ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Development of A BB84-Based Quantum Security System

Prof. Pravin R. Kamble[1], Shriram Narkhede[2], Gayatri Bhosale[3], Shrikant Hundekar[4]

Department of Information Technology, Savitribai Phule Pune University, Pune, India

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150600059

Received: 10 June 2026; Accepted: 15 June 2026; Published: 04 June 2026

ABSTRACT

The rapid advancement of quantum computing poses a serious threat to traditional cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC), which rely on computational difficulty for security. Quantum algorithms like Shor's and Grover's have the potential to break or weaken these methods, putting modern communication systems at risk. To address this challenge, this work presents a quantum-safe com-munication framework that combines the BB84 Quantum Key Distribution (QKD) protocol with Post-Quantum Cryptography (PQC) techniques, aiming to ensure secure data exchange in the presence of quantum-capable adversaries.

In this system, the BB84 protocol is simulated to enable secure key exchange between two parties over a virtual quantum channel. The generated key is refined through processes such as basis matching, error correction, and privacy amplification using SHA-256 to ensure reliability and secrecy. For secur-ing communication, One-Time Pad (OTP) encryption is used alongside HMAC-SHA3-256 to provide both confidentiality and message integrity. Additionally, file encryption is handled using the XChaCha20-Poly1305 algorithm, selected for its efficiency and strong protection against potential vulnerabilities like nonce reuse.

To further enhance security, the framework integrates a hybrid key management approach using the Kyber-512 Key Encapsulation Mechanism (KEM) combined with a Key Deriva-tion Function (KDF), merging classical and quantum-resistant techniques. Experimental results demonstrate the effectiveness of the system, achieving a Quantum Bit Error Rate (QBER) of 2.5% and successful performance in both message and file en-cryption. Overall, this work contributes toward the development of practical and resilient communication systems designed for the emerging quantum era.

Index Terms—Quantum Key Distribution (QKD), BB84 Pro-tocol, Quantum Cryptography, Tensor Networks, Quantum Sim-ulation, QBER Analysis, Eavesdropping Detection, Secure Com-munication Systems

INTRODUCTION

The rapid progress of quantum computing is creating new challenges for current cryptographic systems. Techniques such as RSA and Elliptic Curve Cryptography (ECC), which rely on the computational difficulty of mathematical problems, may become vulnerable as quantum capabilities advance. In particular, algorithms like Shor's and Grover's could signif-icantly weaken these widely used methods, raising concerns about the security of modern communication networks. This situation emphasizes the need for cryptographic solutions that can withstand quantum attacks by combining quantum-based key distribution with quantum-resistant algorithms [12], [17].

Overview of the Proposed System

The proposed quantum-safe communication framework in-tegrates BB84 Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC) to provide a secure way of exchanging both messages and files. In this approach, users begin by transmitting qubits over a quantum channel using the BB84 protocol, generating an initial shared key. This key is then improved through processes such as basis comparison and error correction,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

resulting in a reliable secret key shared between the communicating parties [5], [16].

In addition to the quantum-generated key, a post-quantum key is created using a lattice-based algorithm like Kyber-512. These two keys are combined using a Key Derivation Function (KDF) to produce a hybrid session key. This layered approach strengthens security by ensuring that even if one component is compromised, the other continues to provide protection. Simulation-based validation of such hybrid and QKD systems has been explored in recent frameworks [1], [2], [4].

Encryption Mechanisms

For message transmission, the system uses a one-time pad (OTP) derived from the hybrid key, along with HMAC-SHA3-256 to verify data integrity and authenticity. For file protection, the XChaCha20-Poly1305 algorithm is employed due to its efficiency and strong resistance to common crypto-graphic weaknesses. The system utilizes both quantum and classical channels: the quantum channel is responsible for

secure key generation, while the classical channel handles key reconciliation and the transfer of encrypted data. Such hybrid communication models are increasingly considered essential for building secure and scalable quantum communication networks [18].

Objectives

The main goals of this research are outlined as follows:

- To develop a hybrid quantum-secure communication system that combines BB84 Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC), providing stronger protection against both classical and quantum-based attacks.
- To ensure secure transmission of chat messages by ap-plying One-Time Pad (OTP) encryption together with HMAC-SHA3, thereby maintaining confidentiality, data integrity, and authentication throughout the communica-tion process.
- To enable secure file transfer using the XChaCha20-Poly1305 algorithm, which offers efficient and authenticated encryption suitable for handling large volumes of data.
- To validate the effectiveness of the proposed system through experimental analysis, including key generation, encryption and decryption performance, and evaluation of the Quantum Bit Error Rate (QBER), which is a key metric in QKD systems.

Overall, the proposed framework is designed to be scalable and robust, offering a practical solution for secure commu-nication in environments where both classical and quantum threats must be considered. Its hybrid structure improves fault tolerance and makes it well-suited for next-generation communication systems [18].

LITERATURE REVIEW

This section reviews recent research related to Quantum Key Distribution (QKD) simulation environments, developments in BB84 protocol modeling, the use of tensor-network techniques for quantum system simulation, and approaches to security and attack modeling. The literature is structured into focused subsections, each highlighting how prior studies contribute to and inform the design of the BB84 QKD Simulation System introduced in this work.

QKD Simulation Frameworks and Network Testbeds

Scalable simulation frameworks and network testbeds are fundamental tools for analyzing Quantum Key Distribution (QKD) protocols under realistic network conditions. Wu et al. developed a parallel discrete-event

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

simulation platform for QKD networks that focuses on scalability and event paral-lelism, allowing efficient modeling of complex topologies and diverse traffic scenarios [1]. Building on this foundation, Soler et al. enhanced the NS-3–based simulator QKDNetSim+ by in-corporating more realistic network modules and refining event management, thereby improving the accuracy of network-layer simulations [4]. Similarly, Gkouliaras et al. introduced NuQKD, a modular and extensible framework that supports real-time visualization and allows researchers to integrate new protocol modules and observe their interactive dynamics [2]. Complementing these efforts, Bel et al. offered a compre-hensive perspective on quantum network simulators, detailing the software toolchains and abstraction layers required for complete end-to-end quantum network research [18]. Together, these studies reflect a strong community focus on scalability, modularity, and realism in the development of QKD simulation tools.

BB84 Protocol Studies and Protocol-Level Improvements

The BB84 protocol continues to serve as the foundational model for both educational and experimental QKD research. Pereira et al. examined the robustness of BB84 by propos-ing modifications that reduce the impact of source imper-fections—a critical factor when translating from idealized simulations to physical implementations [16]. Such studies underscore the importance of accounting for hardware limi-tations, including multi-photon emissions and imperfect state preparation, to ensure meaningful performance and security evaluation. The BB84 QKD Simulation System introduced in this work incorporates these practical considerations by allowing users to configure non-ideal conditions and engage in role-based experiments—representing Alice, Bob, or Eve—to explore how such imperfections influence protocol perfor-mance and overall system security.

