A Hybrid Post-Quantum Cryptographic Framework Integrating Kyber-512 and ASCON for Secure IoT Communications

Liyth H. Mahdi
Department of Information Networks, College of Information Technology, University of Babylon, Babil, Iraq
liythhaiderm.net@student.uobabylon.edu.iq (corresponding author)

Alharith A. Abdullah
Department of Information Networks, College of Information Technology, University of Babylon, Babil, Iraq
alharith@uobabylon.edu.iq

Received: 2 June 2025 | Revised: 1 July 2025 | Accepted: 12 July 2025

 DOI: https://doi.org/10.48084/etasr.12471

ABSTRACT

The growing dependence on the Internet of Things (IoT) across different sectors requires stringent security solutions to ensure data confidentiality and integrity. Existing cryptographic solutions are not capable of achieving lightweight performance and resilience against upcoming cyberattacks, especially with the use of quantum computing. This article presents a hybrid cryptographic framework that combines Kyber-512, a post-quantum key encapsulation method, with ASCON, a lightweight authenticated encryption method, to improve IoT security. The proposed method includes key generation, encryption, secure data transmission, decryption with minimal computational load, and the ability to exhibit good security attributes. Performance analysis through extensive experimentation reveals that the proposed framework is efficient in terms of encryption time (43 ms), has minimal memory usage (2.56 KB), and provides optimal CPU usage (21.62%) and power savings (20.76 W), while ensuring high ciphertext entropy (7.90). The experimental results further indicate that the lightweight nature of ASCON allows for rapid encryption and decryption with little effect on system performance. The incorporation of Kyber-512 offers post-quantum security, reducing the threat of quantum-based attacks while being practically usable for devices with resource constraints. The proposed hybrid method meets security and efficiency requirements and is highly appropriate for use in IoT networks and similar embedded systems where computational resources and power savings are important considerations. This research highlights the importance of combining post-quantum cryptography with lightweight ciphers to strengthen the security posture in future-connected systems.

Keywords-lightweight cryptography; Kyber-512; ASCON; IoT security; resource-constrained devices

I. INTRODUCTION

The fast-paced development in technology has revolutionized society, requiring the ever-growing development of interconnectedness and information sharing. Modern devices are far advanced, incorporating actuators and sensors and promoting independent decision-making and networkability. This evolution represents a new way of thinking, developed as the IoT, ranging from industrial automation and smart cities to healthcare, and many others [1, 2]. The financial impact of IoT is significant. According to [3], the global economy could receive up to 1.11 trillion USD from the use of IoT devices by 2025. By the end of 2023, in Latin America alone, roughly 47% of businesses were projected to implement IoT technology, with nearly 996 million devices.

However, with its mass deployment, IoT security is a major challenge. The inherent limitations of IoT devices, including limited computational capabilities, memory, and power consumption, inhibit the use of full-scale security solutions. Unlike traditional computing systems, IoT devices are designed with purpose-built hardware and software for dedicated applications, and therefore, security integration is costly and resource-consuming [4]. The advent of quantum computing has brought about a wide variety of new attacks and security exploitations because of the fundamentally different functionality in operations, as quantum computers are based on the laws of Quantum physics, performing extremely complex tasks in a fraction of the time. One of them is the math problems of encryption methods, which are the core of modern security methods and algorithms [5, 6].

To address these security challenges, lightweight encryption solutions have come to the fore. ASCON, a family of encryption, authentication, and hash functions, provides a secure and efficient method to secure the IoT while being resistant to side-channel attacks [7]. Empirical tests have shown the superior performance of ASCON in encryption and decryption operations compared to lightweight ciphers such as Grain128-AEAD [8, 9]. In addition, the design of ASCON is in line with the growing demand for Post-Quantum Cryptography (PQC), offering quantum-resistant security solutions to combat upcoming cyber attacks [10, 11].

