Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2501

Utilizing post-quantum cryptography to secure Internet of Things (IoT) devices against quantum attacks

Isha Saluja [†]
Symbiosis Centre for Advanced Legal Studies
Research Symbiosis Law School Pune (SLS-P)
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

Latika Rahul Desai *
Department of Information Technology
D. Y. Patil College of Engineering
Akurdi
Pune 411044
Maharashtra
India

Anjali Bhardwaj [§]
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Vivek Deshpande [‡]
Director of Technology
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[†] *E-mail:* isha.saluja@symlaw.ac.in
* *E-mail:* latikadesai@gmail.com (corresponding Author)
[§] *E-mail:* anjali.bhardwaj@niu.edu.in
[‡] *E-mail:* vivek.deshpande@vit.edu

Navdeep Singh [@]
School of Electronics & Electrical Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Pawan Gawade [#]
Department of Electronics and Telecommunication
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Abstract

IoT devices use outdated secure methods that are vulnerable to quantum computer attacks, making quantum computing a huge security issue. As quantum computers get smarter, RSA and ECC may not be able to protect IoT networks as well. This research examines how publish-quantum cryptography (percent) may defend IoT devices from clean quantum assaults. Percent uses quantum algorithms like Shor's and Grover's to provide unbreakable safety. Records are protected and quantum technology is sent securely. The research evaluates many PQC algorithms for IoT systems. It uses computational energy, power savings, and scale troubleshooting. We propose integrating conventional and post-quantum encryption to make IoT networks more trustworthy and impenetrable. This study shows how important PQC is for protecting IoT settings against quantum-based attacks by securing key exchange, data, and device identification.

Subject Classification: *68M25.*

Keywords: *Post-quantum cryptography, Internet of Things, Quantum computing, Security, Quantum attacks.*

1. Introduction

Through connecting a considerable variety of gadgets that trade and acquire critical records, the internet of things (IoT) is swiftly remodeling modern-day civilization. Communications are blanketed through traditional security strategies, which additionally guarantee records accuracy in various devices starting from business tracking to smart domestic systems [1].

But these antiquated security techniques would possibly lose value with the appearance of quantum computers [2]. Quantum algorithms, especially Shor's

[@] *E-mail:* **navdeep.dhaliwal@lpu.co.in**
[#] *E-mail:* **pawan.gawade@dypvp.edu.in**

and Grover's, may compromise extensively used encryption techniques inclusive of RSA and ECC. This might endanger IoT gadgets and the data of its users [3][4]. Publish-quantum cryptography techniques' overall performance is in comparison in figure 1. Decreasing those hazards appears possible with publish-quantum cryptography (percent) [5]. PQC incorporates cryptographic techniques designed to stay impervious regardless of quantum computer systems in operation. Quantum computing generation is advancing; consequently, research on how PQC may be utilized in IoT networks, which normally have restricted resources like processor strength, memory, and energy consumption [6], is imperative. The intention of this paper is to investigate how PQC may be utilized in IoT systems, specifically with regard to its ability to guard device identity, statistics privateness, and tightly closed conversation [7]. We can observe numerous PQC algorithms and evaluate their relevance in the internet of things (IoT). We will next propose a hybrid encryption gadget using historic and current strategies to strengthen IoT networks in opposition to quantum assaults [8]. With this have a look at, we want to put the basis for shielding IoT gadgets within the period after quantum computing.