Tensor Network Methods for Quantum Simulation

Tensor-network-based approaches have become indispens-able for simulating quantum circuits and managing large-scale quantum states efficiently on classical computing resources. Zhao et al. applied tensor-network edge-cutting techniques to simulate large quantum computations on supercomputers, demonstrating a feasible method for emulating circuits beyond conventional state-vector limits [7]. In parallel, Mangini et al. and Melnikov et al. utilized tensor networks for noise characterization and state optimization, showing that these models not only represent complex noise behaviors but can also act as constructive tools for quantum state preparation [3], [6]. Further engineering advances from Huang et al. and Pan et al. introduced parallelized tensor contraction and GPU acceleration, both of which significantly reduce simulation runtime and enhance scalability [8], [10]. Recent surveys and algorithmic contributions, such as those by D´ıez Garc´ıa and Ma´rquez Romero and Pastor et al., consolidate current progress and propose new frameworks for parallel tensor-network algorithms [11], [19]. Together, these studies inform the design of simulation backends that balance high fidelity with practical computational efficiency.

Modeling Noise, Attacks, and Security Metrics

Accurately modeling quantum noise and eavesdropping strategies is essential for assessing the reliability of QKD systems. Mangini et al. employed tensor networks to quantify noise, enabling realistic simulation of imperfect devices and their impact on key security metrics such as the Quantum Bit Error Rate (QBER) [3]. Aizpurua et al. extended this approach by examining tensor-network-based attack models against cryptographic schemes, revealing new potential vul-nerabilities and emphasizing the importance of integrating adversarial perspectives into simulator design [12]. Traditional models—such as intercept–resend, partial interception, and depolarizing channel attacks—remain fundamental for both educational and research-oriented studies, as they help define QBER thresholds and detection mechanisms [12], [16]. Addi-tional contributions by Thompson et al. and Masot-Llima et al. enhance the fidelity of noisy-circuit simulations and introduce stabilizer-based tensor frameworks that can approximate quan-tum dynamics efficiently in specific computational regimes [14], [15].

Scalability and Parallel Algorithms

Scalability remains a major focus in both network-level and circuit-level QKD simulation research. At the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

network scale, Wu et al. and Soler et al. explored parallel discrete-event simulation to handle large numbers of quantum links and communication sessions [1], [4]. At the computational level, Huang et al. and Pan et al. focused on optimizing tensor contraction parallelism for circuit simulation, dramatically im-proving runtime efficiency [8], [10]. Complementary strategies proposed by Pastor et al. use graph-theoretic community de-tection to partition workloads effectively, allowing simulation processes to scale across distributed computing resources [19]. Collectively, these techniques illustrate a growing convergence of network-level and tensor-level parallelism—an integration that enables comprehensive, end-to-end simulation of complex QKD environments.

Integration of Classical Cryptography and Practical Tool-ing

For Quantum Key Distribution (QKD) systems to operate securely in real-world environments, quantum-generated keys must be effectively integrated with classical cryptographic mechanisms to ensure message confidentiality and data in-tegrity. Research such as that of Meddeb [**?**]. illustrates this principle through system-level implementations in practical settings, including Wi-Fi–based quantum communication sce-narios, where hybrid stacks and authenticated channels are essential for maintaining secure end-to-end exchanges [5]. Across the surveyed literature, there is a growing consensus on the importance of incorporating key-derivation functions, authenticated encryption schemes, and HMAC-based integrity validation into QKD simulators. Such integration not only enhances realism but also allows these platforms to emulate the behavior of actual deployment environments. In align-ment with this approach, the BB84 Quantum Key Distribu-tion Simulation System developed in this work implements HKDF for key derivation, HMAC-SHA3 for authentication, and XChaCha20-Poly1305 for encryption—together forming a hybrid cryptographic layer that bridges quantum key gener-ation with classical data protection standards.Research Gaps and Motivation

Although the current body of research provides a strong foundation—covering scalable discrete-event QKD testbeds [1], [4], modular simulation frameworks [2], tensor-network-based quantum circuit modeling for enhanced fidelity [3], [7], and comprehensive security and attack analyses [12]—several critical challenges remain unaddressed. Existing simulators tend to specialize in isolated components, yet few provide end-to-end educational environments that unify interactive visualization, configurable device imperfections, and balanced trade-offs between backend accuracy and computational per-formance. Moreover, there is still a notable lack of frame-works that seamlessly integrate tensor-network computation backends with network-level QKD simulators, preventing a holistic understanding of hybrid quantum–classical behaviors. Another limitation is the scarcity of user-centered tools that enable role-based experimentation—where users can adopt the roles of Alice, Bob, or Eve—while incorporating classical cryptographic primitives for realistic message handling and security validation.

METHODOLOGY

The proposed system follows a layered security design that combines the inherent security advantages of quantum key distribution with the strength of modern lattice-based cryptography. By integrating these approaches, the framework aims to provide protection against both classical and quantum threats [12], [17]. The methodology is organized into five main phases: Quantum Key Distribution, Classical Post-Processing, Post-Quantum Key Exchange, Hybrid Key Derivation, and Secure Application Modules [1], [2].

Phase 1: Quantum Key Distribution (BB84)

The process begins at the **Alice node**, where a random number generator produces a sequence of bits along with corresponding polarization bases (rectilinear $\oplus$ or diagonal$\otimes$). Each bit is encoded into a quantum state (qubit) andtransmitted through a simulated quantum channel [5].

At the **Bob node**, the received qubits are measured using randomly chosen bases. Due to the nature of quantum mea-surement, each qubit collapses into a classical bit value, which is stored as part of Bob's preliminary key. To evaluate the system's robustness, an **Eve module** is introduced to simulate potential eavesdropping. Any interception attempt disturbs the quantum states, making such attacks detectable [16].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Phase 2: Classical post-processing

After the quantum transmission phase, both parties commu-nicate over a classical channel to perform **basis reconciliation**, keeping only the bits measured using matching bases [1], [5]. Next, the system estimates the **Quantum Bit Error Rate (QBER)** by comparing a subset of the shared bits. If the error rate exceeds a predefined threshold (typically around 11%), the session is considered insecure and is terminated. Otherwise, the process continues with **privacy amplification**, where hashing techniques such as SHA-256 are applied to

reduce any partial information that may have been exposed, resulting in a shorter but more secure key [17].

