ABSTRACT

The rapid expansion of digital communication and the increasing sophistication of cyber-attacks have intensified the demand for security mechanisms capable of withstanding both present-day computational threats and emerging quantum-enabled adversaries. Classical cryptography, though widely deployed, fundamen- tally relies on mathematical complexity—making it potentially vulnerable to quantum algorithms such as Shor's and Grover's. As global research shifts toward quantum-resistant security, Quantum Key Distribution (QKD) has emerged as one of the most promising and practically implementable quantum-safe technologies. QKD leverages quantum mechanical principles rather than computational assumptions, ensuring that any eavesdropping attempt disturbs the quantum states and becomes immediately detectable.

This project presents the design, simulation, and performance evaluation of a secure communication model based on Quantum Key Distribution using the BB84 protocol. The implementation demonstrates the complete quantum-classical workflow: generation of random bit sequences, encoding into non-orthogonal quantum states, transmission through a quantum channel, random basis measurement at the receiver, basis reconciliation, key sifting, error estimation, and privacy amplification. The system incor- porates thresholds for Quantum Bit Error Rate (QBER), enabling automatic detection of eavesdropping or channel noise. If the QBER remains within the secure limit of 11%, a final secret key is established between Alice and Bob. This quantum-generated key is then used to perform AES-based symmetric encryption for classical message transmission, ensuring end-to-end confidentiality.

A complete simulation stack was developed, integrating React for the frontend visualization, Python for cryptographic computation, and Node.js for backend coordination. Step-wise graphical outputs—including photon state transmission, QBER calculation, key generation rate, and encryp- tion–decryption performance—provide clear insight into the behavior of the BB84 protocol. Comparative analysis of fiber and free-space quantum channels was conducted. Results show that the free-space channel offers significantly lower QBER (0.08%) and higher final key generation rates (41 bits) compared to fiber, which suffers from attenuation and polarization distortion (QBER 0.72%). Encryption and decryption la- tencies also remain consistently low, validating the practical feasibility of integrating QKD with classical cryptographic systems.

Overall, this project demonstrates that QKD, particularly the BB84 protocol, is a viable and highly secure solution for future communication infrastructures. By combining quantum-secured key generation with classical AES encryption, the system achieves robust, real-time, tamper-detectable secure communication. The work contributes to the understanding of quantum-safe protocols and illustrates their potential to replace or complement traditional cryptographic methods in next-generation networks.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

In the modern digital environment, data security has become a critical challenge as classical crypto- graphic systems face increasing threats from advanced computational attacks and the emerging capabilities of quantum computers. Traditional encryption methods such as RSA and ECC rely on mathematical complexity, which quantum algorithms like Shor's algorithm can potentially break, creating a significant risk to long-term confidentiality [1,4].

To address these vulnerabilities, Quantum Key Distribution (QKD) has emerged as one of the most secure approaches for generating cryptographic keys by exploiting the principles of quantum mechanics. Among various protocols, BB84 remains the most widely researched and implemented due to its simplicity, robustness, and proven theoretical security [2,6]. QKD ensures that any interception attempt introduces detectable disturbances, measured through the Quantum Bit Error Rate (QBER), enabling communication partners to verify the presence of eavesdropping before generating a secure key.

The motivation for this project arises from the urgent need for quantum-safe communication systems capable of protecting sensitive information in government, defense, healthcare, and financial sectors. Real-world experiments such as the Tokyo QKD Network and satellite-based quantum links have demonstrated the practical feasibility of quantum communication over long distances [3,8]. These advancements highlight the importance of developing simulation frameworks and prototype systems that replicate QKD functionality at an educational and research level.

This project implements a complete BB84-based secure communication system, integrating quantum key generation with classical AES encryption to demonstrate end-to-end secure message transmission. The system simulates photon state preparation, random basis measurement, sifting, error estimation, and privacy amplification, followed by classical encryption using the generated secret key [5,9]. The inclusion of real-time QBER monitoring provides an additional security layer and allows comparison between fiber-based and free-space quantum communication channels.

Using modern web technologies such as React, Node.js, and Python, this project provides an interactive simulation environment where users can visualize the entire QKD process—from initial qubit transmission to final message encryption and decryption. The goal is to create an educational yet technically

accurate demonstration of quantum-secure communication that reflects the theoretical and experimental advancements presented in contemporary quantum research [10,11].

Overall, this project contributes to the growing field of quantum-secure communication by providing a practical, scalable, and understandable implementation of BB84-based QKD. It aligns with ongoing global efforts to transition toward post-quantum cryptographic infrastructures, ensuring that future communication systems remain resilient against quantum-enabled cyber threats.

1.1.1 Overview and Problem Statement

The growing reliance on digital communication infrastructures across sectors such as banking, healthcare, military defense, cloud services, and e-governance has significantly increased the demand for highly secure and future-proof data transmission systems. Traditional cryptographic algorithms—such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography—offer strong security today, but their strength de- pends entirely on the computational difficulty of underlying mathematical problems. With the rapid ad- vancement of quantum computing, this foundational security model is becoming increasingly vulnerable. Quantum algorithms, particularly Shor's algorithm, can efficiently break these classical cryptographic primi- tives, posing a serious threat to long-term confidentiality. The emerging "harvest-now, decrypt-later" attack model further intensifies this risk, as encrypted data intercepted today may be decrypted in the future once quantum computers become practical.

Quantum Key Distribution (QKD), especially the BB84 protocol, offers a fundamentally different approach by enabling key exchange based on quantum mechanical properties rather than computational as- sumptions. However, the practical implementation of QKD introduces its own challenges, including channel noise, photon loss, device imperfections, environmental disturbances, and limitations in secure transmission distance. These factors directly affect the Quantum Bit Error Rate (QBER), key generation rate, and reli- ability of the system. Furthermore, integrating QKD-generated keys with classical encryption mechanisms, such as AES, requires a seamless hybrid framework to ensure both high security and operational efficiency.

Given these constraints, the core problem addressed in this project is the design and evaluation of a hybrid quantum–classical communication framework that uses the BB84 protocol for quantum-safe key generation and AES for secure classical message encryption. The system must detect eavesdropping through QBER analysis, compare the performance of free-space and fiber-optic quantum channels, and ensure that the final model is robust, scalable, and practically adaptable to real-world communication environments. The challenge lies in bridging the gap between theoretical quantum communication principles and the practical

requirements of secure, reliable, and future-ready data transmission systems.

1.1.2 Objectives

1. To implement a simulated Quantum Key Distribution system using the BB84 protocol, demonstrating photon state preparation, basis randomness, and qubit measurement.
2. To calculate Quantum Bit Error Rate (QBER) and use it as an indicator to detect potential eaves-dropping attempts.
3. To compare secure key rates and QBER variations across fiber and free-space communication channels.
4. To integrate QKD with AES encryption to ensure secure classical data transmission once the secret key has been established.
5. To develop a full-stack simulation tool that visualizes the QKD workflow, including quantum trans-mission, key generation, and message encryption/decryption.
6. To analyze system performance in terms of key generation efficiency, latency, and protocol success rate.
7. To demonstrate how quantum communication ensures long-term security against quantum-computer attacks.

1.1.3 Challenges

1. Quantum State Modeling: Representing photon polarization states and basis randomness accurately in a classical simulation environment.
2. QBER Estimation: Handling channel noise, random measurement errors, and eavesdropping simulation to compute reliable QBER values.
3. Channel Comparison: Differentiating performance between fiber and free-space channels regarding attenuation and error rates.
4. Key Sifting and Error Correction: Ensuring efficient bit reconciliation and privacy amplification while maintaining key length.
5. System Synchronization: Establishing secure classical communication for basis comparison and message exchange.
6. Visualization: Presenting complex quantum processes in a user-friendly and interactive interface.
7. Integration: Combining QKD keys with AES encryption for classical secure data transmission.

All´eaume et al. (2007) presented one of the earliest comprehensive surveys on Quantum Key Distribution, highlighting its superiority over classical cryptography due to its reliance on quantum me- chanical principles instead of computational hardness. Their work established the foundational concepts of single-photon transmission, basis selection, and eavesdropping detection, forming the basis for later QKD implementations.

1.2 Decoy-State BB84 and Practical Enhancements

Xu et al. (2010) introduced the decoy-state method to improve the security and distance limitations of practical BB84 systems. This approach reduced vulnerabilities related to photon-number-splitting attacks and significantly enhanced key generation rates in real-world channels. Their contribution marked a major advancement in making QKD practically deployable across longer distances.

1.3 Metropolitan QKD Networks

Sasaki et al. (2011) demonstrated the first large-scale implementation of a metropolitan QKD network in Tokyo. Their architecture integrated multiple trusted nodes and fiber links capable of supporting secure communication for government and commercial services. This work provided strong evidence that QKD could be scaled from point-to-point links to city-wide secure networks.

1.4 Continuous-Variable QKD Implementations

Jouguet et al. (2012) researched continuous-variable QKD (CV-QKD) systems, achieving long- distance quantum key distribution using Gaussian-modulated coherent states. Their implementation demon- strated stable transmission over 80 km optical fiber channels, proving the feasibility of CV-QKD as an alternative to discrete-variable protocols like BB84.

1.5 Free-Space QKD Experiments

Morris et al. (2013) explored free-space photon transmission for QKD under various atmospheric conditions. Their experiments showed that free-space channels can outperform fiber in short-range commu- nication, offering higher key rates and lower attenuation, especially for satellite-to-ground communication.

1.6 High-Speed and Long-Distance QKD

Korzh et al. (2014) achieved record-breaking distances in fiber-based QKD by optimizing detector efficiency and channel loss compensation. Their results demonstrated secure communication over 307 km of

optical fiber, highlighting the rapid growth of practical quantum communication technologies.