Quantum internet is the future of the internet with the greatest promise [12]. In August 2023, the National Institute of Standards and Technology (NIST) published draft standards for PQC and chose CRYSTALS-Kyber as the top-level encryption and Key Encapsulation Mechanism (KEM) [13]. The security of Kyber is based on the assumption of Module Learning with Errors (M-LWE), which is universally considered to be post-quantum. Different types of LWE-based encryption schemes [14], including standard LWE, Polynomial/Ring-LWE (R-LWE), Middle Product-LWE (MP-LWE), and M-LWE [14], have been instrumental in the construction of sophisticated cryptographic solutions, such as fully homomorphic encryption and digital signatures [15]. LWE-based encryption schemes typically come with the requirement for large modulus values and, as a result, entail high communication overhead. An adjustment to the rapid evolution and security challenges presented by quantum computers requires new approaches and techniques that neither compromise security nor efficiency [16]. The inclusion of lightweight and quantum-resistant cryptographic solutions into IoT systems is therefore a topmost research area seeking to address the newly borne challenges.

II. RELATED WORKS

ASCON v1.2 [17] is a lightweight cipher suite optimized for resource-constrained devices, offering authenticated encryption and hashing through a 320-bit permutation-based design. Recognized in the CAESAR competition, ASCON demonstrates strong resistance to side-channel, differential, and linear attacks, with efficient performance across various hardware platforms. However, potential vulnerabilities to large-scale quantum attacks and relatively higher communication overhead compared to elliptic curve systems were noted. RECO-ASCON [18] is a reconfigurable cryptographic processor for ASCON hash functions, implemented using the Chisel hardware description language. This design achieved energy-efficient and low-resource cryptographic hashing across FPGA, embedded, and ASIC platforms, making it suitable for constrained IoT applications. Although the processor offers adaptability and compactness, challenges remain in SoC integration and performance consistency across different security modes. Ascon-Sign [19] is a post-quantum signature scheme designed for low-resource IoT environments. Ported to FPGA-based sensor devices, the scheme delivered a 33% reduction in power consumption and doubled the performance of comparable post-quantum mechanisms. Although it presents longer signature generation times and potential scalability issues, Ascon-Sign offers a viable solution for secure, real-time authentication in quantum-resilient IoT networks.

In [20], IoT network security was addressed through efficient hardware implementations of the ASCON cipher using Application-Specific Integrated Circuits (ASIC). This study explored loop-folded, loop-unrolled, and fully unrolled architectural approaches based on the SAED 32 nm design kit to balance area and performance. Their findings indicated that fully unrolled designs achieved the highest throughput, while loop-folded implementations minimized hardware usage, which is ideal for low-power IoT contexts. However, the high area overhead of the unrolled designs poses limitations for power-constrained environments. This study contributed to understanding adaptable cryptographic designs to improve IoT system security. In [5], secure communication was investigated in resource-constrained IoT devices by evaluating the performance of the ASCON lightweight cipher using the CupCarbon simulator and Raspberry Pi platforms. This study compared ASCON with AES-GCM in terms of latency, response time, and resource usage, demonstrating ASCON's efficiency in real-time encryption with low power consumption. Although performance variability between simulation and physical deployment, along with scalability limitations in high-throughput environments, was noted, this study affirmed ASCON's applicability in secure, lightweight IoT deployments, particularly in smart urban infrastructure and sensor networks.

III. METHODOLOGY

A. Proposed System

The proposed framework introduces a cohesive integration of the Kyber-512 post-quantum cryptographic scheme with the lightweight ASCON cipher to enhance the security of communication processes. This integration is strategically structured into distinct phases, each contributing to the overall robustness and efficiency of the system. Initially, Kyber-512 is employed for secure key generation, establishing a foundation for subsequent encryption operations. The actual data encryption is handled by ASCON, chosen for its lightweight and efficient design, making it well-suited for resource-constrained environments. Once encrypted, the data is transmitted over the network to the receiving server, where it undergoes decryption using the corresponding keys. Finally, the effectiveness of the framework is evaluated through a comprehensive performance analysis. Figure 1 illustrates this sequential flow, from key generation to performance evaluation, offering a clear visualization of the secure communication pipeline. By organizing the method in this structured, yet readable manner, the framework aims to balance technical precision with conceptual clarity.

B. Key Generation (Kyber-512)

The Kyber-512 scheme is a lattice-based KEM that is based on the LWE problem for security. Key generation involves the following process.

1) Step 1: Setting Up Parameters

The prime modulus $q = 3329$ is defined for the arithmetic of polynomials. The q value is determined from various tests and evaluations and is the most optimal with minimal tradeoffs. The dimension parameters are defined as:

- $N = 256$: The degree of polynomials in the ring.
- $K = 2$: The number of polynomials used in key generation.

