An Adaptive Dual-Stack QKD-PQC Framework for Secure and Reliable Inter-Site Communication

Alessio Di Santo[1,*], Walter Tiberti[1] and Dajana Cassioli[1]

[1]*Università degli Studi dell'Aquila, L'Aquila, Abruzzo, Italy*

Abstract

The advent of quantum computing imposes unprecedented risks on conventional cryptosystems, necessitating novel secure communication strategies. This work presents a modular, hybrid, and adaptive protocol that integrates *Quantum Key Distribution* (*QKD*) with *Post-Quantum Cryptography* (*PQC*) to maintain continuous, *Quantum-Safe Key Exchanges*, even under adverse network conditions that typically hinder the state-of-the-art *QKD*-based methods. At its core are specialized *Crypto-Machines*, which incorporate *QKD Nodes* compliant with *ETSI-14* standards and modular *PQC* components, thereby supporting seamless transitions among lattice-, hash-, or code-based schemes. A signed, *Quantum-Resistant*, *HOTP*-based mechanism ensures robust mutual authentication. When *QKD* utilization becomes infeasible—due to, for example, fiber tampering—the protocol dynamically shifts to *PQC*, safeguarding ongoing communications. Once a key is established, *AES-256-GCM* encryption provides strong data confidentiality. Simulations have been conducted with the *SeQUeNCe* toolkit to demonstrate the protocol's adaptability and resilience. The results show how *Crypto-Machines* are able to provide *QKD* exchanges under favorable network conditions while also being able to fall-back to *PQC*-based approaches with a minimal impact on the performance. Hence, the proposed stack allows operators to maintain *Quantum-Proof Key Exchanges* where current state-of-the-art solutions are impaired by a low-quality network connection, and thereby offering a forward-looking security framework suited to the quantum era.

Keywords

Quantum Cryptography, Post Quantum Cryptography, Quantum Key Distribution, Cryptography

1. Introduction

Secure exchange of reserved information is essential for modern communication infrastructures supporting financial, defense, and healthcare sectors. However, the advent of quantum computing generated new vulnerabilities such as those exposed through *Shor*'s [1] and *Grover*'s [2] algorithms, and makes very urgent the design of resilient solutions.

Hybrid approaches integrating *Quantum Key Distribution (QKD)* and *Post-Quantum Cryptography (PQC)* have emerged to address these challenges. *Hajny et al.* [3] propose a three-layer scheme combining *QKD*, *Elliptic-curve Diffie–Hellman (ECDH)*, and *PQC* for secure key generation, while *Zeydan et al.* [4] and *Lin et al.* [5] explore *QKD-PQC* integration to enhance blockchain identity management and scalable key establishment, respectively. Other works [6, 7] incorporate adaptive architectures and key management strategies into *5G* networks and distributed systems.

However, existing frameworks often fail to fully address physical-layer vulnerabilities in *QKD*, instead concentrating on advanced cryptographic schemes that integrate both *QKD* and *PQC* implementations. Although these approaches can enhance *Quantum-Proof* security, they are constrained by the need for specific fiber channel conditions to effectively employ *QKD*. As a result, these methods are unsuited for noisy or physically tampered environments.

This paper introduces a novel hybrid and adaptive protocol stack, centered on *Crypto-Machines*, that integrate *QKD Nodes* with *PQC* modules (e.g., lattice-, hash-, and code-based). This system dynamically shifts from *QKD* to *PQC* whenever the communication channel is deemed unreliable or insecure, ensuring seamless and secure inter-site message exchange without dependence on fiber conditions or

Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT

[*] Corresponding author.

alessio.disanto@graduate.univaq.it (A. D. Santo); walter.tiberti@univaq.it (W. Tiberti); dajana.cassioli@univaq.it (D. Cassioli)

0009-0003-0219-534X (A. D. Santo); 0000-0002-4890-5031 (W. Tiberti); 0000-0001-7574-5099 (D. Cassioli)

susceptibility to channel degradation attacks. Additionally, the mutual authentication mechanisms, employed by *Crypto-Machines*, is able to mutually authenticate other protocol's participants in a *Quantum-Safe* way.

Following the recent NIST standards on PQC, we selected *ML-KEM* [8] as the main *Key Encapsulation Mechanism* (*KEM*), *ML-DSA* [9] for authentication and *HMAC*-based one-time passwords (*HOTP*) [10] for robust identity verification. Additionally, an internal key derivation process based on the *Password-Based Key Derivation Function 2 Hash-based Message Authentication Code* (*PBKDF2HMAC*) [11] within *AES-256-GCM* enhances key post-processing, compensating for the lack of privacy amplification in simulation environments like the *SeQUeNCe Toolkit* [12].

We validated the proposed protocol stack through the usage of this toolkit and evaluated how performance are affected by physical variable conditions (e.g., fiber attenuation, polarization fidelity), without requiring physical *QKD* hardware [12, 13, 14]. These tests confirmed the protocol's adaptability, scalability, and practicality in real-world secure communication scenarios.

1.1. Paper's Contribution

The core contributions of this research are as follows:

- We propose a *Dual-Stack Security Framework* consisting in a modular cryptographic component and an encrypted information exchange protocol. The proposed framework combines *QKD* for primary key exchange with *PQC* as a fallback, ensuring an adaptive, secure and reliable communication even under adverse conditions.
- We introduce the *Crypto-Machine*, a modular component that integrates both *PQC* and *QKD*, allowing operators to employ both *QKD Devices* and *PQC Algorithms*. By taking advantage of configurable strategies, the *Crypto-Machine* behavior can be manipulated to fit any real-world situation and provides the best possible performance under every possible network and environmental conditions.
- We simulated and validated the proposed framework via *SeQueNce Toolkit* simulations, which allow to gather preliminary insights on *QKD* limitations, under stressed network conditions, and to show the key role of a fallback mechanism, to guarantee the secure message exchange without any operational issue or delay.