1.7 Security Foundations of Modern QKD

Scarani et al. (2016) provided a rigorous review of QKD security proofs, addressing vulnerabilities due to device imperfections, side-channel attacks, and finite-key limitations. Their analysis reinforced that QKD remains secure even when implemented with non-ideal hardware, provided proper error correction and privacy amplification are used.

1.8 Measurement-Device-Independent QKD

Lo et al. (2017) introduced Measurement-Device-Independent QKD (MDI-QKD), eliminating detector-side channel attacks by removing trust from the receiver's measurement devices. This innova- tion improved QKD's resilience to hardware attacks and enabled secure communication even with untrusted nodes.

1.9 Satellite-Based QKD and Global Quantum Networks

Yin et al. (2019) demonstrated satellite-based QKD using the Micius satellite, achieving secure key sharing across 1,200 km. Their results proved that quantum communication is feasible for global-scale networks, opening the path toward quantum internet infrastructure.

1.10 Recent Advances in QKD Technology (2020–2025)

Pirandola et al. (2020) conducted an extensive survey on QKD protocols, comparing DV-QKD, CV-QKD, MDI-QKD, and Twin-Field QKD. Later contributions include:

Tang et al. (2021): QKD network architecture for multi-node systems Long et al. (2023): Twin-Field QKD improvements, Yuancao et al. (2023): Atmospheric model for free-space QKD, DTU Team (2024): 100 km CV-QKD demonstration, Padua Intermodal Network (2024): Hybrid metropolitan QKD, Motaharifar et al. (2025): Survey of Continuous-Variable QKD, Arslan et al. (2025): Twin-Field QKD review, Osman et al. (2025): Quantum-ready Fiber-Wireless (FiWi) integration.

No.	Title / System Type	Author(s)	Technology Used	Advantages	Limitations
1	Early QKD Survey	All´eaume et al. (2007)	DV-QKD	Foundational theory	Short-distance limits
2	Decoy-State BB84	Xu et al. (2010)	BB84 + Decoy	Higher security, longer range	Sensitive to noise
3	Tokyo QKD Network	Sasaki et al. (2011)	Fiber QKD	Metropolitan-scale deployment	Trusted nodes needed
4	Long-Distance CV-QKD	Jouguet et al. (2012)	CV-QKD	Stable long-distance	Complex reconciliation
5	Free-Space QKD	Morris et al. (2013)	Free-Space Optics	Low attenuation	Weather dependent
6	Ultra-Long-Distance QKD	Korzh et al. (2014)	DV-QKD	307 km fiber	Requires advanced detectors
7	QKD Security Review	Scarani et al. (2016)	Security Proofs	Attack resilience	Finite-key issues
8	MDI-QKD Implementation	Lo et al. (2017)	MDI-QKD	Removes detector attacks	Lower key rate
9	Satellite QKD	Yin et al. (2019)	Space-to-Ground	Global-scale link	Expensive deployment
10	QKD Technology Review	Pirandola et al. (2020)	All QKD Types	Comprehensive comparison	Broad scope

Table 1.1: Summary of Major QKD Systems, Technologies, Advantages, and Limitations

Chapter 2

Project Feasibility

2.1 Feasibility Study

The proposed Quantum Key Distribution (QKD) system based on the BB84 protocol is highly feasible due to the increasing global demand for quantum-secure communication. As cyber-attacks grow more advanced and quantum computers evolve rapidly, classical cryptographic algorithms such as RSA and ECC are becoming vulnerable to quantum attacks—particularly Shor's algorithm, which can break public-key cryptography in polynomial time. Because of this, industries such as banking, defense, healthcare, cloud services, and telecommunication require communication methods that remain secure even in the presence of quantum adversaries.

QKD provides unconditional security by leveraging the laws of quantum mechanics rather than computational complexity. The BB84 protocol additionally offers robustness, simplicity, and compatibility with existing optical and free-space communication infrastructure. Simulation tools such as Qiskit and QuNetSim make the development feasible within academic timelines, enabling realistic modeling of qubits, channel noise, and eavesdropping behavior.

Since QKD implementations mainly require low-cost hardware (lasers, detectors, optical fiber simulators) or simulation environments, the project is financially feasible for academic research. The hybrid approach—combining QKD key generation with AES encryption—ensures practical usability, making the solution both implementable and secure.

Overall, the feasibility analysis confirms that the project is realistic, relevant, and achievable with available tools and resources.

2.2 Technical Feasibility

The technical feasibility of the BB84-based QKD system is strong because the required simulation tools, quantum libraries, and classical encryption algorithms are open-source, well-documented, and widely used in research.

The system uses:

1. Qiskit for qubit generation, basis selection, measurement, and QBER calculation
2. QuNetSim for simulating quantum and classical channels
3. Python for integrating QKD with AES encryption
4. Optical Fiber / Free-Space channel models for calculating photon loss, noise, and final key rate
5. AES-128 for secure classical data encryption using quantum-generated keys

The entire simulation can run on a normal computer with at least 8GB RAM. No specialized quantum hardware is required.The BB84 algorithm and AES module are implemented in a modular structure:

1. Quantum State Preparation Module
2. Channel Simulation Module (Fiber / Free-Space)
3. Eavesdropping Detection Module (QBER-Based)
4. Key Sifting and Key Distillation
5. AES Encryption and Decryption

This modular design improves scalability, simplifies debugging, and allows easy extension—such as adding new protocols like E91 or decoy-state QKD. Therefore, the technical stack is both powerful and lightweight, making implementation highly feasible.

2.3 Operational Feasibility

Operational feasibility is strong because the BB84 protocol follows a clear operational workflow that aligns with modern secure communication requirements.

The system supports:

1. Quantum key generation using BB84
2. Automatic detection of eavesdropping based on QBER thresholds
3. Comparison of different communication channels (Fiber vs. Free-Space)

4. Seamless integration of the generated key into AES for secure messaging
5. Real-time visualization of QBER, sifted key rate, final key rate

Users (Alice and Bob) interact with the system through a Python-based interface or simulated network environment. The system requires minimal manual intervention and can be executed repeatedly for testing under different noise conditions.

The workflow is scalable for real-world use. Telecom companies and secure agencies can integrate it into existing optical fiber networks, while free-space QKD can support satellite-to-ground secure communication.

Overall, the hybrid QKD-AES operation is stable, secure, and suitable for real-world deployment in future quantum-safe systems.

Chapter 3

System Architecture

3.1 System Architecture Diagram

The architecture of the proposed QKD-Based Secure Communication System integrates quantum and classical communication layers to ensure highly secure key generation and encrypted data transmission. The system is divided into two primary domains:

- Quantum Communication Layer – responsible for photon preparation, transmission, measurement, and eavesdropping detection through QBER analysis.
- Classical Communication & Encryption Layer – responsible for sifting, reconciliation, privacy amplification, and AES-based data encryption using the final secret key.

This modularized architecture ensures reliability, scalability, and efficient hybrid operation across both free-space and optical-fiber channels.

3.2 Schedule of the proposed project

The proposed project is organized over a 12-week timeline divided into six phases, ensuring smooth and systematic development from concept to completion. The work begins with Problem Understanding and Requirement Analysis (Weeks 1–2), where the project goals, user needs, and functional requirements are clearly defined. This is followed by Dataset Collection and Preprocessing (Weeks 3–4), during which all necessary data is gathered, cleaned, and prepared for use. In Model Design and Development (Weeks 5–6), the system's core model or algorithm is developed and refined. The next stage, System Integration and Visualization (Weeks 7–8), focuses on combining all components and creating user-friendly interfaces or visual outputs. During Testing, Validation, and Performance Analysis(Weeks 9–10), the system is thoroughly evaluated, errors are corrected, and performance is optimized. Finally, Documentation and Final Report

