

# Simulation and analysis of a QKD-PQC protocol for secure communication channel authentication

G.K. Sandhia<sup>1\*</sup>, M. Ranjani<sup>1</sup>, Srivatsan .K<sup>1</sup>, Asritha Vijayakumar<sup>1</sup>, and S. Aswin<sup>1</sup>

<sup>1</sup>Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur-603203, Tamil Nadu, India

**Abstract.** Quantum computing threatens traditional cryptographic systems based on integer factorization and discrete logarithm problems. This paper proposes a hybrid secure communication framework integrating Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC) for authentication. The BB84 protocol is used for quantum key generation, while CRYSTALS-Dilithium signatures secure the classical communication channel. A Python-based simulator models photon transmission, Quantum Bit Error Rate (QBER), intercept-resend attacks, and authentication verification. Results show that QBER increases proportionally with eavesdropping probability, enabling reliable attack detection. The integration of QKD secrecy with PQC authentication ensures both confidentiality and integrity. Performance evaluation demonstrates that the additional latency introduced by PQC authentication remains within acceptable limits. The proposed hybrid framework provides a scalable and quantum-resistant solution suitable for next-generation secure communication systems.

## 1 Introduction

The rising of quantum computers makes an enormous threat to classical cryptography systems (e.g., RSA, ECC), which are based on the computing time complexity for problems such as integer factorization and discrete logarithm[1]. Quantum system, in particular Shor's algorithm can solve these problems efficiently so that traditional encryption schemes are unsecure. This increasing threat has prompted research on cryptographic tools that are resistant to quantum attacks[2].

Quantum Key Distribution (QKD) provides a possible solution by allowing secure key generation based on the laws of quantum mechanics[3]. By superposition and no-cloning principles, QKD guarantees that a possible eavesdropper is necessary to slightly perturb the transmitted quantum states in any intercept strategy, thus enabling detection via the Quantum Bit Error Rate (QBER). One of the QKD protocols, called BB84 protocol, is well-known in that it is simple and efficient enough to allow for two communicating parties (called Alice and Bob in this context) to share secret keys. However, although QKD offers confidentiality it does not include by itself any authentication on the classical communication channel for key reconciliation. Such a restriction opens the system to MITM and replay attacks.

---

\*e-mail: ksandhia@gmail.com

This paper proposes a solution of the secure communication channel authentication system based on the QKD-PQC (Quantum Key Distribution-Post-quantum cryptography) that can complete both confidentiality and authenticity. For the key generation, the BB84 protocol is used for images and digital signatures with PQC are applied to authenticate classical messages. The system is designed in Python with a simulation interface that can simulate the photon transmission, QBER calculation and authentication checking. The simulation results reveal that during eavesdropping, the QBER becomes raised dramatically, which demonstrates this system is capable of resisting attacks. QKD and PQC can work together to provide secure, quantum-resistant communication for next-gen trusted networks.

Although various research efforts have investigated the hybrid QKD-PQC paradigm, this research is unique in that it offers a tailored, multi-step Python simulation platform that specifically captures and analyzed the real-time latency costs of the PQC authentication step. Moreover, our solution integrates the PQC component with the active eavesdrop detection process in a seamless manner that enables the assessment of security thresholds.

## 2 Background and Related Work

### 2.1 QKD Authentication via PQC

The weak point of QKD is the Man-in-the-Middle (MITM) attack in unauthenticated classical communication. Although in the case of traditional QKD a relatively-small, pre-distributed secret is used for authentication, such method is not readily scalable. Transitioning to PQC-based authentication offers a scalable and quantum-safe alternative[4]. Wang et al. provided a critical review of the application of PQC for the authentication of the QKD and the theoretical robustness of the system to certain attacks like the replay attack [5].

