Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11, November 2025

Implementation of Kyber-Based Post-Quantum Cryptographic Communication using Raspberry Pi

Dr. Aravinda H L
Associate Professor
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology Bengaluru, India

Dr. Vidya Honguntikar
Professor
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology, Bengaluru, India

Chetan R
Student
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology, Bengaluru, India

Ibrahim S
Student
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology, Bengaluru, India

Mayur K N
Student
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology, Bengaluru, India

Sagar B S
Student
Electronics and Telecommunication Engineering, Dr. Ambedkar Institute Of Technology, Bengaluru, India

***Abstract*—Secure communication is becoming increasingly challenging as computational power grows, cyberattacks evolve, and traditional cryptographic methods show their limitations. Widely used public-key algorithms like RSA and ECC, which have protected digital communication for decades, are now vulnerable in the face of advancing quantum computing. Quantum algorithms such as Shor's algorithm can break these classical systems, posing a serious threat to data that needs long-term protection. This growing risk has led to the development of post-quantum cryptography, a new generation of algorithms designed to remain secure against both classical and quantum attacks. Among the different approaches, lattice-based cryptography stands out due to its strong security foundations and efficient performance. In this work, we implement a post-quantum cryptographic method using the CRYSTALS-Kyber algorithm on Raspberry Pi devices. By using two Raspberry Pi modules to securely exchange keys and perform text encryption and decryption, the project demonstrates that quantum-resistant communication can be achieved even on low-cost embedded hardware.**

Keywords— CRYSTALS-Kyber, Post-Quantum Cryptography, Lattice-Based Cryptography, Key Encapsulation Mechanism (KEM), Raspberry Pi, Secure Communication, TCP/IP Transmission, Embedded Cryptographic Implementation..

I. INTRODUCTION

Post-quantum cryptography has become an important research focus as quantum computing continues to advance and threaten the security of traditional cryptographic systems. Classical public-key algorithms like RSA and elliptic curve cryptography depend on mathematical problems that are extremely difficult for today's computers to solve. However, quantum algorithms such as Shor's algorithm can solve these problems quickly, putting the confidentiality and integrity of secure communication at risk. This growing concern has created a strong need for cryptographic methods that can remain secure against both classical and quantum attacks. Post-quantum cryptography addresses this challenge by introducing new sets of algorithms built on mathematical problems believed to be resistant to quantum computers, ensuring long-term protection for key exchange and data transmission.

Among the different categories of post-quantum algorithms, lattice-based cryptography has gained particular attention because of its strong security and practical efficiency. These schemes rely on difficult mathematical problems like Learning With Errors, Ring-LWE, and Module-LWE, for which no efficient classical or quantum solutions are currently known. They offer a high level of security while maintaining good performance, making them suitable for systems that need quick computation or operate with limited resources. Lattice-based cryptography also provides advantages such as relatively compact key sizes, reduced computational overhead, and strong resistance to chosen-ciphertext attacks, making it one of the leading options for future deployment on a large scale.

Within this family of algorithms, the CRYSTALS-Kyber key encapsulation mechanism stands out due to its reliability and efficiency. Kyber was selected by NIST for standardization because it offers a strong balance of security, simplicity, and performance compared to many other post-quantum candidates. It enables secure key exchange by using structured lattice problems to generate shared secrets that remain protected even against quantum-enabled attackers. Its efficient design makes it well suited for embedded systems, communication protocols, IoT devices, and modern networks that require long-term security.

The main objective of this project is to implement a Kyber-based post-quantum key exchange system using Raspberry Pi devices. Two Raspberry Pi 3B+ boards are used—one to perform encryption and the other to carry out decryption—forming a complete secure communication setup. The implementation is done in Python, providing a flexible and accessible platform for testing the algorithm. Through this setup, the project demonstrates that quantum-resistant

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11, November 2025

cryptography can be successfully deployed on simple and affordable embedded hardware, emphasizing its importance for future secure communication systems.