2. Related Work

Existing studies combining *QKD* and *PQC* highlight their potential for post-quantum security but often lack mechanisms to handle physical-layer vulnerabilities and dynamic fallback strategies.

Schatz et al. [15] use *QKD-PQC* for secure *VPN* tunnels, focusing on symmetric key operations, but lacks robust identity verification and fallback procedures. Pedone et al. [16] propose a *QKD-PQC* software stack for cloud environments, prioritizing scalability rather than dealing with channel noise or failover mechanisms. Bakar et al. [17] combine *QKD* and *PQC* to secure *IPsec* tunnels, highlighting cost-performance trade-offs but not dynamic adaptations to environmental disruptions. Alia et al. [18] focus on high-speed *QKD-PQC IPsec VPN* tunnels, yet do not incorporate on-the-fly fallback or identity certification.

Rosales et al. [19] apply *QKD* in mobile contexts without integrating *PQC* fallback or noise handling. Roy et al. [20] analyze *QKD* vulnerabilities but do not propose solutions involving *PQC*.

Our proposed protocol addresses these gaps by employing *ML-DSA* and *HOTP* codes for robust identity verification and modular *Crypto-Machines* to enable real-time switching between *QKD* and *PQC* (e.g., *ML-KEM* [8]) based on environmental conditions. This design aligns with *ETSI-14* standards [21], supports *NIST*-backed standardization efforts [22], and incorporates *PBKDF2HMAC* [11]-based key derivation to provide *privacy amplification*.

The result is an adaptive, dual-stack security framework that maintains continuous, resilient communication despite noise, tampering, or computational attacks. This fully customizable solution can be tailored to any operational context, and can accommodate any chosen *QKD Node* and *PQC* algorithm, while still be regarded as a quantum-proof system. It supports secret message exchanges between sites with no performance degradation, even in scenarios where traditional *QKD*-based methods cannot operate.

3. System Model

The system model setup and the operative scenario are shown in Figure 1. In the proposed model, we assume that two distant sites (A and B) are connected by a multi-core fiber cable supporting quantum and classical communications.

Each site hosts a secure, access-controlled, and shielded room containing a dedicated *Crypto-Machine* and a corresponding *Asset*. Environmental conditions (e.g., temperature, humidity, light) are rigorously maintained to optimize *QKD* device performance and mitigate physical attacks.

When a new message must be exchanged, the process begins with mutual authentication and an evaluation of the fiber's transmission parameters. Based on this assessment, the quantum channel could be utilized to distribute quantum particles. In such a case, once received these quantum particles, the *QKD Node*'s *Error Correction* layer corrects erroneous decoded bits and ensures key consistency between the communicating parties.

This layered model is inspired by the *SeQUeNCe* QKD architecture [23], which separates functionalities into distinct layers. Following a similar approach, the division into layers 0 and 1 emphasizes a clear separation between the quantum physical layer and the subsequent classical error correction processes.

At the center of this architecture is the *Crypto-Machine*, a newly designed modular device integrating *QKD* and *PQC* components (e.g., *ML-KEM*) to deliver a flexible, *Quantum-Proof* cryptographic framework. By unifying *Quantum-Safe* key distribution and post-quantum methodologies, the *Crypto-Machine* can adapt to evolving threats and maintain secure communications under challenging conditions. It incorporates authenticated modules, robust protocols, and a certified bus system that facilitates seamless hardware integration. Each module requires cryptographically signed certificates prior to inclusion, ensuring compliance with emerging standards and supporting rapid, secure updates. Customizable fallback strategies allow the system to swiftly transition from *QKD* to *PQC* when channel conditions degrade.

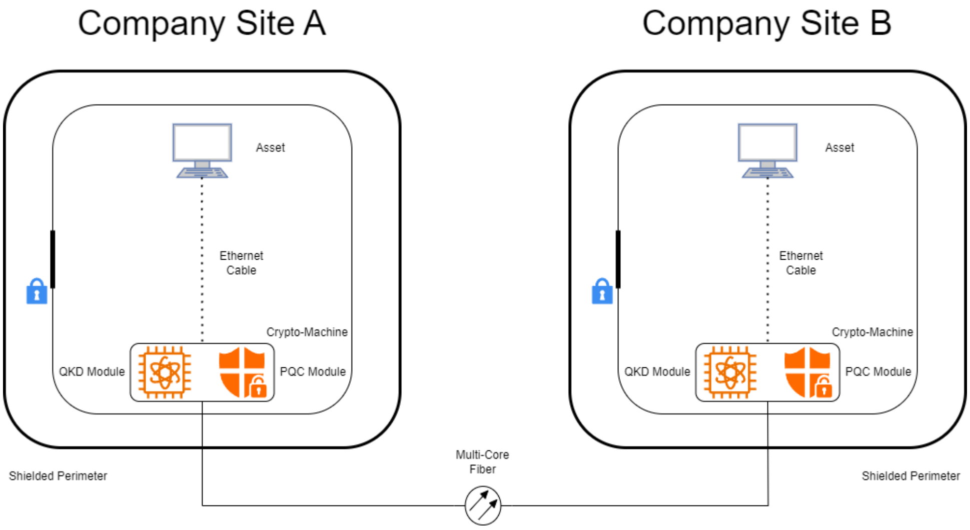


Figure 1: Operative Scenario

The *QKD Nodes*, connected to the *Crypto-Machine* via an *ETSI-14*-compliant Ethernet interface, handle quantum key generation. Although the current *QKD API* does not directly monitor physical-layer conditions, the *Crypto-Machine* provides specialized functions to query the *QKD Node*'s settings for improved situational awareness and potential future enhancements.

