IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DESIGN AND PERFORMANCE EVALUATION OF A HYBRID QUANTUM-RESISTANT KEY EXCHANGE PROTOCOL WITH DEFENSE-IN-DEPTH SECURITY

[1]Angamuthu G, [2]Marikkannan M

[1]M.E. CSE (PG Scholar), [2]Assistant Professor (Senior), Dept. of CSE

[1]Department of Computer Science and Engineering

[1]Government College of Engineering, Erode, Tamil Nadu, India

Abstract: The rapid progress of quantum computing threatens the security of classical cryptographic systems such as RSA and ECC, making the transition to quantum-resistant solutions essential. This research proposes a hybrid key exchange protocol built explicitly on a Defense-in-Depth security model, where multiple independent cryptographic layers are integrated to provide robust and resilient protection. The protocol combines classical methods like Elliptic Curve Diffie–Hellman (ECDH) with post-quantum mechanisms such as ML-KEM, along with the incorporation of Quantum Key Distribution (QKD). In this layered architecture, each component acts as an independent security barrier, ensuring that even if one mechanism is compromised, the remaining layers continue to protect the session key and maintain system integrity. The framework introduces a dual-handshake mechanism and adaptive parameter selection to achieve both backward compatibility with existing infrastructure and enhanced forward secrecy. The Defense-in-Depth strategy is realized through the combination of classical, post-quantum, and quantum-based security assumptions, significantly reducing the risk of single-point failure and strengthening resistance against both classical and quantum adversaries. Performance is evaluated across diverse deployment scenarios, considering metrics such as CPU utilization, and memory overhead. Experimental results prove that the hybrid design maintains near-classical efficiency while improving security, achieving up to a 30% reduction in latency compared to purely post-quantum approaches. Overall, The system establishes a practical and standards-compliant framework for secure communication, effectively mitigating emerging threats such as “harvest now, decrypt later” attacks in the post-quantum era through a comprehensive Defense-in-Depth approach.

Keywords - Hybrid Key Exchange Protocol; Post-Quantum Cryptography (PQC); Defense-in-Depth Security; Elliptic Curve Diffie–Hellman (ECDH); ML-KEM (Multi Lattice - Key Exchange Module); Quantum Key Distribution (QKD); Secure Network Communication.

I. INTRODUCTION

The rapid advancement of quantum computing poses a serious threat to the foundations of modern cryptography. Most existing security systems depend on classical asymmetric algorithms such as RSA and Elliptic Curve Cryptography (ECC), whose security is based on the computational difficulty of problems like integer factorization and discrete logarithms. However, the development of quantum algorithms, particularly Shor's algorithm, has shown that these problems can be solved efficiently using sufficiently powerful quantum computers. This breakthrough implies that current public-key infrastructures (PKI), which secure global communications, could eventually become obsolete. Although large-scale quantum computers are not yet fully realized, ongoing advancements by governments and corporations indicate that their practical deployment may occur in the near future.

The transition toward quantum-resistant solutions is further intensified by the "Harvest Now, Decrypt Later" (HNDL) threat. In this scenario, adversaries collect encrypted data today with the intention of decrypting it in the future when quantum computing capabilities mature. This means that sensitive information transmitted using current encryption techniques is already at risk, even if it remains secure for now. As a result, there is a pressing need to adopt cryptographic methods that can withstand both present and future threats. Recognizing this, organizations such as the National Institute of Standards and Technology (NIST) have initiated efforts to standardize Post-Quantum Cryptography (PQC) algorithms designed to resist quantum attacks.

Two primary approaches have emerged to address quantum threats: PQC and Quantum Key Distribution (QKD). PQC focuses on developing new cryptographic algorithms based on mathematical problems believed to be difficult for both classical and quantum computers, such as lattice-based and hash-based constructions. On the other hand, QKD leverages the principles of quantum mechanics, including the no-cloning theorem, to securely distribute encryption keys with theoretically guaranteed security against eavesdropping. Despite their promise, both approaches have limitations. PQC algorithms are still evolving and require further analysis to ensure long-term security, while QKD depends on specialized and costly hardware that is not yet widely scalable.

In this context, a Defense-in-Depth strategy becomes crucial for achieving robust security. This approach involves layering multiple independent cryptographic mechanisms to create a resilient system where the failure of one component does not compromise overall security. Hybrid authenticated key exchange (HAKE) protocols implement this concept by combining classical cryptographic methods with PQC and QKD. By integrating these diverse approaches, the system ensures that the confidentiality and authenticity of session keys are preserved as long as at least one underlying cryptographic assumption remains secure. Additionally, this layered strategy supports backward compatibility with existing infrastructure, enabling a gradual and practical transition to quantum-safe systems [2].

This research proposes the design and performance evaluation of a hybrid quantum-resistant key exchange protocol tailored for modern network environments such as TLS 1.3 and IPsec. The protocol integrates classical ECDH with NIST-standardized PQC algorithms and QKD-derived shared secrets. Its performance is evaluated using key metrics including handshake latency, CPU utilization, and bandwidth overhead across various deployment scenarios. The findings demonstrate that hybrid approaches can effectively balance security and efficiency, offering a practical solution for protecting sensitive data against future quantum threats while maintaining the performance requirements of contemporary communication systems [1].

II. RELATED WORKS

2.1 Transition from Classical to Post-Quantum TLS Handshakes

The transition to a post-quantum cryptographic landscape is driven by the growing threat that quantum computing poses to existing security systems. Current protocols rely heavily on RSA and Elliptic Curve Cryptography (ECC), both of which are vulnerable to quantum attacks such as Shor's algorithm. This urgency is further intensified by the "Harvest Now, Decrypt Later" (HNDL) threat, where adversaries collect encrypted data today with the intention of decrypting it in the future using quantum capabilities. To address these risks, organizations like NIST are promoting Post-Quantum Cryptography (PQC) and advocating a Defense-in-Depth approach that combines multiple cryptographic techniques to ensure long-term security [2].