Phase 3: Post-Quantum Cryptography (PQC) Integration

Alongside the quantum key generation, the system performs a classical key exchange using the **Kyber-512** algorithm, a lattice-based Key Encapsulation Mechanism (KEM). This approach is designed to resist attacks from quantum algo-rithms, providing an additional layer of security [12]. The PQC component ensures reliable key generation with high agreement rates, complementing the quantum-generated key.

Phase 4: Hybrid Key Establishment

To strengthen overall security, the quantum key and the PQC-generated key are combined using a **Key Derivation Function (KDF)**, specifically HKDF-SHA256. This hybrid key derivation approach ensures that even if one component is weakened, the combined key remains secure [1], [2]. This design improves resilience and makes the system more robust against a wide range of attack scenarios.

Phase 5: Secure Application Modules

The final hybrid key is used across two main application components:

- **Instant Messaging:** Messages are secured using **One-Time Pad (OTP)** encryption, providing strong confi-dentiality, while **HMAC-SHA3-256** is applied to ensure message integrity and authenticity.
- **File Transfer:** File encryption is handled using the **XChaCha20-Poly1305** algorithm, which offers efficient authenticated encryption and is well-suited for protecting large data transfers.

This multi-phase approach ensures that the system maintains a balance between theoretical security guarantees and practical implementation, making it suitable for next-generation secure communication systems [18].

Flow chart: BB84 Quantum Key Distribution Method

Related Work

The increasing capabilities of quantum computing have raised serious concerns about the long-term security of clas-sical cryptographic systems. Widely used techniques such as RSA and Elliptic Curve Cryptography (ECC) are particularly vulnerable to quantum algorithms like Shor's algorithm, which can efficiently solve the mathematical problems underlying their security. As a result, significant research efforts have shifted toward developing quantum-resistant solutions, pri-marily through Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) [12], [17].

The BB84 protocol, originally proposed by Bennett and Brassard, remains one of the most fundamental and widely analyzed QKD schemes. Numerous studies have evaluated its behavior under realistic conditions, including noise, photon loss, and hardware imperfections. These works show that BB84 can reliably detect eavesdropping by monitoring the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

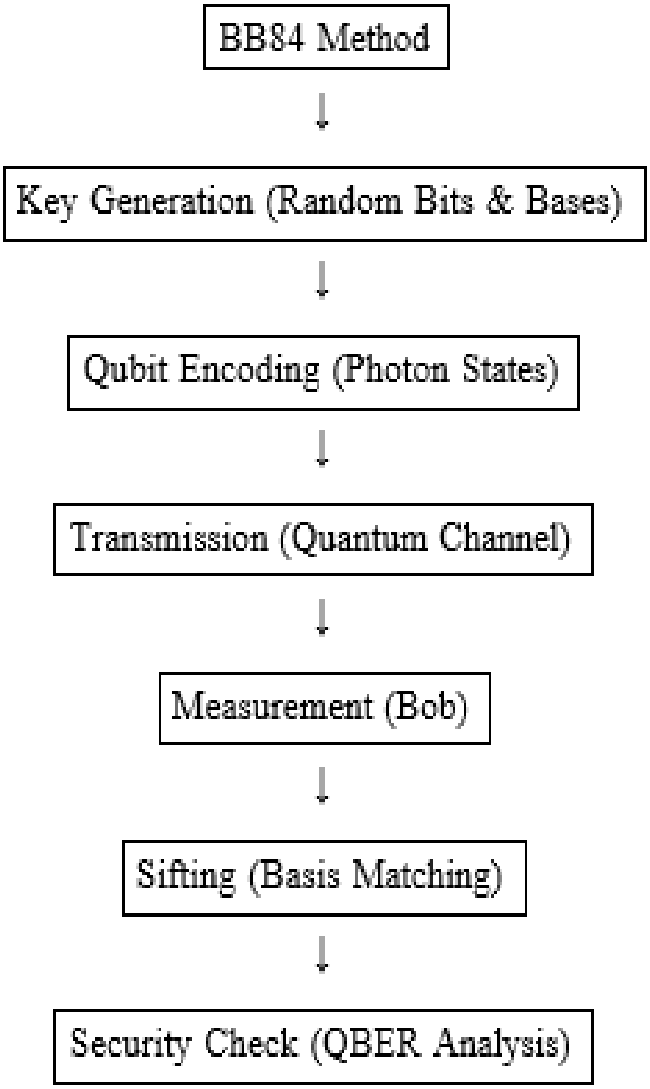

Fig. 1. BB84 Quantum Key Distribution Workflow

Quantum Bit Error Rate (QBER), making it a practical ap-proach for secure key exchange [5], [16]. Simulation tools and frameworks, such as those based on NS-3 and other quantum network simulators, have further helped researchers study BB84 in controlled and scalable environments [1], [2], [4].

More recent research has focused on improving the scal-ability and efficiency of QKD systems. Techniques such as tensor network simulations and advanced modeling approaches allow large quantum systems to be analyzed with reduced computational overhead. These methods make it possible to evaluate QKD performance in more realistic and complex net-work scenarios [7], [14]. Additionally, several enhancements to the BB84 protocol have been proposed to address practical challenges, including source imperfections and measurement inconsistencies [16].

Despite its strong theoretical security, QKD faces practical limitations such as infrastructure complexity, limited trans-mission range, and challenges in integration with existing communication systems. To overcome these issues, hybrid approaches that combine QKD with PQC have been widely ex-plored. Lattice-based algorithms such as Kyber are particularly promising, as they offer resistance to quantum attacks while remaining compatible with classical computing environments [12].

Hybrid QKD–PQC frameworks have gained attention be-cause they merge the strengths of both paradigms. In

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

these systems, keys generated through quantum processes are com-bined with PQC-derived keys using key derivation techniques, ensuring that the overall system remains secure even if one component is compromised. This layered approach improves resilience against both classical and quantum adversaries while maintaining practical deployability [1], [2].

Beyond key exchange, recent work also emphasizes se-cure data transmission using modern symmetric encryption techniques. Methods such as One-Time Pad (OTP), AES,and XChaCha20-Poly1305 are often used alongside QKD-generated keys to ensure confidentiality and integrity. Au-thentication mechanisms like HMAC-SHA3 further strengthen communication by protecting against tampering and replay attacks.

Several studies have also proposed complete end-to-end secure communication frameworks that integrate QKD, PQC, and modern encryption schemes. These systems typically include components for key management, session control, and real-time monitoring of security metrics such as QBER. Experimental results demonstrate that such integrated solutions are feasible and suitable for applications including secure mes-saging, financial systems, and government communications [18].

