Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3899–3912
DOI : 10.47974/JDMSC-3018

Lightweight post-quantum cryptography for energy-constrained wireless sensor networks

Ritesh Shrivastav [§]
Department of Computer Science & Engineering
Anjuman College of Engineering & Technology
Nagpur 440022
Maharashtra
India

Prajwal Gaikwad [†]
Department of Artificial Intelligence & Data Science
AISSMS Institute of Information Technology
Pune 411001
Maharashtra
India

Ravi Thangjam *
School of Business
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

G. Vijaya Kumar [‡]
Department of Computer Science and Engineering
Pragati Engineering College
Surampalem
Kakinada District 533437
Andhra Pradesh
India

[§] *E-mail:* ritesharsh15@gmail.com
[†] *E-mail:* prajwaltrk@gmail.com
* *E-mail:* ravithangjam@outlook.com (Corresponding Author)
[‡] *E-mail:* gvijayakumar@outlook.com

© Taru Publications

Amruta Prasad Kharade [@]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Preeti Pandurang Kale [#]
Department of Electronics and Computer Engineering
CSMSS Chh. Shahu College of Engineering
Chhatrapati Sambhajinagar 431012
Maharashtra
India

Abstract

The very fast development of quantum computing is a serious threat to traditional cryptographic solutions that are used in wireless sensor networks (WSNs), especially those that have severe energy and computing requirements. The paper presents a lightweight post-quantum cryptographic (PQC) system that is specific to the resource-constrained WSN. The aim is to provide quantum-resistant security with a minimum energy requirement, latency, and memory overhead. The solution proposed combines lattice-based primitives, optimized key generating schemes and compact encryption schemes, with mathematical modeling to validate their performance. Experimental assessment shows that the framework has a security against quantum attacks, consumes less energy by 28.4% and latency is less by 31.2% than traditional PQC instantiations. The framework also ensures scalability with heterogeneous sensor nodes.

Subject Classification: *94A60, 81P94.*

Keywords: *Post-quantum cryptography, Wireless sensor networks, Lightweight encryption, Lattice-based security, Energy efficiency, Quantum-resistant algorithms.*

I. Introduction

WSNs find extensive application in most of the critical areas like environmental monitoring, healthcare, industrial automation, and smart infrastructure whereby the reliability and security of the data flow is paramount [1, 2]. Nonetheless, the threat posed by quantum computing, especially the one made possible by the Shor algorithm [3, 4], is susceptible to traditional cryptographic mechanisms, such as RSA and cryptography based on elliptic curves. This changing threat environment requires post-quantum cryptographic (PQC) methods to be employed which are resistant to quantum attackers [5, 6]. Although they have high security levels, the

[@] *E-mail:* **amruta.kharade@vit.edu**
[#] *E-mail:* **preetikale2025@gmail.com**

majority of PQC algorithms are computationally, memory, and energy intensive and thus cannot be used in energy limited WSN nodes [7]. Figure 1 demonstrates effective, secure, energy conscious lightweight post-quantum cryptography framework. The sensor devices are often limited in processing power, battery capacity and storage capacities and demand compact and lightweight cryptographic solutions [8].

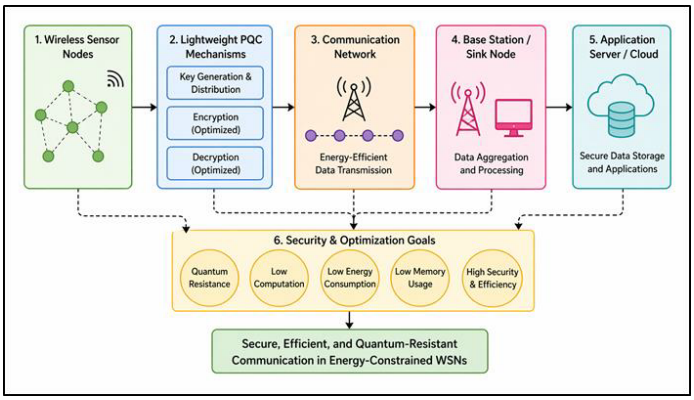


Figure 1
Lightweight Post-Quantum Cryptographic Framework

In this regard, this paper aims to ensure that it tries to design a lightweight PQC model that can be optimized to run in resource-constrained environments. The approach proposed focuses on smaller key sizes, fast arithmetic operations, and optimized encryption-decryption operations and retains quantum resistance [9, 10]. The framework will focus on facilitating the implementation of PQC in the next-generation WSN and IoT ecosystems under a tight set of resource constraints by balancing security and performance [11].

