Quantum Key Distribution with Enhanced PQC Validation

Vlad BERARU, Carmen MILEA
Bucharest University of Economic Studies
beraruvlad21@stud.ase.ro, carmen.milea@csie.ase.ro

Quantum Key Distribution (QKD) provides information-theoretic security based on quantum mechanics, but its practical deployment is limited by its reliance on classical infrastructure and inability to operate as a standalone solution. Recent research emphasizes hybrid approaches that combine QKD with post-quantum cryptography (PQC) to achieve practical and robust security. This paper presents a hybrid key distribution model integrating QKD with the post-quantum key encapsulation mechanism. The two independently generated keys are combined to derive a unified shared secret, enhancing resilience against both classical and quantum adversaries. The system is implemented using a simulated quantum environment, enabling the emulation of quantum communication over classical networks. The proposed approach is validated through a secure image transmission use case, demonstrating the correctness of the hybrid key exchange. The results highlight the feasibility of hybrid classical–quantum cryptographic systems as a practical step toward secure communication in emerging quantum network infrastructures.

Keywords: *Quantum Key Distribution, Post-Quantum Cryptography, Hybrid Cryptography, Quantum Networks, Secure communication*
DOI: 10.24818/issn14531305/30.2.2026.03

1 Introduction

Quantum Key Distribution (QKD) has emerged as one of the most prominent applications of quantum cryptography, offering information-theoretic security based on the principles of quantum mechanics. However, QKD is not a standalone cryptographic solution, but rather a key establishment mechanism that must be integrated with other cryptographic primitives, such as symmetric encryption and authentication protocols [1]. In this context, hybrid and dual key agreement schemes have been proposed, where QKD is combined with classical cryptographic methods to enhance robustness and ensure practical deployability in real-world systems [1]. This perspective highlights the necessity of combining quantum and classical approaches rather than treating QKD as a replacement for existing cryptographic infrastructures.

A broader and more application-oriented view demonstrates the integration of QKD across multiple domains, including banking, healthcare, smart grids, and government communications. While QKD provides strong security guarantees rooted in quantum physics, it remains dependent on classical mechanisms, particularly for authentication, which are typically based on computational assumptions. Consequently, hybrid approaches that combine QKD with post-quantum cryptography (PQC) are increasingly emphasized as a practical path forward, balancing theoretical security with real-world constraints [2].

The deployment of Quantum Key Distribution (QKD) at scale is closely tied to the development of quantum networks. Early visions of the quantum internet describe architectures composed of interconnected quantum nodes capable of storing and processing quantum information, with photons acting as carriers of quantum states between nodes [3]. These networks enable the distribution of quantum information and entanglement across multiple nodes, forming the foundation for secure communication and distributed quantum applications.

Within this context, a fundamental shift introduced by quantum networks is the abstraction of entanglement as a consumable resource. Rather than focusing solely on data transmission, quantum networks can be viewed as systems that provide "*Entanglement as a Service"*, where applications request and utilize

entangled states to perform specific tasks. Unlike classical networks, which deliver data packets between nodes, quantum networks generate and distribute entangled qubit pairs that can be consumed by higher-level protocols. This model enables a wide range of applications, including QKD, quantum teleportation, and distributed quantum computing, all of which rely on the availability of entanglement between distant nodes. Consequently, the primary objective of the network shifts toward the reliable generation, management, and distribution of entanglement as a shared resource [4].

Building upon this perspective, recent research proposes structured communication models that integrate quantum communication into classical networking frameworks, such as OSI or TCP/IP stacks. These approaches introduce layered architectures in which quantum and classical components coexist, enabling interoperability with existing network infrastructures. Within such models, classical channels are responsible for coordination, synchronization, and control, while quantum channels are used for transmitting quantum states and generating cryptographic keys [5].

A defining characteristic of quantum networks is their reliance on quantum mechanical properties that fundamentally differ from classical communication paradigms. While classical systems exchange deterministic bits, quantum networks operate on qubits that can exist in superposition and become entangled, enabling exponentially larger state spaces and advanced functionalities such as quantum teleportation and inherently secure key distribution [3]. The realization of these capabilities depends on the development of suitable physical technologies for generating, transmitting, and storing quantum information. Current implementations rely on a variety of platforms, including superconducting circuits, trapped ions, quantum dots, and photonic systems, each offering different trade-offs in terms of performance and scalability [5].

The evolution of quantum networks reflects a transition from simple point-to-point communication systems toward complex, multi-layered infrastructures supporting diverse applications. Early implementations focused primarily on QKD, often relying on trusted-node architectures and limited communication distances. As research progressed, attention shifted toward enabling long-distance entanglement distribution through mechanisms such as quantum repeaters and advanced network protocols. More recent developments emphasize hybrid architectures that integrate quantum communication within classical networking frameworks, improving scalability and interoperability. This evolution is expected to continue toward fully distributed quantum computing environments, where interconnected quantum devices operate as a unified system, extending beyond secure communication use cases [5].