Mutual authentication is reinforced through a signed (via *ML-DSA* algorithm) *HOTP*-based mechanism, with two distinct modules deployed – one paired with the remote *Crypto-Machine*, and the other with the local *Asset*, as shown in Figure 1 – to prevent impersonation attacks. Both *Crypto-Machines* share a common *HOTP* seed from the time of fabrication.

Employing a dedicated Security Processing Platform (*SPP*) as in [24], can be considered as an interesting idea to further accelerate *AES-256-GCM* encryption while mitigating side-channel vulnerabilities.

Sensitive data, including certificates, keys, and message payloads, resides in dual, isolated memory units for secure storage and rapid erasure. A certificate-validated bus system ensures that only authorized hardware components are integrated, aligning with best practices from automotive and IoT security frameworks [23]. Administrative tasks occur via a secure, physical keypad interface, ensuring strict privilege separation. In summary, the *Crypto-Machine*'s modular design, authenticated hardware infrastructure, and advanced *Quantum-Safe* cryptographic components offer a forward-looking platform that is both robust and adaptable for secure communications. This solution can be readily adopted by financial, healthcare, industrial, and defense organizations. It also provides a solid foundation for new research in *Quantum-based Secret Sharing*, i.e. [25]. By leveraging dual-stack QKD–PQC methods, such approaches could benefit from an adaptive fallback mechanism to ensure consistent secret distribution even under adverse conditions, thereby enhancing the resilience and scalability of future quantum secret sharing schemes without losing its quantum-resistant property.

4. Encrypted Information Exchange Protocol

4.1. Protocol Overview

The Encrypted Information Exchange Protocol follows the following end-to-end communication flow.

We assume that the access to the secure room is tightly controlled, ensuring physical and electromagnetic security. Additionally, *Crypto-Machines* and their corresponding *Assets* have all already been paired with the shared *ML-DSA* public keys.

Initial Crypto-Machine setup — The sender's operator logs into the *Asset*'s segregated terminal, which in turn authenticates against the *Crypto-Machine*, verifying the *ML-DSA* certificate. The operator prepares the message and hands it off to the *Crypto-Machine* for transmission.

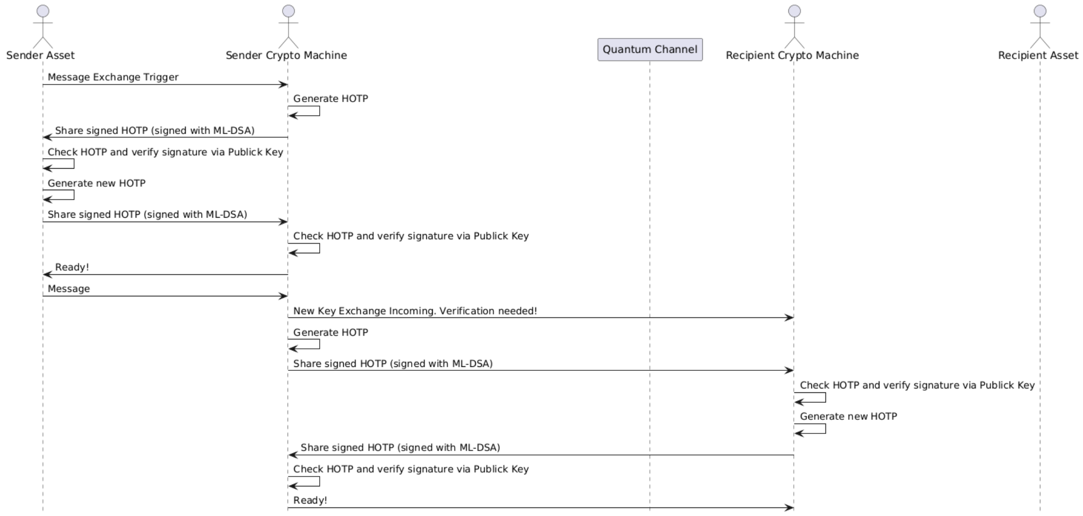

Sender Asset
Sender Crypto Machine
Quantum Channel
Recipient Crypto Machine
Recipient Asset
Message Exchange Trigger
Generate HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Generate new HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Ready!
Message
New Key Exchange Incoming. Verification needed!
Generate HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Generate new HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Ready!

Figure 2: Information Exchange Protocol - Mutual Authentication Phase

Crypto-Machines mutual-authentications — Prior to the key exchange, the *Crypto-Machines* undergo a mutual authentication procedure and perform internal checks based on *HOTP* and *ML-DSA* digital signatures (refer to Section 3). As illustrated in Figure 2, the process begins with the sender generating an *HOTP*, signing it with its private key, and transmitting the resulting signed *HOTP* to the recipient. Upon receipt, the recipient generates its own *HOTP* and then uses the sender's public key to verify the signed message. Once the verification confirms the message's authenticity, the recipient regards the sender as genuine.

The core of this mechanism lies in the sender transmitting only the signed message. Consequently, the recipient must produce the correct cleartext *HOTP* itself to carry out proper validation. This strategy ensures robust mutual authentication, while keeping any sensitive key material confidential.

