International Journal of Computer Science Engineering Techniques – Volume 9 Issue 6, November - December - 2025

Hybrid Quantum-Resistant Key Exchange Protocol for Secure Network Communication

Angamuthu G[1], and Marikkannan M[2]
[1]Department of CSE, Government College of Engineering, Erode, TamilNadu,India.
[2]Department of CSE, Government College of Engineering, Erode, India.
[1]angsan444@gmail.com

Abstract - *In the emerging era of quantum computing, traditional cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC) are at risk from quantum-based attacks. These developments pose a significant threat to secure network communication systems that rely on classical key exchange mechanisms. To overcome this challenge, the proposed work introduces a Hybrid Quantum-Resistant Key Exchange Protocol that combines the strengths of both classical and post-quantum cryptographic algorithms. The hybrid approach integrates Elliptic Curve Diffie–Hellman (ECDH) with a lattice-based post-quantum algorithm, Kyber, to establish a shared session key between communicating entities. This shared key is then utilized for symmetric encryption using AES to ensure confidentiality and data integrity. The system is implemented using Python socket programming to demonstrate secure data transmission between client and server. Performance is analyzed in terms of key generation time, encryption and decryption speed, key size, and computational efficiency. The results validate that the proposed hybrid model provides enhanced resistance against quantum attacks while maintaining acceptable performance, making it suitable for future secure communication systems.*

Keywords - *elliptic curve diffie–hellman, hybrid key exchange, kyber, post-quantum cryptography, quantum computing.*

1. Introduction

Quantum computing poses a serious threat to traditional cryptographic systems like RSA and ECDH, as quantum algorithms such as Shor's can easily break them. To counter this, post-quantum cryptographic (PQC) schemes like the lattice-based Kyber have been developed for security against both classical and quantum attacks. This work proposes a hybrid key exchange protocol that combines ECDH and Kyber to enhance security and compatibility. Both parties generate separate classical and PQC key pairs, exchange public keys, derive two shared secrets, and combine them using SHA-256 to form a hybrid session key, which is then used for AES-based encryption. This hybrid approach ensures backward compatibility, forward secrecy, and quantum resistance, making it a practical solution for secure communication in the post-quantum era.

2. Related Study

The emergence of quantum computing and powerful algorithms like Shor's presents a substantial challenge to classical public-key cryptography (PKC), necessitating the adoption of Quantum-Resistant Key Exchange Protocols [1][16]. A robust solution involves Hybrid Quantum-Resistant Key Exchange Protocols, which integrate multiple cryptographic schemes to achieve resilience against both classical and quantum adversaries [14][13]. One fundamental hybrid approach is the KEM-DEM model, where a Post-Quantum Cryptography (PQC) Key Encapsulation Mechanism (KEM) is used to securely exchange a secret key, and an efficient symmetric cipher like AES is used for subsequent data encryption [16]. PQC KEMs like NIST-standardized ML-KEM (Kyber) are built upon complex mathematical problems, such as the Module Learning with Errors (MLWE) problem over lattices, assumed to be secure even against quantum computers. Related studies have actively explored combining these primitives for constrained environments - for instance, one article proposed a hybrid cryptographic framework integrating Kyber-512 for quantum-resistant key generation with the lightweight authenticated encryption cipher ASCON for efficient data transmission in IoT networks [12].

This particular hybrid model demonstrated improved performance efficiency compared to using Kyber alone [12]. Furthermore, advanced network protocols aim for heightened crypto-agility through triple-hybrid solutions [1]. These mechanisms combine keys generated from classical algorithms (e.g., ECDH), PQC algorithms, and Quantum Key Distribution (QKD) [1]. Such robust triple-hybrid protocols enhance existing systems like TLS 1.3 and IPsec, providing layered security backed by three independent cryptographic assumptions to mitigate vulnerabilities, and offering a future-proof defense against imminent threats such as "harvest now, decrypt later" (HNDL) [1]. The overarching purpose of these hybrid mechanisms is to balance strong quantum security with the practical demands of low computational overhead and energy efficiency in modern network communication systems [1].

2.1. Quantum Computing

The development of quantum computing poses a fundamental threat to the cryptographic security mechanisms currently employed in network communications. Quantum computing is advancing rapidly, using the laws of quantum physics to enable extremely complex tasks in a fraction of the time required by conventional computers [16]. The greatest threat stems from powerful quantum algorithms, primarily Shor's algorithm, which can solve complex mathematical problems underlying traditional cryptographic protocols, such as integer factorization (used in RSA) and discrete logarithms (used in ECC/ECDH), in polynomial time [16].This capability fundamentally compromises the security of current public-key cryptosystems [12].Additionally, Grover's algorithm offers a quadratic speedup for brute-force searches

to find encryption keys, reducing the operations required to break a 128-bit key from approximately 2^{128} to 2^{64}[9].This superiority of quantum computers over classical ones highlights the imminent danger of losing data confidentiality, including the risk of "harvest now, decrypt later" (HNDL) attacks, where encrypted data is collected today to be decrypted later when capable quantum computers are available [1].

