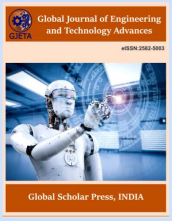
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(RESEARCH ARTICLE)

Check for updates

LIGHTWEIGHT POST-QUANTUM CRYPTOGRAPHY FOR SECURE IOT COMMUNICATION

Arjun Nichal, Payal Kumbhar *, Kshitija Mohite and Akshada Khandekar

Department of Electronics and Telecommunication Engineering, Adarsh Institute of Technology and Research center Vita, Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra, India.
* Corresponding Author

ORCID Details
Arjun Nichal: https://orcid.org/0000-0002-5014-266X
Payal Kumbhar: https://orcid.org/0009-0003-9691-9694
Kshitija Mohite: https://orcid.org/0009-0009-4013-9713
Akshada Khandekar: https://orcid.org/0009-0000-1774-117X

Global Journal of Engineering and Technology Advances, 2026, 29(02), 051–058

Publication history: Received on 29 September 2026; revised on 07 November 2026; accepted on 09 November 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.29.2.0324

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The rapid growth of Internet of Things (IoT) devices has increased the requirement for secure and efficient communication between resource-constrained devices. Conventional cryptographic algorithms provide effective security against existing computational threats; however, the development of large-scale quantum computers may threaten widely used public-key cryptographic techniques. Post-Quantum Cryptography (PQC) provides cryptographic mechanisms designed to remain secure against attacks from both classical and quantum computers.

In this paper we propose a lightweight post-quantum cryptographic solution for the safe communication of IoT, taking into account the low computational power, memory and energy availability of IoT devices. The proposed approach focuses on the selection and evaluation of a suitable lightweight PQC mechanism for IoT environments and analysis of important parameters such as execution time, memory consumption, communication overhead and security considerations. The proposed approach can be evaluated in a prototype-based experimental framework under constrained-device conditions.

The study looks at how post-quantum security can be incorporated into IoT communications, bearing in mind the real world constraints of embedded systems.

Paper proposes a lightweight post-quantum cryptographic solution for secure IoT communication with a specific focus on the constraints of IoT devices in terms of computational power, memory and energy. The paper looks at the selection and evaluation of a suitable lightweight PQC scheme for the IoT context and considers a range of parameters in the analysis including execution time, memory usage, communication overhead and security. A prototype based experimental framework can be used to evaluate the proposed approach under the constraints of a constrained device. The paper shows how post-quantum security can be brought to IoT communication in a practical manner taking into account the realities of the embedded system.

Keywords: Internet of Things, Post-Quantum Cryptography, Lightweight Cryptography, IoT Security, Embedded Systems, Secure Communication, Quantum Computing.

1 INTRODUCTION

The Internet of Things is now an integral part of modern communications systems. IoT refers to the interconnection of sensors, embedded controllers, smart appliances, industrial equipment, healthcare systems and a myriad of other physical devices to a communications network. These devices are constantly exchanging sensitive information over wired and wireless networks.

Security is one of the key issues in IoT systems. The IoT devices themselves are generally very resource constrained in terms of processing power, memory, storage and battery. Security mechanisms which are designed for high performance computers are therefore not always directly transferable to the IoT devices.

The vast majority of existing secure communication systems are based on public key crypto techniques (RSA, ECC etc). These are very secure against the known classical attacks. The problem is that a sufficiently powerful quantum computer could use a quantum algorithm (Shor's algorithm) to solve the mathematical problems that underpin a number of the public key cryptosystems that are currently in use.

Post quantum cryptography is all about developing cryptographic algorithms which are capable of withstanding attack from both classical and quantum computers. As such the move to PQC is becoming an important area of research for future secure communication systems.

This work looks at a lightweight approach to the integration of post-quantum cryptography into IoT communication. The primary aim is to examine the trade-off between security and resource consumption. The framework under consideration takes into account computational time, memory usage, communication overhead and suitability for the constrained nature of the IoT devices.