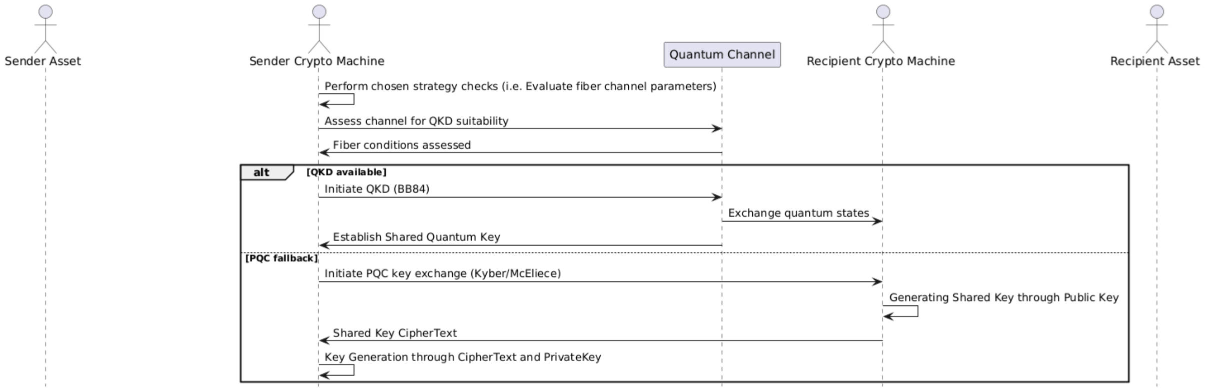

Sender Asset
Sender Crypto Machine
Quantum Channel
Recipient Crypto Machine
Recipient Asset
Perform chosen strategy checks (i.e. Evaluate fiber channel parameters)
Assess channel for QKD suitability
Fiber conditions assessed
alt
[QKD available]
Initiate QKD (BB84)
Exchange quantum states
Establish Shared Quantum Key
[PQC fallback]
Initiate PQC key exchange (Kyber/McEliece)
Generating Shared Key through Public Key
Shared Key CipherText
Key Generation through CipherText and PrivateKey

Figure 3: Information Exchange Protocol - Key Exchange Strategy Application

Quantum Key Exchange attempt — The sending *Crypto-Machine* attempts a *QKD*-based key exchange over the quantum channel (Figure 3). If fiber conditions (noise, signal integrity) fail to meet thresholds, the system automatically switches to *ML-KEM*-based *PQC* key exchange. Those thresholds are context-specific and require an initial on-field learning phase to find the optimal values.
Switch to PQC — In case of failure in establishing a key over the quantum channel, the *Crypto-Machine* will revert to a PQC-based approach (shown as "*PQC fallback*" alternative block in Figure 3). As an example, *ML-KEM* is one of the two proposed alternatives available in the simulation. By assuring the mutual identification of two coupled *Crypto-Machines*, the sender can share its public key with the recipient which will then start the Key Generation process, return the *ciphertext* to the sender and be able to generate an identical key.

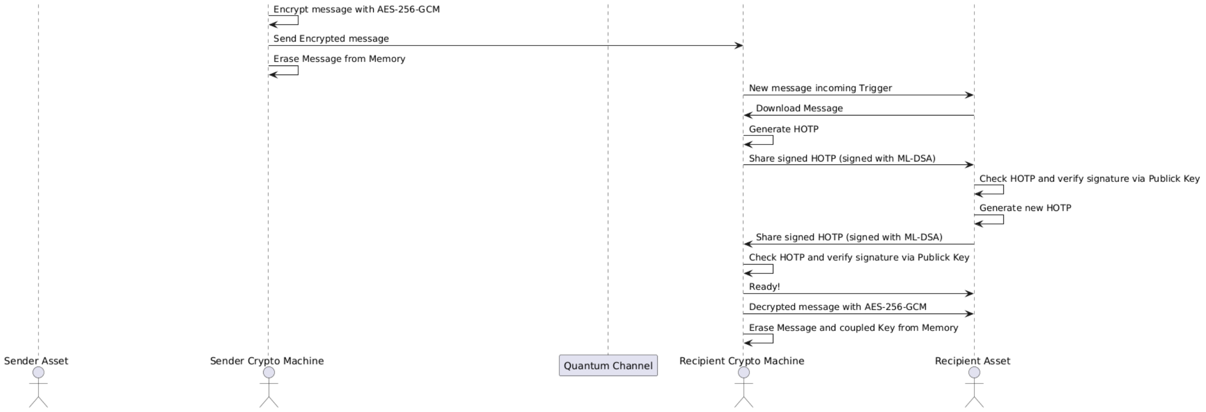

Encrypt message with AES-256-GCM
Send Encrypted message
Erase Message from Memory
New message incoming Trigger
Download Message
Generate HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Generate new HOTP
Share signed HOTP (signed with ML-DSA)
Check HOTP and verify signature via Publick Key
Ready!
Decrypted message with AES-256-GCM
Erase Message and coupled Key from Memory
Sender Asset
Sender Crypto Machine
Quantum Channel
Recipient Crypto Machine
Recipient Asset

Figure 4: Information Exchange Protocol - Message Exchange and Final delivery

Message encryption and delivery — Once a key is secured, a secure block cipher such as *AES-256-GCM* encrypts the message, which is then sent over the classical channel (Figure 4). The receiving *Crypto-Machine* verifies the key and stores the encrypted data securely until the recipient operator, after logging into the secure room's terminal, retrieves and decrypts it.

This adaptive workflow ensures that communication remains secure, efficient, and robust against both physical and cryptographic challenges.

4.2. Protocol's Validation

The proposed *QKD-PQC* protocol was simulated through a Python-based implementation, utilizing the *SeQUeNCe* framework [12] for *QKD* and Python's cryptographic libraries `pqc` and `pycryptodome` for *PQC*.

The simulations replicate secure communication scenarios between two *Crypto-Machines* over quantum channels with varying environmental parameters, such as distance, polarization fidelity, and fiber attenuation, highlighting the system's potential for real-world deployment, addressing both physical-layer vulnerabilities and post-quantum cryptographic challenges. The simulation code is available on GitHub[1].