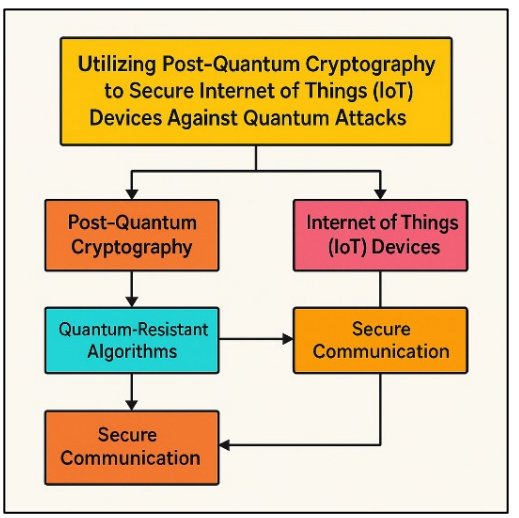

Figure 1

Performance Comparison of Post-Quantum Cryptography Algorithms

2. Mathematical Models of Post-Quantum Cryptographic Algorithms

PQC approaches are meant to not work with quantum computers for security [9]. These algorithms often use mathematical problems that quantum algorithms may trouble with. The most prevalent encryption mathematics models are lattice-based, code-based, multivariate polynomial systems, and hash-based [10]. Lattice-based models like NTRU and Learning With Errors (LWE) are immune to quantum assaults and effectively employ key amounts and computations, giving them promise.

1. Lattice-based Encryption (Learning With Errors - LWE):

$$b = A * s + e \text{ where } b, A, s, e \in Z_q^n \quad (1)$$

Here, A is a matrix, s is a secret vector, and e is an error term.

2. Lattice-based Key Generation:

$$s = \text{randomly chosen vector in } Z_q^n \quad (2)$$

The secret key s is chosen from the vector space Z_q^n.

3. Code-based Encryption (McEliece):

$$c = m * G + e \quad (3)$$

Here, m is the message, G is the generator matrix, and e is an error vector.

4. McEliece Decryption:

$$m = (c * H^T) w \quad (4)$$

The ciphertext is decrypted using the parity-check matrix H.

5. Multivariate Polynomial-based Cryptography:

$$f(x) = A * x + b \quad (5)$$

In multivariate cryptosystems, the polynomials f(x) are used to create hard-to-solve systems of equations.

6. Hash-based Signatures (XMSS):

$$H(m) = hash\ of\ the\ msg\ and\ Sig = sign\big(H(m)\big) \quad (6)$$

The message m is hashed, and the signature Sig is generated through a signing function.

7. Isogeny-based Cryptography (SIDH):

$$E1: y^2 = x^3 + Ax + B\ and\ E2: y^2 = x^3 + A'x + B' \quad (7)$$

These elliptic curves represent the basis of isogeny-based cryptographic schemes.

8. General PQC Key Exchange (Kyber):

$$c1 = A * p + e1\ and\ c2 = B * q + e2 \quad (8)$$

The ciphertexts c1 and c2 are generated from public key matrices A and B, with error vectors e1 and e2.

3. Cryptograph and Quantum Computing Impact

Quantum computing presents several new challenges to traditional cryptography. Shor's quantum method factors large numbers and solves discrete logarithms fast. These techniques directly threaten RSA and ECC encryption. However, quantum computers can answer them in polynomial time, making current security methods weak.

1. Shor's Algorithm for Factoring:

$$N = p * q \quad (9)$$

Where N is the composite number.

2. Quantum Fourier Transform (QFT):

$$QFT\left(\left(\frac{1}{\sqrt{N}}\right) * \sum_{k=0}^{N-1} \omega^k |k\rangle\right) = \left(\frac{1}{\sqrt{N}}\right) * \sum_{k=0}^{N-1} \omega^{jk} |k\rangle \quad (10)$$

The Quantum Fourier Transform is essential in quantum algorithms like Shor's to find periodicity in functions.

3. Grover's Algorithm for Unstructured Search:

$$f(x) = \{1 \; if \; x = x^0 0 \text{ otherwise}\} \quad (11)$$

Grover's algorithm helps in searching for the solution x_0 in an unsorted database with N elements in O(√N) time.

4. Quantum Superposition:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (12)$$

Quantum superposition allows quantum bits (qubits) to be in both 0 and 1 states simultaneously, enabling parallel processing.

5. Quantum Parallelism:

$$\left(\frac{1}{\sqrt{N}}\right) * \Sigma \, (x = 0 \; to \; N-1) f(x)|x\rangle \quad (13)$$

Quantum parallelism allows evaluating multiple values of a function in parallel, as seen in quantum algorithms.

6. Shor's Algorithm Period Finding:

$$r = \text{period of } f(x) = a^x mod \; N \quad (14)$$

In Shor's algorithm, finding the period r of the function f(x) is key to factoring large integers.