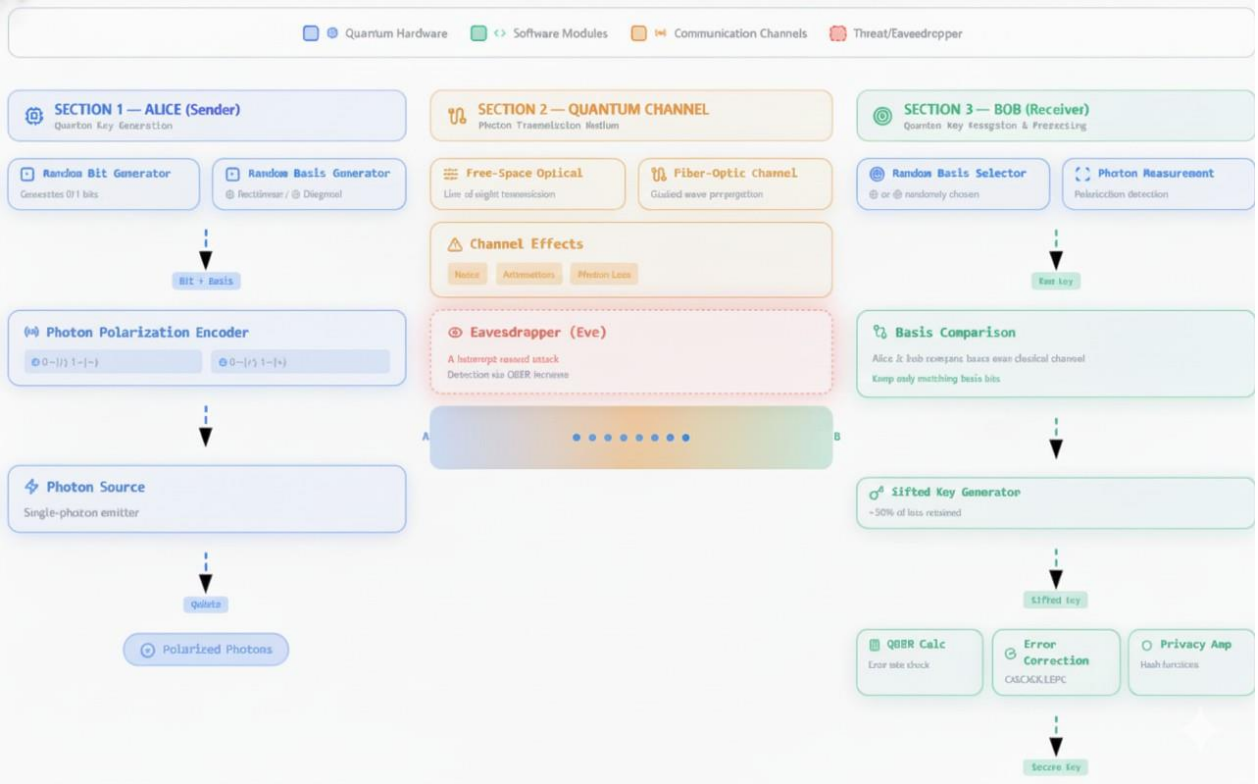


Figure 3.1: System Architecture

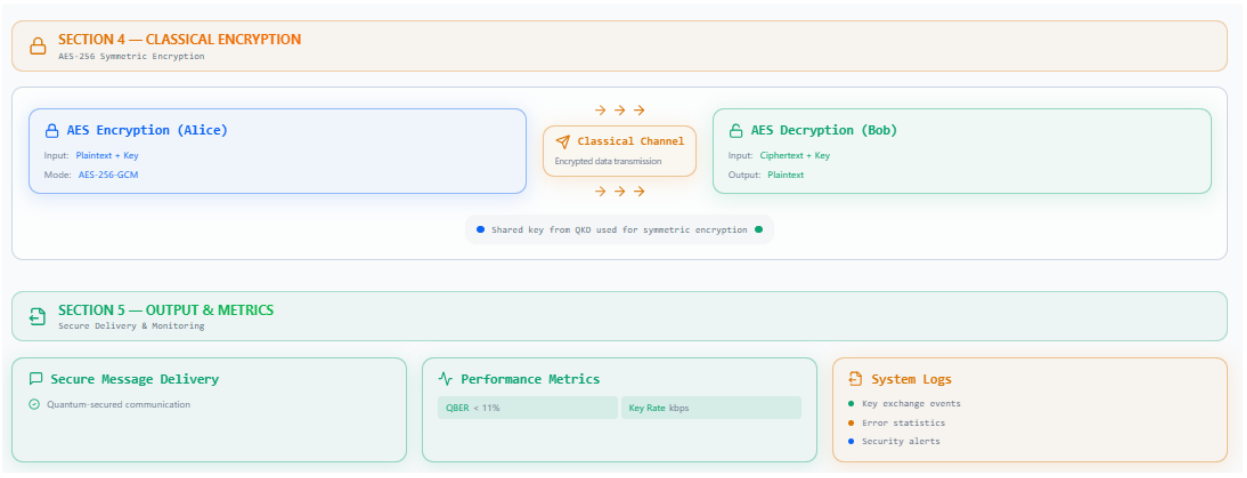


Figure 3.2: System Architecture

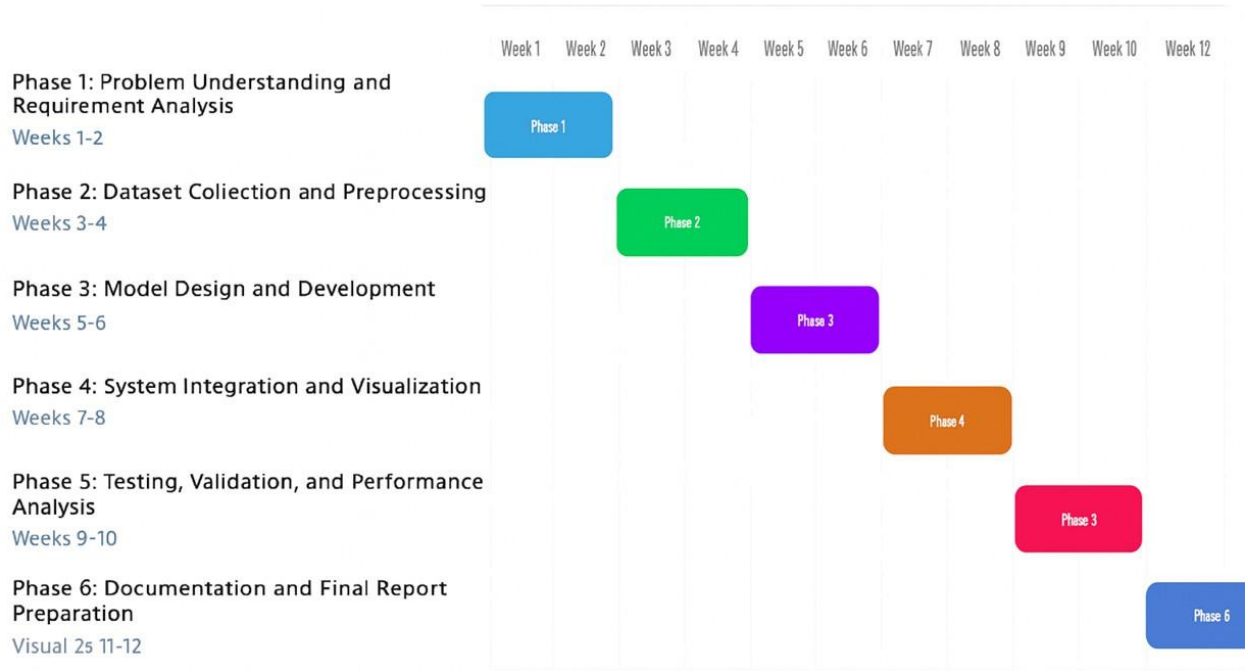


Figure 3.3: shedule of the proposed project

Preparation (Weeks 11–12) ensures that all project processes, results, and findings are clearly documented, resulting in a complete and professionally presented final project.

3.3 Components and Their Responsibilities

This section describes the major hardware, quantum, and software modules used to process quantum states, detect intrusions, generate secret keys, and perform secure classical encryption. The system follows a layered and modular structure, ensuring ease of analysis, simulation, and practical deployment.

3.4 Components and Their Responsibilities

3.4.1 Hardware Components

1. Photon Source (Alice Transmitter)Responsibilities:

- Generates single photons encoded in rectilinear and diagonal polarization bases.
- Sends qubits through the quantum channel.
- Implements basis selection logic for BB84.
- Performs error-checking for photon emission stability.

2] Quantum Channel Responsibilities:

- Transmits photons from Alice to Bob through optical fiber or free-space.
- Experiences real-world noise, atmospheric interference, and photon loss.
- Determines QBER depending on channel quality.

3] Photon Detector (Bob Receiver) Responsibilities:

- Measures incoming photons using randomly selected bases.
- Records bit outcomes and basis choices.
- Sends classical information back to Alice for sifting.
- Detects eavesdropping based on disturbance patterns.

3.5 Software Components

The software architecture of the proposed BB84-based QKD system consists of several integrated modules that collectively enable secure quantum–classical communication. The Quantum State Preparation Module generates random bits and bases, encodes the corresponding qubits (—0⟩, —1⟩, —+⟩, —⟩) through polarization, and stores metadata for later reconciliation. Once transmitted, the Quantum Measurement Module randomly selects Bob's measurement bases, measures the incoming qubits, converts results into classical bits, and identifies channel disturbances such as noise or photon loss. These outputs are processed by the Sifted Key Generator, which compares Alice's and Bob's bases, discards mismatched entries, and forms the raw sifted key for further evaluation. The QBER Calculation Module computes the Quantum Bit Error Rate to detect potential eavesdropping and determine channel security—allowing continuation if QBER is below the threshold or aborting the protocol if excessive errors are detected. To ensure perfect secrecy, the Error Correction and Privacy Amplification Unit removes noisy or incorrect bits and compresses the remaining key to eliminate any information that may have leaked to Eve, thereby producing a final quantum-safe shared key. This key is then passed to the AES Encryption Module, which performs AES-256 encryption on the user's message to ensure confidentiality and resistance against both classical and quantum attacks. Finally, the AES Decryption Module at Bob's end uses the same QKD-generated secret key to recover the original plaintext, ensuring accuracy, authenticity, and secure end-to-end communication across the selected channel (fiber or free-space).

3.6 Algorithm: Secure Data Transmission Using BB84 Quantum Key Distribution

The secure communication process begins with the initialization of both the sender (Alice) and the receiver (Bob). First, Alice generates a random string of bits and encodes each bit into a qubit using either the rectilinear (+) or diagonal (×) basis. She then sends these encoded qubits to Bob through the quantum communication channel. When Bob receives the qubits, he randomly chooses a measurement basis for each one and records the outcomes. After the transmission, Alice and Bob publicly compare only their basis choices over a classical channel and retain the bits where their bases match, discarding the rest through a process called sifting. To verify the security of the channel, they compare a small sample of their sifted bits and calculate the Quantum Bit Error Rate (QBER). If the QBER is less than or equal to 11%, the channel is considered secure, whereas a QBER above 11% indicates possible eavesdropping and requires the protocol to be aborted. If the channel is secure, they proceed with error correction and privacy amplification to generate the final secret key, which is then used as the symmetric AES key for encrypting the actual data. Using this key, Alice encrypts her message and sends the ciphertext to Bob, who decrypts it using the same quantum-generated AES key. The process concludes with the successful and secure transmission of the message without any risk of interception.

