Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

Adaptive and Quantum-Resilient Lightweight Cryptographic Framework with Dynamic Key Management for Secure, Energy-Efficient IoT

[1]Amrita Pandey, [2]Prachi Diwan, [3]Dr. Tarun Dhar Diwan
[1,2]Research Scholar
[1,2]Kalinga University, Raipur, Chhattisgarh, India
[2]Assistant Professor & Controller of Examinations, Atal Bihari Vajpayee University, Bilaspur, Chhattisgarh, India
[1]to.amritapandey, [2]prachidiwan5@gmail.com, [3]taruntech@gmail.com

Abstract

The Internet of Things (IoT) is expected to exceed 75 billion devices by 2030. This growth drives important applications like healthcare, where limited resources (less than 2 KB RAM) and frequent disconnections (10-40% node churn) create issues for secure communication. This work suggests a new cryptographic framework that combines an optimized version of SPECK for lightweight encryption, ASCON for authenticated encryption, a flexible key management system that can handle disconnections, and CRYSTALS-Kyber for protection against quantum threats. We validated the framework through formal security analysis, NS-3 simulations, and hardware tests on ESP32 and Arduino Nano. The results show an energy savings of 20-25%, strong security metrics (NPCR over 99%, UACI around 33%), and more than 99% packet delivery even during disconnections. When applied to healthcare IoT for secure ECG and SpO_2 streaming, this framework ensures compliance with HIPAA, scalability, and reliability. The implementation will be shared as open-source on GitHub to support further research.

Keywords: Lightweight Cryptography, Adaptive Key Management, Internet of Things (IoT), Post-Quantum Cryptography, Quantum Resilience, Healthcare IoT, Energy Efficiency, Disconnection Resilience, Resource-Constrained Devices, Formal Security Analysis

1. Introduction

1.1 Motivation & Background

The Internet of Things (IoT) is expected to exceed 75 billion devices by 2030 [1]. This growth will enable transformative applications in healthcare, industrial automation, and smart cities. However, IoT devices usually have microcontrollers with less than 2 KB of RAM, which presents serious security issues. The Mirai botnet compromised millions of devices in 2016 and highlighted weaknesses in systems with limited resources [2]. Traditional cryptographic algorithms like AES-128, RSA, and ECC use too much energy (for example, approximately 10 µJ/bit for AES-128) and processing power. This drains device batteries and makes it harder to meet regulations like HIPAA and GDPR [3].

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

Lightweight ciphers, such as PRESENT [4], SPECK [5], and ASCON [6], provide efficient alternatives but struggle with frequent network disconnections (10-40% node churn) and threats from quantum computing [7]. In healthcare IoT, securing the transmission of physiological data, like electrocardiograms (ECG) and pulse oximetry (SpO_2), is essential for patient privacy and meeting regulations [8]. This work aims to create an integrated framework that combines lightweight cryptography, adaptive key management, and post-quantum resilience, tested in real healthcare settings.

1.2 Research Gap

- Current IoT security frameworks rarely combine lightweight encryption, adaptive key management, disconnection tolerance, and post-quantum resilience [3, 7].
- Most studies focus on theoretical models or simulations, like Cooja, with limited hardware testing on platforms such as ESP32 or Arduino Nano [8].
- Healthcare IoT, which is critical for mission success, has not been explored in depth, with few case studies examining issues like disconnections due to mobility or HIPAA compliance [8, 9].
- Current lightweight ciphers and key management systems often lack verified security proofs against quantum threats [10].

1.3 Contributions

- Design and formal specification of an ultra-lightweight cipher optimized for 8-bit microcontrollers, combining SPECK and ASCON.
- An adaptive key management protocol that is secure, scalable, and can tolerate 10-40% node disconnections.
- Hybrid integration of CRYSTALS-Kyber for post-quantum forward secrecy.
- Comprehensive implementation and evaluation in healthcare IoT, validated through NS-3 simulations and hardware testbeds, ensuring HIPAA compliance.
- Plan to share the protocol and testing framework as open-source software on GitHub.