By using a configuration file it is possible to manage several different real-world parameters of a *QKD Node*, e.g., exchanged key dimension, fiber's attenuation, polarization fidelity, distance, encoding scheme, receiving and sender light sources and detectors configurations. Furthermore, it is possible to decide which *PQC* algorithm to deploy and which custom strategy to implement. According to our current implementation, available *PQC* algorithms are *ML-KEM* and *McEliece* [26].

Proposed code takes advantage of two entities, representing the sender and recipient, which are instantiated as *CryptoMachines*, integrating both *QKD* and *PQC* functionalities within a modular framework. These *CryptoMachines* embody the hybrid architecture described in the previous sections, combining quantum and classical cryptographic operations driven by a custom fallback mechanism.

The custom created *createCryptoMachinesCouple* function initializes the sender and recipient *Crypto-Machines*, equipping them with *QKD Nodes* (*QKDEndpoint*), selected *PQC* modules, and an exchange strategy. These twin *Crypto-Machines* are paired during initialization, sharing a common *HOTP-seed* for authentication and exchanging their *ML-DSA* public keys. Additionally, each *Crypto-Machine* is paired with its corresponding *Asset*, which independently maintains a unique *HOTP-seed* and exchanges its public key with the associated *Crypto-Machine*.

Each *QKD Endpoint* simulates quantum key distribution using the *SeQUeNCe* library's *QKD Nodes* class, emulating realistic quantum communication environments.

During the setup phase, the newly defined *QKDEndpoint.setupNode* method configures the *QKD Nodes* for both sender and recipient. This includes establishing quantum and classical communication channels, modeled by *SeQUeNCe*'s *QuantumChannel* and *ClassicalChannel* classes. These channels emulate the physical properties of optical fibers and classical links, creating a realistic simulation environment. Additionally, the *BB84* protocol is implemented for quantum key exchange, while the *Cascade* protocol handles error correction [27]. This ensures robust key generation within *SeQUeNCe*'s timeline-driven simulation.

Once the nodes are configured, the system initiates secure communication. The first step involves mutual authentication of the *Crypto-Machines* using *HOTP* and *ML-DSA* digital signatures, as detailed in Section 4.

Following authentication, the system implements adaptable strategies to determine whether to use quantum or classical methods for key exchange. Two strategies are available: the *Static parameters detection* and the *Dynamic exchange*. The first applies predefined thresholds to environmental parameters such as polarization fidelity and fiber attenuation, while the dynamic exchange strategy prioritizes *BB84*-based quantum key exchange and falls back to PQC when quantum channel conditions deteriorate. These strategies are implemented through the *exchangeProtocolStrategy* interface, ensuring flexibility in adapting to various operational scenarios. Under optimal conditions, the *KEMviaQKD* function initiates the *BB84* protocol, leveraging *SeQUeNCe*'s detailed quantum communication simulations to establish a shared quantum key. In adverse conditions, the system dynamically switches to the *KEMviaPQC* function, which utilizes the selected PQC algorithm (e.g., *ML-KEM* or *McEliece*) for key encapsulation and decapsulation. This dynamic approach, shown in Figure 3, ensures the system's resilience against physical-layer challenges.

Once a shared key is established, it is processed within the *AES-256-GCM* encryption module. To enhance entropy and address the absence of privacy amplification in the *SeQUeNCe* toolkit, the shared

[1] https://github.com/alessiobb3b/CryptoMachine-Simulator

key undergoes a derivation process based on *PBKDF2HMAC*, using the exchanged quantum key as the initialization parameter. This derived key is then used to encrypt a user-defined message, which is transmitted securely to the recipient. The recipient decrypts the message using the same derived key, ensuring confidentiality and integrity. Subsequently, the recipient's *Crypto-Machine* notifies its paired *Asset* of the new message. After identity verification, the decrypted message is securely transmitted to the *Asset*, and all references to the message are promptly deleted from both *Crypto-Machines* to maintain data privacy (Fig. 4).

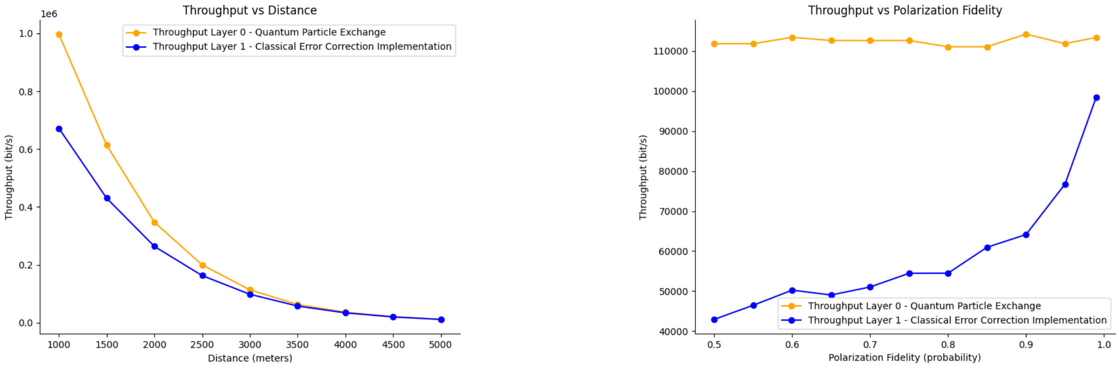
Finally, the simulation records performance metrics, including error rates, throughput, and execution times, outputting these results in JSON format for further analysis. The *SeQUeNCe* framework's detailed event logging and tracking capabilities enhance the accuracy and reliability of these evaluations, demonstrating the protocol's robustness under various simulated conditions.