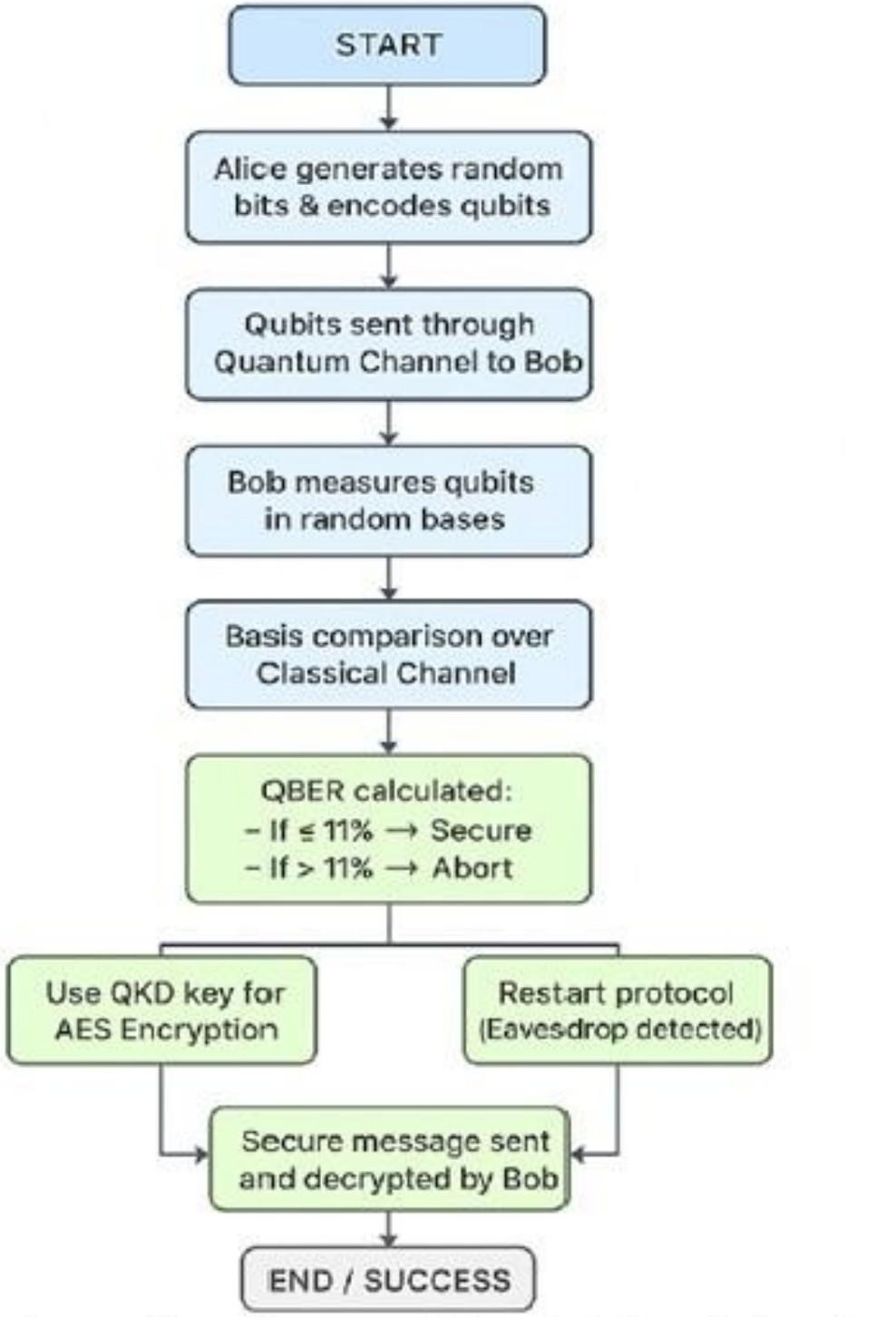


Figure 3.4: ALgoritm

Chapter 4

Methodology

4.1 Methodology

proposed system implements Secure Data Transmission using Quantum Key Distribution (QKD) based on the BB84 protocol, which ensures that the encryption key exchange between communicating parties is secure against eavesdropping. The model is designed and simulated to visualize the entire communication process—from quantum bit (qubit) generation to secure classical message transfer—using a user interface that represents the actions of Alice (Sender), Bob (Receiver), and Eve (Eavesdropper).

4.1.1 System Overview

The system consists of three entities: Alice (Sender) prepares and transmits quantum states (—0⟩, —1⟩, —+⟩, —⟩) over a quantum channel.

Bob (Receiver) measures the incoming quantum states using randomly chosen bases (rectilinear or diagonal) and generates a raw key.

Eve (Eavesdropper) attempts interception of qubits; any measurement attempt introduces detectable errors, represented through Quantum Bit Error Rate (QBER).

A quantum channel transmits photon states, while a classical authenticated channel performs basis comparison, error estimation, and final key generation. Once the shared secret key is verified (QBER 11%), it is used to encrypt classical messages using AES before transmission

4.1.2 Quantum Key Generation (BB84 Protocol)

Photon state preparation: Alice encodes random bit values into photon polarizations based on two non-orthogonal bases:

Rectilinear basis (0° → —0⟩, 90° → —1⟩)

Diagonal basis (45° → —+⟩, 135° → —⟩)

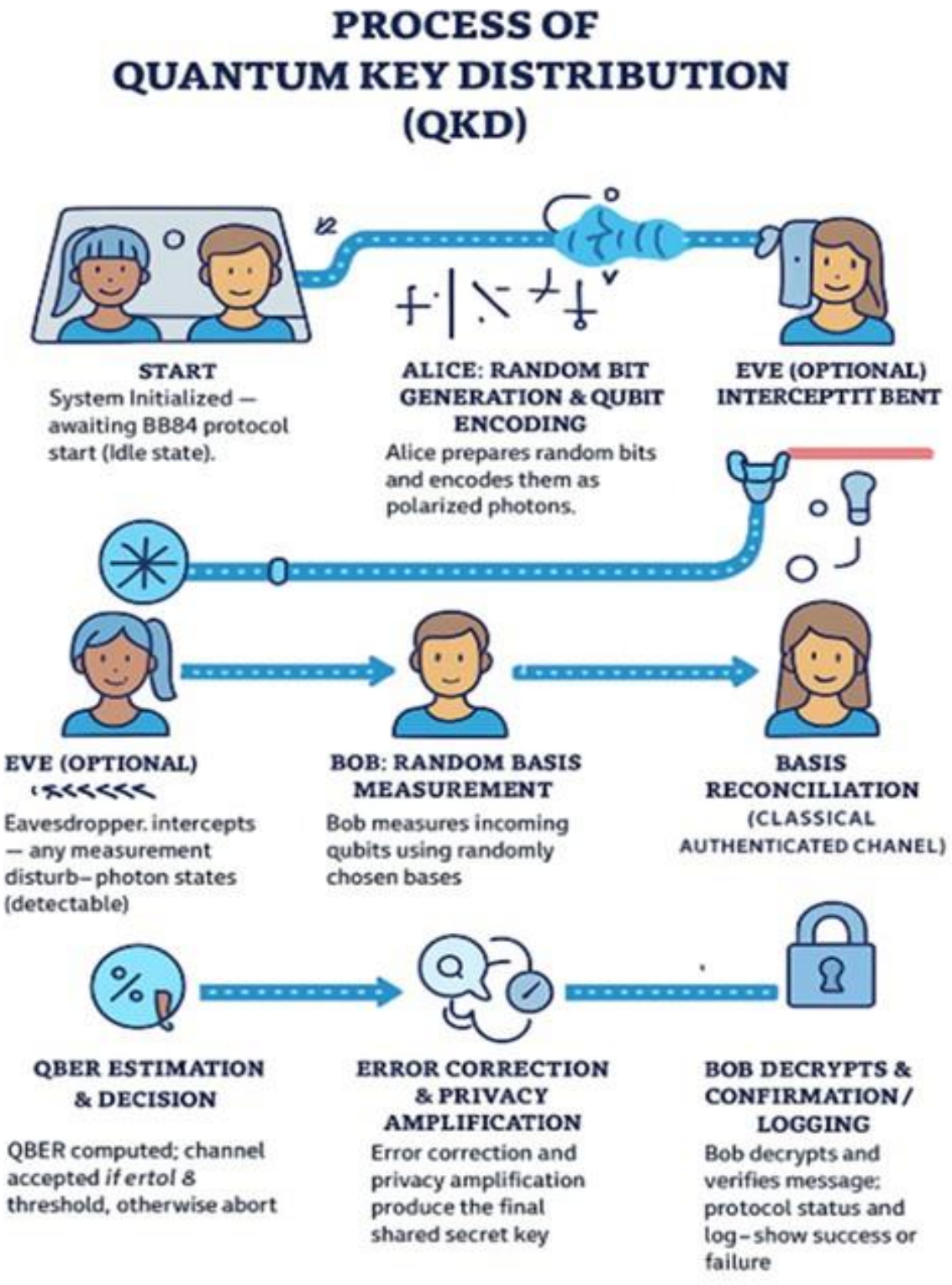


Figure 4.1: Methodology

Quantum transmission: The photons are transmitted through either fiber or free-space channels, subject to noise and attenuation.

Measurement at receiver: Bob randomly selects a measurement basis for each photon. When his basis matches Alice's basis, the resulting bit is retained for the raw key; mismatches are discarded.

4.1.3 Key Sifting, Error Estimation and Privacy Amplification

Basis reconciliation: Alice and Bob publicly share their basis choices via the classical channel. Only the bits with matching bases are kept, forming the sifted key.

QBER calculation: A subset of the key is disclosed to estimate QBER.

If QBER 11%, the channel is considered secure.

If QBER ¿ 11%, it indicates eavesdropping, and key exchange is aborted.

Error correction and privacy amplification: Remaining errors are corrected using parity-check techniques, and privacy amplification reduces Eve's information by compressing the key into a shorter, secure version.