The present work builds on these developments by propos-ing a unified quantum-safe communication framework that combines BB84 QKD, PQC (Kyber), and advanced encryption techniques. Unlike approaches that rely solely on a single security mechanism, this work adopts a hybrid strategy to improve overall robustness, scalability, and real-world appli-cability. Additional features such as simulation support and eavesdropping detection further enhance the system's effec-tiveness.

In summary, existing research highlights a clear movement toward hybrid quantum-safe communication models that in-tegrate both quantum and classical cryptographic techniques. The proposed framework contributes to this direction by offering a flexible and scalable solution designed to address emerging security challenges in the quantum computing era.

Comparative Analysis (Compact Table)

Parameter	Traditional	Proposed
Security Basis	Computational	Quantum + PQC
Quantum Resistance	Low	High
Key Distribution	Classical	Quantum (BB84)
Eavesdropping Detection	No	Yes (QBER)
Encryption	RSA, AES	OTP + HMAC
Randomness	Pseudo	True Random
Scalability	High	Moderate
Future Readiness	Limited	Quantum-Safe

TABLE I COMPACT COMPARISON OF TRADITIONAL AND PROPOSED METHODS

DISCUSSION

The comparison indicates that while traditional crypto-graphic techniques are efficient and widely adopted, their security is increasingly challenged by the emergence of quan-tum computing. Methods such as RSA and ECC, which rely on computational hardness, may no longer provide adequate protection in the near future.

In contrast, the proposed hybrid approach combines quan-tum key distribution with post-quantum cryptographic tech-niques to strengthen overall security. The BB84 protocol enables secure key exchange while also allowing the detection.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

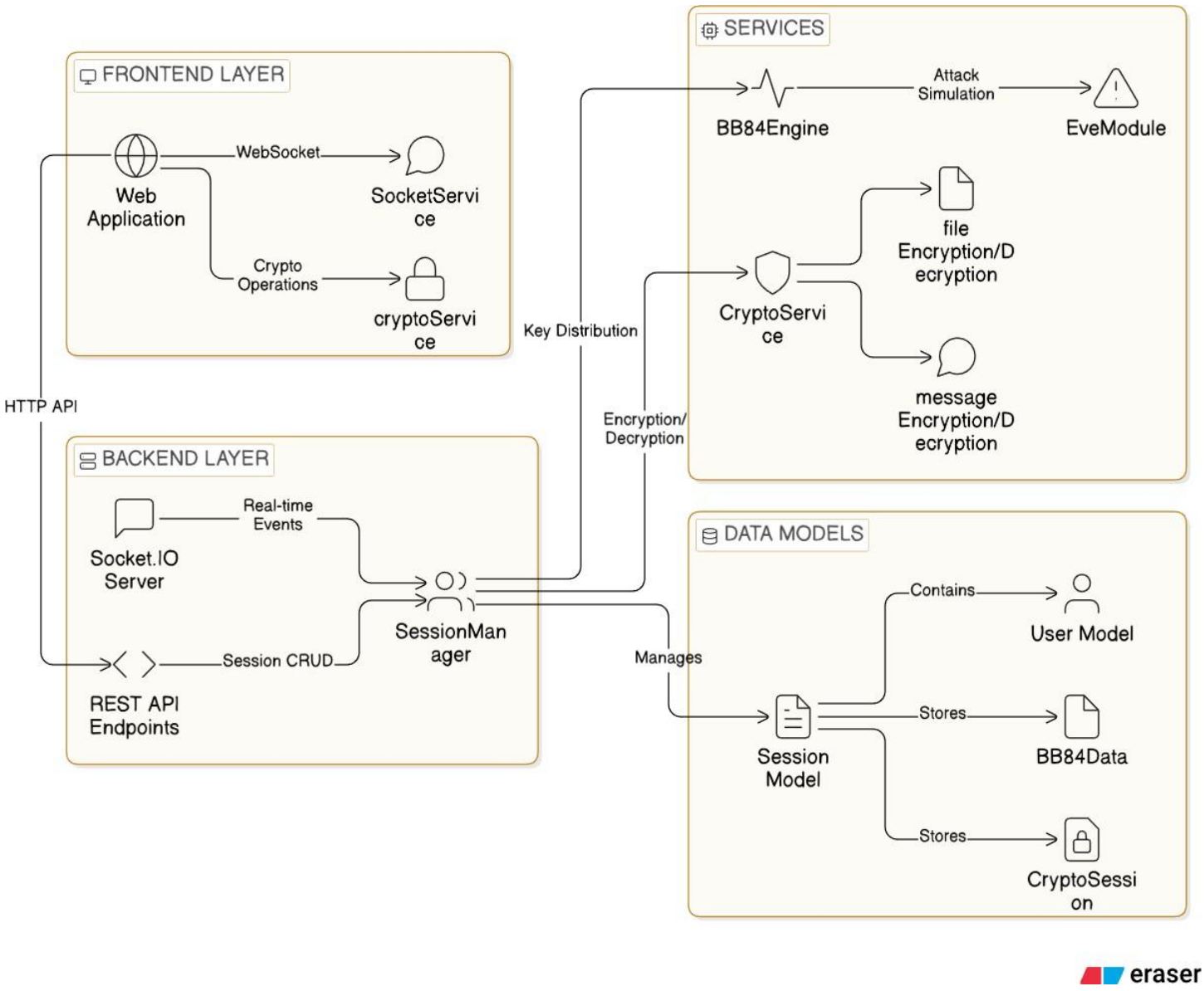

Fig. 2. System architecture diagram of potential eavesdropping through error rate analysis. At the same time, the inclusion of PQC improves practicality and ensures compatibility with existing systems. The use of modern symmetric encryption methods further reinforces both data confidentiality and integrity during communication.

Overall, the results suggest that the proposed system offers a more robust and forward-looking solution. Its ability to address both current and emerging threats makes it a strong candidate for secure communication in the evolving landscape of quantum technologies.

SYSTEM DESIGN AND ARCHITECTURE

The proposed system is structured as a modular framework designed to support secure key generation and protected data transmission. It combines multiple functional layers, including the User Interface and Simulation Engine, the Core Quantum Engine, the Hybrid Key Management Layer, and the Secure Application Layer. This layered design helps organize the system efficiently while improving flexibility and scalability [1], [2].

Architectural Overview

The system workflow begins with the **GUI Dashboard**, where users can configure simulation settings such as the number of qubits and noise parameters. The **Main Simulator** serves as the central controller, coordinating interactions be-tween the sender (Alice), the receiver (Bob), and the optional eavesdropper module (Eve). This

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

design ensures smooth com-munication and synchronization across all components [4], [5].