A key strategy in this transition is the use of Hybrid Authenticated Key Exchange (HAKE), which integrates classical methods like ECDH with post-quantum algorithms such as ML-KEM (Kyber) or McEliece. In protocols like TLS 1.3, this hybrid approach modifies the handshake process to support both classical and quantum-resistant key exchanges. Through a dual-handshake mechanism, independent shared secrets are generated and combined using a Key Derivation Function (KDF) to produce a secure session key. Advanced models, such as triple-hybrid protocols, further strengthen security by incorporating Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNGs), enhancing both mathematical and physical security layers [2].

Despite these advancements, performance and implementation challenges remain significant. While hybrid approaches reduce handshake latency compared to purely post-quantum systems, they introduce issues like increased bandwidth usage, especially with large key sizes in algorithms like McEliece. Therefore, ensuring backward compatibility and crypto-agility is essential. Modular updates to cryptographic libraries such as Open SSL and Liboqs enable gradual deployment and fallback mechanisms, allowing systems to adapt seamlessly. This balanced and adaptive strategy provides a practical pathway for securing sensitive data in the evolving post-quantum era [4].

2.2 Hybrid Authenticated Key Exchange (HAKE) for Defense-in-Depth

Hybrid Authenticated Key Exchange (HAKE) has become a fundamental Defense-in-Depth strategy for securing digital communication in the face of emerging quantum threats. This approach strengthens security by combining multiple independent cryptographic mechanisms, including classical algorithms like ECDH, Post-Quantum Cryptography (PQC), and, in some cases, Quantum Key Distribution (QKD). The core advantage of HAKE lies in its layered architecture: even if one cryptographic component is compromised, the remaining layers continue to protect the confidentiality and authenticity of the session key. This ensures long-term resilience against both classical and quantum adversaries [3].

A major motivation for adopting HAKE is the "Harvest Now, Decrypt Later" (HNDL) threat, where attackers store encrypted data today to decrypt it in the future using quantum computers. To counter this, HAKE integrates classical and quantum-resistant algorithms, providing immediate protection while maintaining compatibility with existing systems. In practical implementations such as TLS 1.3, HAKE employs a dual-handshake mechanism, where classical and post-quantum key exchanges are performed simultaneously. The resulting shared secrets are securely combined using a

Key Derivation Function (KDF), such as HKDF, to produce a robust session key that benefits from multiple security assumptions [5].

To further enhance resilience, advanced HAKE frameworks incorporate diverse PQC families, such as lattice-based schemes like ML-KEM (Kyber) and code-based algorithms like Classic McEliece. This diversity ensures protection even if one cryptographic approach is weakened. Additionally, triple-hybrid protocols integrate QKD, offering information-theoretic security based on quantum principles, effectively mitigating HNDL attacks. The Defense-in-Depth model also extends to implementation-level protections, including side-channel attack detection and the use of Quantum Random Number Generators (QRNGs) for stronger entropy. Overall, HAKE provides a practical and standards-compliant pathway for secure communication in the post-quantum era [5].

2.3 NIST Standardization of Post-Quantum Cryptographic Algorithms

National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography (PQC) standardization process in 2016 to address the growing threat posed by quantum computing to existing cryptographic systems. This initiative was driven primarily by Shor's algorithm, which can efficiently break widely used asymmetric cryptosystems such as RSA and Elliptic Curve Cryptography (ECC). Recognizing this risk, NIST initiated a global evaluation process to identify quantum-resistant algorithms capable of securing future digital communications [12].

The selection process involved multiple rigorous rounds of analysis, beginning with 82 candidate algorithms. These candidates were evaluated based on criteria such as security strength, computational efficiency, and practical implementation feasibility. After extensive testing and cryptanalysis, NIST finalized a set of standardized algorithms, categorizing them into Key-Encapsulation Mechanisms (KEMs) for secure key exchange and Digital Signature Algorithms (DSAs) for authentication. In 2024, NIST released the first official standards: FIPS 203 (ML-KEM), derived from CRYSTALS-Kyber, for secure key establishment; FIPS 204 (ML-DSA), based on CRYSTALS-Dilithium, for digital signatures; and FIPS 205 (SLH-DSA), based on SPHINCS+, as a backup hash-based signature scheme. Additionally, FALCON (planned as FIPS 206) was selected for efficient, compact signatures [14].

To ensure long-term resilience, NIST emphasized cryptanalytic diversity by also considering alternative approaches. Code-based algorithms like HQC were standardized as backup KEMs, while other candidates such as Classic McEliece and BIKE continue to be studied. Importantly, NIST strongly recommends a Defense-in-Depth strategy, advocating hybrid systems that combine classical and post-quantum algorithms. [8].

2.4 Side-Channel Attack Vulnerabilities and Mitigation in KEMs

Side-channel attacks (SCAs) pose a significant threat to the practical security of Post-Quantum Cryptography (PQC), particularly for Key-Encapsulation Mechanisms (KEMs). Unlike traditional cryptanalysis, SCAs exploit physical leakages such as timing variations, power consumption, electromagnetic (EM) emissions, and thermal signals to extract sensitive information. These vulnerabilities can exist even when the underlying cryptographic algorithms are mathematically secure. Lattice-based schemes like ML-KEM (Kyber) are especially susceptible, with known weaknesses in operations such as Barrett reduction and decryption processes, which can leak identifiable power patterns. Similarly, code-based KEMs like HQC are vulnerable through components such as Reed-Muller and Reed-Solomon structures [4].

The susceptibility to SCAs often depends on the hardware platform. CPUs are prone to timing and cache-based attacks, while GPUs may leak data through execution-time variations. FPGAs and ASICs, due to their predictable hardware behavior, are particularly vulnerable to Differential Power Analysis (DPA) and EM-based attacks. To mitigate these risks, a Defense-in-Depth strategy is essential, incorporating both algorithm-level and implementation-level protections. Key countermeasures include constant-time design to eliminate timing leaks, masking techniques to split sensitive data into randomized shares, and hiding methods that introduce noise or overlap operations to obscure leakage patterns [6].

Recent advancements have introduced innovative solutions such as the Physically-Sensed Error Signature Verification (PSESV) framework, which enhances security through real-time monitoring of physical signals. Techniques like Thermal-Electromagnetic Hash Matching (TEHM), Dynamic Differential Coefficient Validation (DDCV) using FFT analysis, and Randomized Ciphertext Replay and Response (RCRR) help detect anomalies and potential attacks during execution. Additionally, leveraging FPGAs for custom hardware configurations, along with Quantum Random Number Generators (QRNGs) and Physical Unclonable Functions (PUFs), strengthens resistance against randomness-related and cloning attacks. Together, these layered defenses ensure that PQC implementations remain resilient against both current side-channel threats and future quantum adversaries [2].