To evaluate the performance and maturity of these technologies, several key performance indicators (KPIs) are commonly used, including coherence time, fidelity, and technology readiness levels. Coherence time defines how long a quantum state can be preserved before decoherence occurs, while fidelity measures the accuracy of quantum state preparation and operations. Recent advancements demonstrate significant progress, with coherence times reaching milliseconds in superconducting systems and much longer durations in trapped-ion platforms, alongside fidelities approaching near-perfect values [5]. Despite these improvements, challenges related to scalability, noise, and stability remain significant barriers to large-scale deployment.

Beyond theoretical models, real-world implementations have demonstrated the feasibility of large-scale quantum communication. A notable example is the satellite-based quantum network using the “Micius” satellite, which enables intercontinental QKD by acting as a trusted relay between distant ground stations [6]. This approach overcomes the distance limitations of optical fibber by leveraging free-space communication, successfully extending BB84-based QKD to distances of up to 7600 km [6]. A more recent demonstration further extends these capabilities, where the “Jinan-1” satellite enabled quantum communication between China and South Africa over

a distance exceeding 12,900 km [7]. These experimental results mark a significant milestone toward global quantum communication infrastructure.

Recent advancements further indicate a shift toward more dynamic and programmable quantum networks. The generate-when-requested (GWR) model introduces the concept of on-demand entanglement generation, improving efficiency compared to traditional approaches that rely on pre-generated and stored entanglement [4]. At the same time, the development of high-level software abstractions, such as QNodeOS, enables the execution of quantum network applications through a hybrid architecture that separates classical and quantum processing into dedicated components [8]. This design facilitates real-time interaction between classical and quantum systems, which is essential for practical deployment.

In parallel, efforts to integrate QKD into existing communication infrastructures have led to scalable and flexible network architectures. The MadQCI framework demonstrates a software-defined networking (SDN) approach for QKD networks, where control and data planes are decoupled to enable centralized management and interoperability across heterogeneous systems [9]. Unlike isolated experimental setups, this approach focuses on real production environments, highlighting the importance of integrating quantum communication within classical telecommunication ecosystems.

In this context, this paper proposes a hybrid key distribution model that combines Quantum Key Distribution with post-quantum cryptographic validation mechanisms to enhance both security and practical deployability. The proposed approach integrates a quantum communication layer, based on BB84-like protocols, with a classical channel employing a post-quantum key encapsulation mechanism, enabling secure key establishment over hybrid communication channels. The system is designed around a client–server architecture, where two entities exchange keys through both quantum and classical means, leveraging quantum-generated randomness while ensuring robustness through computationally secure validation. By combining these complementary paradigms, the proposed solution addresses the limitations of standalone QKD systems, providing improved resilience against both classical and quantum adversaries. This work aims to demonstrate that hybrid classical–quantum key distribution represents a practical and scalable step toward secure communication in future quantum network infrastructures.

2 Architecture

The rapid advancement of quantum computing technologies has raised significant concerns regarding the long-term security of classical cryptographic systems. In particular, the development of quantum processing units introduces the potential to break widely used public-key algorithms through quantum attacks, such as those enabled by Shor's algorithm. This threat model, often referred to as "harvest-now, decrypt-later," highlights the risk that encrypted data intercepted today may be decrypted in the future once sufficiently powerful quantum computers become available.[10]

To mitigate this risk, post-quantum cryptographic (PQC) algorithms have been developed as quantum-resistant alternatives to classical schemes. In this work, the classical communication layer is based on CRYSTALS-Kyber[11], one of the key encapsulation mechanisms selected in the NIST post-quantum cryptography standardization process. Kyber provides computational security against both classical and quantum adversaries, while maintaining efficiency and compatibility with existing communication infrastructures. Within the proposed system, it is used to establish a secure classical channel and to validate the integrity of the key exchange process. Complementing the classical layer, the quantum communication component is based on the BB84 protocol[12], introduced by Charles Bennett and Gilles Brassard in 1984 as the first practical quantum key distribution scheme. BB84 leverages fundamental principles of quantum mechanics, including superposition, the no-cloning theorem, and wave-

function collapse, to enable secure key generation and inherent eavesdropping detection. Any attempt to intercept the quantum transmission introduces measurable disturbances, allowing communicating parties to detect the presence of an adversary.