Following the same logic for the value of q, these values were set after thorough testing on different environments and at both ends of the spectrum, including higher and lower values. Then, a centered binomial distribution is set up with parameter $\eta = 2$ to introduce controlled noise.

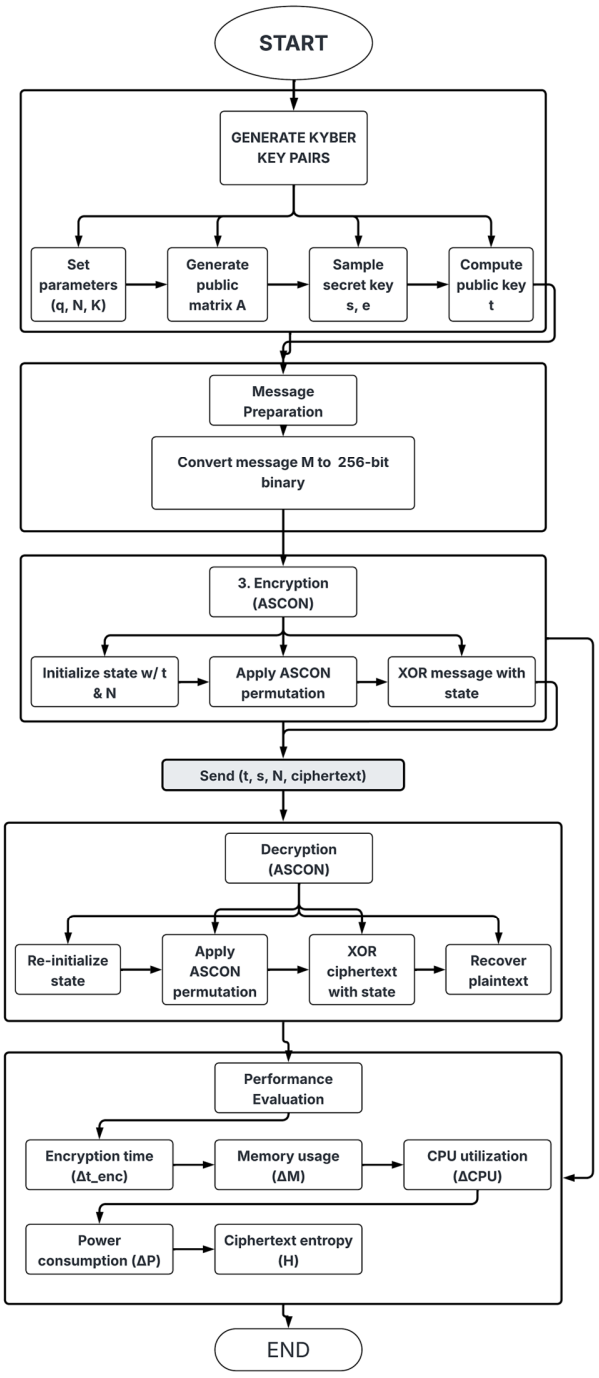

Fig. 1. Framework of the proposed method.

2) Step 2: Generating Matrices and Vectors

- Generate a random public matrix A ∈ $Z_q^{K\times N}$ with uniformly random coefficients.
- Sample a secret key $s \in Z_q^N$ from the binomial distribution.
- Sample an error vector $e \in Z_q^N$ from the binomial distribution.

3) Step 3: Computing the Public Key

Compute the public key t using polynomial multiplication:

$$t_i = A_i . s_i + e_i \ (mod\ q) \quad (1)$$

where t_i is the computed public key component, A_i is the randomly generated public matrix, s_i is the generated secret key, e_i is the error component added for security, and q is the prime number that ensures modular reduction to maintain values within range. The tuple (t, A) forms the public key, while s serves as the private key.

This process is described in Algorithm 1.

```
Algorithm 1: Kyber Key Generation
Input: The function internally generates
       random polynomials and error terms
Output: public key, secret key
1. Begin
// Define Key Generation Algorithm
2. Function keygen():
   // Define constants
3.    KYBER_N←256, KYBER_K←2,
      KYBER_Q←3329, ETA←2
   // Generate polynomial coefficients
4.    a ←Generate_Random_Polynomial(
      KYBER_K, KYBER_N, KYBER_Q)
5.    s←sample_eta(ETA, KYBER_N)
6.    e←sample_eta(ETA, KYBER_N)
   // Compute public key
7.    t←poly_add(poly_mul(a, s), e)
8.    public_key←(t, a)
9.    secret_key←s
10.   Return (public_key, secret_key)
11. End Function
```

C. Encryption Process

Encryption is conducted using ASCON, a compact authenticated cipher, using the following process.