5. Performance Results and Discussion

The results obtained from the simulation of the proposed *QKD-PQC* protocol highlight its practical feasibility and effectiveness in addressing real-world communication challenges, showing a high degree of adaptability, performance, and resilience.

Achieved results are shown as information acquired from two different layers of the simulated *QKD Device*. *Layer 0* represents the information at the physical layer, i.e. directly referred to the quantum particles emitted by the *QKD Device*'s beam. On the other hand, *Layer 1* takes into account a higher stack layer, where it accounts for the classical *Error Correction Mechanisms* (previously defined in Sec. 4.2.

As shown in Figure 5a, at a distance of 1 Km, the protocol performs efficiently, achieving throughput rates of $997,535$ bits/s in the quantum layer and maintaining error-free operation after correction by loosing about one third of its throughput, i.e. $672,136$ bit/s. However, as the distance increases to 3 Km, throughput drops significantly to $113,385$ bits/s, with increased error rates and reduced throughput after performing *Error Correction*. Beyond 5 Km, the quantum layer becomes practically infeasible, with throughput reducing to $11,379$ bits/s. As expected, decreasing the *Layer 0* throughput involves a decreased difference between the throughputs, since the slower rates allows *Layer 1* to keep a slower pace.



(a) Throughput evolution as distance increases

(b) Throughput evolution as polarization fidelity increases

Figure 5: Throughput trend under different parameters variations

Polarization fidelity also plays a crucial role in protocol performance (Fig. 5b). This parameter models the probability that the sender's simulated *QKD Device* polarizes correctly a particle to share. Hence, a fidelity of 0.5 means that one particle out of two is correctly polarized, while the other will be transmitted with an intrinsic error that should be corrected through *Layer 1*.

At higher fidelities, such as 0.99, the protocol achieves near-optimal throughput and minimal error rates (as shown by the increased performances on *Layer 1*). As fidelity drop to 0.75, error rates surge to over 12%, while throughput falls below $111,000$ bits/s. At a fidelity of 0.4, the system is unable to establish a secure key even after extended simulated durations, demonstrating the sensitivity of *QKD* to quantum channel quality. Particle emission rate is not impacted by the lower probability of correctly polarizing the photon, which can be seen as stable. Instead, the *Error Correction Layer* is deeply involved with a grater quantity of erroneous decoded bits.

Similarly, when the distances reaches 3 Km, the latency related to *Shared Key Generation* has a noticeable increase (Figure 6). Past $\sim$10 Km the simulation becomes infeasible as its simulation execution time falls over the boundaries of 20 seconds, marking a noticeable delay in the message exchange that can easily be avoided with the fallback mechanism. Furthermore, *SeQUeNCe* simulation time does not directly match ours, since to reach 20 seconds of simulation, it needs about 2 hours of real-hardware computation. These results underscore the critical impact of distance on *QKD*, with significant degradation occurring as noise and attenuation increase over longer channels, which also requires an enhanced process of error correction that as a trade-off reduces throughput to achieve consistency between keys.

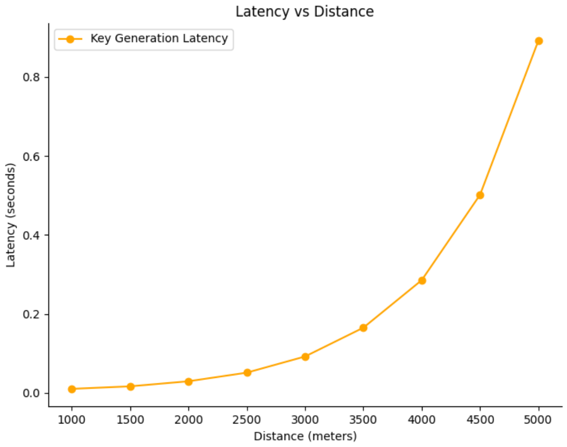


Figure 6: Key Generation latency evolution as distance increases

Fiber attenuation further impacted performance, as shown in Figure 7, with a threefold increase in attenuation from 0.01 dB/Km to 0.03 dB/Km resulting in a simulation execution time which exponentially increases from less than 100 *ms* to over 5 *seconds*. This dramatic increase highlights the necessity of maintaining low-attenuation fibers to support effective *QKD* operations over meaningful distances.

The simulation outcomes validate the robustness and flexibility of our proposed *QKD-PQC* protocol, emphasizing the necessity of a dual-stack security framework to address the highlighted limitation of *QKD* (e.g., fiber attenuation over 0.03 *dB/Km* or distances around 10 *Km*). *PQC* fallback is indeed needed to achieve a feasible *Key Exchange* process that can be dynamically adapted to different situations. As an example, if a *Crypto-Machine* detects an attenuation higher than the known suitable one, it will immediately switch to a *PQC*-based *KEM* to avoid any additional delay in the secure message delivery. This ensures that secure communication can be maintained in critical applications, even when one security layer is compromised or unusable due to the physical mean conditions. The results position the protocol as a comprehensive and forward-looking solution for next-generation secure communications, ready to adapt to evolving quantum and cryptographic challenges.