Experimental and simulation-based studies further highlight the effectiveness of BB84 in practical scenarios. It has been shown that after approximately 25–50 transmitted quantum states, the probability of undetected intrusion becomes very low, demonstrating the protocol's strong security guarantees. At the same time, a trade-off exists between security and performance, as increasing the number of transmitted states improves detection probability but also increases computational and communication overhead. Another important characteristic of BB84 is that it does not rely on entanglement, meaning that each transmitted qubit is independent, simplifying implementation compared to entanglement-based protocols.[13]

From a system perspective, BB84 operates using a hybrid communication model that combines a quantum channel for transmitting qubits with a classical authenticated channel for basis reconciliation and key agreement between the communicating entities. However, practical implementations of BB84 are subject to several limitations, including noise in the communication channel, imperfections in photon generation and detection, and vulnerabilities to certain classes of attacks. Additionally, the protocol may be susceptible to denial-of-service scenarios, where disruption of the quantum channel prevents successful key generation. These constraints highlight the necessity of integrating BB84 within a broader hybrid cryptographic framework, rather than relying on it as a standalone solution.[14]

In addition to BB84, several other quantum cryptographic protocols have been proposed to address secure key distribution using different quantum principles. One notable example is the E91 protocol, introduced by Ekert, which leverages quantum entanglement and Bell's theorem to establish security guarantees based on the violation of classical correlations [15]. Another approach is represented by the DL04 protocol, which enables secure direct communication using a quantum one-time pad mechanism. Despite these advancements, BB84 remains the most widely studied and practically implemented protocol, making it the preferred choice for this work due to its maturity, simplicity, and extensive experimental validation [13], [16].

The implementation of quantum key distribution mechanisms is inherently dependent on the underlying quantum network infrastructure. Foundational studies describe quantum networks as systems composed of interconnected quantum nodes and quantum channels, where nodes are responsible for generating, processing, and storing quantum information, while photons act as "flying qubits" that transmit quantum states between nodes [3], [17]. Within this framework, entanglement distribution plays a central role, enabling communication and coordination between distant entities and serving as the fundamental resource for quantum communication and computation [3], [4], [17].

One of the main challenges in quantum networking is the extension of communication over long distances. Due to losses in transmission channels, entanglement degrades exponentially with distance, limiting the scalability of quantum communication systems. To address this limitation, protocols such as the DLCZ scheme introduce mechanisms for scalable long-distance communication based on atomic ensembles and linear optics[18]. This approach relies on probabilistic entanglement generation, followed by entanglement swapping and purification, allowing entanglement to be extended across multiple network segments. A key innovation of this model is the use of atomic ensembles as quantum memory, enabling the storage and synchronization of quantum states and forming the foundation for quantum repeater architectures [3], [18].

Quantum repeaters further enhance the scalability of quantum networks by enabling the distribution of entanglement over extended distances through intermediate nodes. By dividing long communication paths into smaller segments and performing entanglement swap-

ping, repeaters mitigate the effects of loss and noise, making large-scale quantum communication feasible [3], [17], [18]. These mechanisms are essential for transitioning from point-to-point communication systems to fully connected quantum networks.

From an architectural perspective, quantum communication systems fundamentally differ from classical networks. While classical systems rely on deterministic data transmission, quantum networks operate under constraints imposed by quantum mechanics, including the no-cloning theorem and the probabilistic nature of quantum measurement. As a result, traditional networking techniques such as copying or retransmission are not applicable [19]. Instead, communication relies on entanglement distribution and quantum teleportation, where quantum states are transferred using shared entanglement combined with classical communication [17], [19].

This hybrid communication model is a defining characteristic of quantum networks, where both quantum and classical channels are required for correct operation. Quantum channels are used for transmitting qubits and establishing entanglement, while classical channels handle coordination, synchronization, and protocol execution. The interaction between these two layers is critical, as many quantum protocols depend on classical information exchange to complete their operations [17], [19], [20].

Further insights into this interaction are provided by studies on modular quantum systems, where multiple quantum processors are interconnected to form distributed architectures. In such systems, entanglement-based communication enables the exchange of quantum information between processing units, often using EPR pairs to facilitate teleportation. Network topology plays a significant role in performance, with configurations such as line, ring, star, and fully connected networks influencing communication cost and scalability. Additionally, there exists a trade-off between communication and computation resources, as increasing the number of quantum links can improve parallelism but reduce the number of qubits available for computation[20].

An important observation in these hybrid systems is that classical communication can become a performance bottleneck. Delays in transmitting classical information, such as measurement outcomes required for teleportation, can negatively impact quantum coherence and overall system fidelity. As a result, efficient routing, scheduling, and coordination between quantum and classical layers are essential for achieving high-performance quantum networks. This highlights the need for a full-stack perspective, where hardware capabilities, network design, and protocol behaviour are jointly considered when building scalable quantum communication systems [20].

Because BB84 does not require a fully developed quantum network, but only a mechanism for transmitting qubits between communicating entities, a simplified quantum communication model can be adopted. In particular, the protocol relies on the exchange of quantum states between two nodes, without requiring persistent entanglement distribution or complex network-level coordination. To enable long-distance transmission of quantum states, this work adopts a satellite-based approach inspired by the system proposed by Liao *et al.*, where satellites are used as trusted relays to transmit flying qubits over large distances using free-space optical links [6].