II. PROPOSED SYSTEM

The proposed system implements a post-quantum secure communication model using the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) on Raspberry Pi hardware. The methodology is divided into four major components: system configuration, software environment preparation, communication architecture design, and cryptographic workflow implementation.

A. HARDWARE AND SYSTEM CONFIGURATION

Two Raspberry Pi devices were used to represent the client and server in a secure communication setup. Both devices were configured with Raspberry Pi OS, updated system packages, and connected to the same local Wi-Fi network to enable TCP/IP communication. The Raspberry Pi platform was selected due to its affordability, portability, and suitability for evaluating cryptographic performance under constrained hardware environments. The hardware configuration ensures that the system operates in a realistic environment similar to IoT and edge-computing deployments.

B. SOFTWARE ENVIRONMENT AND LIBRARY SETUP

A dedicated Python virtual environment was created on each Raspberry Pi to isolate dependencies and ensure consistent execution. The Open Quantum Safe (OQS) liboqs-python library was installed to enable CRYSTALS-Kyber operations, including key generation, encapsulation, and decapsulation. Supporting tools such as GCC, CMake, and OpenSSL were also installed to compile and run the necessary cryptographic modules. The software stack used in this implementation consists of Python 3.x, liboqs bindings, required system packages, and the application-level client and server modules.

C. CLIENT-SERVER COMMUNICATION ARCHITECTURE

A TCP socket-based communication model was designed to simulate secure data exchange between two endpoints. The server initializes the communication channel by opening a listening socket on a predefined port. The client connects to the server using its IP address. This TCP architecture ensures reliable, ordered, and loss-free delivery of data such as public keys, ciphertext, and encrypted messages. The communication model allows the Kyber KEM protocol to operate seamlessly on top of the classical network transport layer.

D. CRYSTALS-KYBER ENCAPSULATION WORKFLOW

1) Kyber Mathematical Formulation

$$t = A \cdot s + e \quad (1)$$

$$u = A^T \cdot r + e_1 \quad (2)$$

$$v = t^T \cdot r + e_2 + \text{Encode}(K) \quad (3)$$

$$K' = \text{Decode}(v - u^T s) \quad (4)$$

The Kyber KEM mechanism is based on lattice-based polynomial operations. Equation (1) represents the key generation step, where the server samples a secret vector s and noise vector e to compute the public key component t. During encapsulation, the client generates randomness r and noise terms e_1 and e_2, and computes ciphertext components u and v as shown in Equations (2) and (3). Finally, the server computes the shared secret using Equation (4). Since the shared secret is never transmitted over the network, the system ensures post-quantum secure key exchange.

E. SECURE MESSAGE ENCRYPTION AND DECRYPTION

Once the shared secret is derived independently by both devices, it is used as a symmetric session key for secure message transmission. The client encrypts the plaintext message using the Kyber-derived shared secret, ensuring that the message cannot be understood even if intercepted. The encrypted ciphertext is transmitted over the TCP socket to the server. Upon receiving it, the server applies the same shared secret to decrypt the data and recover the original message. This process confirms the correctness of the key establishment phase and demonstrates secure end-to-end communication between the Raspberry Pi devices.

F. SECURITY WORKFLOW AND KEY MANAGEMENT

The system implements a strict key management workflow to maintain the integrity of post-quantum communication. The server's private key remains stored locally and is never transmitted. During each communication cycle, the client performs encapsulation and generates a unique session key, while the server performs decapsulation to derive the identical shared secret. Since the symmetric key is never transmitted across the network, the system effectively prevents interception and man-in-the-middle attacks. The transient nature of session keys ensures forward secrecy, making the system resilient against both classical and quantum adversaries.

G. LIMITATIONS AND CONSIDERATIONS

While the Kyber KEM is efficient, its performance on Raspberry Pi hardware may be affected by CPU load, memory constraints, and network latency. Wireless LAN may introduce unpredictable delays during ciphertext transmission. Python's high-level encryption routines do not allow explicit memory wiping of secret keys, which can be a consideration in security-critical deployments. Further optimizations such as key rotation, hardened memory handling, and support for hybrid cryptographic mechanisms may be required for large-scale or commercial systems.