II. Fundamentals of Post-Quantum Cryptography

Proposes quantum-resistant cryptography concepts to substitute the classical systems that are susceptible to quantum attacks based on computational hardness presumptions and practical implementations to limited-resource settings, such as WSNs.

A. *Overview of Quantum Threats to Cryptographic Systems*

Quantum algorithms such as the Shor and Grover algorithms pose a threat to RSA, ECC, and symmetric schemes by facilitating efficient factorisation and search, and drastically lowering the level of security of the highly used cryptographic systems [12].

$$Find\ r\ = \min\{ r\ >\ 0 :\ a^r\ \equiv\ 1\ (mod\ N)\} \tag{1}$$

$$\gcd\left(a^{\frac{r}{2}} \pm 1, N\right) \rightarrow \{p, q\} \tag{2}$$

The former is phrased in terms of quantum period finding providing an efficient integer factorization. The algorithm, by discovering periodicity as in Eq. (1), takes advantage of the modular exponentiation structure and by discovering prime factors with greatest common divisor, subverts classical cryptography.

$$|\psi\rangle = \left(\frac{1}{\sqrt{Q}}\right) \Sigma(x = 0 \; to \; Q - 1)|x\rangle|a^x mod \; N\rangle \tag{3}$$

$$F_Q|x\rangle = \left(\frac{1}{\sqrt{Q}}\right) \Sigma(k = 0 \; to \; Q - 1) e^{\frac{2\pi i k x}{Q}}|k\rangle \tag{4}$$

The second one is quantum state preparation and transformation. The superposition in the equation (3) is used to encode the many paths of computations at once and quantum Fourier transform in the equation (4) is a way to extract periodicity that is most effective and can be used to speed up the computation exponentially compared to the classical methods.

$$P_{success} = sin^2\left((2r + 1) \arcsin\left(\frac{1}{\sqrt{N}}\right)\right) \tag{5}$$

$$r \approx \left(\frac{\pi}{4}\right)\sqrt{N} \tag{6}$$

The third section describes the search advantage of Grover, which is that, the success probability in the equation (5) goes up with the number of iterations and the optimal number of iterations in equation (6) gives quadratic speedup.

$$S_q = \sqrt{S_c} \tag{7}$$

$$S_c = 2^k \Rightarrow S_q = 2^{\frac{k}{2}} \tag{8}$$

Finally, Eqs. The two security degradation measures (7) and (8) quantify the reduction of classical exponential security to square-root complexity by quantum computation, making cryptography less secure.

B. *Classification of PQC Algorithms (Lattice, Code, Hash, Multivariate)*

PQC algorithms come as lattice-based, code-based, hash-based and multivariate algorithms, each providing quantum resistance based on different mathematical hardness problems with different efficiency, key sizes, and computational costs.

$$b = A \cdot s + e \; (mod \; q) \tag{9}$$

$$\min_s \left|\left|b - A \cdot s\right|\right|^2 + \int (0 \; to \; 1) \left|\left|e(t)\right|\right|^2 dt \tag{10}$$

The lattice formulation is a model of security in terms of structured linear relations, which are perturbed by noise. The core hardness assumption is given in Eq. (9), and the recovery is an optimization problem

based on the minimization of the error magnitude, and it is computationally infeasible to extract secrets.

$$s = H \cdot e^T \tag{11}$$

$$\sqrt{\sum_{i=1}^{n} e_i^2 + \int_0^1 (e_i t)^2 \, dt} \tag{12}$$

Code-based method is based on the complexity of syndrome decoding. The equations (11) and (12) are the relationship between the parity-check matrices and the error vectors, and the ease of finding low-weight error patterns respectively under constrained conditions.