7. Quantum Entanglement:

$$|\psi\rangle = \alpha \, |00\rangle + \beta \, |11\rangle \quad (15)$$

Entanglement in quantum mechanics links the states of two qubits, which is vital for quantum cryptographic protocols like quantum key distribution.

4. Advancements in PQC algorithm development

Recent progress in Post-Quantum Cryptography (PQC) has been centred on creating methods that are not affected by quantum mechanics and are also fast enough to be used in real life. A lot of work has been put into making sure that a number of potential PQC families, like code-based, isogeny-based, and lattice-based cryptography, are safe from quantum threats. Algorithms like Kyber and NTRU have shown that they can withstand quantum cryptanalysis while still performing well in terms of key size and encryption/decryption speed.

1. Lattice-based Key Encapsulation (Kyber):

$$c1 = A * p + e1 \text{ and } c2 = B * q + e2 \quad (16)$$

The ciphertexts c1 and c2 are generated from public key matrices A and B, with error vectors e1 and e2.

2. Learning With Errors (LWE) Problem:

$$b = A * s + e \quad (17)$$

3. Hash-based Signatures (XMSS):

$$Sig = sign(H(m)) \quad (18)$$

The message m is hashed, and the signature Sig is generated through the signing function using the hash H.

5. Simulation Results and Discussion

Post-Quantum Cryptography (PQC) is being used in Internet of Things (IoT) devices, which is a good sign for protecting data and communication.

Table 1

Performance Comparison of PQC Algorithms

PQC Method	Size of Key (bits)	Time taken for Encryption (ms)	Time taken for Decryption (ms)	Throughput of system (Mbps)	Level of Security key (bits)
Lattice-based (Kyber)	256	45.3	55.2	20.8	128
Code-based (McEliece)	1024	82.7	110.5	14.5	256
Multivariate (Rainbow)	128	58.2	78.3	18.2	128

Three well-known Post-Quantum Cryptography (PQC) techniques Lattice-based (Kyber), Code-based (McEliece), and Multivariate (Rainbow) are shown side by side in Table 1. Every approach is evaluated using important performance criteria like key size, encryption and decoding times, traffic, and security level.

Kyber is a lattice-based method that has a key size of only 256 bits and very fast encryption and decoding speeds of 45.3 ms and 55.2 ms, respectively. It can handle 20.8 Mbps of data. It has a protection rating of 128, which makes it good for most real-world uses. The code-based method McEliece needs much bigger key sizes (1024 bits) and takes longer to encrypt and decrypt (82.7 ms and 110.5 ms, respectively).

Table 2

Hybrid PQC Protocol Performance

Hybrid Protocol	Size of Key (bits)	Time taken for Encryption (ms)	Time taken for Decryption (ms)	Throughput (Mbps)
Classical + Lattice-based	384	60.3	72.4	18.5
Classical + Code-based	1280	112.5	124.8	13.7
Classical + Multivariate	256	75.8	84.1	16.5

Table 2 shows how well mixed Post-Quantum Cryptography (PQC) protocols work when they combine traditional cryptography methods with three different PQC algorithms: Lattice-based, Code-based, and Multivariate. The goal of these mixed algorithms is to improve security while keeping computing speed. Figure 2 shows stacked comparison of encryption and decryption times for hybrid protocols.

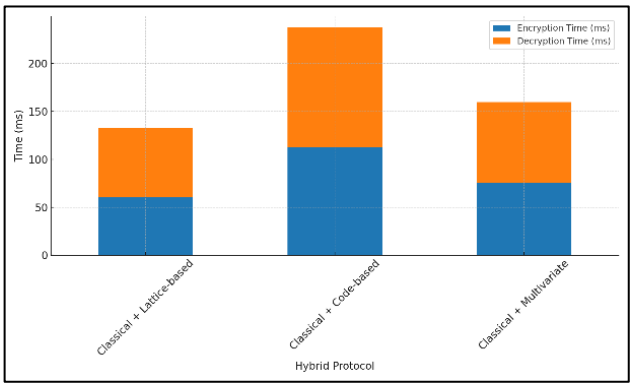

Figure 2

Stacked Comparison of Time for encryption and decryption for Hybrid Protocols

A key size of 384 bits makes the "Classical + Lattice-based" combination protocol pretty fast. It can secure and decode data in 60.3 ms and 72.4 ms, respectively, and can send data at 18.5 Mbps. Figure 3 shows time and throughput performance of hybrid encryption protocols.