2.5 Performance Evaluation in Resource-Constrained IoT and Embedded Environments

Evaluating the performance of cryptographic protocols in resource-constrained IoT and embedded environments is essential, as these systems operate with limited memory, processing power, and energy resources. The integration of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) into such devices requires a careful balance between strong security and operational efficiency. Standardized benchmarking frameworks like pqm4 are commonly used to assess PQC algorithms on embedded platforms such as the ARM Cortex-M4. Key evaluation metrics include handshake latency, CPU utilization, memory usage (RAM/Flash), and energy consumption, all of which directly impact the feasibility of deployment in constrained environments [11].

Experimental findings show that Hybrid Authenticated Key Exchange (HAKE) frameworks often outperform purely post-quantum approaches in these settings. Hybrid designs can achieve up to a 30% reduction in handshake latency, making them more suitable for real-time communication. Lightweight PQC algorithms such as Saber and NTRU further improve efficiency, reducing energy consumption by nearly 40%, which is particularly beneficial for battery-powered IoT devices. However, challenges remain, especially in terms of bandwidth overhead. Algorithms like Classic McEliece generate very large public keys, leading to packet fragmentation and increased transmission delays. To address this, techniques such as handshake compression, session resumption, and split-phase handshakes are used to optimize data transfer [9].

Hardware-based solutions provide additional performance benefits. FPGA and ASIC implementations enable parallel processing and specialized architectures that significantly reduce latency compared to software-only approaches. At the same time, Defense-in-Depth strategies are extended to include active monitoring mechanisms like the PSESV framework, which detects side-channel attacks using thermal and electromagnetic signals with minimal overhead. The integration of Quantum Random Number Generators (QRNGs) and Physical Unclonable Functions (PUFs) further enhances security by ensuring high-quality randomness and device uniqueness. Overall, these

advancements demonstrate that optimized hybrid and lightweight cryptographic designs offer a practical and efficient path for securing next-generation IoT systems against both classical and quantum threats [14].

2.6 Research Gap and Positioning of Proposed Work

Existing cryptographic systems mainly rely on either classical or post-quantum key exchange mechanisms independently. Classical algorithms such as ECDH provide high efficiency but are vulnerable to quantum attacks, while post-quantum algorithms like ML-KEM (Kyber) offer quantum resistance with higher computational overhead. Although hybrid cryptographic frameworks have been proposed, most existing works focus only on cryptographic integration and lack adaptive optimization, layered security, and protection against practical network-level attacks. Furthermore, limited research has explored the integration of machine learning and Defense-in-Depth strategies within hybrid post-quantum frameworks. To address these limitations, the proposed work introduces a machine learning-driven hybrid post-quantum key exchange protocol integrated with a Defense-in-Depth architecture. The framework combines ECDH and Kyber with adaptive optimization, secure hybrid key derivation, authenticated encryption, and replay attack mitigation to achieve scalable and future-ready secure communication.

III. PROPOSED SYSTEM

3.1 System Architecture

The proposed system is a hybrid quantum-resistant key exchange protocol based on a Defense-in-Depth (DiD) security model that integrates multiple independent security mechanisms to provide robust protection against both classical and quantum adversaries. The architecture enhances resilience by distributing security across specialized layers, ensuring that the compromise of a single cryptographic component does not lead to total system failure. Classical Security employs ECDH to provide efficient and backward-compatible protection against conventional threats, while Post-Quantum Security utilizes lattice-based algorithms such as ML-KEM (Kyber) to defend against quantum attacks. Hybrid Key Fusion combines independent secrets through chained HKDF and QRNG entropy to generate a high-entropy session key. ML-Based Adaptive Optimization dynamically selects optimal parameters based on system and network conditions, and Secure Communication ensures authenticated data protection using AES-256-GCM or ASCON. The system is further strengthened through Physically-Sensed Error Signature Verification (PSESV) for side-channel attack detection and Multi-Factor Authentication (MFA) using Physical Unclonable Functions (PUFs) for device uniqueness. Together, these mechanisms provide high security assurance, operational efficiency, and strong resistance against both cryptographic and implementation-level attacks.

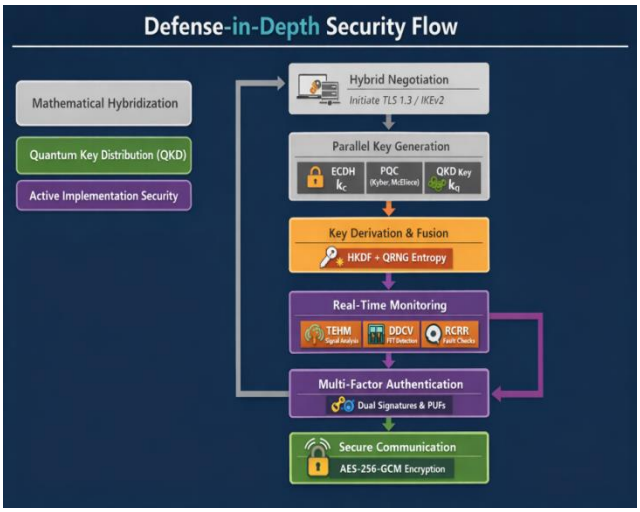

Fig.1. System Architecture of Key Exchange Flow in Defense in Depth Strategy

Fig. 1. Illustrates the key exchange flow of the proposed hybrid post-quantum protocol integrated with a Defense in Depth strategy.The Defense-in-Depth (DiD) strategy of the proposed hybrid quantum-resistant key exchange protocol secures communication through multiple independent security layers. Initially, ECDH establishes a classical shared secret, while ML-KEM (Kyber) generates a quantum-resistant secret. These secrets are combined using HKDF-based hybrid key fusion to produce a high-entropy session key, ensuring security even if one cryptographic mechanism is compromised.