Within the proposed architecture, the quantum communication layer is composed of two Quantum Processing Units (QPUs), corresponding to the communicating entities. Each QPU is responsible for generating, encoding, and measuring quantum states, acting as a quantum node within the system. These units implement quantum interfaces capable of converting stationary qubits, stored in matter-based systems, into flying qubits represented by photons, and vice versa, enabling the transmission of quantum information between distant nodes [3]. The overall system architecture is illustrated in *Fig. 1*, highlighting the interaction between quantum and classical components, as well as the satellite-based communication model.

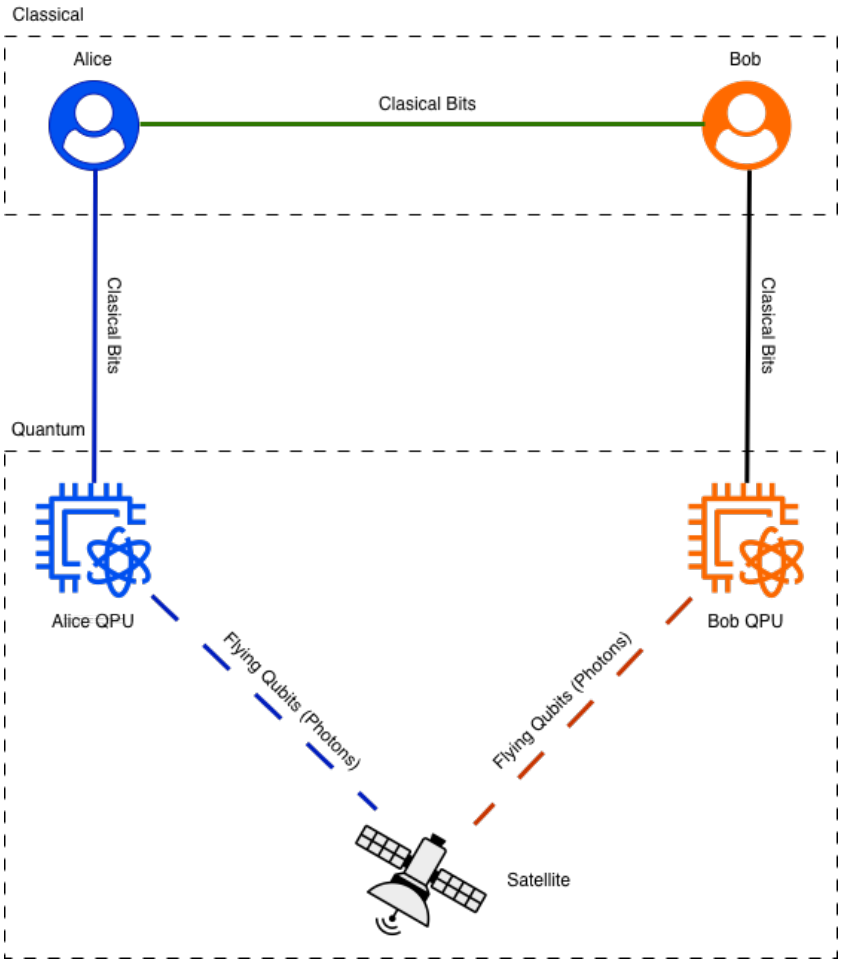


Fig. 1. Hybrid classical–quantum communication architecture.
The system consists of two entities (Alice and Bob), each equipped with a Quantum Processing Unit (QPU) and a classical processing unit. Quantum communication is performed via a satellite relay using flying qubits, while classical communication is established using a post-quantum cryptographic channel.

In addition to the quantum layer, each QPU is coupled with a classical processing unit, which is responsible for handling the classical communication channel. This channel is used to perform protocol coordination tasks such as basis reconciliation, error checking, and key validation, as well as to establish a secure classical connection using post-quantum cryptographic mechanisms. The integration of quantum and classical processing components reflects the hybrid nature of quantum communication systems, where classical communication is essential for the correct execution of quantum protocols [17], [19].

3 The Proposed Solution

Building upon the concepts and architectural models discussed in the previous chapter, the proposed solution implements a hybrid key distribution system that combines classical and quantum communication mechanisms. As highlighted in prior research, Quantum Key Distribution (QKD) cannot operate as a standalone solution and must be integrated with classical cryptographic techniques to ensure authentication and practical deployability. In this work, a hybrid approach is adopted, combining a post-quantum classical key exchange with a BB84-based quantum key generation process.

To enable experimentation without requiring specialized quantum hardware, the quantum communication layer is simulated using software-based quantum computation techniques. Specifically, the system leverages the Java Strange framework[21], as introduced in *Quantum Computing in Action* [22] by Johan Vos, to model quantum states and operations.

Two independent Java-based servers are implemented to act as Quantum Processing Units (QPUs), each responsible for executing the BB84 protocol. These QPUs simulate the behaviour of quantum nodes, including qubit generation, encoding, and measurement.