2.2. Post Quantum Cryptography

Post-Quantum Cryptography (PQC) has emerged as the essential countermeasure, consisting of advanced algorithms designed to resist attacks from quantum computers while remaining secure on classical hardware [16]. The core of PQC relies on complex mathematical problems that are currently assumed to be difficult to solve even with quantum capabilities, particularly lattice-based cryptography [16]. which derives its security from the difficulty of solving problems like the Learning with Errors (LWE) and Shortest Vector Problem (SVP) [16]. To secure key exchange, PQC primarily utilizes Key Encapsulation Mechanisms (KEMs) [4][12]. such as CRYSTALS-Kyber (now standardized by NIST as ML-KEM) and NTRU. These KEMs allow two parties to securely establish a shared secret key, which can then be combined with efficient symmetric algorithms like AES in a hybrid cryptosystem (KEM-DEM) for data encryption [15]. Because many real-world applications, such as IoT devices and 5G mobile equipment, operate with strict constraints on computational power, energy efficiency, and memory, a significant focus of PQC research is optimizing algorithms like Kyber-512 to ensure performance gains and efficiency even against pre-quantum equivalents [4].

2.3. Secured Key Exchange in ECC and Diffie-Hellman

The Diffie–Hellman concept introduced the use of public and private keys in cryptography [13][2], leading to Elliptic Curve Cryptography (ECC), a modern public-key system based on elliptic curves over finite fields [3]. ECC's security relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it computationally infeasible to derive the private key from public parameters [7]. Offering equivalent security to RSA with smaller key sizes, ECC reduces computational cost, memory, and power usage, making it ideal for IoT and WSNs [3][10]. However, quantum algorithms like Shor's can break ECC's security, making it vulnerable to quantum attacks [14].The Elliptic Curve Diffie–Hellman (ECDH) Key Exchange protocol, a variant of the traditional Diffie–Hellman scheme, is valued for its strong security and computational efficiency [12].

In ECDH, two parties (Alice and Bob) establish a shared secret over an insecure channel using elliptic curve point multiplication properties [12]. Both agree on domain parameters and a generator point G [13]; Alice selects a private key dA and computes QA=dA×G, while Bob selects dB and computes QB=dB×G [3]. After exchanging public keys, each computes the shared secret—Alice as SA=dA×QB and Bob as SB=dB×QA—which are mathematically identical since SA=dA×(dB×G)=SB=dB×(dA×G) [15]. The protocol's security relies on the difficulty of the Computational Elliptic Curve Diffie–Hellman Problem (ECDHP), ensuring that an attacker intercepting QA and QB cannot feasibly derive the shared secret without solving the ECDLP [7].

2.4. Improved Key Exchange in ECDH

Classical public-key systems like ECC face vulnerabilities to quantum algorithms such as Shor's and are unsuitable for resource-constrained IoT devices [13]. These issues are addressed through Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEMs) like ML-KEM (Kyber) and NTRU, based on hard lattice problems such as MLWE and SVP, making them resistant to quantum attacks [4]. To reduce PQC's computational overhead, hybrid cryptosystems (KEM-DEM) combine PQC for key exchange with lightweight symmetric ciphers like ASCON for efficient bulk encryption [7]. Further performance gains for high-throughput systems are achieved through hardware optimizations like parallel processing and pipelining of SHA-3, sampling, and NTT in Kyber [10]. For maximum security and crypto-agility, triple-hybrid protocols integrate classical, PQC (ML-KEM), and Quantum Key Distribution (QKD) keys to resist simultaneous attacks on all three systems [14].

2.5. Post Quantum Key Exchange

Post-Quantum Cryptography (PQC) key exchange relies fundamentally on Key Encapsulation Mechanisms (KEMs) to securely establish shared secrets between two parties, providing resilience against quantum threats that compromise classical public-key cryptography (PKC)[13]. This mechanism is based on mathematically hard problems in lattice-based cryptography, such as the Module Learning with Errors (MLWE) problem, which forms the foundation for standardized algorithms like CRYSTALS-Kyber (ML-KEM) and NTRU [5]. The PQC KEM process operates in three distinct stages [3].

First, Key Generation (KEM.KeyGen), where the receiving party produces a public–private key pair. The public key is distributed openly, while the private key (secret key) remains confidential [3][12].

Second, Encapsulation (KEM.Encapsulate), where the sender uses the receiver's public key to generate a random symmetric key (the shared secret) and then encapsulates this key into a ciphertext which is transmitted across the insecure channel [3].

Third, Encapsulation (KEM.Decapsulate), where the recipient uses their private key to successfully retrieve the original symmetric key from the received ciphertext [4]. Once this shared symmetric key is established in a quantum-

resistant manner, it is subsequently used with an efficient symmetric algorithm, such as AES or ASCON, for fast data encryption and decryption [2]. This architecture, often called a hybrid cryptosystem or KEM-DEM, combines the quantum-resistant security of the PQC key exchange with the computational efficiency of symmetric encryption for secure network communication [2].

2.6. Achieving balanced computational efficiency in hybrid PQC–classical key exchange

Achieving balanced computational efficiency in hybrid Post-Quantum Cryptography (PQC)–classical key exchange is critical, particularly for resource-constrained environments like IoT devices, while ensuring quantum resistance [13]. The goal is to maximize the robust security offered by PQC algorithms against quantum adversaries without incurring the excessive computational overhead traditionally associated with them [2].

This balance is achieved by strategically combining the quantum-resistant key establishment phase with the efficient classical/lightweight symmetric encryption phase, forming a hybrid cryptosystem or KEM-DEM (Key Encapsulation Mechanism–Data Encapsulation Method) [5][6]. In this model, the PQC algorithm (like Kyber-512) is only responsible for the key exchange, which is computationally heavy but infrequent, while a highly efficient lightweight symmetric cipher (like ASCON) handles the bulk of the data encryption/decryption [6][7]. This methodology ensures that the intensive PQC key generation steps have minimal long-term impact on overall system performance [4][7].

2.6.1. Important Parameters in Hybrid Key Exchange

Several parameters play crucial roles in determining the computational efficiency and overall security trade-off in a hybrid PQC

Computational Performance Metrics

These parameters directly measure the cost and speed of executing the cryptographic operations, especially on resource-constrained devices (e.g., IoT, 5G UE) [2].