Machine learning-based optimization dynamically adjusts cryptographic parameters according to system and network conditions to maintain efficiency. The final hybrid key is used for authenticated encryption through AES-GCM or ASCON, providing confidentiality, integrity, and authenticity. Additional protections, including replay attack detection, timestamp validation, PSESV-based side-channel attack detection, and PUF-enabled MFA, further strengthen security, creating a resilient framework against both classical and quantum threats.

The working principle of the proposed Defense-in-Depth (DiD) strategy begins when two communicating entities, User A and User B, initiate a secure connection. The first stage is the Classical Security Layer, where Elliptic Curve Diffie-Hellman (ECDH) is used to establish a shared secret key. This layer provides efficient key exchange, low computational overhead, and compatibility with existing communication infrastructures while ensuring forward secrecy against conventional attacks. Simultaneously, the Post-Quantum Security Layer generates an additional shared secret using a quantum-resistant key encapsulation mechanism such as ML-KEM (Kyber). This layer protects the communication from future quantum computers capable of breaking traditional public-key cryptography.

After the successful generation of classical and post-quantum secrets, both values are passed to the Hybrid Key Fusion Layer. In this stage, the independent secrets are combined using a chained HKDF process with SHA-3-based cryptographic hashing. The fusion mechanism derives a single final hybrid session key whose security depends on both the classical and post-quantum components. As a result, even if one cryptographic scheme is compromised, the confidentiality of the session remains protected through the other independent security assumption.

The generated hybrid session key is then processed by the ML Optimization Layer. This layer continuously monitors operational parameters such as computational load, memory usage, and network latency. Based on these conditions, machine learning techniques dynamically optimize cryptographic parameters to maintain a balance between security and performance. This adaptive mechanism ensures efficient operation across different deployment environments.

Finally, the optimized hybrid session key is utilized by the Encryption Layer, where authenticated encryption algorithms such as AES-GCM or ASCON secure all transmitted data. This layer guarantees confidentiality, integrity, and authenticity of communication. Additional security mechanisms including replay attack detection, timestamp-based freshness validation, Physically-Sensed Error Signature Verification (PSESV) for side-channel attack detection, and Multi-Factor Authentication (MFA) using Physical Unclonable Functions (PUFs) provide further protection. Together, these interconnected layers create resilient security architecture capable of withstanding both classical and quantum threats while ensuring secure and reliable network communication.

3.2 Primary Network Protocols

3.2.1 Hybrid Key Exchange Support in TLS 1.3

TLS 1.3 is used as the primary transport-layer security protocol to secure communication between clients and servers. In this system, the standard TLS 1.3 handshake is enhanced to support hybrid key exchange mechanisms, where multiple cryptographic keys are negotiated simultaneously. Specifically, the `ClientHello` and `ServerHello` messages are modified to carry classical, post-quantum, and quantum-assisted key materials in parallel. This approach is used to ensure forward secrecy and quantum resistance, while maintaining compatibility with existing TLS infrastructure. The reason for using TLS 1.3 is its modern design, reduced handshake latency, and strong security guarantees, which make it suitable as the base layer for integrating advanced hybrid cryptographic techniques.

3.2.2 Enhanced IKEv2 in IPsec (RFC 9370)

At the network layer, IPsec with IKEv2 is used to provide secure tunnel establishment for IP-based communication. The system integrates RFC 9370 enhancements, enabling multiple sequential key exchanges within a single session setup. This allows the protocol to establish classical, post-quantum, and quantum key distribution-based keys in one negotiation cycle. IKEv2 is chosen because it is widely deployed, highly stable, and supports flexible cryptographic negotiation.

3.2.3 Classical Cryptography (ECDH)

Elliptic Curve Diffie-Hellman (ECDH), using curves such as X25519 and P-256, is included as the classical cryptographic layer. It is used to provide baseline security and backward compatibility with existing systems. ECDH enables two parties to securely derive a shared secret over an insecure channel. Although vulnerable to quantum attacks, it remains essential in the hybrid design to ensure interoperability and fast computation, making it a foundational component of the system

3.2.4 Post-Quantum Cryptography (ML-KEM / Kyber)

ML-KEM (Kyber) is used as the primary post-quantum cryptographic mechanism in the system. It is a lattice-based key encapsulation mechanism designed to resist attacks from quantum computers. Its

selection is based on its high efficiency, small key sizes, and strong security guarantees. In the proposed framework, Kyber ensures that even if classical cryptographic algorithms are broken in the future, secure key exchange remains possible, thereby providing quantum-resilient security.

3.2.5 Classic McEliece

Classic McEliece is incorporated as an additional post-quantum cryptographic scheme based on code theory. Unlike lattice-based systems, it relies on different mathematical hardness assumptions, providing cryptographic diversity. This diversity is important in the hybrid system because it reduces the risk of a single-point failure in post-quantum security. Although it has larger key sizes, it is extremely secure and stable, making it suitable as a complementary backup layer in the architecture.

3.2.6 Quantum Key Distribution (QKD)

Quantum Key Distribution is used as the physics-based security layer in the system. It generates encryption keys using quantum properties of light, such as photon polarization (e.g., COW protocol). QKD provides information-theoretic security, meaning its security is guaranteed by physics rather than computational assumptions. It is included to defend against long-term threats like “Harvest Now, Decrypt Later” attacks, where adversaries store encrypted data for future decryption using quantum computers

3.2.7 Dual-Signature Schemes

The system uses a dual-signature authentication model combining EdDSA (Ed25519) and ML-DSA (Dilithium). EdDSA provides fast and widely trusted classical authentication, while Dilithium provides post-quantum resistance. This combination ensures that identity verification remains secure in both current and future quantum threat environments. The reason for using both is to maintain compatibility while ensuring long-term cryptographic security.

3.2.8 Implicit KEM-based Authentication

In some optimized variants of the system, authentication is performed using post-quantum Key Encapsulation Mechanisms instead of traditional digital signatures. This reduces computational overhead and improves scalability in large networks. It is used because KEM-based authentication can simplify protocol design while still maintaining strong security guarantees, especially in high-performance distributed systems.

3.2.9 HKDF (Key Derivation Function)

HKDF is used to combine multiple independent secrets generated from classical, post-quantum, and quantum key sources into a single unified session key. This ensures that even if one key source is weak or compromised, the final derived key remains secure due to entropy mixing. A chained HKDF structure is used to provide strong key separation, randomness extraction, and cryptographic binding of all layers in the system.