Within this simulation environment, "flying qubits" are represented as serialized Java objects corresponding to quantum states generated using the Java Strange library. Instead of physical photon transmission, the quantum channel is emulated using standard network sockets, where serialized qubit objects are transmitted between the QPUs. This approach allows the system to replicate the behaviour of quantum communication while remaining fully executable on classical hardware.

Each communicating entity, Alice and Bob, consists of a classical processing component and an associated QPU server. The classical components establish a secure communication channel using a post-quantum key encapsulation mechanism, while the QPUs handle the quantum key generation process. The communication between QPUs, including the simulated transmission of qubits, is performed over the host machine network, effectively emulating a quantum network infrastructure without requiring physical quantum devices or satellite links.

The overall system architecture is illustrated in *Fig. 1*, highlighting the interaction between classical and quantum components within the hybrid communication model. The classical channel is responsible for key encapsulation, coordination, and post-processing, while the quantum channel is used to generate raw key material through the BB84 protocol. The execution flow of the protocol is further detailed in the sequence diagram presented in *Fig. 2*.

Following this architecture, the system executes the key exchange process in multiple stages. Initially, Alice and Bob establish a classical connection and perform a post-quantum key exchange using CRYSTALS-Kyber. Subsequently, the QPUs establish a connection and execute the BB84 protocol, where simulated qubits are generated, serialized, transmitted, and measured. The classical channel is then used for basis reconciliation and key validation.

A key aspect of the proposed implementation is the construction of the final shared secret through the combination of classical and quantum keying material. Both the post-quantum key encapsulation mechanism and the BB84 protocol generate keys of equal length (32 bytes). To derive a unified hybrid key, the two keys are combined using a bitwise exclusive OR (XOR) operation. This ensures that the resulting key inherits security properties from both components, requiring an adversary to compromise both the classical and quantum key exchange mechanisms to recover the final secret.

Formally, if K_{PQC} represents the classical key generated using Kyber and K_{QKD} represents the quantum key obtained through BB84, the final shared key K_H is computed as:

$$K_H = K_{PQC} \oplus K_{QKD}$$

To demonstrate the practical applicability of the proposed approach, the system includes an application-level use case involving secure image transmission.

After the hybrid key is established, Alice encrypts a bitmap (BMP) image using a bytewise XOR operation, applying the hybrid key over the image data. The encrypted image is then transmitted over an unsecured classical communication channel.

Upon reception, Bob applies the same XOR operation using the shared hybrid key to decrypt the image and reconstruct the original content. Due to the symmetric nature of the XOR operation, encryption and decryption are identical processes, ensuring correct recovery of the transmitted data as long as both parties share the same key. Although XOR-based encryption is not intended for production use, it provides a clear and efficient method for validating the correctness of the key exchange process.