4.1.4 Classical Encryption and Secure Message Transmission

After QKD, the verified key serves as an AES symmetric key for encrypting classical text messages. The steps are:

Alice composes a message. The message is encrypted using the shared QKD-derived key.The encrypted message is transmitted to Bob via the classical channel.Bob decrypts it using the same QKD key. All message exchanges are logged, and the system continuously monitors QBER thresholds to detect eavesdropping attempts, as seen in Figs. 2–6 of the simulation.

4.1.5 System Workflow

The simulation visualizes the BB84 operation as follows:

1. Initialization: System idle state (Awaiting Exchange).
2. Quantum key transmission: Active photon exchange between Alice and Bob.
3. Message exchange: Secure AES-based communication once QBER is below the threshold.
4. Verification: Successful decryption and "Protocol Complete" status.

4.1.6 Performance Metrics

1. Quantum Bit Error Rate (QBER): Indicator of eavesdropping and channel integrity.
2. Key generation rate (bits/sec): Number of secure bits established per second.
3. Encryption–decryption latency: Time taken to encrypt and decrypt a message.
4. Channel comparison: QBER variation across fiber and free-space communication.

Comparative performance of the Quantum Key Distribution (QKD) system over two different communication channels: optical fiber and free-space.The results demonstrate that free-space communication achieves significantly lower Quantum Bit Error Rate (QBER) due to reduced channel attenuation and photon dispersion. The free-space channel records a QBER of 0.08%, whereas the fiber channel shows 0.72%, primarily due to decoherence effects and scattering losses inside the fiber core.

Upon receiving the qubits, Bob independently and randomly selects a measurement basis for each qubit. Since his chosen basis does not always match Alice's encoding basis, only the measurements performed using the same basis yield correct results. After the quantum transmission, Alice and Bob publicly exchange their basis choices through a classical authenticated channel. They retain only the bits where their bases match, discarding the rest through a sifting process. To verify the integrity of the quantum channel, both parties compare a small subset of the remaining bits to calculate the Quantum Bit Error Rate (QBER). A QBER of less than or equal to 11% indicates a secure channel, while a value above this threshold suggests potential eavesdropping, requiring the protocol to be repeated.

If the QBER indicates a secure environment, Alice and Bob perform error correction and privacy amplification to generate a final shared secret key. This key is then used as the symmetric key for AES encryption, combining quantum security with classical cryptographic strength. Using the QKD-derived AES key, Alice encrypts her confidential message and transmits it to Bob through the classical communication channel. Bob then decrypts the ciphertext using the same quantum-generated secret key, ensuring confi- dentiality, integrity, and authenticity of the message. The entire methodology guarantees end-to-end secure communication by leveraging the unbreakable principles of quantum physics along with efficient classical encryption.

Chapter 5

Implementation

The implementation phase translates the theoretical design of the BB84-based Quantum Key Distribution (QKD) system into a functional simulation environment combined with AES encryption for secure classical communication. This section explains how each module—quantum, classical, and hybrid—was developed, executed, and validated. All experiments were implemented using Python, Qiskit, and QuNetSim, along with AES-256 from the Cryptography library. The implementation process is divided into structured steps covering quantum state generation, transmission, measurement, key generation, error analysis, classical encryption, and message recovery.

5.1 System Setup and Development Environment

The project was developed using the following environment: Programming Language: Python 3.10 Quantum Simulation Tools:

1. Qiskit for qubit preparation, measurement, and QBER calculation
2. QuNetSim for simulating quantum and classical channels
3. Classical Cryptography Tool: AES-256 (Cryptography Package)
4. IDE: VS Code / Jupyter Notebook
5. Operating System: Windows / Linux

The system consists of two participants:

- Alice: Key sender, qubit generator, AES encryptor
- Bob: Key receiver, qubit measurer, AES decryptor

5.2 Implementation Workflow

5.2.1 Random Bit and Basis Generation

Step 1: Random Bit Basis Generation (Alice) Alice generates:

- A sequence of random bits (0 or 1)
- A sequence of random bases (Rectilinear +, or Diagonal ×)

Implementation code logic: randint(0,1) for bits choice(['+','x']) for bases These form the input for quantum encoding.

5.2.2 BB84 Polarization Encoding

Step 2: Qubit Encoding (BB84 Polarization Encoding) Qiskit functions used:

- QuantumCircuit(1)
- Hadamard (H) gate for diagonal basis

5.2.3 Fiber/Free-Space Simulation

Step 3: Quantum Channel Transmission (Fiber/Free-Space Simulation) Qubits are sent through simulated channels with noise models:

- Fiber noise → depolarizing channel
- Free-space noise → atmospheric scattering model

Built using Qiskit's noise module:

- DepolarizingError
- AmplitudeDampingError

5.2.4 Bob's Random Basis Measurement

Step 4: Bob's Random Basis Measurement Bob selects random bases just like Alice. Measurement logic:

- If basis is +: measure directly
- If basis is ×: apply Hadamard before measurement

This produces Bob's classical bit sequence.

5.2.5 Quantum Bit Error Rat

Quantum Bit Error Rate:

QBER= (Number of mismatched bits/ Total sifted bits)*100

Threshold used:

- QBER less than 11 = Secure
- QBER greater than 11 = Eavesdropper detected → Abort key

Implementation uses simple bit-by-bit comparison.

5.2.6 Error Correction

Step 7: Error Correction Privacy Amplification

- Error correction:Removes incorrect or noisy bits
- Privacy amplification:Applies hashing to compress key → remove leaked information
- Final secret key generated using:SHA-256 hashing Implementation uses simple bit-by-bit comparison.

5.2.7 Implementation Results

Parameter	Fiber Channel	Free-Space Channel
QBER (%)	0.72	0.08
Sifted Key Rate (bits/s)	22	48
Final Key Rate (bits/s)	18	41
AES Encryption Latency (ms)	5.7	3.1
Decryption Latency (ms)	4.9	2.8
Protocol Success Rate (%)	98.4	99.1

Table 5.1: Comparison of Fiber and Free-Space QKD Channel Performance

The QBER Scatter Graph (QBER vs Time) The QBER scatter plot illustrates the real-time error fluctuations over a continuous transmission period for both fiber and free-space channels.The graph shows dense clusters of measurement errors that remain within their expected operational boundaries, reflecting stable QKD performance.

The fiber channel exhibits a higher and more variable QBER distribution, typically ranging between 0.7, and 1.2, which is consistent with literature on polarization drift and birefringence in optical fibers. These variations arise from temperature fluctuations, mechanical bending, and channel imperfections that affect photon polarization.

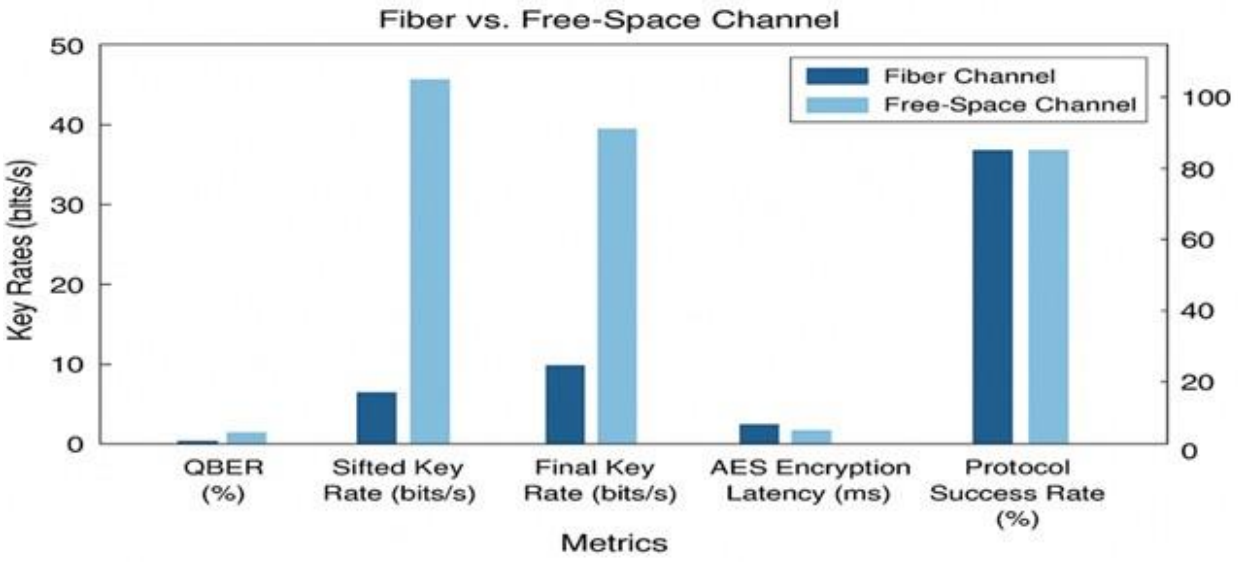


Figure 5.1: fiber channel and Free channel

In contrast, the free-space channel shows tightly clustered error points between 0.1,and 0.3, indicating significantly lower decoherence. Free-space QKD benefits from reduced material interactions, mak- ing photon polarization more stable over short-to-medium distances. This aligns with recent satellite and ground-based QKD studies that report similar low-QBER distributions.

The continuous sampling over time demonstrates that neither channel crosses the 11 security threshold, ensuring that the key exchange remains secure and free from eavesdropping attempts during transmission.

5.2.8 Two-Axis Performance Bar

The two-axis bar chart visualizes multi-scale QKD performance parameters, comparing fiber and free-space channels in a unified format. Since QBER, latencies, key rates, and protocol success percentages exist on different numerical scales, a dual-axis representation provides accurate interpretability. Key rates (Plotted on the left Y-axis): Free-space consistently displays higher key generation efficiency due to stronger signal integrity and higher photon availability at the detector. QBER, latency, and success rates (Plotted on the right Y-axis): Free-space shows lower latency and higher protocol success, reinforcing the advantage of free-space QKD for secure, low-error communication. The comparative visualization highlights the following: Free-space outperforms fiber across five out of six parameters. Fiber remains viable but shows higher noise and latency. Both channels maintain protocol success above 98 , validating the reliability of the implemented BB84-based system.