- **Execution Speed / Computational Time -** these measures the time required to perform the core operations - key generation, encapsulation, and decapsulation (for PQC KEM) [9]. For instance, comparative studies show that Kyber-512 has faster key generation and shared key generation times than classical ciphers like X25519 and secp256r1 on constrained devices. In a hybrid Kyber-ASCON system, the encryption time was approximately 43 ms[14].
- **CPU Utilization / Cycle Count -** Lower CPU cycle counts and moderate CPU usage indicate higher efficiency, helping conserve battery life on mobile devices. In one study, the hybrid scheme averaged moderate CPU usage of 21.624% [8].
- **Energy Consumption / Power Consumption -** This is critical for battery-powered devices. The goal is to minimize energy usage during the cryptographic procedures. One study found that the PQC KEM Kyber-512 was significantly more energy efficient (lower mWh consumption) than pre-quantum equivalents due to its faster execution time. The hybrid Kyber-ASCON scheme showed power consumption of approximately 20.76 W [16].

Resource Constraints and Overheads

These metrics quantify the hardware demands of the hybrid implementation [3] -

- **Memory Usage (RAM/Storage) -** The peak RAM consumption during cryptographic operations is vital for devices with limited resources [9]. Hybrid PQC key material (public keys and ciphertexts) often results in larger sizes compared to ECC keys, requiring careful memory management [13]. However, the hybrid Kyber-ASCON framework achieved minimal memory usage, averaging 2.56 KB during encryption [15].
- **Bandwidth Efficiency (Key and Ciphertext Sizes)** This metric evaluates the size of data transmitted over the network (e.g., public keys and ciphertexts). PQC algorithms typically require substantially larger key exchange payloads than classical cryptography [2]. For example, Kyber-512 outputs a larger ciphertext and public key (approximately 1568 bytes total) than NTRU509 (approximately 1398 bytes total), directly impacting transmission delay and bandwidth usage [14].

Security and Hybrid Architecture

These parameters ensure the resilience and effectiveness of the hybrid approach -

- **PQC Algorithm Security Level -** The chosen PQC algorithm (e.g., Kyber-512, Kyber-768, or ML-KEM-1024) must provide sufficient security against known quantum attacks, typically targeting 128-bit or higher classical security equivalent [4]. Kyber-512 is frequently chosen for constrained devices because it offers an optimal balance between security (128-bit equivalent) and efficiency [6].
- **Combination Strategy (Concatenation vs. Cascade) -** In network protocols like TLS and IPsec, the method used to mix the classical key material (e.g., ECDHE) and the PQC key material (e.g., ML-KEM) determines the resulting security and complexity. The concatenation approach simply aggregates the secrets, while the cascade approach

iteratively updates the secret, relying on the cryptographic robustness of the key derivation function (e.g., HKDF).

- **Side-Channel Attack (SCA) Resistance -** Although hybrid systems offer mathematical security, real-world efficiency must be balanced with resistance to SCAs (timing, power analysis) [9]. Improved key mechanisms must integrate countermeasures like masking, constant-time algorithms, or clock randomization, which often introduce slight computational overhead but are necessary for secure deployment [12].

2.7. Vulnerabilities Attack Analysis and Mitigation in Kyber

The core vulnerability of CRYSTALS-Kyber, despite its theoretical quantum resistance rooted in the hardness of the Module Learning with Errors (MLWE) problem [13]. lies primarily in Side-Channel Attacks (SCAs) on its physical implementation [5]. Attack analysis shows that sophisticated techniques, including deep learning-based side-channel analysis and power analysis, have been successfully employed to compromise even masked or shuffled software implementations of Kyber [6]. Specific Kyber vulnerabilities include leakage during the decryption mechanism, flaws in the Barrett reduction used during decapsulation, and leakage during the message encoding/decoding or Inverse Number Theoretic Transform (INTT) operations [12][15]. Attackers often utilize specially crafted chosen ciphertexts to magnify these leakages, enabling the real-time recovery of the entire secret key with a minimal number of queries or traces. Mitigation strategies to overcome these implementation flaws include utilizing masking techniques (splitting secrets into randomized shares), employing shuffling, enforcing constant-time scheduling for sensitive operations like butterfly computations, integrating randomized clocks, and implementing duplication of cryptographic cores. The standardizing body, NIST, recognized these SCA threats, prompting ongoing research to continually evaluate and enhance the security of Kyber implementations [2].

2.8. Existing Challenges

2.8.1. Complexity of Hybrid Key Exchange Integration

Implementing a hybrid quantum-resistant key exchange protocol combining classical algorithms like ECDH with post-quantum schemes such as Kyber is technically complex. The main challenge lies in securely combining the outputs of both algorithms using a Key Derivation Function (KDF) (e.g., HKDF or SHA-3). Improper mixing or naive concatenation could weaken overall security by allowing one algorithm's weakness to affect the hybrid protocol [13].

2.8.2. Threats from Quantum Computing

With advancements in quantum computing, especially Shor's algorithm, classical cryptosystems like RSA and ECC—based on integer factorization and discrete logarithm problems—are at risk [13]. To counter this, Post-Quantum Cryptography (PQC) introduces algorithms designed to remain secure against both classical and quantum attacks [2].

2.8.3. Role of Post-Quantum Key Encapsulation Mechanisms (KEMs)

In PQC, Key Encapsulation Mechanisms (KEMs) play a vital role in securing communications for VPNs and secure messaging [5]. The lattice-based schemes—CRYSTALS-Kyber and NTRU—have been selected by NIST for standardization.Kyber relies on the Module Learning with Errors (MLWE) problem.NTRU uses polynomial rings and ideal lattices [7].