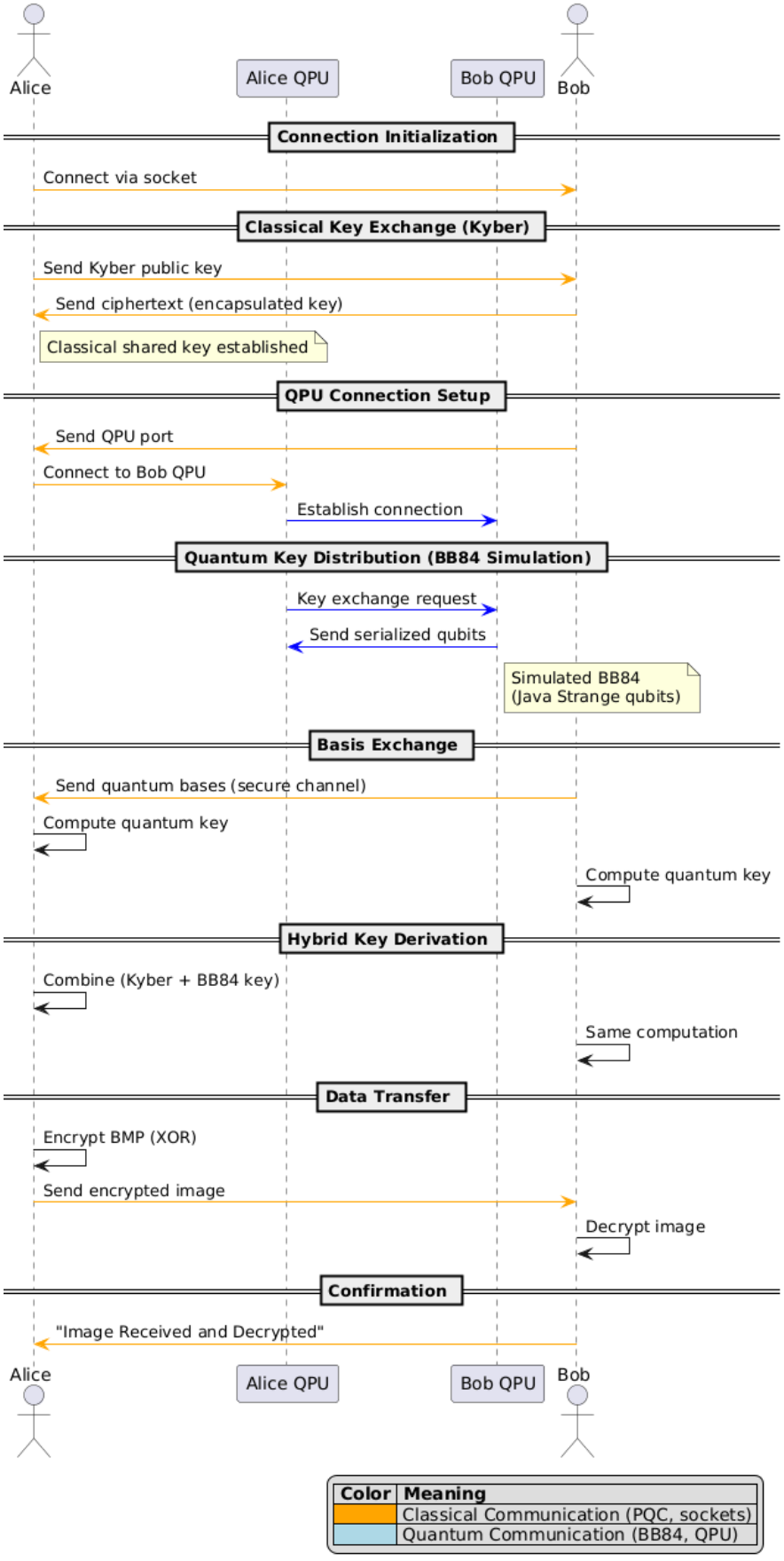


Fig. 2. Sequence diagram of the hybrid classical–quantum key exchange between Alice and Bob.

As illustrated in *Fig. 3*, the application interface provides a visual representation of the entire process. On the sender side (Alice), both the original and encrypted images are displayed, while on the receiver side (Bob), the encrypted and successfully decrypted images are shown. This demonstrates not only the correctness of the hybrid key derivation process but also the integrity of the transmitted data.
Overall, the proposed solution demonstrates the feasibility of integrating simulated quantum key distribution with post-quantum cryptographic mechanisms in a unified system. By combining both paradigms into a practical implementation, the system highlights how hybrid classical–quantum approaches can be used to achieve secure communication in environments where real quantum infrastructure is not yet widely available.

4 Conclusion

The rapid advancement of quantum computing technologies has significantly reshaped the landscape of secure communications, raising fundamental concerns regarding the long-term viability of classical cryptographic systems. In this context, Quantum Key Distribution (QKD) has emerged as a promising paradigm, offering information-theoretic security based on the laws of quantum mechanics. However, as highlighted throughout this work, QKD alone cannot function as a complete cryptographic solution, as it inherently depends on classical mechanisms for authentication, coordination, and practical deployment. Consequently, recent research increasingly emphasizes hybrid approaches that combine QKD with classical and post-quantum cryptographic (PQC) techniques to achieve both robustness and real-world applicability.
This paper contributes to this evolving paradigm by proposing and implementing a hybrid key distribution model that integrates a BB84-based quantum key generation process with a post-quantum key encapsulation mechanism, specifically CRYSTALS-Kyber. The proposed system demonstrates how two independent sources of security—quantum-generated randomness and computational hardness—can be combined into a unified framework. A key aspect of the implementation is the derivation of a shared secret through the bitwise XOR combination of the classical and quantum keys, ensuring that the resulting key inherits security properties from both components. This dual-key approach strengthens resilience against both classical and quantum adversaries, as compromising the final key requires breaking both underlying mechanisms.
To enable practical experimentation, the quantum communication layer was simulated using the Java Strange framework, allowing the modeling of quantum states and operations without requiring specialized quantum hardware. The system architecture, based on two communicating entities (Alice and Bob) equipped with
simulated Quantum Processing Units (QPUs), successfully replicates the behavior of hybrid quantum–classical communication systems. The use of serialized quantum states to emulate flying qubits, combined with classical socket-based communication, provides a flexible and accessible environment for prototyping quantum network protocols.
The experimental validation of the proposed approach was demonstrated through a secure image transmission use case, where the hybrid key was applied to encrypt and decrypt bitmap data using XOR-based operations. Although this encryption method is not intended for production use, it provides a clear and effective mechanism for verifying the correctness and synchronization of the key exchange process. The results confirm that the integration of QKD and PQC mechanisms can be successfully achieved within a unified system, even in the absence of physical quantum infrastructure.
The findings of this study are consistent with broader developments in the field of quantum networking. Recent works[23], such as metropolitan QKD deployments and urban fiber-based quantum communication experiments, demonstrate that hybrid quantum–classical systems are not only theoretically viable but

also practically realizable. These implementations show that quantum and classical communication can coexist within the same infrastructure, supporting high-speed data transmission while leveraging quantum-generated keys for enhanced security. At the same time, advances in quantum memory, entanglement distribution, and quantum repeaters continue to push the boundaries of scalable quantum networks, paving the way toward a global quantum internet.