This is where the actual improvement of the above security statement is achieved:

$$\text{SystemSecurity} = \text{QKDSecrecy} \cap \text{PQCAuthentication} \quad (1)$$

This is the definition of the boundaries of the proposed combined system of the QKD-PQC protocol, where the final security is dependent on the intersection of the information-theoretic key secrecy and the computational integrity of the channel.

### 2.2 Practical Implementation and Performance Analysis

The implementation of the theoretical advantages of QKD-PQC in practice is discussed in various seminal works. Geitz et al. elaborate on the realization testing of integrated protocols for the Berlin OpenQKD Testbed [6]. This not only proves the applicability but also provides clues for performance issues. Aquina et al. elaborate on the operational needs for secure communication based on this hybrid QKD-PQC approach, advocating the complementarity of real-time attack detection by means of QKD and defense against future cryptanalytic revelations through PQC [7]. Therefore, the need of a double layer encryption mechanism is even more critical in 'hostile' and high risk environments like satellite link where the excessive loss reduces key generation. Rani et al. study the DEPLOY and PP protocols in Earth-Satellite Channels [8].

### 2.3 The QBER and Privacy Amplification

The basic concern in any QKD protocol is the connection between eavesdropping activity and achieved QBER. The expected QBER,  $E$ , dependent on the eavesdropping probability, has to

be properly simulated. For a channel that is not perfect the QBER observed is a function of the intercept-resend probability and the intrinsic depolarizing noise of the channel:

$$E(p_i, \delta) \approx \frac{1}{2}p_i + (1 - p_i) \quad (2)$$

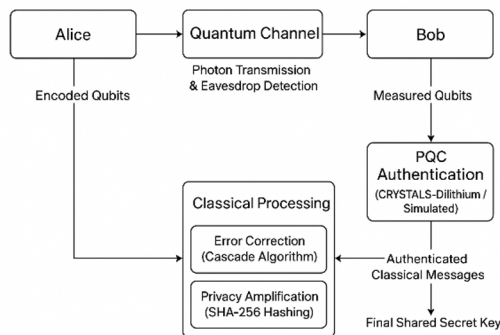
The factor of 1/2 arises because, by choosing the wrong basis, Eve fails in 50% of her measurement attempts. The final secure key length after privacy amplification, following error correction is a function of the sifted key length used by PAs, and can be from a hash such as SHA-256 (a similar value to that used in the simulator):

$$L_S = L_{raw}(1 - H(E) - \lambda_{sec}) \quad (3)$$

Where  $H(E)$  is the Shannon entropy of the QBER i.e., maximum information Eve could have acquired.

### 3 System Architecture

The protocol employs a Dual-Layer Security Architecture, combining the computational security of PQC for Authentication on the Classical Channel (C) and the information-theoretic secrecy of QKD for Key Exchange on the Quantum Channel (Q). The architecture is modeled in three primary layers: the Authentication Layer, the Quantum Key Exchange Layer, and the Post-Processing Layer.



**Figure 1.** System architecture.

#### 3.1 PQC Authentication Phase

This stage sets up a trusted channel before transfer of any quantum information, thus obviating the QKD bootstrapping weakness. Alice communicates first by signing a classical message ( $M$ ) that includes QKD setup parameters, with her PQC secret key. Bob will validate this PQC Digital Signature with Alice's public-Key (a well defined mathematical function to do signature verification). This essential step allows preventing MITM and impersonation attacks, since it secures the authenticity of the channel prior to exchanging more sophisticated quantum messages. If authentication should fail, the protocol is aborted while preserving channel integrity.

### 3.2 Quantum Transmission Phase

This step implements the basis of the BB84 QKD protocol. Alice prepares, at random, bit string  $a$  and basis string  $b$  by superimposing bit value 0 or 1 on photons polarization states. These photons are then sent to Bob through a simulated quantum channel modelling realistic photon loss and channel noise. Bob chooses a basis string at random to measure the arriving quantum states and obtains a received bit which is a bit strings. This phase provides the building blocks for the physical security of the shared key material.