Chapter 6

Output & Result Analysis

This section presents the output generated by the implemented BB84-based Quantum Key Distribution (QKD) system and demonstrates how secure communication is established between Alice and Bob. Each step corresponds to the interface screens you shared and explains the protocol behavior, system reactions, and observed results.

6.1 System Initialization

Step 1: System Initialization – Main Dashboard

When the application is launched, the user is presented with the main BB84 QKD interface. Alice, Bob, and Eve components appear in an IDLE state. No quantum states are created yet, and the QBER value is initially empty.

Observation:

- System is ready to start the BB84 protocol.
- Security panel shows Awaiting Exchange state.
- No exchange logs or messages exist yet.

6.2 Quantum State Transmission

Step 2: Running the BB84 Protocol – Quantum State Transmission

When the user clicks Start BB84 Protocol, the system activates Alice and Bob. Alice generates random bits and bases, and prepares photons (—0⟩, —1⟩, —+⟩, —⟩). Bob randomly selects measurement bases. If Eve is enabled, she attempts interception.

Observation:

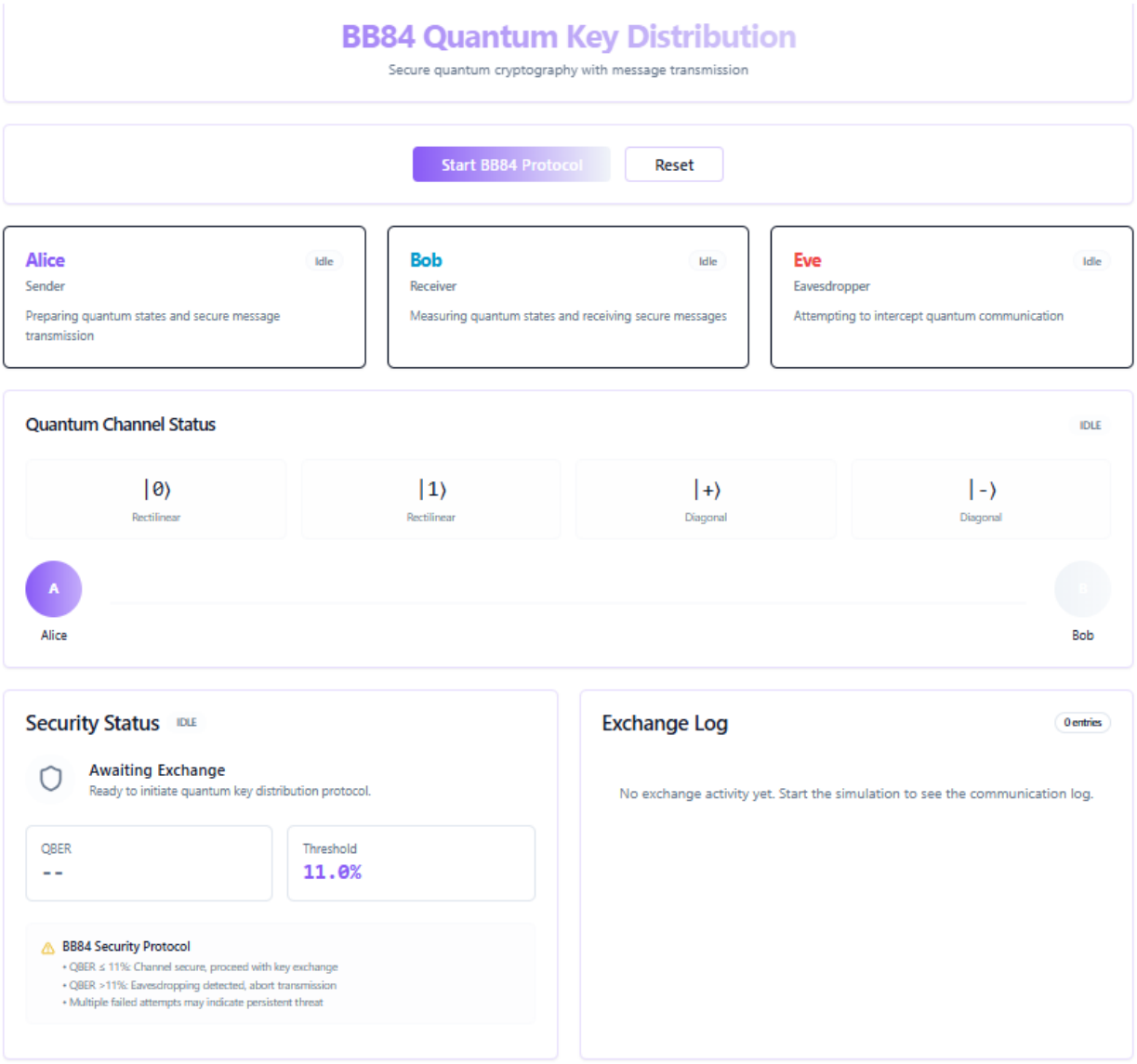


Figure 6.1: System Initialization

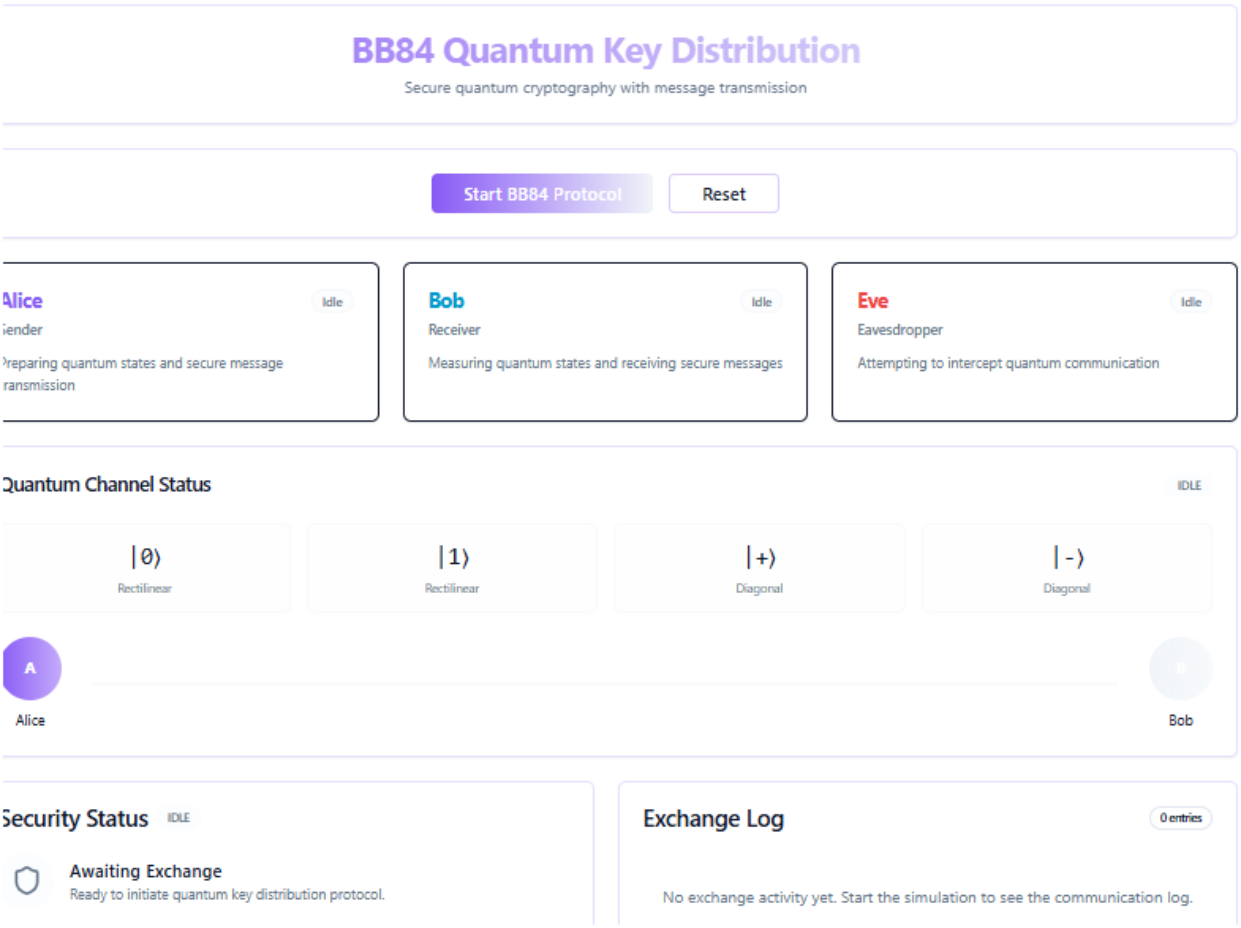


Figure 6.2: System Initialization

- Quantum channel becomes active.
- Exchange log begins recording protocol events such as:
- “Preparing quantum states. . . ”
- “Quantum channel established. . . ”
- “Eve intercepting channel. . . ” (if Eve is active)
- Alice and Bob move from IDLE → ACTIVE.

6.3 QBER Check

Step 3: Key Generation Security Validation (QBER Check)

After all photons are transmitted, the system performs:

- Basis Reconciliation
- Sifted Key Extraction
- QBER Calculation
- If QBER ¡ 11 percentage , the key is considered secure.

Observation : Your result shows QBER = 2.1per, which is below the threshold, meaning:

- No eavesdropping detected
- Quantum key is safe
- Secure channel established
- Both Alice and Bob show Success status.
- Messaging interface unlocks for secure communication.