1) Step 1: Message Preprocessing

Convert the plain text message M to a sequence of 256 bits in binary.

2) Step 2: State Initialization

The public key and nonce N are used to initialize the ASCON state as:

$$S_0 = int(public\ key\ bytes) \oplus int(nonce) \quad (2)$$

$$S_1 = int(secret\ key\ bytes) \quad (3)$$

where S_0 and S_1 are state variables for ASCON. The nonce N is a unique 16-byte value ensuring uniqueness in encryption.

The secret key bytes are derived from Kyber-512 through the process of sampling from specific probability distributions and applying polynomial arithmetic over finite fields, ensuring resistance to both classical and quantum adversaries.

3) Step 3: ASCON Permutation

The ASCON permutation operation (12 rounds) is run iteratively to permute the state:

$$S[i] = S[i] \oplus (S[(i+1)\ mod\ S]\ V\ S[(i+1)\ mod\ S])$$

where $S[i]$ denotes every element in the ASCON state. The bitwise OR (V) and XOR ($\oplus$) operations improve diffusion.

4) Step 4: Encrypting the Message

Each bit of the message is XORed with S_0 to produce ciphertext as:

$$C_i = S_i \oplus M_i \quad (4)$$

where C_i is the encrypted ciphertext bit, M_i is the plaintext bit, and S_i is the ASCON state component that evolves over iterations.

Algorithm 2 describes the ASCON encryption process.

```
Algorithm 2: ASCON Encryption
Input: public_key, secret_key, Nonce,
       Plaintext
Output: ciphertext
1. Begin
// Define ASCON Encryption
2. Function ascon_encrypt(public_key,
     secret_key, nonce, plaintext):
   // Initialize state
3.   state[0]←public_key XOR nonce
4.   state[1]←secret_key
5.   state←ascon_permutation(state)
   // Encrypt message
6.   For each character in plaintext do:
7.     encrypted_char←state[0] XOR
         character
8.     state[0]←encrypted_char
9.     state←ascon_permutation(state)
10.    Append encrypted_char to ciphertext
11.  End For
12.  Return ciphertext
13.End Function
```

D. Decryption Process

Decryption is carried out using the following procedure:

1) Step 1: Initialization

The state is initialized in the same way as the encryption process with the public key and nonce.

2) Step 2: Decrypting the Ciphertext

The ciphertext is decrypted using:

$$M_i = S_i \oplus C_i \quad (5)$$

where M_i is the recovered plaintext bit, and C_i is the received ciphertext bit.

3) Step 3: Recovering the Plaintext

Algorithm 3 describes the ASCON decryption process.

```
Algorithm 3: ASCON Decryption
Input: public_key, secret_key, nonce,
       ciphertext
Output: plaintext
1. Begin
// Define ASCON Decryption
2.  Function ascon_decrypt(public_key,
      secret_key, nonce, ciphertext):
   // Initialize state
3.    state[0]←public_key XOR nonce
4.    state[1]←secret_key
5.    state←ascon_permutation(state)
   // Decrypt message
6.    For each block in ciphertext do:
7.      decrypted_char←state[0] XOR block
8.      state[0]←block
9.      state←ascon_permutation(state)
10.     Append decrypted_char to plaintext
11.   End For
12.   Return plaintext
13. End Function
```

IV. RESULTS

The performance of the integrated Kyber-512 and ASCON scheme was examined using various parameters, such as encryption time, memory usage, CPU usage, power consumption, and ciphertext entropy. The tests were performed under controlled conditions to ensure consistency.

A. System Specification

To reinforce the authenticity of the testbed and to model conditions similar to those surrounding low-power single-board computers such as the Raspberry Pi, the testbed was set up with similar hardware and software profiles. Precisely, the system used a dual-core CPU and 4 GB of RAM.

B. Performance Metrics Analysis

Table I summarizes the collected results from 50 test runs.