The PQC key establishment process includes Key Generation, Encapsulation, and Decapsulation [6].

2.8.4.Hybrid Frameworks for Resource-Constrained Environments

Integrating PQC into IoT and embedded systems demands protocols that balance security, computation, and energy efficiency [11].A KEM-DEM hybrid approach—for instance, using Kyber-512 for key generation and ASCON for lightweight encryption—achieves low memory usage (≈2.56 KB) and moderate CPU utilization (≈21.6%), making it ideal for IoT devices [12][14].

2.8.5. Hardware and Performance Optimization

For cloud-scale and high-throughput systems, PQC performance improves through hardware-level parallelism. Techniques like parallel SHA-3 hashing, optimized sampling, and Number Theoretic Transform (NTT) pipelining can yield up to 23% faster key generation and throughput of 877.192 kOPS [15][16].

2.8.6. Security Vulnerabilities in PQC Implementations

Despite strong theoretical security, PQC implementations such as CRYSTALS-Kyber are vulnerable to Side-Channel Attacks (SCAs), exploiting leaks during decryption or verification [16][2].Common attack targets include the Barrett reduction and re-encryption steps in decapsulation, sometimes enhanced by deep-learning-based power analysis [3].Countermeasures like masking (randomized secret sharing) and shuffling are necessary to mitigate such risks [7].

2.8.7. *Triple-Hybrid Quantum-Resilient Protocols*

To defend against "harvest now, decrypt later (HNDL)" quantum threats, triple-hybrid protocols have been proposed. These combine -

- Classical Cryptography (ECDHE)

- Post-Quantum Cryptography (ML-KEM-1024)
- Quantum Key Distribution (QKD) [8][9]

Such architectures ensure three independent security assumptions must be broken, creating defense-in-depth [10][11].Incorporation into standards like TLS 1.3 and IPsec uses a Quantum Handshake Secret (QHS)—formed by concatenating all shared secrets—before final key derivation via HKDF [12].

3. Protocols for the Proposed System

3.1. Coherent One-Way (COW)

The Coherent One-Way (COW) protocol is a specific type of Quantum Key Distribution (QKD) protocol.

• **Mechanism -** The COW protocol operates by encoding information into coherent pulses of light. These pulses are sent over an optical fiber.

• **Purpose/Security -** It relies on the principles of quantum mechanics to achieve security. The COW protocol is part of the DV-QKD (Discrete Variable QKD) family.

• **Deployment -** The COW protocol is specifically noted as being used in the ID Quantique Clavis3 equipment integrated into an experimental QKD testbed[13][2].

3.2. Post-Quantum Key Exchange Protocols (KEMs)

These protocols are the main focus of quantum-resistant security and are used to securely exchange a secret key [3][4].

• **CRYSTALS-Kyber (or ML-KEM) -** This is the NIST-standardized PKE/KEM algorithm chosen for its security based on the Module Learning with Errors (MLWE) problem over lattices [5]. It is frequently used or proposed for key exchange in environments like IoT, 5G SUCI calculation, TLS 1.3, IPsec, and hybrid frameworks. Kyber has multiple security variants, including Kyber-512 (Level 1 security, typically targeted for resource-constrained devices) and Kyber-1024 (Level 5 security) [6].

• **NTRU -** An early lattice-based encryption scheme that is also a PQC KEM candidate chosen by NIST. NTRU's security is derived from polynomial rings and ideal lattices, relying on the Shortest Vector Problem (SVP). Variants include NTRU HPS 509 (NTRU509), favoured for its small public key and ciphertext sizes, making it ideal for bandwidth-constrained environments [10].

• **CRYSTALS-Dilithium (or ML-DSA) -** This is the NIST-standardized lattice-based digital signature scheme. It is used for authentication (digital signatures) in protocols like TLS 1.3 (ML-DSA-65) and IPsec [13].

• **Supersingular Isogeny Diffie–Hellman (SIDH) -** This is a key exchange protocol that relies on the difficulty of finding isogenies between supersingular elliptic curves. A variant, the extended SIDH (eSIDH), was proposed to accelerate computations, particularly on multicore platforms. The related Supersingular Isogeny Key Encapsulation (SIKE) protocol is a descendant of SIDH [2].

• **Other PQC Candidates/Protocols -** The sources also mention SPHINCS+ and FALCON (both digital signature schemes), BIKE (code-based KEM), HQC (code-based KEM), FrodoKEM (ringless LWE KEM), and Saber (Module-LWR KEM) [8].

3.3. Classical Key Exchange and Authentication Protocols

These established cryptographic methods are primarily used in current systems but are vulnerable to quantum computers -

• **Elliptic Curve Diffie–Hellman (ECDH) -** A key exchange algorithm used to securely establish a shared secret based on the difficulty of the discrete logarithm problem over elliptic curves (ECDLP). Specific implementations mentioned include X25519 (a Montgomery curve widely used for efficiency and speed) and secp256r1 (NIST P-256) (a Weierstrass curve). Both X25519 and secp256r1 are used in the existing 5G-AKA SUCI (Subscriber Concealed Identifier) identification phase [13].

• **Elliptic Curve Cryptography (ECC) -** The general system of public-key cryptography based on elliptic curves [2].

• **ECDH with Digital Signatures -** Protocols extending ECDH to include authentication, such as the CL-PKI (certificate-less Public Key Infrastructure) protocol, which uses ECDH key agreement with ECDSA (Elliptic Curve Digital Signature Algorithm) authentication [13].