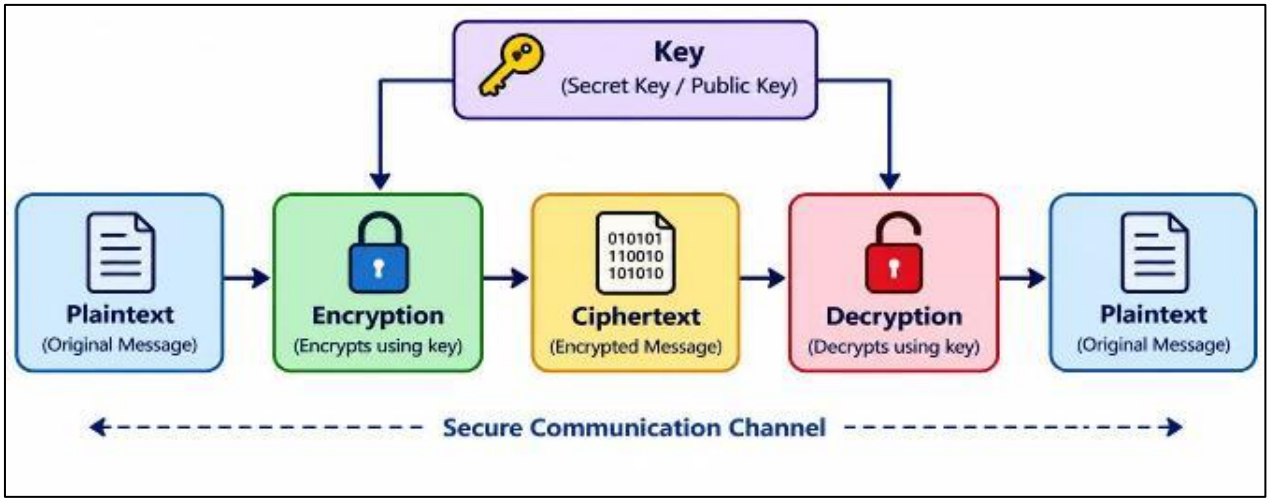


Figure 1: Block diagram of Lightweight Post-Quantum Cryptography for secure IoT Communication

2 RELATED WORK

A number of research papers have looked at the security requirements of IoT systems and the extent to which post-quantum crypto can be applied in the constrained environments that are typical of such systems.

Traditional public key algorithms (RSA, ECC etc) have been used extensively for authentication, key establishment and secure communication. Their long term security against quantum attack is the big issue.

Post quantum crypto covers a number of different mathematical approaches: lattice based, code based, hash based, multivariate and isogeny based. Of these, lattice based has been the most widely researched given its security properties and the fact that it's well suited to the kind of protocols we're used to.

The NIST have gone through a standardisation process for post-quantum cryptographic algorithms and have now selected algorithms for key establishment and for digital signatures.

However the direct implementation of PQC algorithms on the kind of constrained IoT devices we're talking about is likely to add a significant amount of computational and communication overhead. That's why lightweight implementation and parameter selection are so important for any real world IoT deployment.

2.1 Problem statement

IoT devices need to communicate securely whilst operating under very constrained computational, memory and energy resources. Traditional public key cryptography is not going to provide sufficient long term security against quantum attacks.

At the same time, replacing the existing cryptographic primitives with PQC algorithms will result in increased computation time, memory requirements, key sizes and communication overhead.

Therefore, the problem addressed in this work is:

To look at a lightweight post-quantum crypto approach that offers improved resistance to quantum attacks and at the same time has acceptable resource requirements for use in the constrained environment of IoT communications.

The sheer number of IoT devices has created a whole host of security issues in the area of data communication. The traditional cryptographic methods we have today are going to be at risk in the future with the advent of quantum computing. On top of that, the IoT devices themselves are typically very resource constrained in terms of processing power, memory and energy so you're not going to be able to run the very computationally intensive cryptographic algorithms that we're used to.

Hence there is a requirement for a lightweight post-quantum cryptographic solution that can deliver secure communication with minimal computational complexity and resource overhead. The approach proposed involves the combination of post-quantum key establishment with efficient data encryption to secure the sensitive IoT data as it is transmitted.

The fundamental issue is one of balancing security with computational efficiency, memory usage and communication overhead. The proposed framework is therefore designed to look at the viability of lightweight post-quantum crypto for secure IoT communication.

The aim is to build a secure and resource efficient communication framework for the IoT environment, taking into account the potential threat from quantum computing.

2.2 Objectives

The main objectives of the proposed work are:

- To study the security requirements of IoT communications.
- To assess the limitations of conventional public key crypto in the post quantum world.
- To look at a viable PQC mechanism for the constrained IoT devices.
- To design a secure IoT communication framework using the chosen PQC mechanism.
- To measure computational time, memory usage and communication overhead.