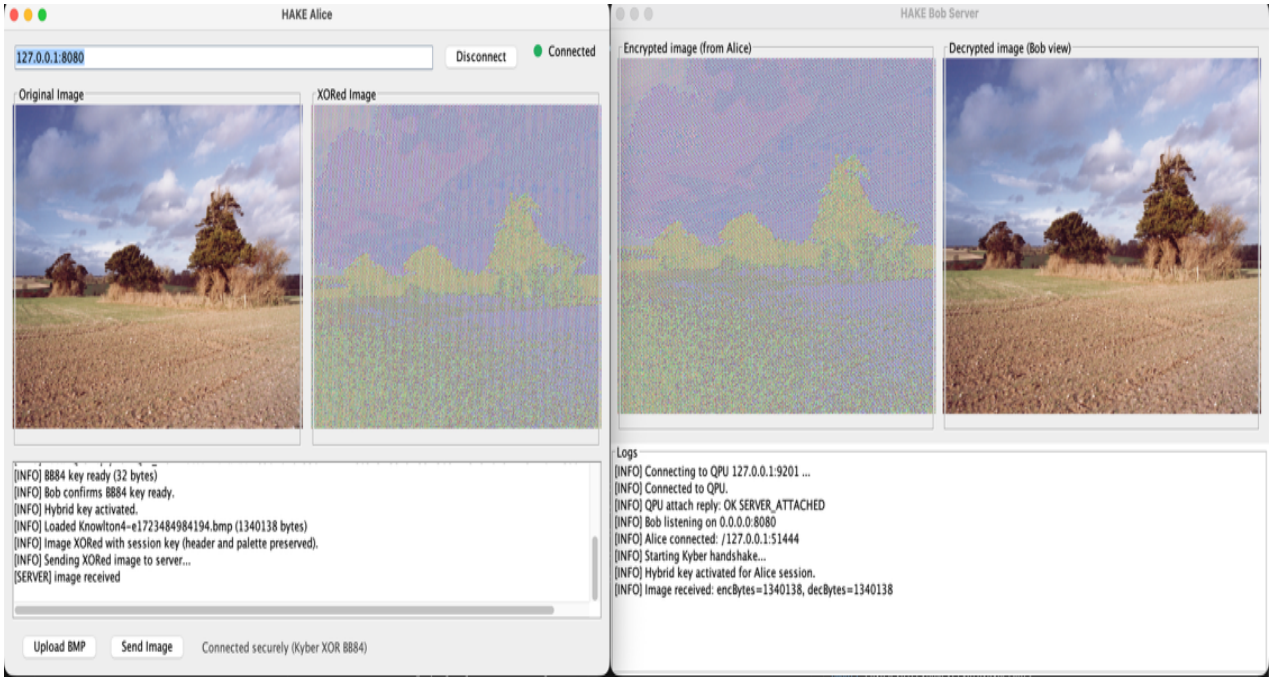


Fig. 3. Application interface showing XOR-based image encryption and successful decryption using the hybrid key.

Despite these promising developments, several challenges remain. The proposed implementation relies on simulated quantum components, which do not fully capture the physical limitations of real-world quantum systems, such as decoherence, photon loss, and noise. Additionally, protocols like BB84 face practical constraints related to transmission efficiency and vulnerability to denial-of-service attacks. These limitations highlight the need for continued research into more robust protocols, improved hardware technologies, and scalable network architectures.

Future work may explore the integration of entanglement-based protocols, such as E91, as well as the incorporation of quantum repeaters and advanced network topologies to support long-distance communication. Furthermore, replacing the demonstration-level encryption mechanism with standardized cryptographic algorithms, such as AES, would enable a more realistic evaluation of hybrid key distribution in practical applications[24]. Another promising direction involves leveraging emerging quantum network simulators and programmable frameworks to extend the system toward more complex and distributed scenarios.

In conclusion, this work demonstrates that hybrid classical–quantum key distribution represents a practical and effective approach to secure communication in the emerging quantum era. By combining the complementary strengths of QKD and post-quantum cryptography, and by providing a functional prototype that bridges theory and implementation, this study contributes to the ongoing transition from experimental quantum communication systems to scalable, real-world quantum network infrastructures.

References

[1] R. Alléaume *et al.*, “Using quantum key distribution for cryptographic purposes: a survey,” 2014. [Online]. Available:

https://arxiv.org/abs/quant-ph/0701168

[2] N. Aquina *et al.*, "A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography," *EPJ Quantum Technol.*, vol. 12, no. 1, Dec. 2025, DOI: 10.1140/epjqt/s40507-025-00350-5.

