iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

PERFORMANCE EVALUATION OF HYBRID POST-QUANTUM TLS (PQ-TLS) FOR SECURE CLIENT-SERVER COMMUNICATION

B. Dhanush[1]*, ED. Dhanusu, Dr. K. Rohini[2]
[1] UG Student, Department of Computer Applications, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
[2] Professor, Department of Computer Applications, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India

ABSTRACT
The digital age has ushered in a dependency on secure communication and data protection. Every day, vast amounts of sensitive information—ranging from personal data and financial transactions to government communications—are exchanged over networks. This security is largely ensured through modern cryptographic algorithms that protect confidentiality, integrity, and authenticity. However, the emergence of quantum computing poses a significant threat to these systems, potentially rendering many classical cryptographic techniques obsolete. Quantum computers, leveraging the principles of quantum mechanics, have the theoretical ability to perform complex computations exponentially faster than classical computers. With the development of quantum algorithms such as Shor's algorithm and Grover's algorithm, it becomes evident that once large-scale quantum computers become a reality, widely-used encryption schemes such as RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman may no longer be secure. Quantum-resistant cryptography, also known as post-quantum cryptography, aims to develop cryptographic algorithms that are secure against both classical and quantum attacks. This project focuses on the study and analysis of quantum-resistant cryptographic algorithms and presents the design, implementation, and evaluation of a Hybrid Post-Quantum TLS (PQ-TLS) framework. Experimental results demonstrate that the hybrid approach maintains efficient performance with sub-4-second response latencies and 100% data fidelity during encrypted transmission.

Keywords:
Post-Quantum Cryptography, PQ-TLS, CRYSTALS-Kyber, Hybrid Encryption, Network Security.

1. INTRODUCTION

The digital age has brought a critical dependency on secure communication across diverse network infrastructures. Sensitive data, including financial transactions, medical records, and government communications, rely on the security of asymmetric and symmetric cryptographic primitives. However, the anticipated arrival of large-scale quantum computers introduces a major vulnerability. In 1994, Peter Shor demonstrated that a quantum computer could factor large integers and compute discrete logarithms in polynomial time, thereby neutralizing both RSA and ECC. Later, Lov Grover demonstrated an algorithm that accelerates brute-force attacks on symmetric keys, requiring organizations to double key lengths to maintain parity in security.

To address these threats, the National Institute of Standards and Technology (NIST) has led a multi-year effort to standardize post-quantum cryptographic (PQC) algorithms. This paper focuses on the integration of these emerging standards into the existing Transport Layer Security (TLS) protocol, creating a robust, hybrid infrastructure that combines classical public-key algorithms with post-quantum key encapsulation mechanisms (KEMs).

2. LITERATURE SURVEY

Researchers have investigated the transition to post-quantum cryptography from various angles. Petar Radanliev (2024) discussed the convergence of artificial intelligence and quantum cryptography, emphasizing that AI can enhance the resilience of quantum cryptographic protocols. Mattsson et al. (2021) provided a comprehensive review of the vulnerabilities of classical protocols and highlighted the necessity of hybrid solutions as an intermediate step in the migration process. Furthermore, NIST's 2022 announcement of finalists—including CRYSTALS-Kyber for encryption and Dilithium for digital signatures—has provided a definitive baseline for practical implementation.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Algorithm	Type	Key Size / Signature Size
CRYSTALS-Kyber	Lattice-based (KEM)	1184 bytes / 1088 bytes
CRYSTALS-Dilithium	Lattice-based (Signature)	1312 bytes / 2420 bytes
SPHINCS+	Hash-based (Signature)	32 bytes / 17 KB
Classic McEliece	Code-based (KEM)	261 KB / 128 bytes

3. THEORETICAL FOUNDATIONS OF LATTICE-BASED CRYPTOGRAPHY

The security of CRYSTALS-Kyber is rooted in the Learning With Errors (LWE) problem. Unlike RSA, which relies on integer factorization, LWE involves finding a secret vector given noisy linear equations. Kyber specifically uses Module-LWE, offering a balance between efficiency and security. The noise added to the equations ensures that even quantum computers cannot efficiently solve the system of equations. These problems are believed to be resistant to Shor's algorithm because there is no known quantum hidden subgroup problem that maps directly to lattice structures.