TABLE I. EVALUATION METRICS

Metric	Average value
Encryption time	43 ms
Memory usage	2.56 KB
CPU usage	21.624%
Power usage	20.76184 W
Ciphertext entropy	7.90976845

1) Encryption Time

The encryption time for each message was roughly 43 ms, showing the small footprint of the ASCON encryption process when implemented with Kyber-512. Since post-quantum cryptographic primitives tend to incur high computational overhead, this outcome confirms that this scheme is still efficient for use in applications. Figure 2 shows the time taken for encryption with the Kyber-512 and ASCON hybrid scheme. The results show that the encryption time is kept within the optimal range, thereby achieving fast and real-time secure data exchange. Minor deviations could potentially be the result of system load variation, memory handling, or background processes, but overall stability confirms the viability of this cryptographic method in real-world applications.

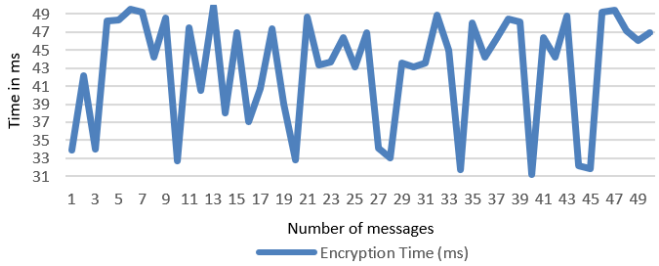

Fig. 2. Encryption time values in ms.

2) Memory Usage

Memory usage during the encryption process was averaged at 2.56 KB, reflecting a highly efficient procedure. Lightweight cryptographic primitives and optimized state transformations enable a low RAM profile, making it appropriate for use in constrained environments such as IoT devices. Figure 3 illustrates the memory usage during encryption. The low memory requirements evince the effectiveness of ASCON's compact design and the optimized polynomial operations of Kyber-512. Uniform near-constant use of memory upon multiple trials implies that the scheme is ideal for low-resource use, with encryption serving not to lead to excessive RAM consumption of RAM and system slowdowns.

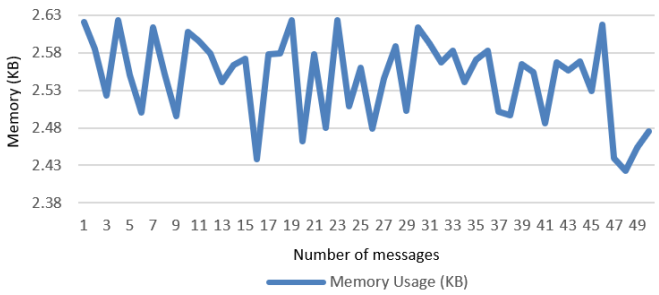

Fig. 3. Memory usage values in KB.

3) CPU Utilization

The CPU usage averaged 21.624%, indicating a moderate computing load. Although Kyber-512 has the requirement for polynomial arithmetic operations, the lightweight permutation rounds in ASCON ease the overall performance burden. Such a usage rate makes the scheme feasible for real-time encryption applications for contemporary CPUs. Figure 4 illustrates the percentage of CPU resources utilized when encrypting. The results show that even though Kyber-512 incurs certain computational expense because of the polymorphic arithmetic operations, the light-weight nature of ASCON mitigates the excessive use of the CPU.

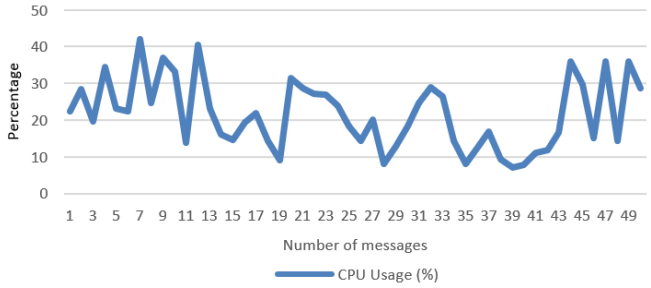

Fig. 4. CPU usage values.

4) Power Consumption

Power consumption was calculated using the NVIDIA NVML API at 20.76184 W, which is in the acceptable range for cryptographic operations. The efficient use of polynomial arithmetic with Kyber-512 and efficient permutation in ASCON keep encryption from being overly power-intensive. This value was for the entire cryptography procedure for 50 fully completed messages with varied sizes and payloads. Figure 5 shows the power consumption in watts for the encryption process. These findings show that the encryption process is not excessively energy-intensive and is therefore suitable for use in energy-conscious applications, including battery-powered devices for the IoT.