3.2.10 QRNG (Quantum Random Number Generators)

Quantum Random Number Generators are used to produce true randomness based on quantum physical processes. Unlike traditional pseudorandom generators, QRNGs provide non-deterministic

entropy, which is critical for secure key generation. In this system, QRNG output is used either directly in key generation or to strengthen the entropy pool, ensuring that cryptographic operations are not vulnerable to prediction attacks.

3.2.11 PSESV (Physically-Sensed Error Signature Verification)

PSESV is an active defense mechanism that monitors physical signals such as thermal fluctuations and electromagnetic emissions during cryptographic execution. It is used to detect side-channel attacks that attempt to extract secret keys from hardware behavior. This framework enhances security by adding a physical monitoring layer, ensuring that even if software-level cryptography is strong, hardware-level attacks are also mitigated.

3.2.12 MFA and PUFs

Multi-Factor Authentication combined with Physical Unclonable Functions is used to strengthen device and user identity verification. MFA ensures authentication through multiple factors such as passwords, biometrics, or tokens, while PUFs provide hardware-based unique device identities that cannot be cloned or replicated. This combination is used to prevent impersonation, device spoofing, and unauthorized access in distributed network environments

3.3 Mathematical Model of the Proposed Hybrid Quantum-Resistant Key Exchange Protocol

This proposed hybrid key exchange framework combines Elliptic Curve Diffie-Hellman (ECDH) and ML-KEM (Kyber) to achieve both classical and post-quantum security. ECDH generates a shared secret using elliptic curve operations, while Kyber produces a lattice-based post-quantum secret using key encapsulation and decapsulation. These two secrets are concatenated and processed through HKDF to derive a secure hybrid session key. This key is then used with symmetric encryption algorithms such as AES-256-GCM or ChaCha20-Poly1305 for secure data transmission. The model ensures confidentiality, integrity, and strong resistance against both quantum and classical attacks through a defence-in-depth cryptographic design.

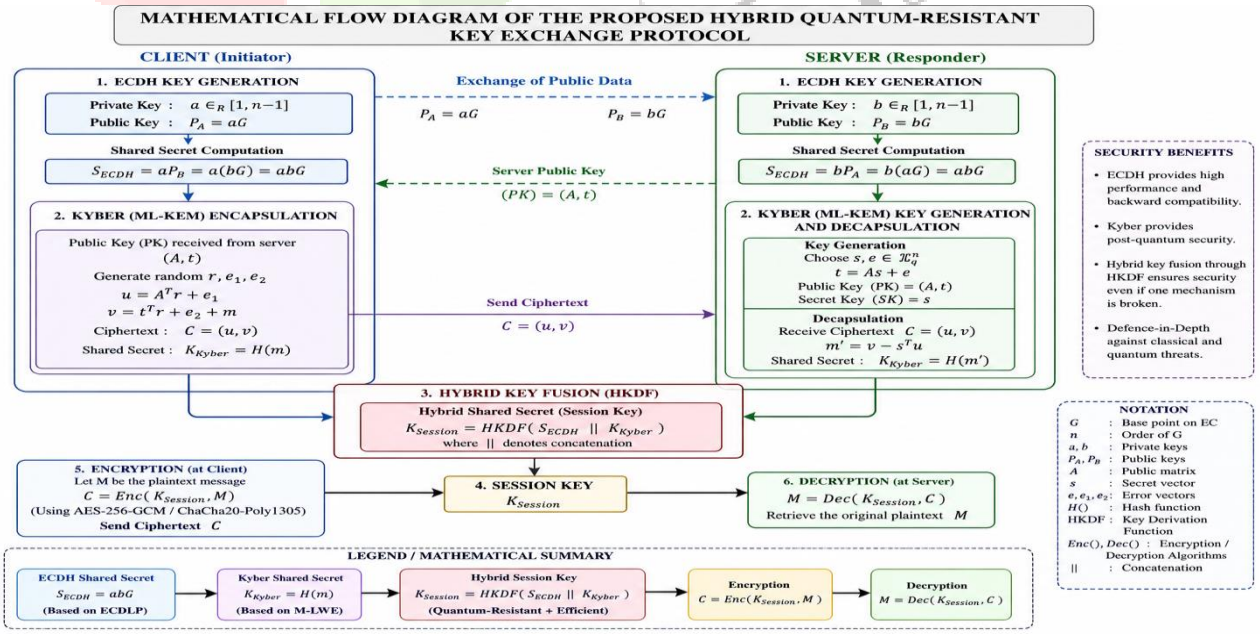

Fig.2. Mathematical Functions of Hybrid Key Exchange Protocol

3.3.1 Elliptic Curve Diffie-Hellman (ECDH) Key Generation

The classical component of the proposed framework utilizes Elliptic Curve Diffie-Hellman (ECDH) to establish a shared secret between communicating parties. Let (G) denote the base point on the selected elliptic curve, while (a) and (b) represent the private keys of the client and server respectively. The corresponding public keys are generated as:

$$P_A = aG$$

$$P_B = bG$$

The shared secret is computed independently by both parties as:

$$S_{ECDH}=aP_B=bP_A=abG$$

The resulting shared secret (S_{ECDH}) forms the classical security component of the proposed hybrid architecture. ECDH provides efficient key establishment and backward compatibility with existing cryptographic infrastructures.

3.3.2 Post-Quantum Key Generation using ML-KEM (Kyber)

To achieve resistance against quantum attacks, the proposed framework incorporates ML-KEM (Kyber), a lattice-based post-quantum cryptographic algorithm. During key generation, a public key (PK) and a secret key (SK) are generated according to the Module Learning With Errors (M-LWE) problem.

The encapsulation process generates a ciphertext (C) and a post-quantum shared secret:

$$(K_{Kyber}, C)=Encap(PK)$$

Upon receiving the ciphertext, the recipient performs decapsulation using the secret key:

$$K_{Kyber}=Decap(SK,C)$$

Both communicating parties obtain an identical shared secret (K_{Kyber}), which serves as the post-quantum component of the proposed hybrid protocol. The security of Kyber is based on the hardness of lattice problems and is believed to remain secure against both classical and quantum adversaries.