Our dual QKD–PQC framework adds only minimal overhead compared to single-approach solutions. The main extra cost comes from the *adaptive strategy*, which briefly checks channel parameters (e.g., polarization fidelity, distance) before deciding whether to use QKD or switch to PQC. This decision process is short, and subsequent key exchanges—QKD or PQC—run at speeds comparable to standalone

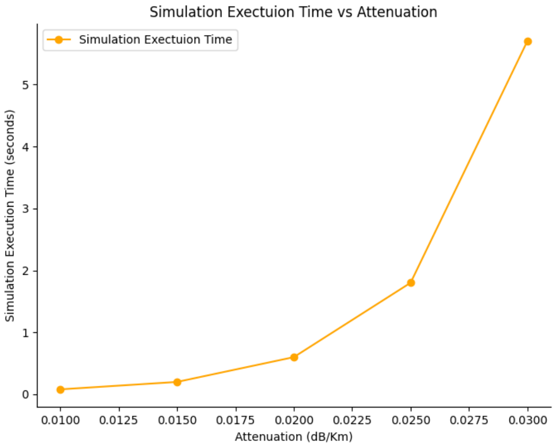


Figure 7: Execution Time evolution as fiber's attenuation increases

QKD or PQC systems.

Moreover, promptly detecting unfeasible QKD conditions and switching to PQC prevents time-consuming, failed quantum exchanges. Thus, the overhead for decision-making is effectively offset by avoiding fruitless QKD attempts. Overall, our hybrid approach preserves high throughput while ensuring robust quantum-safe security.

Overall, the protocol ensures a secure, adaptable, and reliable communication framework, as it incorporates state-of-the-art techniques to protect against a wide array of quantum-era and classical threats, such as:

- System-wide threats, including *Man-in-the-Middle (MiTM)* attacks, prevented through the implementation of *ML-DSA* and *HOTP*-based mutual authentication [28], and *Denial-of-Service (DoS)* attacks, countered by channel redundancy, monitoring, and fallback routing [29];
- *Side-Channel Attacks (SCA)*, mitigated by electromagnetic shielding, noise injection, and randomized timings [30];
- *QKD*-specific attacks like the *intercept-resend* strategy, thwarted by monitoring the quantum bit error rate (*QBER*) and triggering *PQC* fallback upon anomalies [29];
- *Photon Number Splitting (PNS)* attacks, mitigated by decoy-state protocols [30];
- *trojan-horse* attempts, neutralized via optical isolators and wavelength filters [31];
- *Detector blinding*, addressed by self-check mechanisms and randomized parameters [29];
- collective attacks, reduced by privacy amplification and robust error correction [28].

PQC components face threats like *SCA*, mitigated by constant-time algorithms, randomized operations, and tamper-resistant hardware [30]. *Fault Injection Attacks (FIA)* are countered by error-detection codes and secure reboot mechanisms [32, 33]. *Rowhammer* exploits are limited by *ECC* and secure memory isolation [31], while *Kleptographic* and *Signature Correction* attacks are addressed through rigorous code audits, formal verification, and fault-tolerant signature schemes [28, 30]. *Lattice Reduction Attacks* are contained by selecting high-dimension lattices and robust security parameters, ensuring resistance to approximation algorithms such as *Lenstra–Lenstra–Lovász* (*LLL*) or *Block Korkin-Zolotarev* (*BKZ*) algorithms.

6. Conclusion

This study presented a dual-protocol stack integrating *Quantum Key Distribution (QKD)* and *Post-Quantum Cryptography (PQC)* into a modular, future-ready framework. By leveraging *Crypto-Machines* equipped with *QKD Nodes* and recent Post-Quantum standards, the protocol dynamically shifts between quantum and post-quantum mechanisms, ensuring secure and reliable communication despite environmental challenges. Simulations validated our system and confirmed that factors like fiber distance, polarization fidelity, and attenuation critically affect *QKD* performance. While *QKD* excels under optimal conditions, it becomes unreliable at long distances or in harsh environments. Our protocol's seamless fallback to *PQC* key exchange maintains security under these adverse scenarios, underscoring the importance of a dual-stack approach.

A key advantage is modularity, enabling easy integration of new cryptographic standards (e.g., hash- or code-based) as they emerge, thus ensuring adaptability amid evolving quantum and classical threats. This approach enhances resilience against physical-layer attacks and ensures robust fallback mechanisms. Future efforts will test the protocol in multi-node networks, at greater distances, under higher noise, attacks and eventually with physical hardware implementations.

Acknowledgment

This work is supported by the project ISP5G+ (CUP D33C22001300002), which is part of the SERICS program (PE00000014) under the NRRP MUR program funded by the EU-NGEU.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Proc. of the 35th Annual Symposium on Foundations of Computer Science, 1994.

[2] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, ACM, 1996, pp. 212–219.

[3] J. Hajny, P. Muzikant, L. Malina, J. Havlin, P. Tuma, Open-source post-quantum encryptor: Design, implementation and deployment, Scitepress (2024). URL: https://www.scitepress.org/Papers/2024/128392/128392.pdf.

[4] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, et al., Integrating quantum-secured blockchain identity management in open ran for 6g networks, in: 2024 IEEE 49th International Conference, 2024. URL: https://ieeexplore.ieee.org/abstract/document/10639816/.

[5] J. Lin, H. K. Lo, J. Johannsson, et al., Distributed symmetric key establishment: A scalable quantum-safe key distribution protocol, in: 2024 IEEE 49th International Conference, IEEE, 2024. URL: https://ieeexplore.ieee.org/abstract/document/10639637/.

[6] M. Mehic, L. Michalek, E. Dervisevic, Quantum cryptography in 5g networks: A comprehensive overview, IEEE Surveys and Tutorials (2023).

[7] E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, Quantum key distribution networks–key management: A survey, arXiv preprint (2024). URL: https://arxiv.org/pdf/2408.04580.

[8] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, D. Stehle, CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM, in: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 2018. doi:10.1109/EuroSP.2018.00032.

[9] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, Crystals-dilithium: A lattice-based digital signature scheme, Cryptology ePrint Archive, Paper 2017/633, 2017. URL: https://eprint.iacr.org/2017/633.pdf, available at https://eprint.iacr.org/2017/633.