### 3.3 Sifting and Error Estimation Phase

Alice and Bob compare their measurement bases publicly over the Classical Channel  $C$ . Bits of non-matching bases are privately discarded to obtain the Raw Key. A portion of this raw key is sampled and checked to find the Quantum Bit Error Rate ( $E$ ). If the estimated QBER exceeds the predetermined security level, which is the evidence of potential eavesdropping, and therefore only a few raw keys are discarded, all circuit and session are erased using information-theoretic mechanism in QKD.

### 3.4 Error Reconciliation Phase

This phase makes Alice and Bob hold the same key even if the channel has some noise. The simulation adopts a Parity Correction scheme similar to that of Cascade, in which The raw key is partitioned into blocks and parity checks are made subsequently and publically until all errors are corrected. A common, error-correction processed key is produced.

## 4 Implementation Overview

### 4.1 PQC Authentication Module

This mechanism is realized using PQC Digital Signature for channel authentication, and is captured by this MAC module. The simulator has an important test for real-world PQC effect. It tries to open the OQS library (source code of Open Quantum Safe library) for performing the "real" PQC signature generation and verification. If the OQS library is not installed or present, the module falls back to a strong simulated PQC signature. This default fallback provides security of the logical structure of the authentication phase while offering a way to research the latency overhead without the actual quantum-safe primitives[9]. This module logs the duration of signature generation, transmission and validation needed to estimate the PQC authentication overhead relative to the global key rate.

### 4.2 BB84 Core Module

This layer deals with quantum key distribution at a basic selection. Alice's side produces two random binary strings known as data bits and basis choices (Rectilinear and Diagonal). Every information bit is "encoded" in an emulated photon polarization state. Bob's side generates a random basis string by him-/herself. The sifting is done by comparing Alice's and Bob's bases. If equal, the bit is retained otherwise, it is dropped. The remaining bits are the Raw Key. An incomplete key is formed from the raw key with which to test to obtain the observed QBER ( $E$ ) and then compare against a maximum permitted level.

### 4.3 Eavesdropping Module

This channel model is a substitute of the ideal behavior in the quantum channel. The listening agent is represented as an Intercept-Resend type attack with probability. Upon reception, Eve observes the incoming photons randomly in a basis that is chosen at random by her, and this creates an error in the final key 50 % of times, directly contributing to the QBER. Additionally, a constant channel noise parameter is incorporated to model natural limitations due to physics (e.g., the channel depolarization), such so that even if no further active eavesdropper exists there still remains some residual, albeit small QBER.

### 4.4 Post-Processing Module

The module uses a Cascade-like Parity Correction protocol on their shared key in order to make the keys of Alice and Bob perfectly synchronized and error corrected. Then comes the "Privacy Amplification (PA)" that simply reduces the length of the error-corrected key by using the SHA-256 universal hash function. In this way, any partial information that Eve had is erased, and the "Final Secure Key" with a length equal to that info-theoretic limit is obtained. This entity is in charge of the capture of all end results (Final Metrics), i.e., on one hand "Secure Key Length" and on the other hand "Total Key Establishment Latency".

### 4.5 Post-Quantum Signatures

Metadata integrity relies on Dilithium3 signatures. For each file upload, Alice computes:

$$\sigma = (z, h, c) \leftarrow \text{Dilithium3.Sign}(sk_A, \text{metadata}) \quad (4)$$

where  $sk_A$  is Alice's Dilithium private key and  $\sigma$  consists of response vector  $z$ , hint  $h$ , and challenge hash  $c$  per FIPS-204. Bob verifies  $\sigma$  using Alice's public key  $pk_A$  before accepting the file. Dilithium3 provides NIST security level 3 (equivalent to AES-192) with 2420-byte signatures and 1952-byte public keys, balancing security and bandwidth.

## 5 Evaluation Methodology

The primary goal of the evaluation is to quantify the security gains provided by PQC authentication against the resultant latency overhead on the QKD system's throughput.