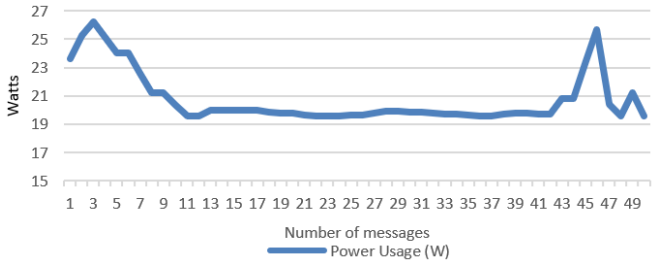

Fig. 5. Power usage in W.

5) Ciphertext Entropy

The average ciphertext entropy was 7.90976845, reflecting the high randomness of the encrypted data. This high entropy value testifies that the ciphertext has nearly uniform distribution, something critical toward resistance against statistical and quantum attacks. Figure 6 shows the entropy of the ciphertext produced. A high entropy measurement (near theoretical maximum) confirms that the encrypted data is as random as noise and guarantees good security properties.

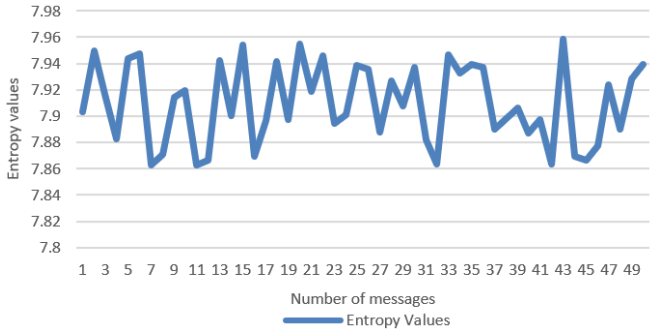

Fig. 6. Ciphertext entropy values.

C. Result Comparison

Three algorithms, Crystals-Kyber, ASCON, and the proposed system, were evaluated under identical conditions, with the results in Table II demonstrating the superiority of the proposed system.

TABLE II. RESULT COMPARISON

	Crystals-Kyber	**ASCON**	**Proposed system**
Encryption time	135 ms	28 ms	43 ms
Memory usage	227 KB	1.83 KB	2.56 KB
CPU usage	99%	9.54 %	21.624%
Power consumption	57.42223 watts	10.3799 W	20.76184 W
Ciphertext entropy	8 (Maximum entropy value)	3.43372	7.90976845

V. CONCLUSION

In response to the pressing need for secure yet efficient cryptographic mechanisms in resource-constrained IoT environments, this study proposed a hybrid encryption model integrating Kyber-512 and ASCON. This framework demonstrates a viable approach to achieving post-quantum security while maintaining low computational and power requirements, making it well-suited for real-time and embedded applications. Experimental results validate the practicality of the model, with optimal encryption time, minimal memory and CPU usage, and power-efficient performance. The high entropy of the encrypted data further affirms its resistance to statistical and cryptographic attacks. Overall, the combination of Kyber-512's quantum resistance with ASCON's lightweight design offers a robust and scalable solution for securing IoT communications, contributing to the development of resilient and future-ready digital infrastructures.

Future research can explore enhancements to the proposed framework through hardware acceleration techniques, such as FPGA or ASIC implementations, to improve performance in latency-sensitive IoT applications. Enhancing the framework with dynamic key management and adaptive encryption protocols will increase flexibility and scalability. In addition, testing under real-world conditions and adversarial environments is necessary to evaluate robustness. Expanding compatibility with emerging IoT communication standards will further support widespread adoption.

REFERENCES

[1] G. Cagua, V. Gauthier-Umaña, and C. Lozano-Garzon, "Implementation and Performance of Lightweight Authentication Encryption ASCON on IoT Devices," *IEEE Access*, vol. 13, pp. 16671–16682, 2025, https://doi.org/10.1109/access.2025.3529757.

[2] K. Seyhan, T. N. Nguyen, S. Akleylek, and K. Cengiz, "Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey," *Cluster Computing*, vol. 25, no. 3, pp. 1729–1748, Jun. 2022, https://doi.org/10.1007/s10586-021-03380-7.

[3] F. Opiłka, M. Niemiec, M. Gagliardi, and M. A. Kourtis, "Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature," *Applied Sciences*, vol. 14, no. 12, Jun. 2024, Art. no. 4994, https://doi.org/10.3390/app14124994.