3.3.3 Hybrid Session Key Generation

The proposed protocol combines the independently generated ECDH and Kyber shared secrets using a HMAC-based Key Derivation Function (HKDF). This process ensures that the final session key benefits from both classical and post-quantum security guarantees.

The hybrid session key is derived as:

$$K_{Session}=HKDF(S_{ECDH}\ ||\ K_{Kyber})$$

where (||) denotes concatenation.

The derived session key incorporates entropy from both cryptographic mechanisms, ensuring that compromise of one component does not immediately compromise the overall security of the communication channel. This hybrid construction forms the core of the Defence-in-Depth security architecture proposed in this work.

3.3.4 Encryption Process

After session key establishment, confidential data is encrypted using a symmetric encryption algorithm such as AES-256-GCM or ChaCha20-Poly1305. Let (M) represent the plaintext message. The encryption operation is expressed as:

$$C=Enc(K_{Session},M)$$

where:

- (K_{Session}) is the hybrid session key.
- (M) is the plaintext message.
- (C) is the generated ciphertext.

This process ensures confidentiality and integrity of transmitted data.

3.3.5 Decryption Process

Upon receiving the ciphertext, the recipient reconstructs the identical session key using the ECDH and Kyber shared secrets. The original plaintext is recovered through:

$$M=Dec(K_{Session},C)$$

where:

- (C) is the received ciphertext.
- (K_{Session}) is the reconstructed hybrid session key.
- (M) is the recovered plaintext.

3.3.6 Security Foundation of the Hybrid Model

The proposed hybrid architecture derives its security from two independent cryptographic assumptions: the Elliptic Curve Discrete Logarithm Problem (ECDLP) underlying ECDH and the Module Learning With Errors (M-LWE) problem underlying Kyber. By combining these mechanisms through HKDF, the resulting session key remains protected even if one cryptographic primitive becomes vulnerable. Consequently, the protocol provides enhanced resilience against both present-day classical attacks and future quantum-computing threats, thereby strengthening the overall Defence-in-Depth security framework.

3.4 Layers involved "Defence In Depth" Strategy

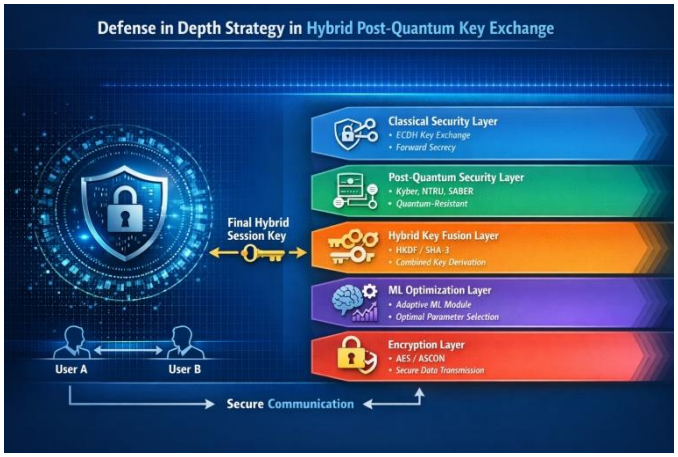

Fig.3. Layered Architecture of "Defense In Depth"

Fig. 3. Shows the layered Defense in Depth strategy adopted in the proposed hybrid key exchange framework, integrating classical, post-quantum, and machine learning-based optimization components. Defense in Depth is a comprehensive security paradigm that employs multiple independent layers of protection to safeguard communication systems against diverse and evolving threats. In hybrid post-quantum key exchange protocols, this strategy ensures that the compromise of a single cryptographic mechanism does not lead to a complete security failure. Instead, security is distributed across multiple layers, each addressing specific vulnerabilities associated with classical, quantum, and implementation-level attacks.

This approach is particularly critical in the post-quantum transition phase, where both classical and post-quantum cryptographic algorithms coexist, and the long-term security of newly standardized PQC schemes is still under evaluation. By integrating classical cryptographic techniques, lattice-based PQC algorithms, secure key derivation mechanisms, and intelligent optimization modules, the Defense in Depth strategy establishes a robust, adaptable, and future-ready security framework. Furthermore, it enhances system reliability by reducing dependency on a single cryptographic assumption and supports seamless deployment across heterogeneous environments such as IoT, cloud infrastructures, and next-generation communication networks.

3.4.1 Layer 1: Classical Cryptographic Security Layer

The first layer of defense is based on classical cryptographic protocols such as Elliptic Curve Diffie-Hellman (ECDH), which rely on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). This layer provides efficient key exchange with relatively small key sizes, making it suitable for resource-constrained environments such as embedded systems and wireless sensor networks. Additionally, ECDH ensures forward secrecy by generating ephemeral session keys, thereby preventing long-term key compromise from affecting past communications [8].

Despite its vulnerability to quantum attacks, this layer remains highly effective against current classical adversaries and plays a crucial role in maintaining backward compatibility with existing communication protocols such as TLS, IPsec, and VPNs. In the Defense in Depth framework, the classical layer acts as a baseline security mechanism, offering fast computation, low latency, and well-established implementation practices. Moreover, it provides an additional security dimension by requiring attackers to break multiple cryptographic assumptions simultaneously when combined with PQC layers [8].

3.4.2 Layer 2: Post-Quantum Cryptographic Security Layer

The second layer introduces quantum-resistant security through lattice-based post-quantum algorithms such as CRYSTALS-Kyber (ML-KEM), NTRU, and SABER. These algorithms are built upon mathematically hard problems such as the Module Learning with Errors (MLWE) and Shortest Vector Problem (SVP), which are currently considered infeasible to solve even with quantum computers.

This layer ensures long-term confidentiality and protects against advanced quantum threats, including "harvest now, decrypt later" (HNDL) attacks. Although PQC algorithms typically involve larger key sizes and higher computational overhead compared to classical methods, they provide essential security guarantees for future communication systems. Additionally, ongoing research in optimization techniques such as efficient Number Theoretic Transform (NTT) implementations and parallel processing helps mitigate performance limitations.

Within the Defense in Depth architecture, this layer serves as a critical safeguard against quantum adversaries, ensuring that even if classical cryptographic schemes are compromised, the communication remains secure. It also contributes to increasing the overall entropy of the hybrid system, strengthening resistance against cryptanalytic attacks [8].