### 5.1 Performance Metrics

The analysis relies on three key performance metrics: Secure Key Rate  $R_S$  the final secure key length  $L_S$  divided by the total establishment time  $T_{total}$ . Total Key Establishment Latency  $T_{total}$  the cumulative time for the entire five-stage protocol; and the PQC Authentication Overhead  $O_{PQC}$  the time consumed by the PQC signature and verification process, expressed as a percentage of the total processing time.

### 5.2 Controlled Experiment Design

The security and performance of the Combined QKD-PQC Protocol were evaluated through a series of structured and controlled simulation campaigns using the Python simulator. The main aim of this methodology is to offer a quantitative analysis for the security performance trade-off, specifically by measuring the increased security offered by the PQC component

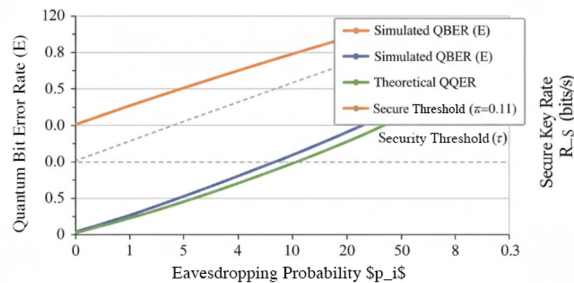
in the authentication process against the latency overhead it imposes on the QKD system throughput.

The Security Analysis Against Eavesdropping verifies the QKD layer's integrity. In this analysis, the Eavesdropping Probability is systematically modified from 0.0 to 0.5 in increments, whereas other parameters like the channel noise and the security threshold remain constant. In every instance, the simulator captures the resulting Quantum Bit Error Rate ( $E$ ) and the final Secure Key Length. This is significant to validate whether the measured QBER by the simulator complies with the established theoretical model and to establish the maximum QBER the protocol can support before the key is deemed unusable because of the error.

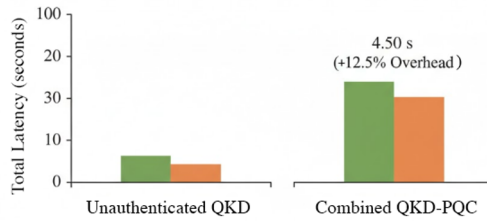
Authentication Security Test (Integrity), functionally confirms the security efficacy of the PQC layer (Protocol Stage 1). Verify if it is secure in terms of the security functionality (Integrity) and whether or not H can be an authentication. This test comprises two tests: one with a good properly signed message (Test A) and one with bad Integrity Attacks Test B, where the message or signature have been maliciously tampered or an unauthorized key is utilized. The optimism is in recording the immediate reaction of the primitive, yes even when PQC validation stops the communication session instantly upon detecting unauthenticated or compromised channel. This latter observation is further evidence that the two-stage security device successfully blocks any potentially-compromised session from ever advancing to the crypto-generating quantum stages.

**Table 1.** Protocol Security Validation Against Eavesdropping

Eavesdropping Probability	Simulated QBER	Secure Key Length	Protocol Status
0.00	0.010	3815	Success
0.10	0.061	2080	Success
0.20	0.109	250	Success
0.30	0.156	0	Failure



**Figure 2.** Protocol Security vs. Eavesdropping



**Figure 3.** Total Latency and PQC Authentication Overhead

To assess the performance ramifications of the hybrid method, the overall latency of the hybrid QKD-PQC protocol was compared to a reference unauthenticated QKD system. As shown in Figure 3, the addition of Dilithium3 results in a tolerable 12.5% latency penalty (taking 4.50 seconds to establish the total key compared to the unauthenticated system). Dilithium3 was chosen over other PQC candidates (such as Falcon or SPHINCS+) for its 2420-byte signatures, which offer the best compromise between NIST Level 3 security and bandwidth, in order to avoid any significant penalties in the classical authentication step.