[3] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, Jun. 2008, doi: 10.1038/nature07127.

[4] T. R. Beauchamp, S. Gauthier, and S. Wehner, "White Paper on Quantum Internet Computer Science Research Challenges," 2025. [Online]. Available: https://arxiv.org/abs/2511.16745

[5] A. Meddeb, "Quantum internet building blocks state of research and development," *Computer Networks*, vol. 261, p. 111151, 2025, doi: https://doi.org/10.1016/j.comnet.2025.111151.

[6] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017, doi: 10.1038/nature23655.

[7] huaxia, "Update: Chinese-led team achieves world's first 10,000-km quantum-secured communication," XINHUANET.com. Accessed: Mar. 18, 2026. [Online]. Available: https://english.news.cn/20250320/19c7c2858c71440ba23f4b496c86c3cb/c.html?utm_source=chatgpt.com

[8] C. Delle Donne *et al.*, "An operating system for executing applications on quantum network nodes," *Nature*, vol. 639, no. 8054, pp. 321–328, 2025, DOI: 10.1038/s41586-025-08704-w.

[9] V. Martin *et al.*, "MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities," *npj Quantum Inf.*, vol. 10, no. 1, p. 80, 2024, doi: 10.1038/s41534-024-00873-2.

[10] S. Kelly, "Breaking RSA: How Quantum Computing Threatens Today's Digital Security," May 2025.

[11] J. Bos *et al.*, "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018, pp. 353–367. doi: 10.1109/EuroSP.2018.00032.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014, DOI: 10.1016/j.tcs.2014.05.025.

[13] D. Martinez Barreto and C. J. Ramos-Salas, *Quantum Cryptography, BB84 Protocol*. 2024. DOI: 10.13140/RG.2.2.26217.67681.

[14] P. Winiarczyk and W. Zabierowski, "BB84 analysis of operation and practical considerations and implementations of quantum key distribution systems," Jan. 2011.

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[16] SujayKumar Reddy M and Chandra Mohan B, "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol," 2023. [Online]. Available: https://arxiv.org/abs/2312.05609

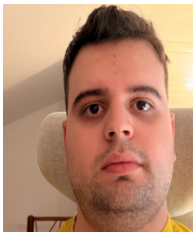
[17] B. Hildebrand, A. Ghimire, F. Amsaad, A. Razaque, and S. P. Mohanty, "Quantum communication networks: Design, reliability, and security," *IEEE Potentials*, vol. 44, no. 1, pp. 4–10, 2025, Doi: 10.1109/MPOT.2023.3322015.

[18] K. Fang, J. Zhao, X. Li, Y. Li, and R. Duan, "Quantum NETwork: from theory to practice," *Science China Information Sciences*, vol. 66, no. 8, Jul. 2023, DOI: 10.1007/s11432-023-3773-4.

[19] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, 2020, DOI: 10.1109/MNET.001.1900092.

[20] P. Escofet *et al.*, "On the Impact of Classical and Quantum Communication Networks Upon Modular Quantum Computing Architecture System Performance," in *2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*, IEEE, Aug. 2025, pp. 984–995. DOI: 10.1109/qce65121.2025.00110.

[21] RedFX Quantum, "Java Strange." Accessed: Mar. 18, 2026. [Online]. Available: https://github.com/redfx-quantum
[22] Johan Vos, "Quantum Computing in Action," 2022.
[23] J. F. Dynes *et al.*, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, no. 1, p. 101, 2019, DOI: 10.1038/s41534-019-0221-4.
[24] S. Kucera *et al.*, "Demonstration of quantum network protocols over a 14-km urban fiber link," *npj Quantum Inf.*, vol. 10, no. 1, p. 88, 2024, DOI: 10.1038/s41534-024-00886-x.



Vlad BERARU is currently a master's student in IT and Cyber Security within the Department of Informatics and Cybernetics at the Bucharest University of Economic Studies. Alongside his studies, he is a master's researcher at the university, focusing on the development and analysis of audit products for AI security. His research interests include artificial intelligence, cybersecurity, and the evaluation of software systems, with an emphasis on ensuring reliability and security in modern applications. He has practical experience in building web applications, backend systems, and network-based solutions, as well as integrating AI models into real-world projects. Currently, he is working as a software developer, continuing to expand his expertise in scalable systems and emerging technologies.

Carmen MILEA holds a B. Sc. In Informatics from the Faculty of Mathematics and Computer Science, University of Bucharest (2019), and an M. Sc. In IT&C Security from the Faculty of Economic Cybernetics, Statistics and Informatics, Bucharest University of Economic Studies (2021). Since 2026, she has been a Teaching Assistant at the Bucharest University of Economic Studies, where she teaches Multi-Paradigm Programming with Java. Her research interests include industrial automation security, network communication protocols, and IoT security frameworks.