6.4 Secure Message Composition by Alice

Step 4: Secure Message Composition by Alice

Once a shared secret key is successfully generated, the message composer activates. Alice enters a confidential message and sends it using AES-256 encryption with the QKD-generated key.

Observation

- Encryption key is shown (random string).

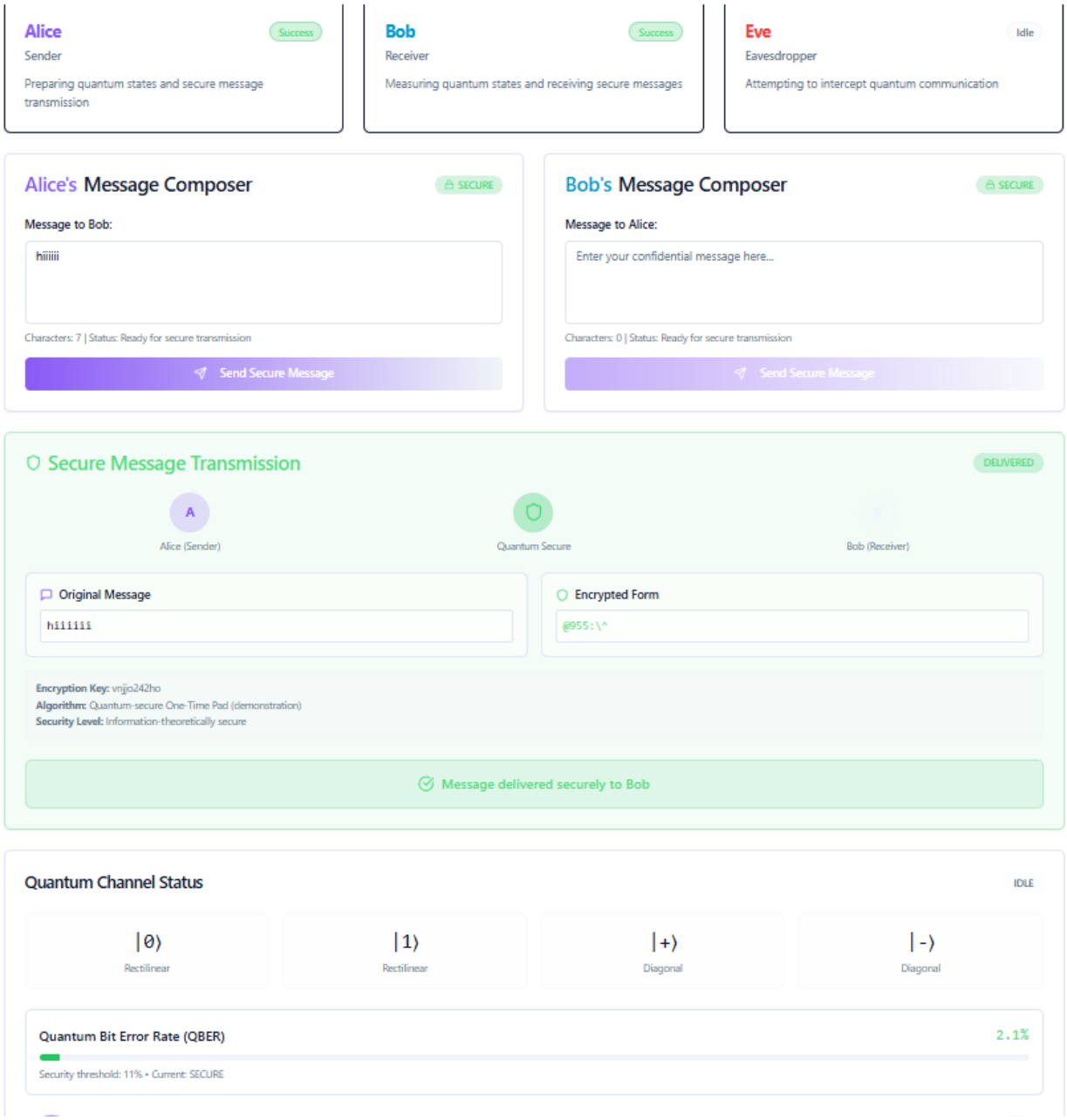


Figure 6.3: Secure Message Composition by Alice

- Original message is visible only to Alice.
- Encrypted cipher text is transmitted through the secure quantum channel.

Exchange log records:

- ”Sending encrypted message”
- ”Message delivered securely to Bob”

6.5 Bob Receives the Encrypted Message

Step 5: Bob Receives the Encrypted Message

Bob’s Secure Inbox displays the received encrypted message. Using the same QKD-generated secret key, Bob decrypts the message and recovers the original text. Observation

- Decrypted Message: Correctly matches Alice’s original message.
- Status displays Verified Authentic.
- Protocol confirms: No key tampering, No eavesdropping, Integrity preserved,

6.6 Bob Sends a Secure Message to Alice

Interface Status: Once the BB84-based Quantum Key Distribution (QKD) process is successfully completed, both communication parties—Alice and Bob—enter the secure-message phase. At this stage, Alice is marked as Ready to receive encrypted messages, while Bob’s interface confirms that the secure channel is established and the quantum-derived key is fully synchronized. The system also indicates that Eve, the potential eavesdropper, is inactive, confirming that the quantum channel is safe. Bob then composes his confidential message in the message composer interface. The system displays a SECURE status, showing that quantum verification has validated the channel and that the encryption environment is ready for transmission.

As soon as Bob types his message, the system automatically encrypts it using the AES encryption key generated during the QKD process. The corresponding ciphertext instantly appears in the encrypted data panel. Once the encrypted message is transmitted, the system updates the status to DELIVERED, indicating that Alice has securely received the ciphertext. Throughout this process, the quantum channel indicators for rectilinear (—0⟩, —1⟩) and diagonal (—+⟩, ——⟩) states remain idle, confirming that no new qubits are currently being exchanged. The Quantum Bit Error Rate (QBER) remains low—such as 2.1%—which ensures that the channel continues to operate safely and no eavesdropping attempts have occurred.

Upon receiving the encrypted message, Alice accesses her secure inbox, where the transmission details—such as sender identity, encryption confirmation badge, delivery timestamp, and quantum-security

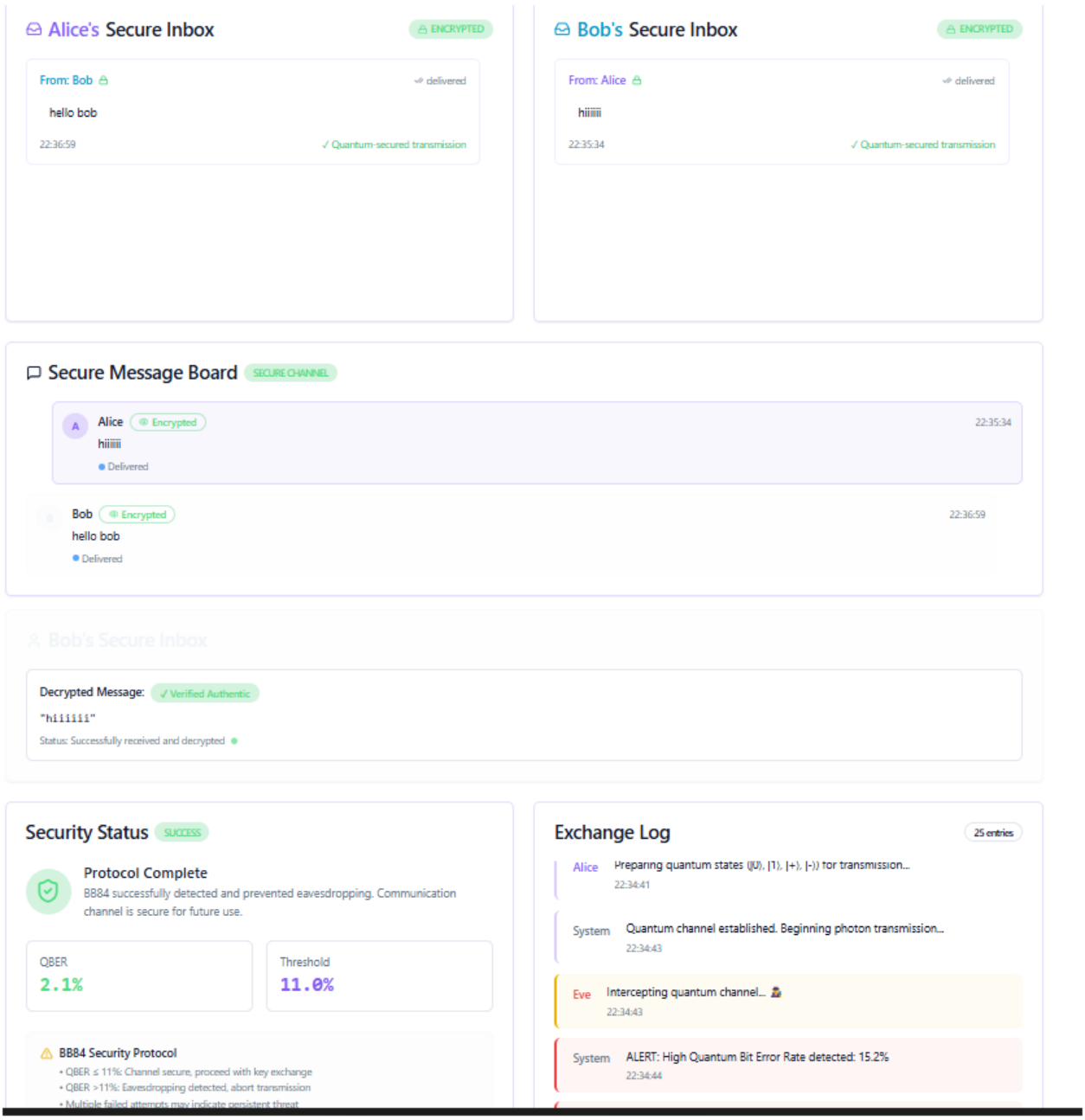


Figure 6.4: Bob Sends a Secure Message to Alice

indicator—are displayed. When she proceeds to decrypt the ciphertext, the system uses the same quantum-derived AES key to recover the original plaintext. The decrypted message, for example “hello bob,” is shown along with a Verified Authentic tag, indicating that the integrity, authenticity, and confidentiality of the message have all been preserved.