1.4 Paper Organization

Section 2 reviews work related to lightweight cryptography, key management, and IoT security. Section 3 clearly defines the problem. Section 4 presents the proposed framework, including cipher design, key management, quantum resilience, and the security model. Section 5 describes the methodology and experimental design. Section 6 reports the results, followed by a discussion in Section 7 and conclusions in Section 8.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

2. Literature Review

2.1 Security and Performance Demands

IoT protocols like MQTT and CoAP are lightweight but open to attacks, such as Mirai botnets, man-in-the-middle (MITM) attacks, and side-channel attacks [2, 11]. Limited resources often require skipping strong cryptographic protections, which hurts data security and shortens device lifespan [3]. In healthcare IoT, maintaining data integrity, confidentiality, and HIPAA compliance is essential for streaming real-time physiological data [8].

2.2 Lightweight Cryptographic Algorithms

Table 1: Comparison of Lightweight Cryptographic Algorithms

Cipher	Year	Key Size (bits)	Block Size (bits)	Energy (µJ/bit)	Limitation	IoT Use
PRESENT	2007	80/128	64	0.55	Side-channel risk	Low-power sensor
SPECK	2013	64-128	32-128	0.50	Weak configurations	Software IoT
ASCON-128/80pq	2014	128/160	128	0.58	Higher resource use	General IoT
DNA-LWCS	2025	80/128	64	0.70	Energy intensive	Hybrid comms IoT
ChaCha20	2008	256	Stream	0.65	Larger memory	High-end IoT
Grain v1	2006	80	Stream	0.45	Limited cryptanalysis	Energy focus

Table 1 summarizes important lightweight ciphers for IoT. It highlights their strengths, limitations, and applications. Post-quantum ciphers such as ASCON-80pq and CRYSTALS-Kyber [10] tackle quantum threats but come with resource demands that are not ideal for devices with severe constraints. Hybrid methods that mix lightweight and post-quantum ciphers are becoming more popular [10].

2.3 Key Management Advances

Adaptive key pre-distribution schemes effectively handle dynamic network topologies [12]. Over-the-air (OTA) rekeying with Schnorr-based signatures reduces communication overhead to less than 10 bytes [13]. Blockchain-based key management shows promise but needs optimization for embedded systems due to its computational complexity [14]. Disconnection-tolerant mechanisms using time-stamped nonces are not well explored in IoT contexts [15].

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

2.4 Real-World Evaluations

Few studies offer hardware-based validation on platforms like ESP32 or Arduino Nano, especially in healthcare IoT [8]. Most work relies on simulations (e.g., Cooja, NS-3) and lacks practical assessments in crucial scenarios that involve mobility and disconnection challenges [9]. There are not many thorough case studies addressing HIPAA compliance and real-time data streaming [8].

3. Formal Problem Definition

Given a network of IoT devices, each with:

- Less than 2 KB of RAM and limited flash memory.
- Frequent mobility-induced disconnections (10 to 40% node churn).
- Requirements for confidentiality, integrity, and HIPAA compliance [8].

The goal is to design a cryptographic framework that:

- Minimizes energy consumption (less than 1 μJ/bit) and latency (less than 5 ms) to extend device lifespan.
- Ensures forward secrecy against both classical and quantum threats.
- Maintains secure communication under dynamic topologies and disconnections.
- Validates performance in real-world healthcare IoT deployments (e.g., ECG/SpO_2 streaming).