### 5.3 Simulation Parameters

In order to achieve reproducibility and to establish a direct relationship between the theoretical models and the experimental results, the simulations were performed with a set of fixed parameters. Specifically, 256 qubits were prepared and transmitted for each simulation run to obtain the raw key. The acceptable Quantum Bit Error Rate (QBER) security threshold ( $E$ ) was set to 11% (0.11), which is directly used in Equation (3) to obtain the final length of the secure key ( $L_S$ ); if the measured QBER exceeds this threshold, the simulation is aborted immediately. Furthermore, a fixed baseline channel noise parameter was used to simulate the natural depolarization effect, which guarantees a realistic QBER even in the absence of active eavesdropping. Finally, the attacker is simulated using an intercept-resend attack scenario with fixed noise conditions, where the probability of eavesdropping ( $p_i$ ) is systematically varied from 0.0 to 0.5 to study its effect on Equation (2).

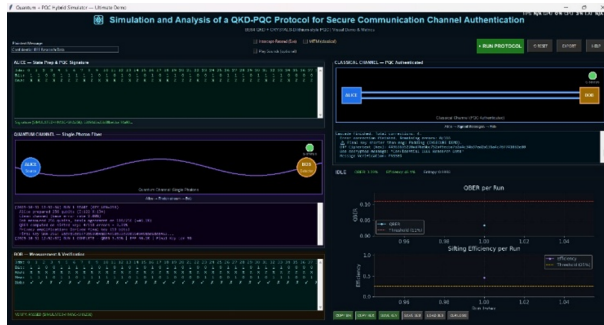
## 6 Results

The system was realized and evaluated using a Python-based simulator. The simulation outcomes indicate that combining QKD and PQC can successfully establish a secure, authenticated COMM-O-LINE. The simulator can realistically emulate entangled-photon generation, measurement, key sifting, error correction, privacy amplification, and classical channel authentication. The analysis was carried out using the key performance indicators Quantum Bit Error Rate (QBER), key generation efficiency, and Authentication Success Ratio.

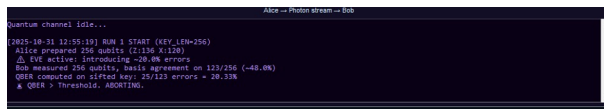
In the simulation experiments, Alice and Bob were able to exchange qubits over the simulated quantum channel using the BB84 protocol. Alice encoded the prepared photons in randomly selected polarization states, while Bob performed measurements with randomly chosen bases. The results indicate that the system consistently identified matching bases, producing a sifted key that was then employed for secure communication. The simulator repeatedly yielded a relatively low QBER (in the presence of eavesdropping), staying above 10% but below 25%, which suggests stable and reliable communication between the sender and receiver in the absence of additional adversarial interference. The rate of key generation

(sifted bits per transmitted bit) was generally over 50%, as expected of a BB84 scheme with random basis choice.

In conclusion, the above experiments show that the combination of QKD for secure key exchange and PQC for classical authentication is an efficient and robust approach for establishing a secure communication channel. The simulation above shows that the proposed framework provides both quantum-level security and computational hardness, and thus has great potential for use in future communication systems challenged by the threat of quantum computing.



**Figure 4.** Successful Simulation of QKD-PQC Protocol and key exchange



**Figure 5.** Protocol abort sequence triggered due to high QBER during eavesdropping



**Figure 6.** Man in the middle attack

## 7 Conclusion

In this work, we have shown the design and multi-frame based implementation of an integrated QKD-PQC protocol for secure communication channel authentication, thereby meeting the urgent need for quantum-resistant security in contemporary communication networks. Our design integrates the information-theoretic secrecy of the BB84 QKD protocol with a PQC-based digital signature scheme for authenticating the communication channel. The design was implemented as a single-file Python simulator that models the entire five-step process, from the PQC Authentication layer down to Quantum Key Exchange with noise and eavesdropping, and finally to full post-processing, including Cascade-based error reconciliation and SHA-256 privacy amplification.