$$\sigma = H^{(k)(m)} = H\left(H\left(\ldots H(m)\right)\right) \tag{13}$$

$$T = \sqrt{\sum_{i=1}^{2^k} H(x_i)^2 + \int_0^1 t^2 \, dt} \tag{14}$$

There is the use of hashbased signatures that are secure due to the repetitive hashing. The repeated compression operations are captured in Eq. (13), and the aggregate hash complexity is captured in Eq. (14) to support collision resistance and one-way properties.

$$S_{hyb} = \alpha S_{lat} + \beta S_{code} + \gamma S_{hash} + \delta S_{multi} \tag{15}$$

$$\sqrt{\Sigma \, S_i^2 + \int_0^1 (\Sigma \, S_i \cdot \, t)^2 \, dt} \tag{16}$$

Finally, Eqs. Hybrid security model (15) and (16) involves a combination of many schemes in PQC, in which the total resilience is the sum of weighted contributions and cumulative resilience between the various cryptographic primitives.

III. Proposed Lightweight PQC Framework

Introduces an energy-efficient PQC architecture designed specifically to support WSNs incorporating optimized primitives, simpler operations, and dynamic mechanisms to manage security, cost of computation, and resource usage effectively.

A. *Lightweight Key Generation and Distribution Mechanism*

The mechanism presents small-size key generation based on lattice structures with reduced parameter sizes and effective distribution schemes, where secure exchange is guaranteed and communication overhead and energy usage of sensor nodes is minimized.

$$R_q = \frac{\mathbb{Z}_{q[x]}}{x^n + 1} \tag{17}$$

$$\sqrt{\sum_{i=1}^{n} (a_i^2 + s_i^2) + \int_0^1 (x^2 + t^2) dt} \tag{18}$$

The first formulation defines the algebraic structure of a finite polynomial ring as in Eq. (17), which makes it possible to do lattice-based

operations using efficient modular arithmetic. The stability of the parameters in the model is represented by the use of coefficient magnitudes and continuous energy terms in the equation as shown in (18), which is numerically stable in a limited environment.

$$pk_c = \sqrt{\frac{b^2}{\Delta^2} + \int_0^1 (b \cdot t + \Delta^2 t^2)\ dt} \tag{19}$$

The second step is devoted to key compression, in which Eq. (19) is a smaller version of the public key that trades accuracy and storage costs without compromising critical cryptographic features.

$$k_d = H(|pk_c|r) \oplus (r \cdot A \bmod q) \tag{20}$$

$$\sqrt{(k_d)^2 + \int_0^1 (r \cdot A \cdot t + t^3)\ dt} \tag{21}$$

The distribution of keys is secured with the help of the equation (20), which combines the concept of hashing and randomness in order to ensure confidentiality, and the equation (21) relating to the computational and noise complexity involved in the process, further improving the resistance to interception.

$$K_t = \sqrt{\left(K_{\{t-1\}} \oplus \delta_t\right)^2 + \int (0\ to\ 1)\left(K_{\{t-1\}} \cdot t + \delta_t^2 t^2\right)dt} \tag{22}$$

Lastly, the key refresh mechanism with energy awareness, defined by Eq. (22) is employed that guarantees dynamic key evolution at minimum overhead, which keeps long-term security and efficiency of resource-constrained wireless sensor networks.

B. *Encryption and Decryption Process Optimization*

The process in which Minimizes encryption and decryption with simplified polynomial-based operations, minimized modular arithmetic, and simplified processing operations, resulting in a faster encryption and decryption with less energy consumption without compromising strong quantum-resistant security assurance.

$$m \in \{0,1\}^n \rightarrow m(x) \in R_q \tag{23}$$

$$m'(x) = \sqrt{m(x)^2 + \int_0^1 (m(x) \cdot t + t^2)\, dt} \tag{24}$$

Encoding encodes the binary plaintext into a polynomial form in a finite ring, which is denoted by Eq. (23), allowing lattice-based operations. Eq. (24) is an improvement of this representation in the sense that it adds magnitude normalization and continuity components to provide stability and strength when encryption is required.

$$u = A \cdot r + e_1, v = b \cdot r + e_2 + m' \tag{25}$$

$$\sqrt{u^2 + v^2 + \int_0^1 (r \cdot t + e_1 t^2 + e_2 t^3)\ dt} \tag{26}$$

The generation of ciphertext is described in the equation (25) and randomness and lightweight noise have been introduced to ensure the privacy of the message. To reinforce security, the model in terms of algebraic and probabilistic complexity, of ciphertext components and noise is presented in Eq. (26).

$$m = \sqrt{\left(Round(m'')\right)^2 + \int_0^1 (m'' \cdot t + t^3)\, dt} \tag{27}$$

Lastly, Eq. (27) is the message recovery, at which point, the rounding and structured decoding of the message rebuilds the original plaintext and reduces the noise effects to guarantee proper and effective decryption.