Component Breakdown

The architecture is divided into specialized modules, each handling a specific part of the communication process:

Core Engine (Tensor Networks): This module uses tensor network techniques, such as Matrix Product States

TABLE II COMPARISON BETWEEN PRIOR WORK AND THE BB84 QKD SIMULATION SYSTEM (THIS PROJECT).

(MPS), to simulate complex quantum states and noise behavior efficiently on classical systems [7], [14].

- **QKD Engine (BB84):** Responsible for implementing the BB84 protocol, including qubit preparation, transmission

Ref.	Focus / Contribution	Approach & Scale	Attack Models / UI	Crypto Integration / Key Use
[1] X. Wu et al. (2022)	Scalable QKD network testbed; parallel discrete-event simulation	Discrete-event, parallel simulation with emphasis on scalability and performance	Basic channel noise; not focused on varied eavesdropper (Eve) attack strategies; minimal, research-focused metrics	No integrated real-time one-time pad (OTP) or file-encryption demonstration
[2] Gkouliaras et al. (2024)	NuQKD: Modular simulation framework	Modular components; extensible simulator	Configurable channel effects; limited GUI; framework-oriented with limited visualization	Simulates key establishment, but not a complete cryptographic stack
[3] Mangini et al. (2024)	Tensor-network noise characterization	Tensor-network-based noise modeling; device-focused	Detailed noise characterization for NISQ devices; no real-time pedagogical UI	Not targeted at demonstrating practical key usage

SimulationNoise /Visualization Classicalthrough a simulated quantum channel, and measurement at the receiver end [16], [17].

- **Key Manager:** Combines the quantum-generated key and the PQC-derived key using HKDF-SHA256 to produce a secure hybrid session key. This approach improves resilience by ensuring that security does not rely on a single method [1], [2].
- **Crypto Service:** Provides essential encryption mecha-nisms, including One-Time Pad (OTP) for secure mes-saging and XChaCha20-Poly1305 for efficient and au-thenticated file encryption.
- **Eve Simulator:** Simulates potential attacks such as intercept-resend strategies and noise injection. These ac-tions help evaluate system security by analyzing their effect on the Quantum Bit Error Rate (QBER) [16].

Communication and Sequence Flows

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

The system operates through two main communication sequences:

Quantum Key Establishment Sequence:

Initialization: Alice generates a random sequence of

[**?**], [6]–[11],

[13], [14]

[12],

[20]Aizpurua et al., 2024

[17]–[19](2024–

2025)Tensor-network methods: scalabil-ity, contrac-tion schedul-ing, GPU accelera-tion

Tensor-network-based cryptana-lytic attacks (preprints)

Recent surveys / simula-tors /Tensor networks, edge-cutting, GPU and parallel strategies

Theoretical andexperi-mental attack analysis via TN methodsVaries: surveys, simulator overviews,Some include noise models and methods for large-circuit simula-tion

Attack modeling at algo-rithmic level (crypt-analysis)Cover noise and attacks at a highResearch-oriented outputs; not user-facing UIsNo peda-gogical UIMostly research sum-mariesNot focused on direct applica-tion of keys to OTP/encryption UX

Emphasizes vulnera-bilities ratherthan en-cryption demo

Typically do not bundle a full inter-bits along with corresponding polarization bases using the BB84 protocol [16].

1) **Quantum Transmission:** The encoded qubits are trans-mitted to Bob through a quantum channel. Any inter-ception attempt introduces detectable disturbances in the form of increased QBER [5].

2) **Basis Sifting:** Alice and Bob compare their measure-ment bases over a classical channel and retain only the matching bits to form a shared key [1].

3) **Security Validation:** The system evaluates the QBER. If it exceeds an acceptable threshold (typically around 11%), the session is terminated to prevent insecure communication [17].

4) **Finalization:** If the key is deemed secure, privacy am-plification (e.g., SHA-256) is applied to produce the final secret key [17].

Authenticated Secure Message Flow: Message trans-parallel algo-rithms for QKD andparallel algorith-mic contribu-tionslevel; al-gorithmic solutions and frame-worksactive encryption-demo platformmission follows a structured process involving encryption, authentication, and delivery. The plaintext is encrypted us-ing a keystream derived from the hybrid key (OTP-based

This workquantum simula-tion

IntegratedQiskit-Configurable Full in-End-to-approach). To ensure integrity and authenticity, an HMAC-

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

SHA3-256 tag is generated using additional metadata such as session identifiers and sequence numbers. On the receiver side, decryption is only performed after successful verification

(BB84 QKDSimulation System)BB84simula-tion,backedper-photonattackstrate-giesteractive

web UI (Al-end demo: HKDF-of the authentication tag, ensuring that tampered messages are rejected.

real-timesimula-(intercept-ice/Bob/Eve SHA256

visual-ization, attack emula-tion,tion (classical emula-tion), Web-resend, partial inter-cept, depolar-roles), live QBER

graphs, siftingderiva-tion, OTP

message encryp-System Class Structure

The system design is supported by a structured class ar-chitecture. The **SessionManager** maintains active sessions

session lifecycle and crypto-graphic demoSocket real-time sessions, UI for multi-role interac-tionsizing), channel-noise simula-tion, QBER

analyticsanima-tions, attack sliders, session dash-boardtion, HMAC-SHA3-256,

XChaCha20-

Poly1305 file en-cryptionidentified by unique IDs, while the **FileService** handles secure

Key Idea: Measurement disturbs quantum states, enabling detection of eavesdropping [17].

QBER Calculation:

$$QBER = \frac{N_{error}}{N_{total}} \quad (1)$$

where N_{error} is the number of mismatched bits and N_{total}

is the total number of compared bits.