2.3 PROPOSED METHODOLOGY

The approach proposed is to secure the IoT communications using lightweight post-quantum cryptographic schemes. The primary aim is to provide confidentiality, authentication and data integrity with minimal computational complexity, memory and communication overhead.

2.3.1 System Initialization

The IoT devices and the receiving system are initially set up with the required comms parameters. The system will then identify the communicating devices and set up the requisite crypto components. The use of lightweight algorithms is intended to reduce resource consumption and enable efficient operation on devices with constrained processing power.

2.3.2 Key Generation and Establishment

A post-quantum crypto algorithm is used to establish a shared secret between the two communicating devices. The key establishment is designed to be resistant to attack from both classical and quantum computers. The shared secret that is established is then used to derive the symmetric encryption keys that will be used to protect the data that is transmitted. Good key management is of course essential to prevent unauthorised access.

2.3.3 Device Authentication

Authentication ensures that the communication is between the right devices. The communicating parties will authenticate the relevant keys or credentials before any sensitive information is exchanged. This reduces the risk of an attack via unauthorised access or impersonation. The authentication mechanisms that are selected will be appropriate to the security requirements and the computational constraints of the IoT environment.

2.3.4 Data Encryption

Once the shared secret has been established the IoT device will use a symmetric encryption algorithm to encrypt the original data. Lightweight encryption is used to reduce processing time and compute requirements whilst still providing data confidentiality. The data is encrypted so that it becomes ciphertext which is effectively unreadable to anyone who doesn't have the key. Of course proper nonce management and secure key handling are also important for security.

2.3.5 Secure Data Transmission

The encrypted data is sent via the IoT communication channel to the receiving device. As the data is encrypted the message itself won't be revealed if it's intercepted. The communication mechanism should be such as to minimise the amount of data that is transmitted in order to keep the bandwidth usage and communication overhead to a minimum.

2.3.6 Data Decryption and Integrity Verification

At the receiving end the device uses the appropriate cryptographic key to decrypt the ciphertext and recover the original information. Prior to accepting the received message the receiver will perform the appropriate verification to check both its integrity and authenticity. If the verification fails the message is rejected. This is of course a way of protecting the system against message modification and a number of other forms of attack on the communication.

2.3.7 Overall Security

The proposed approach is to use post-quantum key establishment combined with symmetric encryption and appropriate authentication and integrity mechanisms.

Flow chart

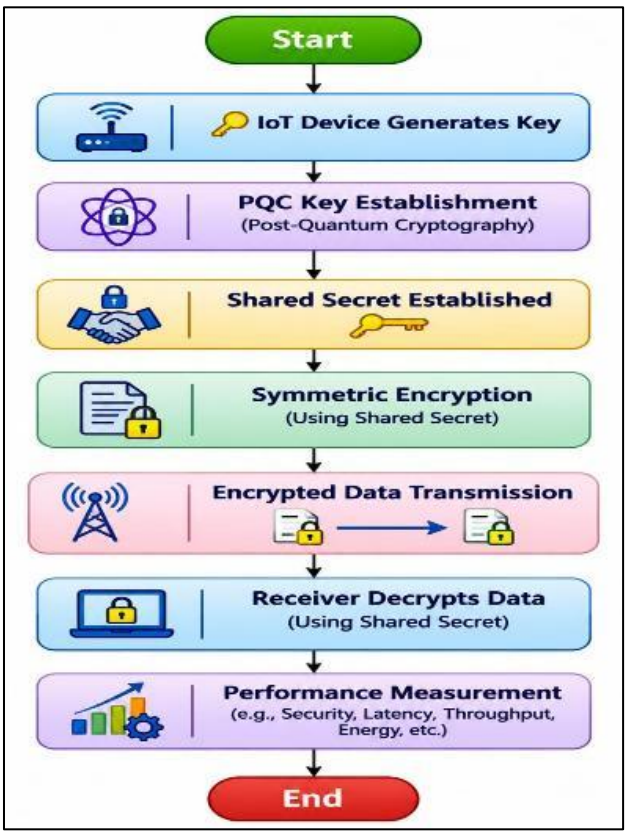


Figure 1: Flowchart of the proposed PQC-based secure IoT communication.