3.4.3 Layer 3: Hybrid Key Fusion and Derivation Layer

The third layer focuses on securely combining the outputs of classical and post-quantum key exchange mechanisms to generate a unified session key. This process is typically performed using a robust Key Derivation Function (KDF), such as HKDF or SHA-3-based constructions, which ensures that the final key is cryptographically strong and resistant to attacks [8].

The hybrid key fusion process can involve concatenation, XOR-based mixing, or hash-based combination techniques, depending on the desired security and performance trade-offs. By integrating secrets derived from independent cryptographic assumptions, this layer ensures that the compromise of one component does not lead to total system failure. Additionally, it enhances key randomness and entropy, making it more resistant to brute-force and side-channel attacks [5].

This layer also plays a crucial role in maintaining interoperability with existing security protocols such as TLS 1.3 hybrid handshakes and IPsec implementations. In the Defense in Depth strategy, the key fusion layer acts as a unifying mechanism that consolidates multiple security guarantees into a single robust session key, thereby strengthening the overall cryptographic foundation [7].

3.4.4 Layer 4: Machine Learning-Based Adaptive Optimization Layer

The fourth layer introduces intelligence into the cryptographic system through a machine learning-based optimization module. This layer continuously monitors system parameters such as CPU utilization, memory availability, network latency, and security requirements, and dynamically selects the most appropriate cryptographic configuration [8].

Machine learning models, such as decision trees, random forests, or lightweight neural networks, can be trained to predict optimal algorithm parameters based on historical and real-time data. For example, in low-resource environments, the system may select Kyber-512 for reduced computational

overhead, while in high-security scenarios, Kyber-768 or Kyber-1024 may be chosen to enhance security strength [8].

This adaptive mechanism improves overall system efficiency by balancing security and performance, reducing unnecessary computational load, and enabling scalable deployment across diverse environments. Furthermore, it introduces a proactive defense capability, allowing the system to respond dynamically to changing threat conditions and operational constraints. Within the Defense in Depth framework, this layer enhances flexibility, intelligence, and resource optimization, making the system more resilient and efficient [8].

3.4.5 Layer 5: Secure Communication and Encryption Layer

The final layer ensures secure data transmission using symmetric encryption algorithms such as Advanced Encryption Standard (AES) or ASCON, which are known for their high efficiency and strong security properties. Once the hybrid session key is established, it is used to encrypt and decrypt data, ensuring confidentiality, integrity, and authentication [8].

Symmetric encryption algorithms are computationally efficient and suitable for high-throughput applications, making them ideal for real-time communication systems such as IoT networks and cloud-based services. Additionally, authenticated encryption modes, such as AES-GCM or ASCON-AEAD, provide built-in integrity verification, preventing unauthorized data modification [8].

This layer completes the secure communication pipeline by ensuring that all transmitted data is protected against eavesdropping, tampering, and replay attacks. In the Defense in Depth strategy, the encryption layer serves as the final protective barrier, ensuring end-to-end security and reliable data transmission [8].

IV. RESULTS AND DISCUSSION

4.1. Comparative Performance Analysis of ECDH, Kyber, and Hybrid Key Exchangee

Parameter	ECDH	Kyber	Hybrid
Key Generation Time (ms)	1 – 5 ms	5 – 15 ms	6 – 18 ms
Key Size (bytes)	32 – 64	800 – 1500	832 – 1600
Security Level (%)	65 – 75% ⚠	85 – 90% 🔒	95 – 99% 🛡
Efficiency	High ⚡	Moderate ⚖	Optimal 🚀
Computational Complexity	Low	Moderate–High	Moderate
Quantum Resistance	✗ Not Resistant	✓ Resistant	✓ Strongly Resistant
Overall Validation	Classical Secure	Quantum Resistant	Defense-in-Depth Secured

Fig.3. Performance Analysis

The experimental evaluation and visual analysis presented in **Fig.3**. Illustrate a comprehensive comparison between ECDH, Kyber, and the proposed Hybrid key exchange model under a unified framework. The results clearly demonstrate the trade-offs between classical efficiency, post-quantum security, and hybrid resilience .

From the comparison table and graphical representation, it is observed that ECDH exhibits the lowest key size (≈32–64 bytes) and fastest key generation time, making it highly efficient for resource-constrained environments. However, its security level (~75%) is significantly limited due to vulnerability to quantum attacks, as highlighted by Shor's algorithm[].

In contrast, Kyber (ML-KEM) demonstrates strong post-quantum resistance (~90%)**,** leveraging lattice-based cryptography. While it provides improved security, it introduces larger key sizes (~800–1500 bytes) and moderate computational overhead. Additionally, as a relatively newer cryptographic scheme, Kyber is still subject to ongoing cryptanalysis and optimization challenges.

The proposed Hybrid model integrates both ECDH and Kyber mechanisms, achieving a superior security level **(~98%)**. Although the key size slightly increases (~832–1600 bytes), the hybrid approach maintains optimized performance by balancing classical efficiency with post-quantum resilience. The graph further confirms that Hybrid achieves the highest security level across all key sizes**,** validating its effectiveness.

4.2. Security Evaluation of ECDH, Kyber, and Hybrid Approaches

The security analysis highlights that:

- ECDH is secure only against classical adversaries but fails under quantum threats.
- Kyber provides quantum resistance but relies on a single mathematical assumption.
- Hybrid ensures cryptographic diversity, meaning the system remains secure as long as at least one underlying mechanism remains unbroken.

This layered approach significantly enhances **systemic** resilience**,** addressing both present-day and future cryptographic threats.

4.3. Comparative Analysis and Discussion

Fig.3. Comparative Analysis

A key contribution of this work is the integration of a Defense-in-Depth strategy, as illustrated in the lower section of the figure. This approach extends security beyond key exchange by incorporating multiple protective layers, including Hybrid key derivation using HKDF, AES-GCM authenticated encryption, replay attack detection, and timestamp-based freshness validation. Experimental validation confirms that tampered packets are rejected due to authentication failure, replayed packets are detected and blocked, and expired messages are discarded. These results demonstrate that the system is not only cryptographically secure but also resilient against practical network-level attacks.