III. RESULTS AND DISCUSSION

The system was tested using two Raspberry Pi devices functioning as the client and server. The server generated a Kyber768 keypair and listened on port 5000, while the client connected using the assigned IP address. Both devices executed the Kyber key establishment, ciphertext exchange, and message encryption workflow successfully.

A. SUCCESSFUL SHARED SECRET ESTABLISHMENT

The client performed encapsulation and transmitted the ciphertext to the server. The server applied decapsulation using

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11, November 2025

its private key. Both sides produced an identical shared secret, confirming correct implementation of the Kyber KEM.

B. MESSAGE ENCRYPTION AND DECRYPTION

The client encrypted the message "post quantum cryptography" using the derived session key. The server decrypted the message correctly, proving that the symmetric encryption process works reliably with the Kyber-generated shared secret.

C. EXECUTION OUTPUT

Client Terminal Output:

1. "Connecting to 192.168.x.x port 5000"
2. "Sent encapsulation ciphertext; shared secret established locally"
3. "Encrypted message sent; done."

Server Terminal Output:

1. "Keypair generated; listening on port 5000"
2. "Shared secret established (kept secret)"
3. "Decrypted message: post quantum cryptography"

These results validate the feasibility of deploying PQC mechanisms such as Kyber on resource-constrained embedded hardware.

D. EXECUTION FLOW VALIDATION

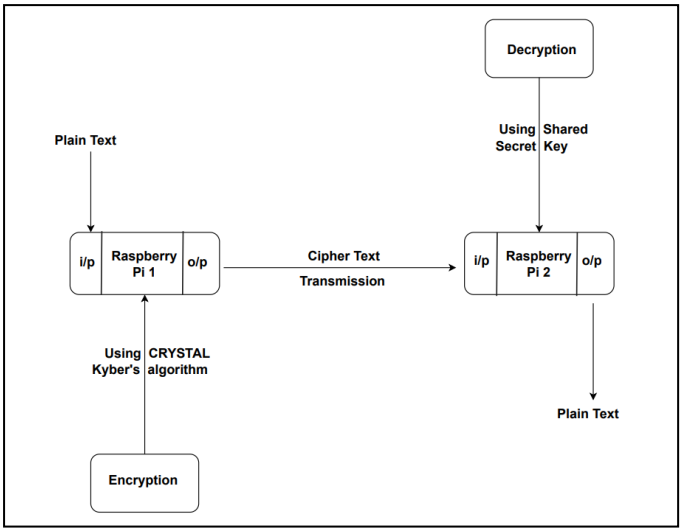

Fig. 1. End-to-end execution workflow of the implemented Kyber-based secure communication system, showing plaintext encryption on Raspberry Pi 1, ciphertext transmission over TCP/IP, and Kyber-derived symmetric decryption on Raspberry Pi 2.

The block diagram represents the operational behavior of the system during real-time execution. Raspberry Pi 1 receives plaintext input and performs CRYSTALS-Kyber encapsulation to generate a session-specific shared secret. This shared secret is then used as a symmetric key to encrypt the plaintext, producing ciphertext that is transmitted to Raspberry Pi 2 through a TCP/IP socket. Upon receiving the ciphertext, Raspberry Pi 2 executes Kyber decapsulation to reconstruct the identical shared secret locally, after which the encrypted data is decrypted to recover the original plaintext. The successful reproduction of the shared secret on both devices and the accurate recovery of the plaintext confirm the correctness, reliability, and post-quantum resilience of the implemented communication pipeline.