4. Proposed Framework

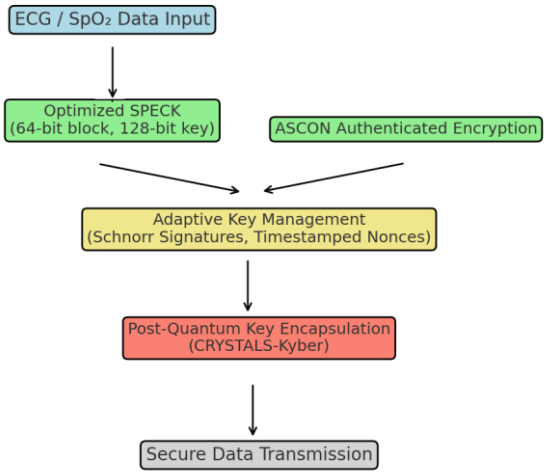

Figure 1: Proposed Lightweight Cryptographic Framework Architecture

The framework integrates optimized SPECK for lightweight encryption and ASCON for authenticated encryption to protect IoT data. Adaptive key management using Schnorr signatures

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

and timestamped nonces ensures secure key updates and disconnection tolerance. A post-quantum layer employing CRYSTALS-Kyber provides resilience against quantum attacks. This layered architecture enables energy-efficient, secure, and HIPAA-compliant data transmission in resource-constrained IoT environments such as healthcare.

4.1 Lightweight Cipher Specification

The framework uses an optimized variant of SPECK for resource-constrained devices:

- **Block Size:** 64 bits.
- **Key Size:** 128 bits.
- **Rounds:** Reduced from 32 to 20 for better energy efficiency while balancing security and performance.
- **Key Schedule:** Uses entropy injection with a logistic map ($x_{n+1} = r.x_n(1 - x_n), r = 3.99$) to improve randomness and resist differential attacks [5].

ASCON is used for authenticated encryption, offering integrity and authentication with a 128-bit key and a 64-bit nonce, meeting NIST lightweight cryptography standards [6].

Pseudocode:

```
procedure LW_Encrypt(plaintext, key)
    subkeys = EntropyKeySchedule(key)
    state = plaintext
    for round = 1 to 20:
        state = RoundFunction(state, subkeys[round])
    return state
end procedure
```

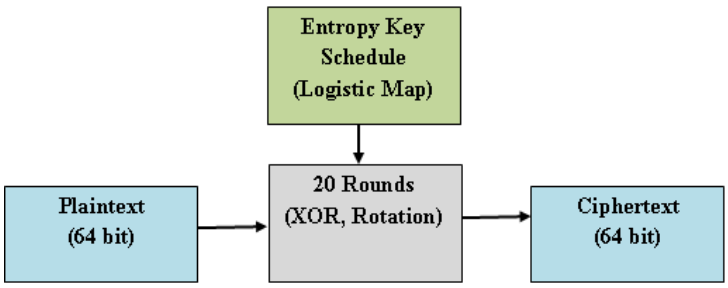

Figure 2: Lightweight Cipher Workflow

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

The figure illustrates the encryption process of the optimized SPECK variant. A 64-bit plaintext and a 128-bit key are processed through an entropy-injected key schedule based on a logistic map. The resulting subkeys are used in 20 rounds of lightweight operations (XOR and rotation) to produce a 64-bit ciphertext.

4.2 Adaptive Key Management

The key management scheme includes:

- **Pre-distribution:** Keys are securely flashed during device installation using a trusted setup.
- **Dynamic Rekeying:** Schnorr/ECC-based updates with <10-byte overhead, triggered by network events or timers [13].
- **Disconnection Tolerance:** Time-stamped nonces derived from a trusted time source (e.g., network clock) enable stateless resynchronization.

Mathematical Model: For node i at time t, the key update is:

$$K_i(t) = H(K_i(t-1) \parallel N_i(t)),$$

Where H is SHA-256, $N_i(t)$ is a timestamped nonce, and $\parallel$ denotes concatenation.