2.4 System architecture

The system architecture shows the full flow of a lightweight post-quantum cryptography (PQC) based secure IoT communication. It comprises six distinct stages: data collection, encryption at the source, transmission, decryption at the receiver, gateway/server processing and output.

2.4.1 Data Collection

IoT sensors are used to collect environmental data (temperature, humidity, gas levels etc). The data is then passed to the security layer.

2.4.2 Encryption at Source

The PQC security layer is responsible for key generation and key encapsulation to establish a shared secret. That secret is then used to derive the encryption key which is used to protect the IoT data prior to transmission.

2.4.3 Transmission

The data is sent over a communication channel (Wi-Fi, LoRa, 4G, 5G etc) and encryption is used to ensure the confidentiality of the data in transit.

2.4.4 Decryption at Receiver

The receiver carries out key decapsulation to derive the shared secret and hence the required decryption key. The received data is then decrypted and verified prior to any further processing.

2.4.5 Gateway/Server

The gateway/server takes the data that's been received, does the appropriate authentication checks and then stores that information for later use.

2.4.6 Output

The data is processed and presented via an application which provides monitoring, analytics and a UI.

Conclusion: The architecture incorporates post-quantum key establishment, data encryption, secure transmission and receiver side verification to enable secure IoT communication taking into account the resource constraints of the IoT devices.

2.5 IMPLEMENTATION FRAMEWORK

The system could be implemented on a constrained embedded platform or in a simulated IoT environment.

A suitable experimental setup may contain:

- IoT/embedded device
- Sensor module
- Microcontroller or single-board computer
- Communication interface
- Gateway/server
- PQC software library
- Performance-monitoring software

For the initial software based prototype the PQC mechanism can be implemented and tested on a PC or single board computing platform. It can then be ported to the resource constrained embedded platform.

The experiment is to record the execution time and resource requirements of the selected crypto ops.

2.6 Working of the Implementation Framework :

The implementation framework is a set of interlocking components which allow secure communication from the IoT device to the receiving server. The sensor module will be gathering data from the environment, the microcontroller will be processing that data and the PQC software library will be doing the required crypto operations to enable the secure communication and protect the data.

The encrypted data is sent via a communications interface (e.g. Wi-Fi, LoRa, cellular) to the gateway or server. It is then processed and validated at the receiving end prior to being passed on to the relevant application. Appropriate authentication and integrity mechanisms are in place to protect the communication against unauthorised access and data tampering.

2.7 Performance Evaluation

The performance monitoring software assesses the efficiency of the proposed framework in terms of execution time, memory usage, ciphertext size and communication overhead. This enables an evaluation of the framework's computational demands and its suitability for deployment on resource constrained IoT devices.

The feedback from the performance measurements can be used to identify potential areas for improvement in the cryptographic processing and in the use of resources. Experimental testing is of course required to confirm the performance and efficacy of the proposed approach.

2.8 Experimental parameters

The following parameters should be measured during experimentation:

Table 1: Parameters to be measured

Parameter	Measurement
Key generation time	Time required to generate key pair
Encapsulation time	Time required to establish shared secret
Decapsulation time	Time required to recover shared secret
Memory usage	RAM/ROM requirement
Ciphertext size	Size of transmitted cryptographic data
Communication overhead	Additional bytes introduced by security

3 RESULTS AND DISCUSSION

The benchmark results show that ML-KEM-512 can do key generation, key encapsulation and key decapsulation with fairly reasonable execution times. The public key and ciphertext sizes will have a bearing on the communication overhead in an IoT scenario. Those are the sorts of parameters you'd want to be aware of when assessing the practicality of PQC for IoT. The actual performance will of course be platform and implementation dependent.

Table 2: Reference Benchmark Result for ML-KEM-512

Parameter	Measurement
Key generation time	6.49 ms
Encapsulation time	4.61 ms
Decapsulation time	4.49 ms
Memory usage	800 bytes
Public key size	1632 bytes
Ciphertext size	768 bytes
Data processing size	32 bytes

3.1 Security analysis

The security analysis looks at the potential of the proposed lightweight PQC-based framework to secure IoT communications against a range of security threats. The framework is designed to provide improved security through the use of secure key establishment, data encryption and appropriate verification.