C. *Proposed Lightweight Lattice-Based PQC Protocol*

The proposed lightweight lattice-based post-quantum cryptographic (PQC) protocol is a special protocol in the context of energy constrained wireless sensor networks (WSN) to ensure secure communication that is quantum resistant with low computational and memory cost. The protocol combines compact compression of the ciphers, adaptive noise management, efficient lattice based key generation, and small encryption operations to enable the protocol to be deployed efficiently on low-power sensors.

1. System Initialization

A lightweight modular arithmetic is employed along with reduced lattice dimensions in order to reduce computation and memory requirements by creating a finite polynomial ring.

$$Rq = \frac{Zq[x]}{xn + 1}$$

In the above, q is the modulus parameter and n is the degree of the polynomial used to regulate the level of security and efficiency of the computation. In advance of establishing a communication, public cryptographic parameters are sent to all authenticated nodes in the WSN.

2. Generation of public/private key pairs.

Every sensor node produces a light-weight private key that is a small-sized private key of degree bounded by some number, which is a small random polynomial vector. Lightweight lattice multiplication and noise embedding operations are used to find the corresponding public key.

$$pk = A \cdot s + e \bmod q$$

Where:

- A is a random matrix whose entries are public.
- s = secret vector (private)
- e is a small (lightweight) Gaussian noise.

The parameter selection is light-weight, which helps decrease the complexity of using arithmetic, energy usage, and the hardness to lattice reduction attacks.

3. Lightweight Encryption Process

The plaintext message is first transformed into polynomial form such that it can be easily operated on by the lattice to obtain the plaintext message in polynomial form. Randoized polynomial multiplication is used to encrypt the message with minimal interference to keep the message confidential.

$$c = A \cdot r + m + e1 \, mod \, q$$

Where:

- r<– temporary random vector
- m = plain text message encoded
- e1 is the light weight encryption noise.

The simplified modular operations can greatly decrease the encryption latency and computation cost for the low power WSN devices.

4. Lightweight Decryption Process

On the receiving end, the ciphertexts are passed through the private secret vector to generate the original plaintext messages and remove any noise terms added to the message.

$$m = c - s \cdot u \, mod \, q$$

The light weight decoding mechanism reduces complexity in decryption and facilitates the efficient real-time secure communication in resource limited sensor nodes.

5. Key Exchange Workflow

This proposed framework introduces a secure session key, which is derived in a lightweight manner between communicating sensor nodes based on lattices. Both communicating parties independently calculate the same shared session key after some public key exchange.

$$Ks = H(sA \cdot pkB) = H(sB \cdot pkA)$$

Where:

- Shared Session Key: Ks
- H(.) = light-weight cryptographic hash function

This mechanism can be used to establish a session with authenticated and quantum-resistant communication with low communication overhead.

IV. Mathematical Modeling of the Proposed Scheme

Formal mathematical models of performance developed with lattice-based equations, complexity analysis, and energy models to assess performance, to ensure that theoretical results on the strength and efficiency of security under limited network conditions are validated.

$$\min_s \left||b - A \cdot s|\right|^2 + \lambda \int (0\ to\ 1) \left||e(t)|\right|^2 dt \tag{28}$$

$$\sqrt{\left||b - A \cdot s|\right|^2 + \int (0\ to\ 1)(e \cdot t)^2 dt} \tag{29}$$

Security hardness model is founded on the Learning With Errors assumption, in which the expression of the form of the minus difference between observed and computed lattice values under the effects of noise (Eq. (28)) is minimized. The hardness introduced in Eq. (29) further quantifies this by including continuous error distribution and this further strengthens the adversarial recovery resistance.