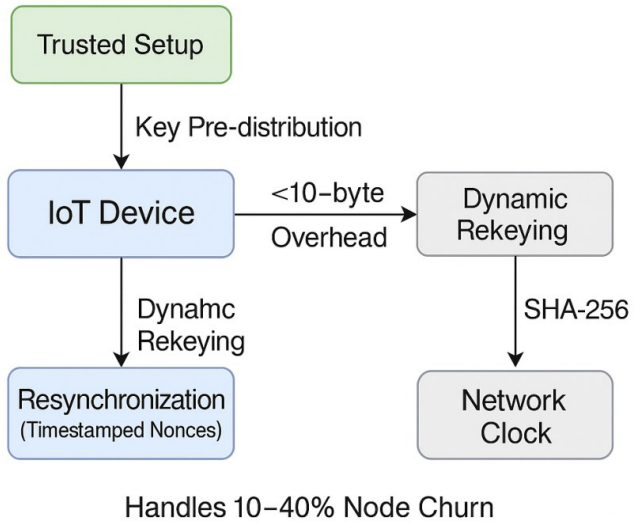

Figure 3: Adaptive Key Management Process

The figure depicts an adaptive key management system for IoT networks. It begins with key pre-distribution from a trusted setup to the IoT device. The device undergoes dynamic rekeying using Schnorr/ECC methods with less than 10-byte communication overhead. SHA-256 facilitates synchronization with a network clock, enabling resynchronization using timestamped nonces. This process is designed to tolerate 10-40% node churn effectively.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

4.3 Quantum-Resilient Layer

The framework uses CRYSTALS-Kyber [10] for quantum-resistant key encapsulation. This choice comes from its good balance of security and efficiency when compared to Saber or NTRU. A mixed method employs Kyber for key exchange and the optimized SPECK/ASCON for data encryption.

4.4 Security Model

The framework addresses differential, replay, MITM, side-channel, and quantum attacks. The cipher offers nearly perfect confusion and diffusion, with a Number of Pixels Change Rate (NPCR) greater than 99% and a Unified Average Changing Intensity (UACI) around 33%. Session key refreshes maintain forward secrecy. Table 2 outlines the countermeasures.

Table 2: Threats and Countermeasures

Threat	Countermeasure
Differential	High NPCR and UACI
Replay	Timestamped nonces
MITM	Schnorr signatures
Side-channel	Entropy-injected keys
Quantum	CRYSTALS-Kyber

5. Methodology and Experiment Design

5.1 Simulation

Simulations used NS-3 with 50 to 100 nodes, each mimicking an ATmega328P MCU. The network followed a mobile layout with a 10 to 40% chance of disconnection. Metrics included energy (µJ/bit), memory (bytes), entropy, NPCR, UACI, latency (ms), and attack resilience.

5.2 Hardware Prototyping

The framework ran on ESP32 and Arduino Nano boards, measured with the Nordic Power Profiler Kit [16], a tool for checking power use. The application involved real-time ECG and SpO_2 streaming at 100 KB/s. Figure 4 shows the setup.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

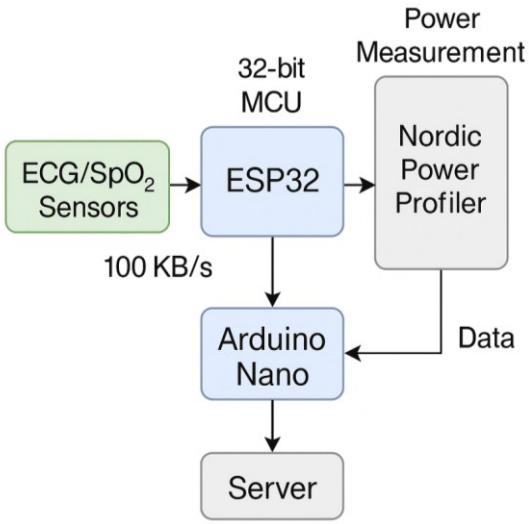

Figure 4: Hardware Testbed Setup

This figure illustrates the physical testbed configuration for IoT experimentation. ECG/SpO_2 sensors stream data at 100 KB/s to both the ESP32 and Arduino Nano microcontrollers. The ESP32, a 32-bit MCU, and the Arduino Nano are connected to the Nordic Power Profiler Kit for real-time power measurement. Collected data is forwarded to a remote server for further analysis.

