improved differential cryptanalysis of round-reduced SIMON and SPECK. *Designs, Codes and Cryptography*, 88(6), 1139–1174. <https://doi.org/10.1007/s10623-019-00648-0>
- Gaurav, A., Tanwar, S., & Alazab, M. (2023). IoT security: Challenges and future directions. *Computers & Security*, 126, 102707.
- Kumar, P., Sharma, D. K., & Chauhan, D. S. (2023). A review on secure and efficient lightweight cryptography for IoT applications. *Journal of Ambient Intelligence and Humanized Computing*. <https://doi.org/10.1007/s12652-023-04482-4>
- Lee, J., Lee, D., & Kwon, D. (2015). Efficient hardware implementation of the HIGHT block cipher for low-resource environments. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E98.A(1), 244–246. <https://doi.org/10.1587/transfun.E98.A.244>
- MarketsandMarkets. (2023). *IoT market forecast 2024–2030*. <https://www.marketsandmarkets.com>
- Mohammed, A., Ahmed, M., & Younis, M. (2022). Security challenges in IoT: A lightweight cryptographic perspective. *IEEE Internet of Things Journal*, 9(4), 2523–2535.
- Morris, S., Liu, Y., Mouha, N., & NIST Lightweight Cryptography Team. (2022). *Lightweight Cryptography Standardization Process – Finalists*. National Institute of Standards and Technology (NIST). <https://csrc.nist.gov/projects/lightweight-cryptography>
- NIST. (2023). *Lightweight Cryptography Standardization Process – Finalists*. <https://csrc.nist.gov/Projects/lightweight-cryptography>
- Roman, R., Najera, P., & Lopez, J. (2018). Securing the Internet of Things. *Computer*, 51(9), 28–35.
- Sethi, P., & Sarangi, S. R. (2022). Security challenges in IoT devices: Current developments and future directions. *IEEE Internet of Things Journal*, 9(4), 3010–3022. <https://doi.org/10.1109/JIOT.2021.3108974>
- Statista. (2023). *Number of IoT connected devices worldwide 2019–2030*. <https://www.statista.com>
- Statista. (2024). *Internet of Things (IoT) connected devices worldwide*. <https://www.statista.com>
- Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., & Omar, M. (2023). Security of industrial IoT: Recent advances and future directions. *Future Generation Computer Systems*, 137, 85–100. <https://doi.org/10.1016/j.future.2022.07.015>
- Yin, H., Wang, L., & Liu, Z. (2021). A review of lightweight block ciphers for resource-constrained IoT devices. *IEEE Access*, 9, 24915–24936.
- Zhang, H., Zhao, X., & Lin, J. (2023). Evaluating security and performance trade-offs in lightweight encryption for IoT. *Computers & Security*, 132, 103087. <https://doi.org/10.1016/j.cose.2022.103087>
- Zhang, Y., Wang, J., & Wang, Y. (2022). Lightweight encryption algorithms for industrial IoT: A performance evaluation. *IEEE Transactions on Industrial Informatics*, 18(10), 6931–6940. <https://doi.org/10.1109/TII.2021.3115569>