Condition:

$$QBER < 11\% \Rightarrow \text{Secure Communication} \quad (2)$$

2) 2. Post-Quantum Cryptography (Kyber KEM): Kyber is a lattice-based Key Encapsulation Mechanism used to generate a quantum-resistant key [12].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Key Generation:

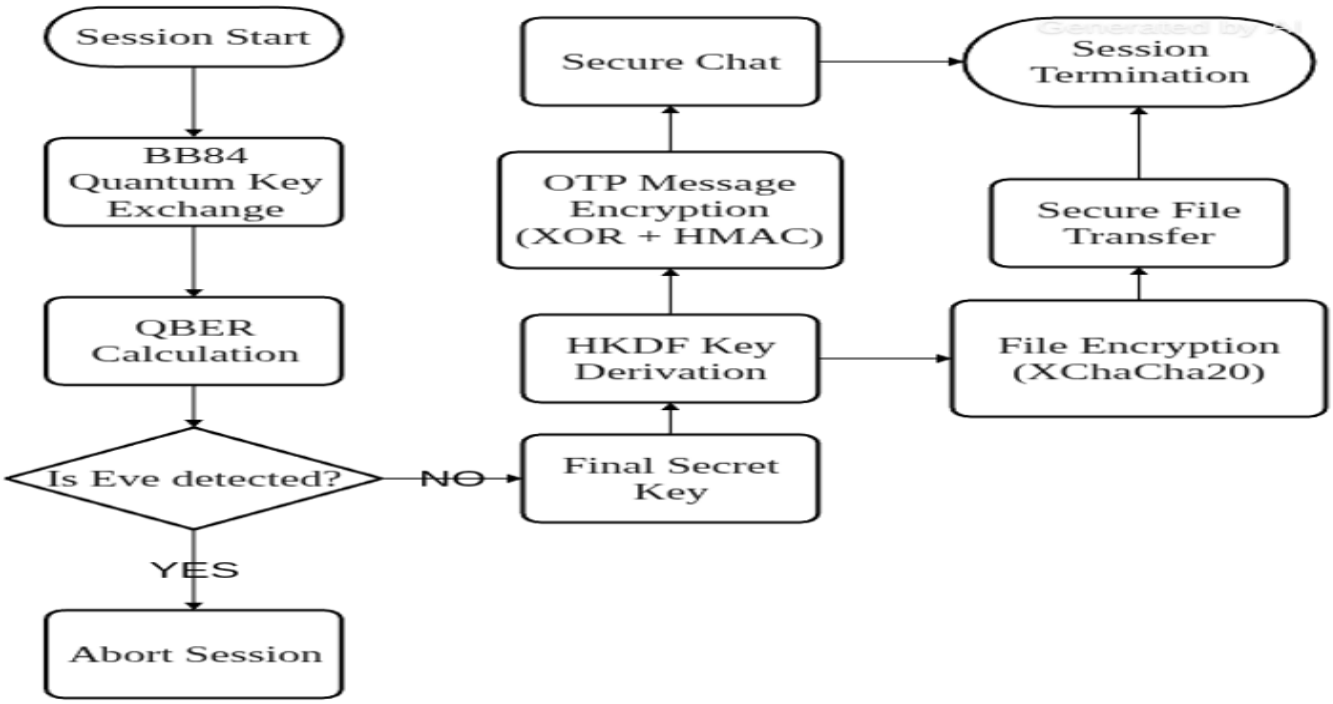

Fig. 3. System flow chart

Encapsulation:(pk, sk) = KeyGen() (3)

storage and transfer of large files using hybrid encryption keys. Communication between system components is managed through **WebSocket-based interactions**, enabling real-time data exchange with minimal delay [18].

Limitations and Assumptions

- **Classical emulation:** The current implementation sim-ulates quantum behavior on classical hardware, which limits scalability compared to real quantum systems. However, tensor network methods help improve effi-ciency for larger simulations.
- **Authenticated classical channel:** The system assumes the availability of a secure classical channel for tasks such as basis reconciliation. While full authentication mechanisms are not implemented, the framework allows for future integration.
- **Device imperfections:** Real-world imperfections, such as detector inefficiencies and photon losses, are mod-eled through configurable parameters. However, achiev-ing high accuracy requires calibration with experimental data, as discussed in prior studies [16].

ALGORITHM USED:

The proposed system implements a hybrid quantum-safe communication framework by integrating Quantum Key Dis-tribution (QKD), Post-Quantum Cryptography (PQC), and modern symmetric encryption techniques. The design ensures secure key generation, authentication, and data transmission resistant to both classical and quantum attacks [12], [17].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Algorithms Used

1) 1. BB84 Quantum Key Distribution (QKD): The BB84 protocol is used for secure key exchange based on quantum mechanics. Alice encodes random bits into qubits using ran-dom bases, and Bob measures them using randomly chosen bases [16].$(c, K_{PQC}) = \text{Encaps}(pk)$ (4)

Decapsulation:

$K_{PQC} = \text{Decaps}(c, sk)$ (5)

3. Hybrid Key Derivation (HKDF): The final session key is derived by combining QKD and PQC keys:

$K_{session} = \text{HKDF}(K_{QKD} \oplus K_{PQC})$ (6)

This ensures enhanced security through a hybrid approach [1], [2].

4. One-Time Pad (OTP) Encryption: OTP provides the-oretically perfect secrecy using XOR operation:

$C = P \oplus K$ (7)

$P = C \oplus K$ (8)

where P is plaintext, C is ciphertext, and K is the key.

5. HMAC-SHA3-256 (Authentication): Ensures message integrity and authenticity:

$\text{HMAC} = H(K \oplus \text{opad}, ||, H(K \oplus \text{ipad}, ||, m))$ (9)

where m is the message and H is the SHA3-256 hash function.

6. XChaCha20-Poly1305 (File Encryption): Used for authenticated encryption of files:

$C = \text{Enc}(K, N, P)$ (10)

$\text{Tag} = \text{Auth}(K, C)$ (11)

where K is the key, N is nonce, P is plaintext, and C is ciphertext.

SUMMARY

The proposed system integrates both quantum and classical cryptographic techniques to form a layered and more robust security framework. The BB84 protocol supports secure key exchange and enables the detection of eavesdropping through error rate analysis, which has been widely validated in prior research [16], [17]. In parallel, the use of the Kyber algorithm introduces a quantum-resistant mechanism for key exchange, strengthening the system against potential quantum-based at-tacks [12].

To protect data during transmission, the system incorpo-rates symmetric encryption techniques such as One-Time Pad (OTP), HMAC, and XChaCha20. These methods collectively ensure confidentiality, integrity, and authentication of the trans-mitted information. By combining quantum key distribution with post-quantum and symmetric cryptographic methods, the framework achieves a balanced and resilient design that is capable of addressing both current security needs and future challenges arising from advances in quantum computing [1], [2].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

RESULTS AND DISCUSSION

The performance of the proposed Quantum-Safe Commu-nication System was evaluated through a set of experiments focusing on key generation, encryption efficiency, and overall system reliability. The findings demonstrate the practicality of combining BB84 Quantum Key Distribution (QKD) with Post-Quantum Cryptography (PQC) and modern encryption methods to achieve a secure communication framework.

Quantum Key Distribution Performance

The BB84 protocol was analyzed by transmitting qubits between Alice and Bob under simulated channel conditions. Key performance indicators included the total number of qubits sent, the rate at which measurement bases matched, and the resulting Quantum Bit Error Rate (QBER). These metrics provide insight into both the efficiency of key generation and the system's ability to detect potential eavesdropping.