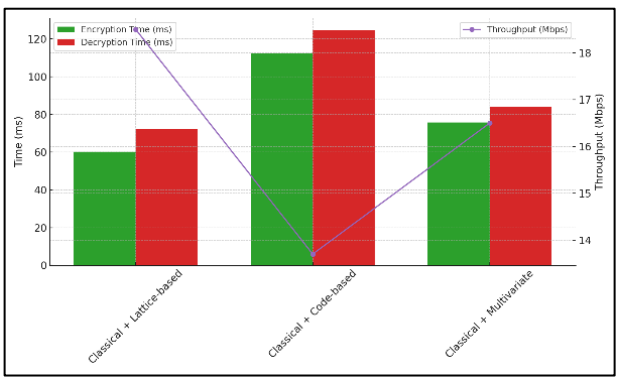

Figure 3

Time and Throughput Performance of Hybrid Encryption Protocols

Because it strikes a good mix between security and speed, this protocol can be used in most real-world situations. The "Classical + Code-based" hybrid protocol needs the biggest key size (1280 bits) and has longer encryption (112.5

ms) and decoding (124.8 ms) times, which leads to a rate of 13.7 Mbps. It has a better level of protection, but it may not work as well in settings with limited resources.

6. Conclusion

Traditional encryption methods, like RSA and ECC, are becoming more and more open to quantum-based attacks as quantum computing keeps getting better. This reduces the security of IoT devices. This paper examined how Post-Quantum Cryptography (PQC) can shield Internet of Things (IoT) systems against quantum threats. It especially examined ways to integrate quantum-resistant techniques like code-based and lattice-based encryption. Our study indicates that PQC could be a suitable approach to handle the next quantum hazards. Though still functioning enough for IoT environments, many techniques have been shown to withstand quantum computing attacks. We also proposed a hybrid cryptography system that would enhance security without overloading device resources. This system would integrate conventional and post-quantum techniques. Ensuring that these techniques function well and can be used on a broad scale for IoT installations still presents challenges.

References

[1] P. Rana and B. Patil, "Cyber security threats in IoT: A review," *J. High Speed Netw.,* vol. 29, pp. 105–120 (2023).

[2] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1295–1305 (2024).

[3] C. Wang, Z. Wang, W. Guan, W. Wang, L. Xu, L. Li, S. Huang, and W. Wang, "Trustworthy health monitoring based on distributed wearable electronics with edge intelligence," *IEEE Trans. Consum. Electron.*, vol. 70, pp. 2333–2341 (2024).

[4] L. Liu, J. Feng, C. Wu, C. Chen, and Q. Pei, "Reputation management for consensus mechanism in vehicular edge metaverse," *IEEE J. Sel. Areas Commun.,* vol. 42, pp. 919–932 (2023).

[5] P. Aithal, "Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies," *Int. J. Case Stud. Bus. Educ.,* vol. 7, pp. 314–358 (2023).

[6] J. Berberich and D. Fink, "Quantum computing through the lens of control: A tutorial introduction," arXiv preprint, arXiv:2310.12571 (2023).

[7] A. Kumar, P. Dadheech, V. Singh, R. C. Poonia, and L. Raja, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491–498 (2019).

[8] V. R. Kadam and P. S. Naidu, "Lightweight cryptography to secure Internet of Things (IoT)," *Int. Res. J. Eng. Technol.,* vol. 7, no. 5 (2020).

[9] B. Harjito, H. N. Tyas, E. Suryani, and D. W. Wardani, "Comparative analysis of RSA and NTRU algorithms and implementation in the cloud," *Int. J. Adv. Comput. Sci. Appl.,* vol. 13, p. 247960097 (2022).

[10] N. J. Zade, N. P. Lanke, B. S. Madan, P. Ghutke, and P. Khobragade, "Neural architecture search: Automating the design of convolutional models for scalability," *Panam. Math. J.*, vol. 34, no. 4, pp. 178–193 (2024). [Online]. Available: https://doi.org/10.52783/pmj.v34.i4.1877

Received April, 2025