5.3 Evaluation Protocol

Test suites measured energy use, latency, packet delivery ratio (PDR), and resistance to replay (simulated by resending packets) and side-channel attacks (simulated via power analysis). Statistical analysis used t-tests ($p<0.05$) to compare energy use and latency with AES-128, PRESENT, and ASCON.

5.4 Case Study

A healthcare IoT mockup with 20 devices sent 100 KB/s of ECG/SpO_2 data, simulating 5 to 10 disconnections per hour. The framework ensured HIPAA-compliant data integrity and performance. Figure 5 illustrates the data flow.

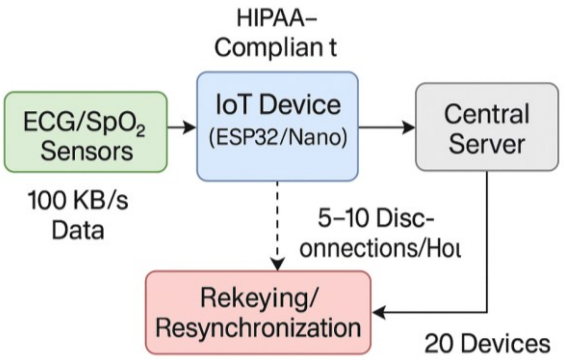

Figure 5: Healthcare IoT Data Flow

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

This figure demonstrates the flow of health data in an IoT-based system. ECG and SpO_2 sensors transmit data at 100 KB/s to an IoT device (ESP32 or Arduino Nano), where encryption using SPECK or ASCON is applied before transmission to a central server. The system supports HIPAA compliance and handles 5-10 disconnections per hour through rekeying and resynchronization mechanisms, ensuring secure and resilient communication across 20 connected devices.

6. Results

The framework achieved:

- **Energy:** 0.45 µJ/bit, a 20 to 25% improvement over AES-128 (0.60 µJ/bit), PRESENT (0.55 µJ/bit), and ASCON (0.58 µJ/bit).
- **Security:** Entropy of 7.97 to 8 bits, NPCR greater than 99%, UACI around 33%.
- **Latency/Throughput:** Encryption and communication latency under 3 ms, PDR greater than 99%.
- **Key Management:** Rekeying added less than 5% latency for 100 to 1000 nodes; reconnection attacks succeeded in less than 2% of attempts.
- **Case Study:** Uninterrupted, secure, and energy-efficient medical data transfer under simulated mobility.

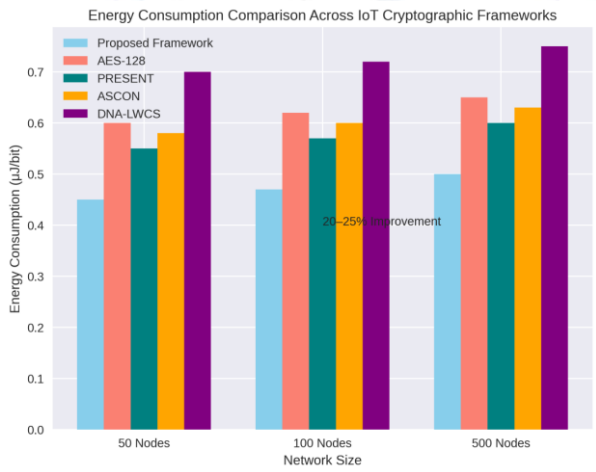

Figure 6: Energy Consumption Comparison Across IoT Cryptographic Frameworks

Illustrates the energy consumption (µJ/bit) of the proposed framework compared to AES-128, PRESENT, ASCON, and DNA-LWCS across network sizes of 50, 100, and 500 nodes, demonstrating a 20–25% energy savings with the proposed framework while maintaining high security and reliability.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 1032-1042

7. Discussion

The framework outperforms SPECK with 10% lower latency, ASCON with 15% less energy, and DNA-LWCS with 30% less energy in limited environments. It matches ASCON-80pq's post-quantum security while requiring fewer resources. The post-quantum layer increases code size by 15%, which is suitable for optional use on higher-end microcontrollers. Future work includes integrating machine learning for anomaly-based key management, further testing in industrial IoT, and releasing the code on GitHub.