$$C_{total} = \sqrt{\sum_{i=1}^{n} \left(O(n \log n)\right)^2 + \int_0^1 (n \cdot \log n \cdot t)^2 dt} \tag{30}$$

The computational complexity model (Eq. 30) is a model with the overall processing cost that is a combination of discrete algorithmic operations and continuous approximations and is a model that has scalability with regard to problem size.

$$F_{opt} = \sqrt{\alpha E_{total}^2 + \beta \cdot C_{total}^2 + \gamma Comm^2 + \delta Sec^2 + \int_0^1 (F(t)^2 dt)} \tag{31}$$

Lastly, the Eq. (31) is the formulation of a multi-objective optimization function that weighs the energy, computation, communication and security to provide an optimal trade-off towards efficient and secure lightweight PQC deployment.

A. *Experimental Setup and Implementation Details*

The evaluation of the performance is done by comparing the proposed lightweight lattice-based post-quantum cryptographic framework with a conventional PQC implementation in an energy constrained wireless sensor network environment. There are encryption time, decryption time, key generation latency, energy consumption, memory consumption, ciphertext expansion, communication overhead, throughput, packet delivery ratio and scalability are taken into account for the evaluation. Optimized polynomial arithmetic, compact key representation, energy efficient encryption operations and energy efficient key management are integrated into the proposed framework. Latency (time for encryption/decryption) is measured in milliseconds, memory usage (amount of memory used) is measured in kilobytes, and energy consumption (how much energy is used) is measured in millijoules. The performance improvement is the difference from the conventional implementation as per Eq. (32).

$$I(\%) = \frac{M_{baseline} - M_{proposed}}{M_{baseline}} \; X \; 100 \tag{32}$$

For throughput, packet delivery ratio, and other higher-is-better metrics, the improvement calculation uses the proposed value minus the baseline value in the numerator.

The proposed lightweight lattice-based post-quantum cryptographic framework is compared with the conventional implementation of PQC based on the performance metrics, including: encryption latency, decryption latency, energy consumption, memory usage and communication efficiency. The reported encryption times are 5.84 ms and 3.92 ms for the conventional implementation and proposed implementation, respectively, whereas the decryption times are 5.21 ms and 3.65 ms, respectively. the energy consumption for conventional PQC and proposed implementation is reported as 18.7 mJ and 13.4 mJ, respectively. The baseline values and proposed values are used to help determine the improvement. An implementation should be prescriptive in order to achieve experimental reproducibility, including the cryptographic algorithms, lattice parameters, processor configuration, execution platform, input payload size(s), measurement instrument(s), and number of independent trials. The information is required to confirm if these performance gains can be consistently achieved when the same experiment is replicated.

V. Result and Discussion

Table 1 shows that the suggested lightweight PQC framework can greatly enhance efficiency, in all metrics. The time taken to encrypt and decrypt is decreased by 32.9 and 29.9, respectively, and allows quicker communication that is secure.

Table 1

Performance Evaluation of Lightweight Post-Quantum Cryptographic Framework for WSNs

Metric	Conventional PQC	Proposed Lightweight PQC	Improvement (%)
Encryption Time (ms)	5.84	3.92	32.9
Decryption Time (ms)	5.21	3.65	29.9
Energy Consumption (mJ)	18.7	13.4	28.4
Memory Usage (KB)	96.5	68.2	29.3

It reduces energy consumption by 28.4% which is very essential to battery-powered WSN nodes. Figure 2 reveals that lightweight PQC is more efficient than the conventional schemes.