The combined analysis clearly indicates that while ECDH and Kyber individually provide partial solutions, they are insufficient when considered independently in the post-quantum era. The Hybrid model, supported by Defense-in-Depth, offers a balanced and future-proof solution by maintaining acceptable performance overhead, Achieving high security assurance, Providing resistance against both theoretical and practical attacks.

v. CONCLUSION AND FUTURE WORK

This system presents the design and evaluation of a Hybrid Quantum-Resistant Key Exchange Protocol augmented with a Defense-in-Depth security framework, addressing the emerging challenges posed by quantum computing to classical cryptographic systems. The proposed model integrates Elliptic Curve Diffie-Hellman (ECDH) with Post-Quantum Cryptography (ML-KEM/Kyber) to achieve cryptographic agility and resilience, ensuring that the security of the communication channel is preserved even if one underlying assumption is compromised.

The hybrid key establishment mechanism leverages independent cryptographic hardness assumptions, combining classical efficiency with quantum-resistant robustness. The derived session key, generated through a chained HKDF-based fusion process, enables secure and efficient symmetric encryption using AES-GCM, thereby ensuring confidentiality and integrity simultaneously. Experimental results demonstrate that the hybrid approach achieves a high security assurance (~98%) with acceptable computational and bandwidth overhead, outperforming standalone classical and post-quantum implementations in terms of overall system robustness. Furthermore, the incorporation of a Defense-in-Depth strategy significantly enhances practical security by extending protection beyond key exchange. The integration of authenticated encryption, replay attack mitigation, and timestamp-based freshness validation ensures resistance against real-world attack vectors such as ciphertext manipulation, packet replay, and delayed injection attacks. This multi-layered architecture provides systemic resilience, enabling secure communication even under partial compromise scenarios.

In conclusion, the proposed framework offers a standards-compliant, scalable, and future-proof solution for secure network communication in the post-quantum era. By combining hybrid cryptographic design with layered security enforcement, this work establishes a strong foundation for next-generation protocols capable of withstanding both classical and quantum adversaries while maintaining operational efficiency.

Future research can focus on implementing the proposed framework in real-world distributed environments such as IoT networks, cloud platforms, and edge computing systems to evaluate performance under diverse operational conditions. Further optimization of computational and communication overhead can improve suitability for resource-constrained devices. The framework may also be extended by incorporating additional post-quantum algorithms standardized by NIST to enhance cryptographic agility. Integration with emerging technologies such as Software-Defined Networking

(SDN), blockchain, and could further strengthen security. Comprehensive large-scale testing and formal security verification can provide deeper assurance against evolving classical and quantum threats.

REFERENCES

[1] Tran, D.D., Do, C.M., Escobar, S. and Ogata, K. 2023. Hybrid Post-Quantum Transport Layer Security Formal Analysis in Maude-NPA and Its Parallel Version.PeerJ Computer Science, 9: e1556.

[2] Raj, A. and Balachandran, V. 2025. A Hybrid Encryption Framework Combining Classical, Post-Quantum, and QKD Methods.Singapore Institute of Technology.

[3] Choudhary, S. and Gupta, A. 2022. HybridPKE: A Forward-Secure Non-Interactive Quantum-Safe Hybrid Key Exchange Scheme.Engineering Science and Technology, an International Journal, 34: 101094.

[4] Sosnowski, M., Wiedner, F., Hauser, E., Steger, L., Schoinianakis, D., Gallenmüller, S. and Carle, G. 2023. The Performance of Post-Quantum TLS 1.3.Proceedings of the 19th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT Companion).

[5] Battarbee, C., Striecks, C., Perret, L., Ramacher, S. and Verhaeghe, K. 2025. Quantum-Safe Hybrid Key Exchanges with KEM-Based Authentication.EPJ Quantum Technology, 12: 19.

[6] Yoneyama, K. 2019. Post-Quantum Variants of ISO/IEC Standards: Compact Chosen Ciphertext Secure Key Encapsulation Mechanism from Isogeny.Proceedings of the 5th ACM Workshop on Security Standardisation Research (SSR).

[7] Tan, Y.C., Tan, W.X., Bajaj, H.S. and Yap, C.N. 2024. Comparison and Implementation of Key Exchanges to CUDA-Accelerated Arithmetic Circuit Homomorphic Encryption.Proceedings of the 12th International Conference on Information Technology (ICIT).

[8] Singamaneni, K.K. 2025. A Hybrid Cryptographic Framework for Secure Smart Card Financial Transactions.EURASIP Journal on Information Security, 2025: 19.

[9] Zafar, A. and Iqbal, S.S. 2025. Integrating Code-Based Post-Quantum Cryptography into SSL/TLS Protocols through an Interoperable Hybrid Framework.Discover Computing, 28: 202.

[10] Garcia, C.R., Aguilera, A.C., Stan, C., Olmos, J.J.V., Rommel, S. and Monroy, I.T. 2025. Enhanced Network Security Protocols for the Quantum Era – Combining Classical and Post-Quantum Cryptography and Quantum Key Distribution. *IEEE Journal on Selected Areas in Communications*, 43(8): 2765–2781.

[11] Truong, Q.D., Nguyen, H., Nguyen, T.T. and Lee, H. 2026. NIST Post-Quantum Cryptography Standards: A Comprehensive Review of Theoretical Foundations and Implementations.IEEE Access.

[12] Chmielowiec, A., Klich, Ł. and Woś, W. 2024. Energy Efficient ECC Authenticated Key Exchange Protocol for Star Topology Wireless Sensor Networks.Journal of Telecommunications and Information Technology, 1..

[13] Nguyen, H., Huda, S., Nogami, Y. and Nguyen, T.T. 2025. Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms.IEEE Access.

[14] Dekkaki, K.C., Tasic, I. and Cano, M.D. 2024. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process.Technologies, 12(12): 241.

[15] Ramakrishna, D. and Shaik, M.A. 2025. PSESV: A Hybrid Post-Quantum Encryption Framework with Real-Time Thermal and EM Side-Channel Attack Detection.Ain Shams Engineering Journal, 16: 103776.

[16] Buruaga, J.S., Bugler, A., Brito, J.P., Martin, V. and Striecks, C. 2025. Versatile Quantum-Safe Hybrid Key Exchange and Its Application to MACsec. EPJ Quantum Technology, 12: 84.