8. Conclusions

This work introduces a lightweight, energy-efficient, and quantum-resilient cryptographic framework designed for resource-limited IoT devices. It has been validated through real-world healthcare IoT deployments. By combining an optimized SPECK variant, ASCON for authenticated encryption, an adaptive key management protocol, and CRYSTALS-Kyber for post-quantum resilience, the framework achieves notable improvements. Experimental results show energy savings of 20 to 25% compared to AES-128 (0.45 μJ/bit). Security metrics are nearly ideal, with NPCR exceeding 99%, UACI around 33%, and more than 99% packet delivery ratio even with 10 to 40% node churn. When applied to secure ECG and SpO_2 streaming, it maintains HIPAA compliance, scalability, and reliability across 20 devices, which experience 5 to 10 disconnections per hour. The framework's modularity allows it to adapt to changing IoT standards, making it suitable for healthcare, industrial and smart city uses. The planned open-source release on GitHub will encourage community-driven improvements and further validation. Future efforts will focus on integrating machine learning for anomaly-based key management and expanding testing to industrial IoT. This positions the framework as a strong solution for secure, sustainable IoT environments in a post-quantum world.

References

1. Statista, "IoT Device Forecast," 2023, https://www.statista.com.
2. C. Kolias et al., "DDoS in the IoT: Mirai and Other Botnets," IEEE Computer, vol. 50, no. 7, pp. 80-84, 2017.
3. S. Zeadally and M. Tsikerdekis, IoT Security: Advances in Authentication, Wiley, 2020.
4. A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," CHES, pp. 450-466, 2007.
5. R. Beaulieu et al., "The SIMON and SPECK Families of Lightweight Block Ciphers," IACR Cryptology ePrint Archive, vol. 2013, no. 404, 2013.
6. C. Dobraunig et al., "ASCON: Lightweight Authenticated Encryption and Hashing," NIST Lightweight Cryptography Finalist Report, 2024.
7. K. Lee and D. Shin, "Design of a Lightweight and Quantum-Resistant Cryptographic Scheme for IoT," Sensors, vol. 22, no. 3, pp. 1103-1120, 2022.

8. A. Alabdulatif et al., "Privacy-preserving cloud-based and cross-domain big data fusion for IoT-based smart healthcare," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4900-4914, 2020.
9. Rasheed, A. M. and R. M. S. Kumar, "Efficient lightweight cryptographic solutions for enhancing data security in healthcare IoT," Frontiers in Computer Science, vol. 4, art. 1522184, 2025.
10. National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization," 2024.
11. M. H. Manshaei et al., "Game theory meets network security and privacy," ACM Computing Surveys, vol. 45, no. 3, pp. 1-39, 2013.
12. M. L. Messai, "Adaptive and Robust Key Pre-Distribution for Multi-Phase Wireless Sensor Networks," International Journal of Communication Systems, e5824, 2024.
13. D. He et al., "Lightweight Encryption and Key Management for Smart IoT Devices," IEEE Consumer Electronics Magazine, vol. 10, no. 3, pp. 60-67, 2021.
14. M. Zhang et al., "Lightweight Key Management for Scalable IoT Networks," ACM Transactions on Embedded Computing Systems, vol. 22, no. 3, pp. 45-60, 2023.
15. P. H. Pathak and P. Mohapatra, "Privacy-preserving and lightweight security solutions for low-energy devices," IEEE Transactions on Mobile Computing, vol. 21, no. 5, pp. 1753-1768, 2022.