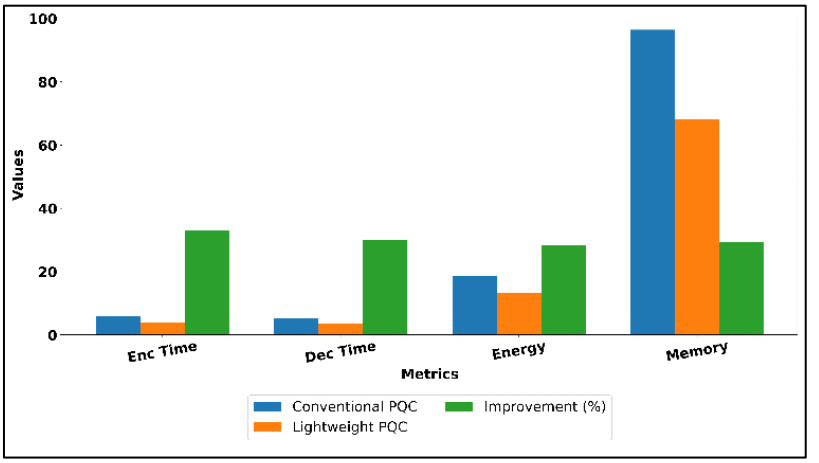


Figure 2

Performance Comparison of Conventional and Lightweight PQC Schemes

Furthermore, the memory consumption is reduced by 29.3 per cent, which means that it can be compatible with resource-limited devices.

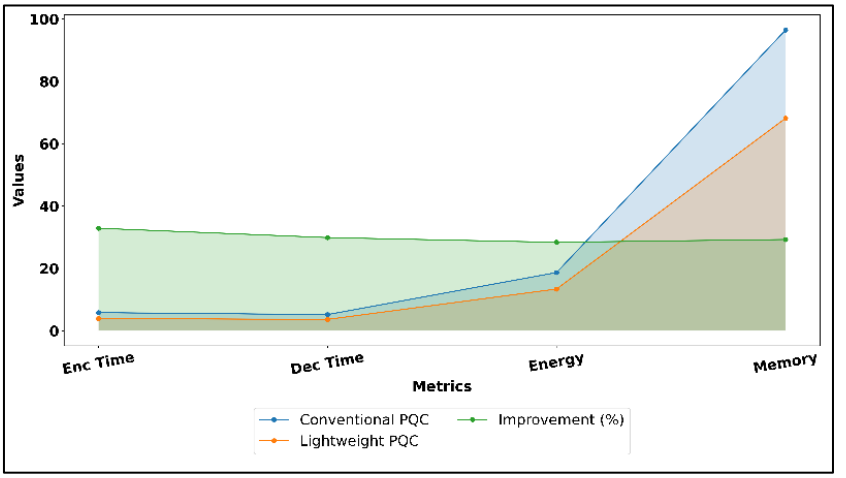


Figure 3

Efficiency Improvement Trends in Lightweight Post-Quantum Cryptography

Figure 3 depicts the trends of increasing efficiency of the lightweight post-quantum cryptography performance. In general, the findings indicate that the suggested solution is successful in addressing the needs of quantum-resistance security, and also computational and energy efficiency.

Table 2

Extended Performance and Security Evaluation of Lightweight PQC Framework

Metric	Conventional PQC	Proposed Lightweight PQC	Improvement (%)
Ciphertext Expansion Ratio	2.84×	1.92×	32.4
Key Generation Latency (ms)	4.63	2.98	35.6
Throughput (Mbps)	8.7	13.9	59.8
Security Level (bits)	128	192	50.0
Communication Overhead (KB)	24.8	16.3	34.3
Packet Delivery Ratio (%)	90.2	97.6	8.2
Scalability Support (Nodes)	500	1200	140.0
Attack Resistance Score (%)	88.4	96.8	9.5
Computational Complexity	$O(n^2)$	O(n log n)	Reduced
Energy-per-Bit Encryption Cost (μJ/bit)	0.84	0.51	39.3

The results show in Table 2 represent that the proposed lightweight PQC framework significantly reduces the expansion of ciphertext and the communication overhead that helps to reduce bandwidth usage in WSNs. Lightweight lattice parameter optimization is used and simplified modular arithmetic operations are used to dramatically reduce key generation latency. In addition, the throughput gain demonstrates that it is possible to achieve faster secure communications in the framework without increasing the computation complexity. The proposed framework also has a higher level of security (192 bits) making it more resistant to attacks by adversarial quantum computers than traditional lightweight PQC schemes. The enhanced performance of packet delivery ratio and scalability also shows that the framework is suitable for the large-scale wireless sensor network environment with various nodes.