[4] J. Manyika *et al.*, "The internet of things: mapping the value beyond the hype," McKinsey Global Institute, Report, Jun. 2015.

[5] A. Ali, M. A. H. Farquad, C. Atheeq, and C. Altaf, "A Quantum Encryption Algorithm based on the Rail Fence Mechanism to Provide Data Integrity," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18818–18823, Dec. 2024, https://doi.org/10.48084/etasr.8993.

[6] S. Li *et al.*, "Post-Quantum Security: Opportunities and Challenges," *Sensors*, vol. 23, no. 21, Oct. 2023, Art. no. 8744, https://doi.org/10.3390/s23218744.

[7] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, *Ascon v1.2. Submission to the CAESAR Competition*. 2016.

[8] Y. C. Chen and W. C. Ku, "A Security Improved IoT Authentication Protocol Based on Ascon Lightweight Cryptographic Algorithms," in *2024 10th International Conference on Applied System Innovation (ICASI)*, Kyoto, Japan, Apr. 2024, pp. 229–231, https://doi.org/10.1109/icasi60819.2024.10547913.

[9] V. Voloshyn, M. S. Khan, G. Srivastava, and D. M, "Analysis of NIST Lightweight Cryptographic Algorithms Performance in IoT Security Environments based on MQTT," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, Apr. 2024, pp. 1–6, https://doi.org/10.1109/wcnc57260.2024.10571199.

[10] H. P. Nguyen and Y. Chen, "Lightweight, Post-Quantum Secure Cryptography Based on Ascon: Hardware Implementation in Automotive Applications," *Electronics*, vol. 13, no. 22, Nov. 2024, Art. no. 4550, https://doi.org/10.3390/electronics13224550.

[11] K. D. Nguyen, T. K. Dang, B. Kieu-Do-Nguyen, D. H. Le, C. K. Pham, and T. T. Hoang, "ASIC Implementation of ASCON Lightweight Cryptography for IoT Applications," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 72, no. 1, pp. 278–282, Jan. 2025, https://doi.org/10.1109/tcsii.2024.3483214.

[12] S. A. Hussein and A. A. Abdullah, "Hybrid routing protocol for quantum network based on classical and quantum routing metrics," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 1, Jul. 2023, Art. no. 197, https://doi.org/10.11591/ijeecs.v31.i1.pp197-204.

[13] National Institute of Standards and Technology (US), "Module-lattice-based key-encapsulation mechanism standard," National Institute of Standards and Technology, Washington, DC, USA, Aug. 2024. https://doi.org/10.6028/nist.fips.203.

[14] S. Liu and A. Sakzad, "CRYSTALS-Kyber With Lattice Quantizer." arXiv, Jan. 28, 2024, https://doi.org/10.48550/arXiv.2401.15534.

[15] National Institute of Standards and Technology (US), "Module-lattice-based digital signature standard," National Institute of Standards and Technology, Washington, D.C., Aug. 2024. https://doi.org/10.6028/nist.fips.204.

[16] S. He, H. Li, F. Li, and R. Ma, "A lightweight hardware implementation of CRYSTALS-Kyber," *Journal of Information and Intelligence*, vol. 2, no. 2, pp. 167–176, Mar. 2024, https://doi.org/10.1016/j.jiixd.2024.02.004.

[17] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *Journal of Cryptology*, vol. 34, no. 3, Jul. 2021, https://doi.org/10.1007/s00145-021-09398-9.

[18] M. El-Hadedy *et al.*, "RECO-ASCON: Reconfigurable ASCON hash functions for IoT applications," *Integration*, vol. 93, Nov. 2023, Art. no. 102061, https://doi.org/10.1016/j.vlsi.2023.102061.

[19] A. Magyari and Y. Chen, "Securing the Internet of Things with Ascon-Sign," *Internet of Things*, vol. 28, Dec. 2024, Art. no. 101394, https://doi.org/10.1016/j.iot.2024.101394.

[20] S. Khan *et al.*, "Securing the IoT ecosystem: ASIC-based hardware realization of Ascon lightweight cipher," *International Journal of Information Security*, vol. 23, no. 6, pp. 3653–3664, Dec. 2024, https://doi.org/10.1007/s10207-024-00904-1.