• **STAKE (Star Topology Authenticated Key Exchange) -**A new energy-efficient ECC-based authenticated key exchange protocol designed specifically for star topology wireless sensor networks [5].

• **RSA -** Mentioned as a classical PKC algorithm vulnerable to Shor's algorithm, typically used for key negotiation [16].

• **AES-256-GCM and ChaCha20-Poly1305 -** These are high-security symmetric encryption algorithms considered quantum-resistant if key size is sufficient, and they are used for data encryption after the key is established via key exchange protocols [5].

• **ASCON -** A lightweight authenticated encryption (AEAD) method and cipher suite, optimized for resource-constrained devices, often integrated into hybrid frameworks for efficient data encryption [6].

3.4. Hybrid and Network Protocols

These protocols specify how various cryptographic schemes are combined and implemented within network security layers -

• **Triple-Hybrid Protocols -** Solutions that combine three independent cryptographic assumptions - classical cryptography (e.g., ECDHE/X25519), PQC (e.g., ML-KEM/Kyber), and QKD (e.g., COW) to achieve enhanced quantum-resilient defense-in-depth [7].

• **TLS 1.3 -** A network security protocol where hybrid and triple-hybrid solutions are implemented for key exchange and authentication [9].

• **IPsec/IKEv2 -** The security protocol backbone for VPNs, where IKEv2 (Internet Key Exchange Protocol Version 2) is modified using RFC 9370 to integrate hybrid PQC and QKD key exchanges [9].

3.5. Parameter Based Protocol Selection

The determination of the "best" protocol for a hybrid quantum-resistant key exchange depends on balancing the need for robust post-quantum security with the crucial requirements of computational efficiency and performance in network communication. Based on the sources, protocols featuring Kyber (ML-KEM) demonstrate the strongest combination of efficiency and security, particularly when optimized for resource-constrained environments.

Kyber-512 as the Core PQC Primitive for Hybrid Efficiency

The most compelling protocol for achieving a balance of security and improved performance in resource-constrained environments (like IoT and mobile devices) is Kyber-512 when integrated into a hybrid architecture [13][2].

3.5.1. Performance Superiority over Classical and PQC Alternatives

Kyber-512 is recognized for its operational efficiency, often showing better performance metrics than classical pre-quantum ciphers (ECDH) and other PQC competitors (NTRU), making it ideal for the computationally intensive key exchange phase [2][3].

Classical Comparison - Kyber-512 exhibited faster computations and lower energy consumption than classical elliptic curve algorithms X25519 and secp256r1 when tested on constrained devices like Raspberry Pi and Mini-PC. For example, Kyber-512 was found to be approximately 82.4% faster than secp256r1 in public key generation at the Core Network (CN) side [7].

PQC Comparison (NTRU) - Kyber-512 consistently maintained a lower cumulative execution time and better performance across three critical metrics—execution speed, memory usage, and power consumption—compared to NTRU509, especially on IoT devices. For instance, on the Raspberry Pi, Kyber-512's key generation time was significantly faster (less than 100 µs) compared to NTRU509 (more than 600 µs), indicating less computational overhead [11][12].

3.5.2. Security and Efficiency Trade-Offs -

The key benefit of using Kyber is that it is a NIST-standardized KEM (ML-KEM) based on the Module Learning with Errors (MLWE) problem, ensuring post-quantum security against Shor's algorithm, specifically achieving approximately 128-bit classical security equivalent at the Kyber-512 level [13]. However, PQC introduces significant byte overhead due to larger public key and ciphertext sizes compared to ECC, where NTRU509 offers a slight advantage in bandwidth efficiency (1398 bytes total vs. 1568 bytes for Kyber-512) for limited-bandwidth scenarios like satellite communications [8].

Optimal Hybrid Strategy - Kyber-512 and ASCON (KEM-DEM)

For scenarios emphasizing lightweight performance and energy efficiency (e.g., IoT and embedded systems), the hybrid combination of Kyber-512 for key exchange and ASCON for symmetric data encryption provides superior overall efficiency and robust security [15]. This hybrid cryptosystem (KEM-DEM) leverages the strengths of both protocols

Mechanism - Kyber-512 performs the resource-intensive but infrequent secure key generation (Key Encapsulation Mechanism), while the lightweight ASCON (Authenticated Encryption method) handles the actual data encryption and decryption quickly and efficiently [15].

Performance Improvement - This hybrid framework demonstrated optimal performance results for constrained devices, including a fast encryption time of 43 ms (significantly lower than Kyber alone at 135 ms), minimal memory usage (2.56 KB), and moderate CPU usage (21.624%). The lightweight nature of ASCON significantly mitigates the computational expense incurred by Kyber-512's polynomial arithmetic [4].

Highest Security Option - Triple-Hybrid Protocols

For environments where the highest level of assurance is prioritized, such as network backbones (TLS 1.3, IPsec, VPNs), the most secure strategy involves triple-hybrid protocols, which combine three cryptographic assumptions - Classical ECDH/X25519, a PQC KEM (ML-KEM-1024), and Quantum Key Distribution (QKD)[7]. This provides quantum-resilient defense-in-depth, ensuring that three independent cryptographic assumptions must be broken before the protocol becomes vulnerable. While this offers the maximum security against both classical and quantum attacks, it introduces increased latency (approximately 48 ms overhead in a real-world TLS 1.3 implementation) primarily due to the QKD key retrieval procedure [11].