A primary driver for immediate PQ-TLS adoption is the 'Harvest Now, Decrypt Later' threat. Adversaries are currently intercepting and archiving encrypted traffic protected by classical RSA/ECC. Once a Cryptographically Relevant Quantum Computer (CRQC) is built, this archived data can be decrypted retrospectively. For data with a security life of ten years or more, such as medical records or intelligence, waiting for quantum computers to exist before switching is already too late.

4. PROPOSED SYSTEM ARCHITECTURE

The proposed architecture employs a hybrid cryptographic framework that combines classical encryption techniques, such as RSA and Elliptic Curve Cryptography (ECC), with post-quantum cryptographic (PQC) algorithms. This dual-layered approach ensures backward compatibility with legacy devices while preparing infrastructure to withstand attacks from powerful quantum computers.

One practical implementation of this concept is Hybrid TLS (PQ-TLS), which integrates post-quantum key exchange algorithms—like CRYSTALS-Kyber—alongside traditional RSA or ECDH within the TLS handshake. PQ-TLS ensures that secure communications remain protected even if one cryptographic method is compromised. The derivation of the session key involves concatenating the shared secrets from both the classical and post-quantum layers, which are then processed through a Hash-based Key Derivation Function (HKDF).

5. IMPLEMENTATION METHODOLOGY

The system is implemented as a client-server socket communication framework using Python 3.10. The components are loosely coupled and organized into modules: Hybrid Key Exchange (Kyber + ECDH), Digital Signature (Dilithium), Symmetric Encryption (AES-256), and Socket Communication. Integration with libraries like liboqs (Open Quantum Safe) provides the necessary PQC primitives.

6. PERFORMANCE EVALUATION

To validate the operational feasibility, performance evaluation was conducted across 50 repeated runs. Key metrics analyzed include key generation time, handshake latency, and memory consumption. While Kyber-768 is computationally efficient (encapsulation in ~0.04 ms), the larger key sizes increase network overhead.

Metric	Classical Setup	Hybrid PQ-TLS	Status
Key Generation Time	12 ms	125 ms	PASS
Handshake Latency	110 ms	2500 ms	PASS
Memory Usage	45 MB	85 MB	PASS
Data Fidelity	100%	100%	PASS

7. ANALYSIS AND FUTURE SCOPE

The experimental results show that while handshake latency increases by approximately 22 times, the absolute value (2.5 seconds) is acceptable for most non-real-time applications. The primary bottleneck is the transmission of larger public keys and ciphertexts over the network, rather than CPU processing. Future work will focus on optimizing the packet fragmentation issues that occur when PQ-TLS payloads exceed the standard 1500-byte MTU limit of Ethernet frames.

8. CONCLUSION AND FUTURE ENHANCEMENTS

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

The quantum threat necessitates a proactive evolution of cryptographic practices. By integrating CRYSTALS-Kyber and other PQC standards into the TLS handshake, the proposed framework delivers robust protection against 'harvest now, decrypt later' attacks without requiring immediate abandonment of classical encryption.

9. REFERENCES

1) Sood, R. (2024). Challenges and Advancements in Quantum-Resistant Cryptography. SSRN.
2) Mattsson, J., Sullivan, N., & Barnes, R. (2021). Post-Quantum Cryptography and NIST Standardization Efforts. arXiv.
3) Alagic, G. et al. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST.
4) Cloudflare Research. (2023). Hybrid Post-Quantum TLS: Deploying Quantum-Resistant Key Exchange in Real-World Applications.
5) Mosca, M. (2018). Cybersecurity in a Quantum World: Will We Be Ready? IEEE Security & Privacy.
6) Stebila, D., & Mosca, M. (2023). Post-Quantum TLS Handshake Performance. Journal of Cryptology.
7) NIST. (2023). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard.