S. Bala Chandran, 2025, 13:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Secure Communication System Using Quantum Cryptography

S. Bala Chandran, Dr. S. Prasanna
Technology & Advanced Studies (VISTAS), Chennai, India

Abstract: Quantum cryptography offers an attack-proof model for communication that is resistant to quantum computing advances. This study proposes a hybrid model that unifies Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC) to ensure security in diverse networks. Efficient key distribution, life-cycle management, and performance monitoring are facilitated through a collaborative Quantum Key Management System (QKMS) and Q-controller. By having QKD in the center and using PQC in the user terminals, this model overcomes the limitations based on the range and expense of QKD. Scalable, fault-tolerant, and end-to-end secure communications are made possible by the proposed approach.

Keywords: Quantum Cryptography, Secure Communication, QKMS, Q-Controller, Key Management.

I. INTRODUCTION

The quick strides in quantum computing are making conventional cryptographic methods such as RSA and ECC vulnerable to attacks from quantum computing. Methods such as Shor's can potentially compromise widely used public-key encryption protocols, thus gravely jeopardizing secure communication. It is against this backdrop that quantum cryptography has been proposed as a new alternative, which leverages the principles of quantum mechanics to enable data confidentiality. Quantum Key Distribution (QKD) is a key part of this phenomenon, as it enables secure symmetric key exchange while potentially signifying unauthorized eavesdropping. However, QKD is inherently limited by several practical factors, such as high expense, limited operational ranges, and 1:1 communication. To mitigate these limitations, this paper suggests a hybrid communication model of QKD and Post- Quantum Cryptography (PQC), thus enabling practical implementation as well as safeguarding against future threats.

This convergence creates an economically efficient, scalable, and robust platform for enabling secure communication in research, defence, and national networks.

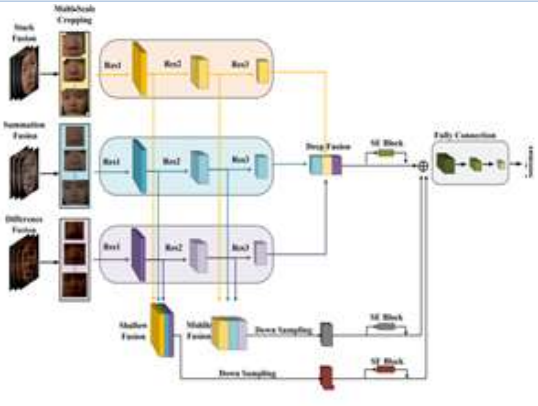

Fig. 1 Our Website Design.

II.LITERATURE SURVEY

The development of secure communication networks has been significantly impacted by quantum computing advancements and the vulnerabilities it poses to conventional encryption protocols. Shor (1994) proved that quantum algorithms could factor large numbers efficiently, which undermines conventional RSA encryption and poses an urgent need for security solutions that can resist quantum attacks. Bennett and Brassard (1984) first introduced the BB84 protocol, which facilitates Quantum Key Distribution (QKD) based on quantum mechanics principles [1]. Later

implementations, including the DARPA Quantum Network (Elliott et al., 2003), SECOQC (Peev et al., 2009), and Tokyo QKD (Sasaki et al., 2011), proved that large-scale QKD systems could be implemented in real-world environments [2][3][4]. However, those systems were typically marred by cost, distance, and one-to-one communication limitations. To overcome these issues, many researchers developed hybrid models that combine QKD with Post-Quantum Cryptography (PQC), which aims to make conventional cryptographic algorithms quantum-resistant. Ma et al. (2016) highlighted the importance of Quantum Random Number Generators and simulated QKD components to construct scalable networks [5]. The National Institute of Standards and Technology (NIST) launched a multi-round assessment of PQC algorithms like Kyber, SABER, and Dilithium, preferring a hybrid approach to quantum-safe encryption [6]. Kim et al. (2018) introduced the KREONET model, which suggests using QKMS and Q-Controllers for enhanced key routing and management in research networks [7]. Länger and Lenhart (2009) analyzed the challenges of standardizing QKD systems and recognized the need for universal communication interfaces like ETSI QKD 014 [8]. Zhang et al. (2018) and Zhao (2019) have conducted more recent research that explores embedding satellite links, and real-time monitoring in quantum-secure networks for extended national and defense applications [9][10].

III.MODULE-WISE DESCRIPTION

The proposed Secure Communication System based on Quantum Cryptography is based on modular units whose collaboration delive rs efficient key distribution, encryption, management, and control within a quantum-proof network. The major modules are listed below:

1. QUANTUM KEY DISTRIBUTION (QKD) MODULE

Quantum Key Distribution (QKD) module is the backbone of secure communication in quantum cryptographic networks. It produces and sends symmetric cryptographic keys based on quantum properties like photon polarization and quantum entanglement. The module guarantees that any attempt at interception by an eavesdropper will introduce detectable anomalies based on quantum measurement principles, i.e., by the no-cloning theorem. Some of the most widely used QKD protocols include BB84, MDI-QKD (Measurement Device-Independent QKD), and CV-QKD (Continuous Variable QKD), each providing trade-offs between range, security, and deployment complexity.

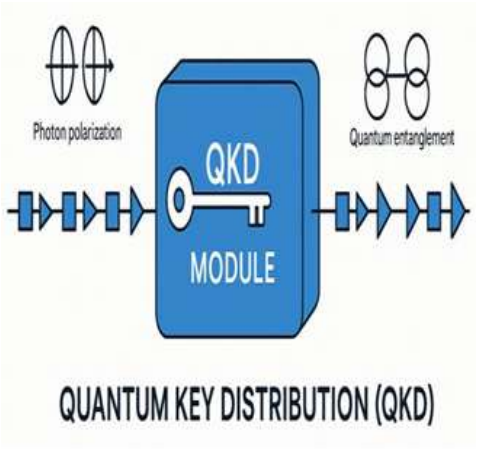

Fig. 2 Quantum Key Distribution Module.
Fig. 2 Quantum distribution.

2. POST-QUANTUM CRYPTOGRAPHY (PQC) MODULE

The Post-Quantum Cryptography (PQC) module is an essential fallback and complement to QKD, particularly in cases where quantum infrastructure is unavailable or not viable. In contrast to QKD's reliance on physical quantum channels, PQC algorithms execute on standard hardware but are made quantum computer decryption-proof. The module is formed by NIST-approved algorithms like Kyber (for key encapsulation) and Dilithium (for digital signatures), which utilize lattice cryptography and are extremely efficient with robust post- quantum security assurances. The PQC module is mainly located at the application and user levels, providing secure data encryption and signature verification based on current internet infrastructure. It provides end-to-end security even in cases where QKD cannot be practically implemented due to cost or distance constraints. The module also handles algorithm agreement, integration with TLS v1.3, and fallback

in the case of QKD channels being interrupted.

Fig. 3- Post-Quantum Cryptography Module.

2. QUANTUM KEY MANAGEMENT SYSTEM (QKMS) MODULE

3.

Fig- 4 Quantum Key Management System Module.

The Quantum Key Management System (QKMS) module is the key to the secure operation of hybrid quantum networks. Its main purpose is to handle symmetric keys produced by QKD systems and transform them into service keys for use by encryption applications. The QKMS module manages the entire life cycle of these keys—from generation, storage, verification, renewal, expiration, to revocation. It also enables key relay over long distances by serving as a trusted intermediary between geographically dispersed nodes, allowing scalable deployment of QKD. In multi-node networks, the QKMS maintains consistency through key synchronization and state monitoring across distributed systems. This module interacts with network security protocols and accommodates policies for service-specific key management, such as setting key length, lifetime, and access levels. It enables high availability through redundancy, replication, and failover. By imposing granular control over the use of keys and secure routing, the QKMS improves the flexibility and resiliency of quantum-secured networks.

4. Q-CONTROLLER MODULE

The Q-Controller module is the master management module in the quantum-secure communications framework. It offers overall coordination and management of all the elements of a network, including a plurality of instances of QKMS modules and QKD devices. The Q-Controller performs the tasks of registering network entities, topological mapping, and determination of best path key relays using distance-considerate algorithms that consider distance, key availability, and channel status. The Q- Controller dynamically manages routing tables and informs QKMS modules of relay route configurations or changes thereto. The Q-Controller controls key profiles, device authentication, and performance threshold settings at an enterprise level. Among its primary functions is real-time monitoring of quantum and public channels with automatic fault detection and performance testing incorporated. The Q-Controller keeps disruption logs, tracks key inventory between nodes, and offers redundancy planning for low-downtime applications.

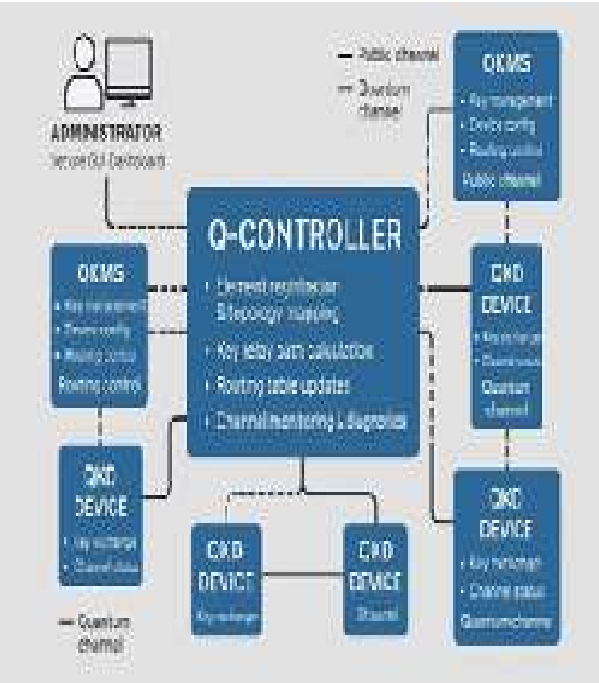

Fig- 5 Q-Controller Module.

5. SECURITY & MONITORING MODULE

Fig. 6 Security & Monitoring Module.

The Security and Monitoring module is responsible for ensuring the integrity, reliability, and trust of the quantum communication network. The module has been designed to continuously monitor system activities, such as key exchanges, cryptographic processes, and user activities. The module strictly records all significant events—such as key request, errors, and disturbances—and categorizes them according to severity levels. Intrusion detection functions are implemented to discover attempts to violate authorization, unusual traffic patterns, or violations of defined rules. The module also supports auditing features, such as timestamped activity logs and forensic examination of cryptographic events.Performance indicators such as throughput, latency, quantum bit error rate, and key loss ratio are collected and monitored continuously. Alarms and alerts are generated when thresholds are exceeded to enable proactive control.

6. INTEGRATION AND INTERFACING MODULE

The Integration and Interfacing module serves to connect quantum cryptographic elements to the currently available digital environments. It serves as a protocol translation and abstraction layer, thereby providing smooth interaction between heterogeneous QKD devices, classical networks, and user-level applications. This module guarantees that quantum key data—irrespective of manufacturer or form—is converted to a standard form, e.g., ETSI QKD 014, prior to use by higher-level systems such as the QKMS. It facilitates interfacing with secure applications such as VPNs, TLS-protected services, and data storage systems through the provision of generated and formatted service keys. Moreover, the module enhances interoperability between proprietary QKD solutions (e.g., Toshiba, ID Quantique) and broadly accepted encryption schemes. Its design encompasses secure API gateways, URI/IP-based service key requests, and adapter modules for legacy systems. Through the provision of modular and plug-and-play interfaces, the Integration and Interfacing module facilitates a vendor-independent and extensible quantum security infrastructure for long-term deployment.

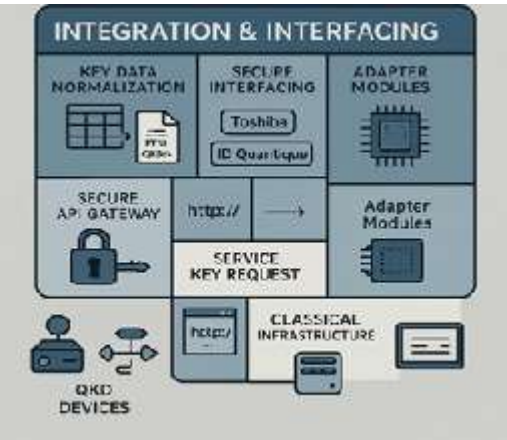

Fig- 7 Integration & Interfacing Module.

IV.FAULT TOLERANCE AND NETWORK RESILIENCE IN QUANTUM CRYPTOGRAPHIC SYSTEMS

To ensure fault tolerance and network resilience for the reliability and availability of a quantum-secured network, the system needs to ensure uninterrupted secure communication despite hardware failures, link degradations, or cyber-physical attacks. This section explains how the system ensures uninterrupted secure communication in the event of hardware failures, link degradations, or cyber-physical attacks. Redundant QKD paths, dynamic rerouting protocols, and real-time error correction mechanisms are incorporated in the network to foresee interruptions in advance. Quantum Repeaters and error-tolerant QKMS nodes function with self-checking and failover capabilities to avoid single points of failure.

Moreover, distributed consensus algorithms ensure secure multi-party agreement on key management operations, ensuring system coherence even in the event of partial outages. Periodic penetration testing and simulated attack scenarios are used to test resilience. This multi-layered mechanism increases the robustness of the quantum infrastructure, enabling secure communication to continue under adverse conditions.

IV.CONCLUSION

The Quantum Cryptography-based Secure Communication System introduced here offers a future-proof solution to addressing the threat quantum computing poses to traditional encryption. By integrating Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) into a single adaptable system, it offers robust, scalable, and long- term secure communication in various network environments. Every aspect—ranging from key generation and relay to monitoring and access control—has been designed to offer high security, fault tolerance, and transparent operations.

One of the major strengths of the system is its hybrid architecture, which marries the physical security of Quantum Key Distribution (QKD) with the pragmatic flexibility of Post-Quantum Cryptography (PQC). The inclusion of features such as the Quantum Key Management System (QKMS) and Q-Controller enables improved key management and real-time network monitoring. The architecture can be employed in national research networks, defence communications, and critical infrastructure in the future. With more automation, AI-driven monitoring, and satellite QKD, the system can be an integral part of global secure quantum communication networks.

References

[1]C. Bennett & G. Brassard, Quantum Cryptography: Public-Key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[2]S. Elliott, D. K. K. Lee & D. C. Miller, The DARPA Quantum Network, Quantum Communications and Quantum Networking, 2003.

[3]T. Peev, J. P. Torno, A. Poppe, et al., The SECOQC Quantum Communication Network in Vienna, Journal of Quantum Information Processing, 2009.

[4]T. Sasaki, A. Yoshizawa, & H. Koashi, Field Test of Quantum Key Distribution over a 50-Kilometer Fiber Network, Proceedings of the IEEE Conference on Quantum Communications, 2011.

[5]L. Ma, X. Zhang, & Y. Chen, Quantum Random Number Generators and Simulation of QKD Components, Journal of Quantum Information and Technology, 2016.

[6]N. Institute of Standards and Technology (NIST), Post-Quantum Cryptography (PQC) Algorithm Evaluation, 2018.
[7]H. Kim, S. Park, & W. Kim, KREONET Model: Efficient Key Routing and Lifecycle Management for Research Networks, Journal of Quantum Network Security, 2018.
[8]T. Länger & P. Lenhart, Challenges in the Standardization of QKD Systems: The ETSI QKD 014 Approach, Journal of Cryptographic Engineering, 2009.
[9]Y. Zhang, H. Zhang, & S. Wang, Satellite Quantum Communication Networks for National Security, Quantum Communication and Networking Journal, 2018.
[10]J. Zhao, Quantum Networks and Real-Time Monitoring for National Defense Applications, Journal of Network Security, 2019.