4. Key Exchange Mechanism

4.1. Classical Key Exchange Mechanisms

Classical key exchange protocols, such as Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH), allow two parties to securely establish a shared secret using discrete logarithms or elliptic curve mathematics. While efficient and widely used in TLS, VPNs, and IoT systems, they are vulnerable to quantum attacks, as quantum computers can efficiently solve the underlying mathematical problems [1].

4.1.1. Diffie-Hellman (DH)

Diffie-Hellman (DH) is one of the earliest public-key cryptography protocols that enable two parties to securely derive a shared secret over an insecure channel. It relies on the mathematical difficulty of solving discrete logarithms, ensuring that an eavesdropper cannot easily compute the shared key from intercepted messages. Despite its foundational role in cryptography, DH is vulnerable to quantum attacks, as quantum computers could efficiently solve discrete logarithms using Shor's algorithm [5].

4.1.2. Elliptic Curve Diffie-Hellman (ECDH)

Elliptic Curve Diffie-Hellman (ECDH) is a more efficient variant of DH, leveraging elliptic curve mathematics to achieve equivalent security with smaller key sizes. This makes it faster and more suitable for modern applications such as TLS, VPNs, and IoT devices. While ECDH maintains the classical security benefits of DH, it still suffers from quantum vulnerability; meaning that future quantum computers could compromise keys generated using this algorithm. Nevertheless, ECDH remains widely deployed due to its efficiency and compact key representation [7].

4.2. Post-Quantum Key Exchange Mechanisms

Post-quantum key exchange algorithms, such as CRYSTALS-Kyber, NTRU, and SABER, are designed to resist quantum attacks by using lattice-based cryptography. They provide secure session key generation even in the presence of quantum adversaries but involve larger key sizes and higher computational requirements than classical methods [15].

To address the threat posed by quantum computers, post-quantum cryptography (PQC) key exchange mechanisms have been developed. CRYSTALS- Kyber is a lattice-based Key Encapsulation Mechanism (KEM) selected by NIST as a standard for PQC. It allows secure derivation of session keys resistant to quantum attacks and is practical for modern protocols like TLS 1.3 and VPNs. Its main limitation is the larger key sizes and higher computational requirements compared to classical algorithms [10].

Other post-quantum schemes include NTRU and SABER, which are lattice-based KEX protocols optimized for efficiency and low-resource environments. NTRU offers fast key generation and encryption, while SABER provides smaller cipher texts and faster computation suitable for IoT and embedded systems. These PQC algorithms are designed to maintain security in a quantum computing era, though the increased resource demands must be considered in constrained deployments [16].

4.3. Hybrid Key Exchange Mechanisms

4.3.1. Classical Component

The first stage of a hybrid key exchange involves the classical algorithm, typically Elliptic Curve Diffie-Hellman (ECDH). In this stage, both parties generate their ephemeral elliptic curve key pairs and exchange public keys over the network. Using the received public key and their own private key, each party computes a shared secret. This classical component ensures forward secrecy and maintains compatibility with existing network protocols, forming the foundational security layer of the hybrid mechanism [1].

4.3.2. Post-Quantum Component

The second stage incorporates a post-quantum algorithm such as Kyber or NTRU, which is resistant to quantum attacks. Both parties generate post-quantum key pairs or cipher texts and exchange them securely. Each party then derives a shared secret using the post-quantum algorithm. This stage adds quantum-resistant security to the protocol, ensuring that even if quantum computers become capable of breaking classical schemes, the session key remains secure [10].

4.3.3. Key Combination and Final Session Key

In the final stage, the outputs from the classical and post-quantum stages are combined securely to produce the final hybrid session key. Typically, a Key Derivation Function (KDF) such as HKDF or SHA-3 is used to merge both secrets into a single robust session key. This hybrid key inherits forward secrecy from the classical algorithm and quantum resistance from the post-quantum component, offering a future-proof, practical solution for secure communications. Protocols like CECPQ2, OQS Hybrid TLS, and IETF hybrid TLS drafts implement this stage-wise approach to ensure strong security without compromising performance or compatibility [13].

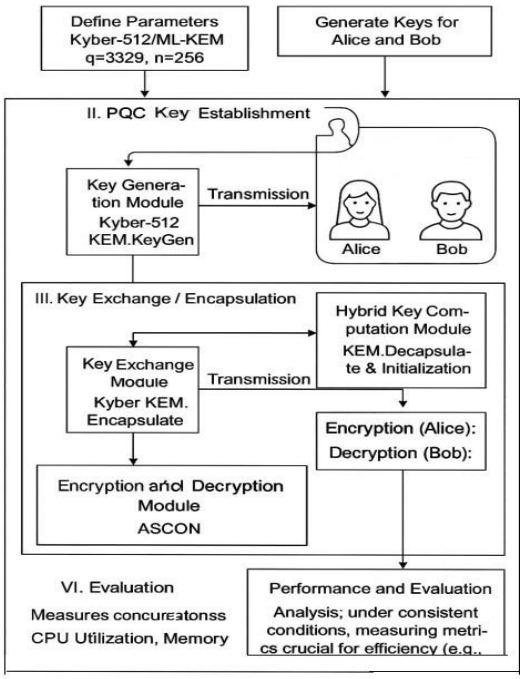

Fig.1. System Architecture

In the **Fig.1.** The architecture illustrates a hybrid post-quantum cryptographic framework combining Kyber-512 (ML-KEM) for secure key establishment for lightweight encryption–decryption, ensuring efficient and quantum-resistant communication between Alice and Bob.This hybrid key inherits forward secrecy from the classical algorithm and quantum resistance from the post-quantum component, offering a future-proof, practical solution for secure communications.