3.1.1 Data Confidentiality

The IoT data is encrypted prior to transmission to prevent unauthorised users from being able to access the sensitive information. Only a receiver with the correct cryptographic key can decrypt the data.

3.1.2 Quantum Resistance

Post quantum cryptographic algorithms are designed to be secure against both classical and quantum computers. Their use will help to mitigate future threats to the security of IoT communications.

3.1.3 Authentication

Authentication is all about verifying the identity of the devices that are communicating before any sensitive data is exchanged. It's a way of ensuring that an unauthorised device doesn't get access to the system.

3.1.4 Data Integrity

Integrity checking is used to detect any unauthorised modification of the message that has been transmitted. The receiver will check the integrity of the received data prior to accepting and processing it.

3.1.5 Key Security

Secure key establishment and proper key management go a long way to protect the cryptographic keys from being accessed by an unauthorised party. The shared secret can then be used to derive a symmetric key for use in data encryption.

3.1.6 Replay Attack Protection

An attacker may attempt to retransmit previously captured messages. Nonces, sequence numbers or timestamps can be used to identify retransmissions and thus improve the security of the communication.

3.1.7 Man-in-the-Middle Attack

An attacker could potentially intercept or alter the communications between the IoT devices. The risk of this can be reduced through the use of proper authentication, secure key establishment and integrity checks.

3.1.8 Resource Efficiency

IoT devices have very limited processing power, memory and energy. The cryptographic techniques selected therefore need to be evaluated in terms of execution time, memory usage and communication overhead.

3.2 Overall Security Assessment

The proposed framework is a combination of post-quantum key establishment with symmetric encryption and appropriate authentication and integrity mechanisms. The aim is to protect the IoT data from unauthorised access, eavesdropping and tampering, all while taking into account the resource constraints of the IoT devices. Actual implementation and testing would be required to confirm the security and performance of the framework.

3.3 Advantages

The proposed approach provides the following potential advantages:

- Enhanced security: provides improved security for IoT communication via the combination of post-quantum crypto with appropriate encryption.
- Quantum Resistance: uses post-quantum cryptographic techniques which are designed to be resistant to attack by a future quantum computer.
- Data Confidentiality: encrypts the sensitive IoT data before it's transmitted so that an attacker can't get at the original data.
- Secure key establishment: helps the communicating devices to establish a shared secret which can then be used to derive the encryption keys.
- Authentication support: appropriate authentication mechanisms to verify device identity and prevent unauthorised access.
- Data Integrity: Integrity checking is used to detect any unauthorised modification to the information that's being transmitted.
- Resource efficiency: lightweight crypto techniques can help to reduce the computational complexity and memory requirements on the resource constrained IoT devices.

4 CONCLUSION

This paper describes a lightweight post-quantum cryptographic scheme for the secure communication of data in the context of IoT devices. With the ever increasing number of IoT devices being deployed and the looming threat of quantum computing, there is a clear need to have secure communication in place for the post-quantum world.

The proposed framework is all about integrating a suitable PQC mechanism into an IoT communication system, taking into account the computational requirements, memory usage and communication overhead. Rather than having a computationally expensive public key operation on every packet, it would be possible to use a PQC key establishment followed by symmetric encryption for the actual data.

Experimental evaluation using actual implementation measurements will provide a quantitative assessment of the proposed approach. The work forms the basis for further research into practical and resource efficient post-quantum security for IoT systems.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The authors would like to express their sincere gratitude to their project guide for providing valuable guidance, suggestions, and continuous support throughout this research work. We are also thankful to our faculty members and institution for providing the necessary encouragement and resources to complete this paper.

Disclosure of conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this research paper. No financial or personal relationship have influenced the work presented in this paper.

REFERENCES

[1] National Institute of Standards and Technology .Post-Quantum Cryptography.” NIST.

[2] National Institute of Standards and Technology. “Module-Lattice-Based Key-Encapsulation Mechanism Standard.” NIST.

[3] National Institute of Standards and Technology. “Digital Signature Schemes Based on Structured Lattices.” NIST.

[4] Stallings W. Cryptography and Network Security: Principles and Practice. Pearson.

[5] Tanenbaum AS. and Wetherall DJ. Computer Networks. Pearson.

[6] Akyildiz IF. Sankarasubramaniam WY, and Cayirci E. “Wireless Sensor Networks: A Survey.” Computer Networks. vol. 38, no. 4. pp. 393–422.