[10] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranenko, Rfc 4226: Hotp: An hmac-based one-time password algorithm, https://www.ietf.org/rfc/rfc4226.txt, 2005. Internet Engineering Task Force (IETF) Request for Comments.

[11] H. Choi, S. C. Seo, Optimization of pbkdf2 using hmac-sha2 and hmac-lsh families in cpu environment, IEEE Access 9 (2021) 40165–40177. doi:10.1109/ACCESS.2021.3065082.

[12] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, M. Suchara, Sequence: a customizable discrete-event simulator of quantum networks, Quantum Science and Technology 6 (2021). URL: https://dx.doi.org/10.1088/2058-9565/ac22f6. doi:10.1088/2058-9565/ac22f6.

[13] R. Zhou, X. Wu, M. Suchara, A simulator of atom-atom entanglement with atomic ensembles and quantum optics, in: IEEE Quantum Computing and Engineering (QCE), 2023, pp. 215–223. doi:10.1109/QCE53715.2023.00026.

[14] X. Wu, M. Suchara, R. Kettimuthu, Parallel simulation of quantum networks with distributed quantum state management, ACM Transact. on Modeling and Computer Simulation 34 (2024). doi:10.1145/1234567.

[15] D. Schatz, F. Altheide, H. Koerfgen, M. Rossberg, Virtual private networks in the quantum era: A security in depth approach, Semanticscholar (2023). URL: https://pdfs.semanticscholar.org/5444/ef5520a82b8c4b71d8382707abdb960af87b.pdf.

[16] I. Pedone, A. Atzeni, D. Canavese, A. Lioy, Toward a complete software stack to integrate quantum key distribution in a cloud environment, IEEE Access (2021). URL: https://ieeexplore.ieee.org/abstract/document/9505594/.

[17] R. A. Bakar, F. Cugini, D. Lawo, Wireless and fiber-based post-quantum-cryptography-secured ipsec tunnel, Future Internet (2024). URL: https://www.mdpi.com/1999-5903/16/8/300.

[18] O. Alia, O. Amer, M. Pistoia, 100 gbps quantum-safe ipsec vpn tunnels over 46 km deployed fiber, arXiv preprint (2024). URL: https://arxiv.org/abs/2405.04415.

[19] D. Rosales, A. Khan, A quantum key distribution system for mobile platforms with highly indistinguishable states, arXiv preprint (2024). URL: https://arxiv.org/pdf/2411.19880.

[20] P. Roy, C. Benjamin, Sequential attack impairs security in device-independent quantum key distribution, arXiv preprint (2024). URL: https://arxiv.org/pdf/2411.16822.

[21] ETSI, Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API, ETSI Group Specification GS QKD 014 V1.1.1, 2019. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf.

[22] N. I. of Standards, T. (NIST), Nist releases first 3 finalized post-quantum encryption standards, 2024. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[23] M. Ye, X. Feng, S. Wei, Hisa: Hardware isolation-based secure architecture for cpu-fpga embedded systems, in: 2018 IEEE/ACM International Symposium on Microarchitecture (MICRO), IEEE, 2018.

[24] E. Choi, J. Park, K. Han, W. Lee, Aesware: Developing aes-enabled low-power multicore processors leveraging open risc-v cores with a shared lightweight aes accelerator, Engineering Science and Technology, an International Journal 60 (2024) 101894. URL: https://www.sciencedirect.com/science/article/pii/S2215098624002805. doi:https://doi.org/10.1016/j.jestch.2024.101894.

[25] A. Di Santo, W. Tiberti, D. Cassioli, Security and fairness in multi-party quantum secret sharing protocol, IEEE Transactions on Quantum Engineering (2025) 1–18. doi:10.1109/TQE.2025.3535823.

[26] H. Singh, Code based cryptography: Classic mceliece, 2020. URL: https://arxiv.org/abs/1907.12754. arXiv:1907.12754.

[27] D. Tupkary, N. Lütkenhaus, Using cascade in quantum key distribution, Physical Review Applied 20 (2023). URL: http://dx.doi.org/10.1103/PhysRevApplied.20.064040. doi:10.1103/physrevapplied.20.064040.

[28] S. Hoque, A. Aydeger, E. Zeydan, Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design (2024). URL: https://dl.acm.org/doi/abs/10.1145/3659997.3660033.

[29] S. P. Kish, J. Zhuang, A. Chhabra, Mitigation of channel tampering attacks in continuous-variable quantum key distribution, Physical Review Research 6 (2024) 023301. URL: https://journals.aps.org/prresearch/pdf/10.1103/PhysRevResearch.6.023301.

[30] S. Kundu, B. Roy, E. Alkim, On the masking-friendly designs for post-quantum cryptography, IACR Cryptology ePrint Archive 2023 (2023) 1732. URL: https://eprint.iacr.org/2023/1732.pdf.

[31] M. Krelina, Quantum communication countermeasures, arXiv preprint arXiv:2310.08728 (2023). URL: https://arxiv.org/abs/2310.08728.

[32] K. Xagawa, A. Ito, R. Ueno, J. Takahashi, N. Homma, Fault-injection attacks against nist's post-quantum cryptography round 3 kem candidates, in: Advances in Cryptology – ASIACRYPT 2021, volume 13091 of *Lecture Notes in Computer Science*, Springer, 2021. URL: https://doi.org/10.1007/978-3-030-92075-3_2. doi:10.1007/978-3-030-92075-3_2.

[33] M. Wolf, A. Weimerskirch, C. Paar, Security in automotive bus systems, in: Workshop on Embedded Security in Cars (ESCAR), Springer, 2004.