Metric	Observed Value
Total Qubits Transmitted	1000
Matching Basis Count	502
Raw Key Length	502 bits
QBER	2.5%
Final Key Length	489 bits

TABLE III EXPERIMENTAL RESULTS OF BB84 QKD (HALF-WIDTH TABLE)

The measured QBER of 2.5% is well below the acceptable threshold of 11%, indicating that the communication channel remains secure. This low error rate suggests that any potentialeavesdropping or noise has minimal impact on the transmis-sion. Furthermore, the consistent key generation process high-lights the robustness of the BB84 protocol, demonstrating its ability to maintain reliable performance even under simulated noisy conditions.

Post-Quantum Cryptography Performance

The PQC module, implemented using the Kyber-512 algo-rithm, was evaluated for key generation time and reliability.

Metric	Observed Value
Algorithm Used	Kyber-512
Average Key Generation Time	0.15 sec
Key Agreement Success Rate	100%
Key Size	512 bits

TABLE IV PQC KEY EXCHANGE RESULTS (HALF-WIDTH TABLE)

The results obtained from the PQC module indicate stable and efficient key generation, suggesting its suitability for integration with QKD-based systems in real-time applications. The consistency in performance highlights its reliability as a complementary security layer within the overall framework.

Hybrid Key Derivation Analysis

The session key is generated by combining the keys ob-tained from both QKD and PQC using a Key Derivation Function (HKDF). This hybrid approach strengthens security by ensuring that the compromise of one key source does not expose the entire system.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

$$K_{session} = HKDF(K_{QKD} \oplus K_{PQC}) \quad (12)$$

The resulting hybrid key exhibits strong randomness and a uniform distribution, making it well-suited for secure crypto-graphic applications.

Encryption and Authentication Performance

1) Message Encryption (OTP + HMAC): The messaging component was evaluated using inputs of varying lengths to as-sess consistency and performance. The results show that OTP-based encryption effectively preserves confidentiality, while HMAC-SHA3-256 provides reliable verification of message integrity and authenticity.

2) File Encryption (XChaCha20-Poly1305): The file en-cryption module was tested across different file sizes to measure efficiency and reliability. The findings indicate that the XChaCha20-Poly1305 algorithm delivers fast and secure encryption, making it suitable for protecting larger data trans-fers without compromising performance.

End-to-End System Performance

The complete system was evaluated for end-to-end com-munication: The system demonstrated consistent performance with no failures, confirming its robustness and reliability.

Metric	Observed Value
Messages Tested	20
Encryption Success	100%
Decryption Success	100%
HMAC Verification	100%

TABLE V MESSAGE ENCRYPTION RESULTS (HALF-WIDTH TABLE)

DISCUSSION

The experimental findings highlight the effectiveness of the proposed hybrid quantum-safe communication framework. The BB84 protocol consistently produced secure keys with a low Quantum Bit Error Rate (QBER), indicating strong resistance to eavesdropping attempts. This aligns with existing studies that demonstrate the reliability of BB84 in detecting unauthorized interception through error analysis [16], [17]. In addition, the integration of Post-Quantum Cryptography (PQC) enhances the system by enabling secure key exchange over classical channels while remaining resistant to quantum-based attacks [12].

The hybrid key derivation mechanism further strengthens the system by combining independently generated keys from QKD and PQC. This layered approach ensures that even if one component is weakened, the overall security of the system is preserved. Such hybrid models have been shown to improve robustness and fault tolerance in quantum-safe communication architectures [1], [2].

From a data protection perspective, the use of One-Time Pad (OTP) encryption provides strong confidentiality, while XChaCha20-Poly1305 ensures efficient and authenticated en-cryption for larger data transmissions. Together, these tech-niques contribute to maintaining both data integrity and per-formance.

When compared to traditional cryptographic approaches, the proposed system offers improved security, particularly in the context of emerging quantum threats. However, this added security comes with increased system complexity and computational overhead due to the integration of multiple cryptographic components.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Overall, the results suggest that the proposed framework achieves a practical balance between security, efficiency, and scalability. This makes it a promising solution for secure communication in future quantum-aware environments [18].

CONCLUSION

The implemented BB84-based QKD system successfully demonstrates secure key distribution, effective detection of eavesdropping, and seamless integration with classical cryptographic techniques for both messaging and file transfer. These results support its potential for building reliable and quantum-resilient communication systems.

CONCLUSION AND FUTURE WORK

CONCLUSION

This work presented the design and implementation of a quantum-safe communication system that integrates Quantum Key Distribution (QKD), based on the BB84 protocol, with Post-Quantum Cryptography (PQC) and modern symmetric encryption techniques. The proposed hybrid approach ad-dresses the growing security concerns associated with tra-ditional cryptographic methods in the context of advancing quantum computing technologies [12], [17].

The BB84 protocol demonstrated consistent performance in generating secure keys, with a low Quantum Bit Error Rate (QBER), allowing reliable detection of potential eaves-dropping attempts. These results are consistent with prior studies highlighting the effectiveness of BB84 in secure key exchange [16]. In addition, the integration of PQC, partic-ularly the Kyber Key Encapsulation Mechanism, provides a quantum-resistant alternative for classical key exchange, further strengthening the system's overall security [12]. By combining QKD and PQC through a hybrid key derivation process, the framework achieves a layered security model that remains robust even if one component is compromised [1], [2].

For data protection, the use of One-Time Pad (OTP) encryp-tion ensures strong confidentiality, while HMAC-SHA3-256 provides message integrity and authentication. Furthermore, XChaCha20-Poly1305 enables efficient and secure file en-cryption, making the system suitable for practical applications involving large data transfers. These combined mechanisms contribute to a balanced design that supports both security and performance.

Experimental evaluation confirms the reliability and effec-tiveness of the proposed system. The framework achieved high success rates in key generation, encryption, and decryption, with minimal delays and no observed authentication fail-ures. Compared to conventional cryptographic approaches, the proposed model offers improved resilience against quantum-based threats while maintaining practical feasibility through simulation-based implementation.

Overall, this research demonstrates that integrating quantum and post-quantum techniques can form a strong foundation for next-generation secure communication systems. The pro-posed framework helps bridge the gap between theoretical advancements in quantum cryptography and real-world imple-mentation, contributing toward the development of scalable and future-ready communication infrastructures [18].