5. Functions of Key Generation and Exchange

5.1. Setup Phase - Generate Keys for Alice and Bob

Parties agree on Kyber-512/ML-KEM parameters, such as prime modulus q=3329 and polynomial degree n=256[6].

5.2. PQC Key Establishment -

Bob (Receiver) generates the quantum-resistant Public Key (pk_{Bob}) and Secret Key (sk_{Bob}).

Bob securely transmits pk Bob to Alice.

5.3. Key Exchange / Encapsulation -

- Alice Encapsulates Key - Alice (Sender) uses pkBob to generate a random Shared Symmetric Key (K) and its corresponding Ciphertext (ct) [15].
- Transmission - Alice sends ct to Bob.

5.4. Key Derivation - Hybrid Key Computation Module (KEM.Decapsulate& Initialization)

- Bob Decapsulates Key - Bob uses his skBob and the received ct to recover the Shared Symmetric Key (K).
- Hybrid Initialization - K (the PQC-derived secret) and a Nonce are used to initialize the ASCON State for authenticated encryption, establishing the hybrid link [15].

5.5. Data Communication - Encryption and Decryption Module (ASCON)

- Encryption (Alice) - ASCON (a lightweight authenticated cipher) uses the initialized state and K to encrypt the Plaintext (M), producing the final Ciphertext (C)[16].
- Decryption (Bob) - Bob uses the same shared key K and state initialization to perform ASCON Decryption to recover the Plaintext (M)[15].

5.6. Evaluation - Performance and Evaluation Module

- Analysis - The hybrid system is evaluated under consistent conditions, measuring metrics crucial for efficiency (e.g., CPU Utilization, Memory Usage, Power Consumption, and Encryption Time). This confirms the suitability of the hybrid scheme for resource-constrained devices [5].

6. Results and Discussions

6.1 Integration of PQC with Lightweight Ciphers

Show that combining CRYSTALS-Kyber (ML-KEM) with lightweight symmetric ciphers such as ASCON in a KEM–DEM design reduces computational overhead while preserving quantum resistance. Reported performance figures include CPU utilization ≈ 21.624 % and memory usage ≈ 2.56 KB for the Kyber-512 + ASCON configuration [9][13]. These results substantiate the design choice in this paper to pair a PQC KEM with a lightweight AEAD cipher: the empirical evidence indicates the hybrid approach is practical for battery- and memory-constrained devices and thus appropriate as the baseline for our Python prototype and future embedded implementations.

6.2 Performance in Resource-Constrained and 5G Systems

Comparative evaluations demonstrate that Kyber-512 can achieve superior key-generation speed and energy efficiency on constrained hardware relative to classical elliptic-curve schemes such as X25519 and secp256r1 [12]. The author interprets these findings to mean that adopting a Kyber-based hybrid in 5G UE and IoT scenarios is not only secure but may offer performance advantages; thus, the proposed ECDH–Kyber hybrid is justified for mobile system integration and provides a feasible upgrade path from current ECC-based deployments.

6.3 High-Throughput and Cloud-Scale Optimization

Hardware-centric optimizations (parallel SHA-3, efficient sampling, NTT pipelining) applied to Kyber produced notable throughput and latency gains e.g., a ~23% reduction in computation latency and 877.192 kOPS aggregate throughput on TSMC 40 nm platforms (Chou et al. [15]). The author concludes that while the current work targets software-level proof-of-concept, these hardware results indicate scalability: the hybrid protocol presented here can be adapted for cloud/data-center deployments given proper architectural support and scheduling.

6.4 Triple-Hybrid Protocol Evaluation and Latency Trade-offs

Triple-hybrid constructions (classical ECDHE/X25519 + ML-KEM + QKD) have been integrated into TLS/IPsec prototypes with modest computational overhead (≈ 3 ms in IKEv2) but with non-trivial QKD retrieval latency (≈ 57 ms per session) due to key-management operations [1][2]. The author's assessment is that triple-hybrid approaches provide highly desirable defense-in-depth for critical backbones, but practical adoption requires network-level optimizations (e.g., caching, asynchronous QKD key staging) to mitigate session latency in interactive applications.

6.5 Security and Implementation Concerns (Side-Channel Attacks)

Implementation-level analyses reveal that CRYSTALS-Kyber can leak sensitive information through Side-Channel Attacks (SCAs), notably during decapsulation, Barrett reduction, and INTT computations; advanced attacks (including deep-learning–assisted power analysis) have succeeded against partially protected implementations [12][4]. From the author's viewpoint, this underscores two points for the proposed architecture: (1) software-only hybrid implementations must follow constant-time coding practices and avoid naïve optimizations that introduce timing/power leakage; and (2) future work should evaluate hardware-assisted countermeasures (masking, shuffling, randomized clocks) before deployment in adversarial environments.

6.6 Network Overhead and Packet Size Impact

PQC public-key and ciphertext sizes increase packet payloads (e.g., Kyber-512 output ≈ 847 bytes in a 5G SUCI context vs. ≈ 111–112 bytes for classical ECC) which affect bandwidth and latency [16]. In the author's view, this overhead is an acceptable trade-off for quantum resistance when mitigated by practical measures: session resumption reduced key exchange frequency, and compression/aggregation where applicable. The proposed hybrid scheme therefore recommends operational strategies (e.g., longer-lived session keys with periodic rekeying) to minimize the transmission cost.

6.7 Consolidated Observations

Synthesizing the referenced findings, the author draws the following evidence-based conclusions relevant to the proposed hybrid model Feasibility for constrained devices Kyber-512 + ASCON provides acceptable CPU and memory footprints for IoT-scale systems [13].
Energy and latency advantages: PQC KEMs can be competitive or superior to ECC for key generation on constrained hardware [12].Scalability with hardware support: Architectural scheduling enables Kyber to meet cloud-scale throughput requirements [15].Security caveats: Side-channel resistance must be explicitly engineered into implementations [12][4].Deployment trade-offs: Larger key sizes and QKD retrieval latencies require network-level mitigation strategies [2][16].