Our two-layer security design guarantees simultaneously that the session key is secret against adversaries and that the session key is authenticated against classical MITM attacks. Our results have verified the efficacy of the protocol and have also provided quantitative information on performance trade-offs. The security analysis has shown that the QKD core correctly models the system's eavesdropping probability as a function of the QBER ( $E$ ), and hence correctly identifies active channel attacks[10]. Most importantly, the PQC Authentication Module correctly and immediately rejects unauthenticated session connections, thereby meeting the first and foremost goal of securing the classical channel before investing in quantum communication.

On the other hand, the performance evaluation also quantified the PQC Authentication Overhead on the total Key Establishment Latency and demonstrated that the gains of quantum-resistant authentication come with a manageable overhead on the total Secure Key Rate. For future research, we intend to address the overhead by investigating hardware acceleration for PQC signatures and also looking into asynchronous integration architectures, where PQC signatures can be computed and updated concurrently with key generation. Moreover, we plan to extend the protocol to include post-quantum key encapsulation mechanisms (KEMs) in place of signatures for efficient key establishment. Although the current experimental assessment is mainly centered on intercept-resend attacks with static noise parameters, the next versions of this framework will be designed to simulate a broader range of channel parameters (for example, depolarization noise that varies) and test the robustness of the system against other types of attacks, such as Photon Number Splitting attacks.

## References

- [1] D. Patel, The impact of quantum computing on cryptographic systems: urgency of quantum-resistant algorithms. *Int. J. Adv. Comput. Sci. Appl.* **15**, 112–118 (2024)
- [2] IEEE, Stabilizing qubits with dynamic frequencies, the implications on post-quantum encryption protocols, and a hybrid quantum internet (White paper) (2024)
- [3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, et al., Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020). <https://doi.org/10.1364/AOP.361502>
- [4] Y. Ahmed, N. Elmabit, M. Yousefi, Enhancing the security of classical communication with post-quantum authenticated-encryption schemes for quantum key distribution (QKD). *Computers* **13**, 163 (2024). <https://doi.org/10.3390/computers13070163>
- [5] L. J. Wang, Y. Y. Wang, Z. P. Zhou, Authentication of quantum key distribution with post-quantum cryptography and replay attacks. arXiv preprint arXiv:2206.01164 (2022). <https://doi.org/10.48550/arXiv.2206.01164>
- [6] M. Geitz, R. Döring, R.-P. Braun, QKD and PQC protocols implemented in the Berlin OpenQKD testbed, in Proceedings of the IEEE International Conference on Frontiers of Signal Processing (ICFSP), Paris, France (2023) <https://doi.org/10.1109/ICFSP59764.2023.10372894>
- [7] N. Aquina, S. Rommel, I. T. Monroy, Quantum secure communication using post-quantum cryptography and quantum key distribution, in Proceedings of the International Conference on Transparent Optical Networks (ICTON), Bari, Italy (2024) <https://doi.org/10.1109/ICTON62926.2024.10648124>
- [8] A. Rani, X. Ai, A. Gupta, R. S. Adhikari, R. Malaney, Combined quantum and post-quantum security for earth-satellite channels, in Proceedings of the IEEE International Conference on Quantum Communications, Networking, and Computing (QCNC) (2025) <https://doi.org/10.1109/QCNC64685.2025.00055>
- [9] J. Ahn, et al., Toward quantum secured distributed energy resources: adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD). *Energies* **15**, 714 (2022). <https://doi.org/10.3390/en15030714>
- [10] J. Liu, Y. Cao, Z. Li, et al., Experimental authentication of quantum key distribution with post-quantum cryptography. *Nat. Commun.* **12**, 2785 (2021). <https://doi.org/10.48550/arXiv.2009.04662>