FUTURE WORK

While the proposed system shows promising results, several directions can be explored to further enhance its capabilities:

- **Real-World Quantum Hardware Integration:** Future implementations can focus on deploying the system using actual quantum communication hardware, such as photon sources and detectors, instead of relying solely on simu-lation environments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

- **Advanced QKD Protocols:** Exploring alternative QKD protocols, such as E91 or Measurement-Device-Independent QKD (MDI-QKD), could improve security and reduce vulnerabilities related to device imperfections [17].
- **Improving Key Generation Efficiency:** Further opti-mization of error correction and privacy amplification techniques may help reduce noise effects and increase key generation rates.
- **Scalability and Multi-User Support:** Extending the system to support multiple users and larger quantum networks would enhance its applicability in real-world communication infrastructures.
- **Integration of Additional PQC Algorithms:** Incorpo-rating other post-quantum algorithms, such as NTRU or Dilithium, can provide greater flexibility and strengthen the hybrid security model.
- **Real-Time Application Development:** The framework can be extended into practical applications such as secure messaging or file-sharing platforms with web or mobile interfaces.
- **Performance Optimization:** Future work can focus on reducing computational overhead and improving latency to enable smoother real-time communication.
- **Advanced Security Analysis:** Further investigation into side-channel attacks, quantum hacking strategies, and more sophisticated adversarial models would help en-hance the system's overall resilience.

In summary, the proposed hybrid quantum-safe communica-tion system provides a strong foundation for ongoing research in secure communication technologies and supports the de-velopment of practical, scalable solutions for the emerging quantum era.

REFERENCES

1. X. Wu, B. Zhang, G. Chen, and D. Jin, "A Scalable Quantum Key Distribution Network Testbed Using Parallel Discrete-Event Simulation," ACM Transactions on Modeling and Computer Simulation, vol. 32, no. 2, article 11, pp. 1–25, Feb. 2022. doi: 10.1145/3490029.
2. I. Gkouliaras, A. Kordas, K. Vlachos, and C. Kollmitz, "NuQKD: A Modular Quantum Key Distribution Simulation Framework," Ad-vanced Physics Research, vol. 3, no. 1, pp. 1–15, Jan. 2024. doi: 10.1002/apxr.202400016.
3. S. Mangini, M. Grossi, M. W. Johnson, and R. Oru´s, "Tensor network noise characterization for near-term quantum computers," Physical Re-view Research, vol. 6, no. 2, p. 023174, Apr. 2024. doi: 10.1103/Phys-RevResearch.6.023174.
4. D. Soler, J. Cillero, P. Dafonte, and J. A. Ferna´ndez-Veiga, "QKDNet-Sim+: Improvement of the Quantum Key Distribution Simulator for NS-3," arXiv preprint arXiv:2402.10822, Feb. 2024. [Online]. Available: https://arxiv.org/abs/2402.10822.
5. A. Meddeb, F. Guen, and H. Touati, "Interactive simulation of quan-tum key distribution protocols and application in Wi-Fi networks," Wireless Networks, vol. 29, no. 6, pp. 1759–1774, Aug. 2023. doi: 10.1007/s11276-023-03438-x.
6. A. Melnikov, A. Termanova, S. V. Dolgov, F. Neukart, and M. R. Perelshtein, "Quantum state preparation using tensor networks," Quan-tum Science and Technology, vol. 8, no. 4, p. 045016, Jul. 2023. doi: 10.1088/2058-9565/acd9e7.
7. Y.-Q. Zhao, R.-G. Li, J.-Z. Jiang, C. Li, H.-Z. Li, E.-D. Wang, W.-F.
8. Gong, X. Zhang, and Z.-Q. Wei, "Simulation of quantum computing on classical supercomputers with tensor-network edge cutting," Phys-ical Review A, vol. 104, p. 032603, Sep. 2021. doi: 10.1103/Phys-RevA.104.032603.
9. C. Huang et al., "Efficient parallelization of tensor network contraction for simulating quantum computation," Nature Computational Science, 2021.
10. J. Tindall, M. Fishman, M. Stoudenmire, and D. Sels, "Efficient tensor network simulation of IBM's Eagle kicked Ising experiment," arXiv preprint arXiv:2306.14887, Jun. 2023.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

11. F. Pan, X. Gao, L. Zhao, and L. Lin, "Efficient quantum circuit simulation by tensor network methods on modern GPUs," arXiv preprint arXiv:2310.03978, Oct. 2023.
12. M. D´ıez Garc´ıa and A. Ma´rquez Romero, "Survey on computa-tional applications of tensor network simulations," arXiv preprint arXiv:2408.05011, Aug. 2024.
13. B. Aizpurua, S. Patra, J. Etxezarreta Martinez, and R. Oru´s, "Hacking cryptographic protocols with tensor network attacks," arXiv preprint arXiv:2409.04125, Sep. 2024. [Online]. Available: https://arxiv.org/abs/ 2409.04125.
14. A. M. Pastor, J. M. Badia, and M. Castillo, "A community detec-tion–based parallel algorithm for quantum circuit simulation using tensor networks," The Journal of Supercomputing, vol. 80, pp. 5212–5233, Dec.
15. 2023.
16. A. P. Thompson, A. Arrasmith, A. Anand, and M. Cerezo, "Accurately simulating noisy quantum circuits with tensor networks," arXiv preprint arXiv:2501.13237, Jan. 2025. [Online]. Available: https://arxiv.org/abs/ 2501.13237.
17. S. Masot-Llima and A. Garcia-Saez, "Stabilizer Tensor Networks: Universal Quantum Simulator on a Basis of Stabilizer States," Phys-ical Review Letters, vol. 133, no. 23, p. 230601, Dec. 2024. doi: 10.1103/PhysRevLett.133.230601.
18. M. Pereira, L. Pereira, and H.-K. Lo, "Modified BB84 quantum key distribution protocol robust to source imperfections," Physical Review Research, vol. 5, no. 2, p. 023065, Jun. 2023. doi: 10.1103/PhysRevResearch.5.023065.
19. M. Geng, "Advances of Quantum Key Distribution and Network Nonlocality," Entropy, vol. 27, no. 9, p. 950, Sep. 2025. doi: 10.3390/e27090950.
20. O. Bel, H. Shapira, A. Tzitrin, and M. Shapiro, "Simulators for quantum network modeling," Computer Networks, vol. 254, p. 110009, Mar. 2025. doi: 10.1016/j.comnet.2025.110009.
21. A. M. Pastor, J. M. Badia, and M. Castillo, "A community detec-tion–based parallel algorithm for quantum circuit simulation using tensor networks," The Journal of Supercomputing, vol. 81, pp. 14285–14302, Jan. 2025. doi: 10.1007/s11227-025-06918-3.
22. A. Berezutskii et al., "Tensor networks for quantum computing," arXiv preprint arXiv:2503.08626, Mar. 2025.