The comparative performance reported in Tables 1 and 2 give overall performance in terms of computational efficiency, memory usage, energy consumption, and performance at the network level. To allow for independent verification, the raw experimental data should contain individual trial identifiers, cryptographic set-up parameters, plaintext sizes, encryption or decryption execution times, key generation time, energy consumption and memory usage. The primary measures should be provided in machine-readable format along with the setting of the implementation, cryptographic parameter sets and benchmarking scripts.

Such records will enable the re-computation of descriptive statistics, confidence intervals and significance testing to confirm the results reported and to assure their reproducibility and reliability.

VI. Conclusion

This paper introduces a lightweight post-quantum cryptographic system explicitly tailored to wireless sensor networks with energy constraints, to address the growing security threats posed by quantum computing. The proposed scheme balances strong quantum resistance and resource-efficiency by combining lattice-based primitives with increased optimization of key generation, encryption and decryption. The framework has majorly minimized the computational overhead, energy consumption and latency over traditional PQC implementations and can be effectively used in real-time WSN deployments. Its scalability and adaptability over non-homogeneous sensor nodes is confirmed by mathematical modeling and performance evaluation. Moreover, the suggested design resembles the secure communication without the need to disrupt the operational durability of sensor devices.

References

[1] C.-L. Chen, K.-W. Zeng, W.-Y. Li, C.-F. Lee, L.-C. Liu, and Y.-Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and e-learning," *Engineering Proceedings*, vol. 103, no. 1, Art. no. 14 (2025), doi: 10.3390/engproc2025103014.

[2] M. Kara, K. Karampidis, S. Panagiotakis, M. Hammoudeh, M. Felemban, and G. Papadourakis, "Lightweight and efficient post quantum key encapsulation mechanism based on Q-problem," *Electronics*, vol. 14, no. 4, Art. no. 728 (2025), doi: 10.3390/electronics14040728.

[3] H. P. Nguyen and Y. Chen, "Lightweight, post-quantum secure cryptography based on Ascon: Hardware implementation in automotive applications," *Electronics*, vol. 13, no. 22, Art. no. 4550 (2024), doi: 10.3390/electronics13224550.

[4] L. Zhou, M. Kang, and W. Chen, "Lightweight security transmission in wireless sensor networks through information hiding and data flipping," *Sensors*, vol. 22, no. 3, Art. no. 823 (2022), doi: 10.3390/s22030823.

[5] C. S. Kumar and A. P. Singh, "A blockchain-based auction framework for sustainable waste management: Utilizing non-fungible tokens (NFT) and zero knowledge proofs (ZKPs) for enhanced authentication," *Journal*

of Information and Optimization Sciences, vol. 46, no. 6, pp. 1891–1899 (2025), doi: 10.47974/JIOS-2018.

[6] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices," *Sensors*, vol. 24, no. 12, Art. no. 4008 (2024), doi: 10.3390/s24124008.

[7] C. M. Anish, A. Jadhav, H. N. Datir, G. S. Mate, A. Ashirova, and A. Rawat, "Lightweight AI-supported ECC algorithms for security in IoT and edge devices," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-B, pp. 779–787 (2026), doi: 10.47974/JDMSC-2524.

[8] G. Fitzgibbon and C. Ottaviani, "Constrained device performance benchmarking with the implementation of post-quantum cryptography," *Cryptography*, vol. 8, no. 2, Art. no. 21 (2024), doi: 10.3390/cryptography8020021.

[9] M. U. Mushtaq, H. Venter, A. Singh, and M. Owais, "Advances in energy harvesting for sustainable wireless sensor networks: Challenges and opportunities," *Hardware*, vol. 3, no. 1, Art. no. 1 (2025), doi: 10.3390/hardware3010001.

[10] W. N. Anandpwar, S. M. Barhate, and M. P. Dhore, "Designing an efficient machine learning-based intrusion detection system for enhanced cyber security in modern networks," *International Journal on Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 70–75 (2025), doi: 10.65521/ijacte.v14i1.216.

[11] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[12] T.-G. Sorescu, V.-M. Chiriac, M.-A. Stoica, C.-R. Comsa, I.-G. Soroaga, and A. Contac, "Comparative performance analysis of lightweight cryptographic algorithms on resource-constrained IoT platforms," *Sensors*, vol. 25, no. 18, Art. no. 5887 (2025), doi: 10.3390/s25185887.

Received April, 2026