IV. CONCLUSION

This work demonstrates the complete implementation of a post-quantum secure communication system using the CRYSTALS-Kyber KEM on Raspberry Pi hardware. By integrating Kyber-based key exchange with TCP socket communication, the system achieves secure message transmission resistant to future quantum attacks. The successful encryption and decryption of data confirm the correctness of the proposed architecture. The methodology shows that post-quantum cryptography can be deployed effectively even on lightweight IoT-class devices. Future work may include extending the system to hybrid cryptographic models, multi-node communication, and real-time security monitoring.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project supervisor for providing continuous guidance, technical support, and valuable insights throughout the development of this work. The authors also acknowledge the Department of Electronics and Telecommunication Engineering for offering the necessary laboratory facilities, Raspberry Pi hardware, and software resources required for experimentation. Finally, the authors thank their peers and mentors for their encouragement and constructive feedback, which greatly contributed to the successful completion of this research.

REFERENCES

[1] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, "CRYSTALS–Kyber: a CCA-secure module-lattice-based KEM", IEEE European Symposium on Security and Privacy, 2018.

[2] Aikata Aikata, Ahmet Can Mert, Samuel Pagliarini,"KaLi: A Crystal for Post-Quantum Security Using Kyber and Dilithium", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, VOL. 70, NO. 2, 2023.

[3] Hasham Sarwar, Anjum Ashraaf, Bahria University Islamabad, "Analysis of Post Quantum Cryptography Algorithms concerning their applicability to IoT devices", engrxiv.org, 2024.

[4] Maram, Varun; Xagawa, Keita, "Post-Quantum Anonymity of Kyber", Cryptology ePrint Archive, 2022.

[5] Kalyan Nakka, Seerin Ahmad, Taesic Kim EE & CS Texas A&M University-Kingsville,"Post-Quantum Cryptography (PQC)-Grade IEEE 2030.5 for Quantum Secure Distributed Energy Resources Networks", IEEE ISGT Conference, 2024.

[6] Duc Tri Nguyen, Viet B. Dang and Kris Gaj EE & CSE, George Mason University, Fairfax, VA, USA,"A High-Level Synthesis Approach to the Software/Hardware Codesign of NTT-based Post-Quantum Cryptography Algorithms", International Conference on Field-Programmable Technology (ICFPT), 2019.

[7] LI Jian, LI Na1, ZHANG Yu, WEN Shuang, DU Wei, CHEN Wei and MA Wenping, China,"A Survey on Quantum Cryptography", Chinese Journal of Electronics Vol.27, No.2, Mar. 2018.

[8] Sherdel A. Käppler Bettina Schneider University of Applied Sciences and Arts Northwestern Switzerland FHNW "Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms"EPiCSeries in Computing Volume 84, 2022, Pages 61–71,2022

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11, November 2025

[9] Mr. Abhishek Sharma, Dr Amit Kumar SRM Institute of Science and Technology, Delhi – NCR Campus, KIET, Ghaziabad," A Survey on Quantum Key Distribution", 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2019.
[10] Neha Junagade, Dr. Sheetal U Bhandari, Pimpri Chinchwad College of Engineering,), Pune, India" Comparative Study of Quantum Algorithms: A Comprehensive Analysis", 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2024.
[11] V.Thamilarasi,PramodKumarNaik,IshaSharma, CHRIST (Deemed to be University), Pune Lavasa Campus, India, "Quantum Computing-Navigating the Frontier with Shor's Algorithm and Quantum Cryptography",International Conference on Trends in Quantum Computing and Emerging Business Technologies, 2024.
[12] Indumathi Saikumar, "DES – Data Encryption Standard," IRJET, 2017
[13] Hengki T. Sihotang et al., "Design and Implementation of RSA Cryptography Algorithm in Text File Data Security," J. Phys. Conf. Ser., 2020
[14] Keerthi K. and Dr. B. Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption," ICCPCT, 2017
[15] Prashant P. Pittalia, "A Comparative Study of Hash Algorithms in Cryptography," IJCSMC, 2019
[16] M. A. Al-Shabi, "A Survey on Symmetric and Asymmetric Cryptography Algorithms in Information Security," IJSRP, 2019