7. Conclusion

The implementation of Hybrid Quantum-Resistant Key Exchange Protocols shows that strong quantum security can be achieved with practical performance, even on limited devices. For constrained IoT systems, combining Kyber-512 KEM with the ECDH provides an optimal balance Kyber handles secure key establishment while ECHD manages frequent encryption efficiently, achieving 43 ms encryption time, and 2.56 KB memory usage, and 21.624% CPU utilization, ideal for real-time, low-power applications. In high-throughput environments like cloud servers, hardware optimization through parallelization and pipelining of SHA-3, sampling, and NTT operations improves performance by reducing latency by 23% and reaching up to 877.192 kOPS, demonstrating Kyber's scalability and efficiency.

However, practical hybrid deployments face challenges from Side-Channel Attacks (SCAs), as Kyber implementations can leak information during decapsulation and Barrett reduction, allowing attackers to infer secret keys even under basic masking protections. Future work should integrate advanced SCA and fault injection countermeasures into hardware architectures. Additionally, research must enhance higher PQC levels (Kyber-768, Kyber-1024) and integrate Quantum Key Distribution (QKD) into fast protocols like TLS and IPsec to minimize latency and achieve seamless, quantum-secure communication.

References

[1] Carlos Rubio García, Abraham Cano Aguilera, Catalina Stan, Juan José Vegas Olmos, Simon Rommel, Idelfonso Tafur Monroy. "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, IEEE. vol. 43, No.8, pp. 2765-2781, 2025.

[2] Hien Nguyen, Samsul Huda, Yasuyuki Nogami, Tuy Tan Nguyen. "Security in Post-Quantum Era - A Comprehensive Survey on Lattice-Based Algorithms". IEEE Access. vol. 43, No.17, pp. 2765-2781, 2025.

[3] Andrzej Chmielowiec, Leszek Klich, and Weronika Woś. "Energy Efficient ECC Authenticated Key Exchange Protocol for Star Topology Wireless Sensor Networks. Journal Of Telecommunications and Information Technology". vol. 43, No.15, pp. 1-9, 2024.

[4] Jiongen Xiao, Yi Liu, Yi Zou, Dacheng Li,Tao Leng. "An Efficient Elliptic Curve Cryptography-Based Secure Communication with Privacy Preserving for Autonomous Vehicle". Journal of Advanced Transportation. vol. 43, No.3, pp. 2765-2781, 2024.

[5] Daniel Cervantes Vázquez, Eduardo Ochoa-Jiménez, Francisco Rodríguez Henríquez. "Extended super singular isogeny Diffie–Hellman key exchange protocol - Revenge of the SIDH". IET Information Security. vol. 15, No.12, pp. 364-374, 2021.

[6] Tanksale, V. Efficient. "Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices". Electronics, MDPI. vol. 13, No.4, pp. 3631-3645, 2024.

[7] Sina Baghbanijam, Hanie Sanaei, Mahdi Farajzadeh. "An Improved Authentication & Key Exchange Protocol Based on ECDH for WSNs". vol. 43, No.5, pp. 2765-2781,2025.

[8] Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschädl, Alexander Szekely, Stefan Tillich. "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks. Lecture Notes in Computer Science", Springer. vol. 57, No.46, pp. 112-127, 2009.

[9] Khan Q, Purification S, Chang S.Y. "Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber)". MDPI. vol. 16, No.13, pp. 617, 2025.

[10] EhsanM.A,AlayedW,Rehman A.U, HassanWU, ZeeshanA. "Post-Quantum KEMs for IoT - A Study of Kyber and NTRU". Symmetry, MDPI. vol. 17, No.11, pp. 881, 2025. 17.

[11] ChouS.H, YangY.H, ChinW.L, ChenC, TsaoC.Y, TungP.L. "High-Throughput Post-Quantum Cryptographic System - CRYSTALS-Kyber with Computational Scheduling and Architecture Optimization". Electronics, MDPI. vol. 14, No.12, pp. 2969, 2025.

[12] IavichM,KuchukhidzeT. "Investigating CRYSTALS-Kyber Vulnerabilities - Attack Analysis and Mitigation". Cryptography, MDPI. vol. 8, No.15, pp. 7, 2024. 8.

[13] Liyth H. Mahdi, Alharith A. Abdullah. "A Hybrid Post-Quantum Cryptographic Framework Integrating Kyber-512 and ASCON for Secure IoT Communications", Engineering, Technology & Applied Science Research. vol. 15, No.26, pp. 527, 2025.

[14] Vinayak Tanksale. "Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices", Electronics, MDPI. vol. 13, No.10, pp. 3631, 2024.

[15] Shih-Hsiang Chou, Yu-Hua Yang, Wen-Long Chin, Ci Chen, Cheng-Yu Tsao, Pin-Luen Tung. "High-Throughput Post-Quantum Cryptographic System - CRYSTALS-Kyber with Computational Scheduling and Architecture Optimization", Electronics, MDPI. vol. 14, No.6, pp. 2969, 2025.

[16] M. Awais Ehsan, Walaa Alayed, Amad Ur Rehman, Waqar ul Hassan, Ahmed Zeeshan. "Post-Quantum KEMs for IoT - A Study of Kyber and NTRU", Symmetry, MDPI. vol. 17, No.4, pp. 881, 2025.