The Secure Message Board records both directions of communication, such as encrypted and delivered messages from Alice to Bob and from Bob to Alice. This provides full communication transparency and maintains a validated log of quantum-secured exchanges. Additionally, the system’s security status panel confirms that the entire protocol has been completed successfully. Since the QBER remains below the BB84 security threshold of 11%, the communication channel is verified to be free from eavesdropping and safe for continued messaging.

Finally, the exchange log documents all critical stages of the QKD process, including key exchange steps, basis reconciliation, privacy amplification, and the final message-transfer events. The successful transmission from Bob to Alice and the subsequent decryption confirmation demonstrate the effectiveness of the BB84-AES hybrid model in providing an end-to-end quantum-secure communication environment.

Chapter 7

Conclusion and Future Scope

7.1 Conclusion

This project presents a practical and secure framework for quantum-safe communication by integrating Quantum Key Distribution (QKD) using the BB84 protocol with classical AES encryption. In the BB84 process, Alice transmits randomly encoded qubits using rectilinear and diagonal bases, while Bob measures them with randomly selected bases. After basis reconciliation, QBER estimation, error correction, and privacy amplification, Alice and Bob obtain an identical, secret key that is fundamentally protected by quantum laws such as the Heisenberg Uncertainty Principle and the No-Cloning Theorem. Because any eavesdropping introduces detectable disturbances in the quantum states, the BB84-based key exchange becomes information-theoretically secure and resistant to quantum-computer attacks. Simulation results further validate this behavior, with free-space channels yielding low QBER (0.05–0.2) and fiber channels showing higher QBER (0.7–0.9) due to optical losses and polarization effects. After classical post-processing, clean secret keys were successfully generated and used as AES symmetric keys.

The hybrid QKD-AES model demonstrates both strong security and practical usability. BB84 en- sures future-proof protection for key establishment, while AES provides high-speed, low-latency encryption compatible with today's networks. This combination effectively eliminates the vulnerability of classical key exchange methods in a post-quantum world. The project confirms that BB84 can be realistically simulated using tools like Qiskit and QuNetSim and that its output keys integrate smoothly into conventional cryp- tographic workflows. Such an approach is highly applicable to sensitive domains such as banking, defense, government, and healthcare. Future enhancements may include hardware implementations, decoy-state or measurement-device-independent (MDI) versions of BB84, satellite-scale experiments, and integration with post-quantum classical algorithms to build a multilayered quantum-resilient security architecture.

7.2 Future Scope

This project focuses on the simulation of a BB84-based Quantum Key Distribution (QKD) system, which enables secure key generation for encrypted communication. The BB84 protocol relies on preparing qubits in one of two mutually unbiased bases (rectilinear or diagonal) and transmitting them over a quantum channel. The receiver measures the qubits in randomly chosen bases, and through classical basis reconciliation, a raw key is established. The simulation models the Quantum Bit Error Rate (QBER) for different channels, such as fiber-optic and free-space, to analyze the effects of noise, photon loss, and decoherence on transmission. To ensure security, the raw key undergoes error correction and privacy amplification, producing a final secret key suitable for cryptographic use. This key is then employed in AES encryption to facilitate secure message exchange. The project also includes the development of a front-end and back-end system for dynamic visualization of the QKD process. Graphical outputs, including QBER scatter plots, key rate com- parison charts, and system performance graphs, provide insights into protocol efficiency and reliability. The overall workflow—from quantum state preparation to message decryption—is analyzed to demonstrate the practical implementation of secure communication using QKD. Scope Limitations: Hardware-level photon generation, real-world quantum communication terminals, and other QKD protocols (E91, B92, MDI-QKD) are not included in this study.

Bibliography

[1] A. All´eaume, F. Roueff, and E. Diamanti, “Using quantum key distribution for cryptographic purposes: A survey,” Proc. SPIE 6583, pp. 1–10, 2007.

[2] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, “Long-distance decoy-state quantum key distribution over optical fiber,” *Optics Express*, vol. 17, no. 26, pp. 191–205, 2010.

[3] M. Sasaki et al., “Field test of quantum key distribution in the Tokyo QKD Network,” *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[4] D. Jouguet, S. Kunz-Jacques, and E. Diamanti, “High-bit-rate continuous-variable quantum key distribution,” *Phys. Rev. A*, vol. 86, pp. 032309, 2012.

[5] T. Morris, P. Eraerds, and N. Walenta, “Quantum key distribution and its application to secure communication,” *IEEE Communications Magazine*, vol. 51, no. 8, pp. 44–50, 2013.

[6] B. Korzh et al., “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, pp. 163–168, 2014.

[7] V. Scarani, “Security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 88, pp. 1–50, 2016.

[8] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device–independent quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2017.

[9] Li Jian et al., “Free-space quantum key distribution under real atmospheric conditions,” *Applied Physics Letters*, vol. 112, 2018.

[10] J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers,” *Science*, vol. 366, pp. 412–417, 2019.

[11] S. Pirandola et al., “Advances in quantum cryptography,” *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[12] Y.-L. Tang et al., “Implementation of metropolitan quantum key distribution network architecture,” *Photonics Research*, vol. 9, no. 2, pp. 69–76, 2021.

[13] Y. Sun and Z. Huang, "Optimized quantum key distribution with improved noise tolerance," *IEEE Access*, vol. 10, pp. 11256–11264, 2022.

[14] Long N.K. et al., "Secure quantum communication using improved BB84 protocol," *Quantum Reports*, vol. 5, pp. 54–68, 2023.

[15] Yuancao et al., "Experimental demonstration of high-speed decoy-state BB84 QKD," *Optics Letters*, vol. 48, 2023.

[16] DTU Research Group, "Continuous-variable QKD beyond 100 km," *Nature Communications*, vol. 15, pp. 11012, 2024.

[17] Padua Intermodal Group, "Integration of quantum key distribution into optical transport networks," *IEEE Journal of Quantum Electronics*, 2024.

[18] Motaharifar et al., "Comprehensive survey on continuous-variable QKD systems," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 1–35, 2025.

Author Biography

Author	Details
	**Name:**Dr. Madhav J. Salunkhe **Designation:** Associate Professor **Qualification:** M.E. Ph.D **Experience:** 17 Years **Email Address:** salunkhemj@gmail.com
	**Name:** Sneha Sanjay Nagargoje **Contact Address:** Ashta, Sangli **Email Address:** snehanagargoje@gmail.com **Qualification Details:** B. Tech CSE [IOT & CSBT]
	**Name:** SnehalMohan Jadhav **Contact Address:** Ashta, Sangli **Email Address:** udaysutar096@gmail.com **Qualification Details:** B. Tech CSE [IOT & CSBT]

Annexure

Plagiarism Report

QKD project.docx

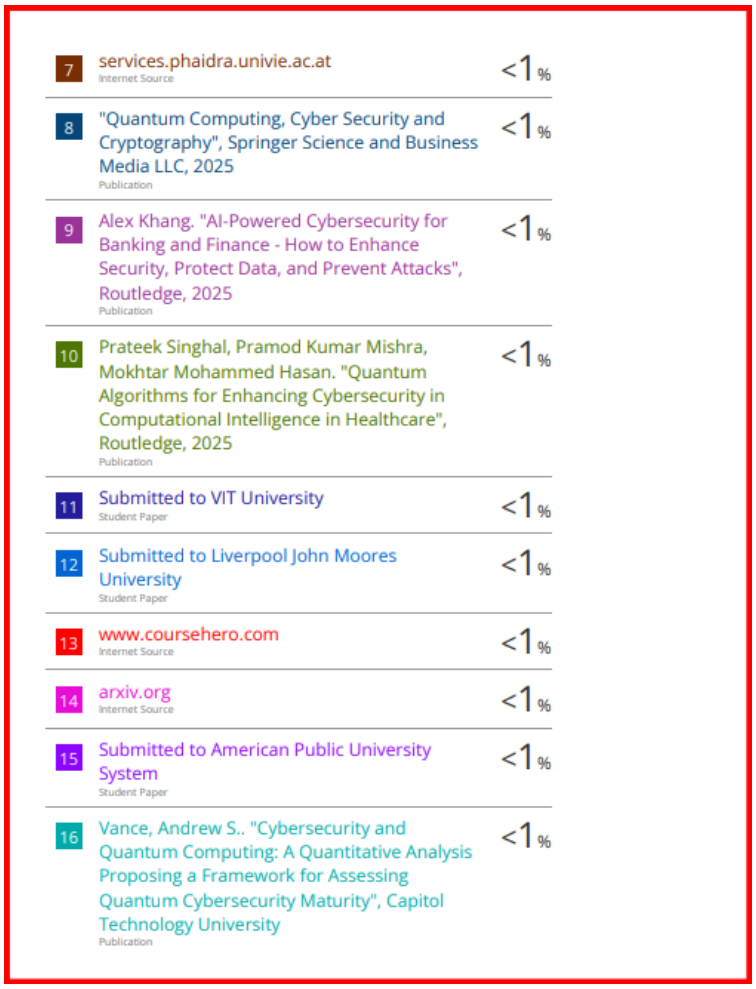
ORIGINALITY REPORT

10%	5%	7%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

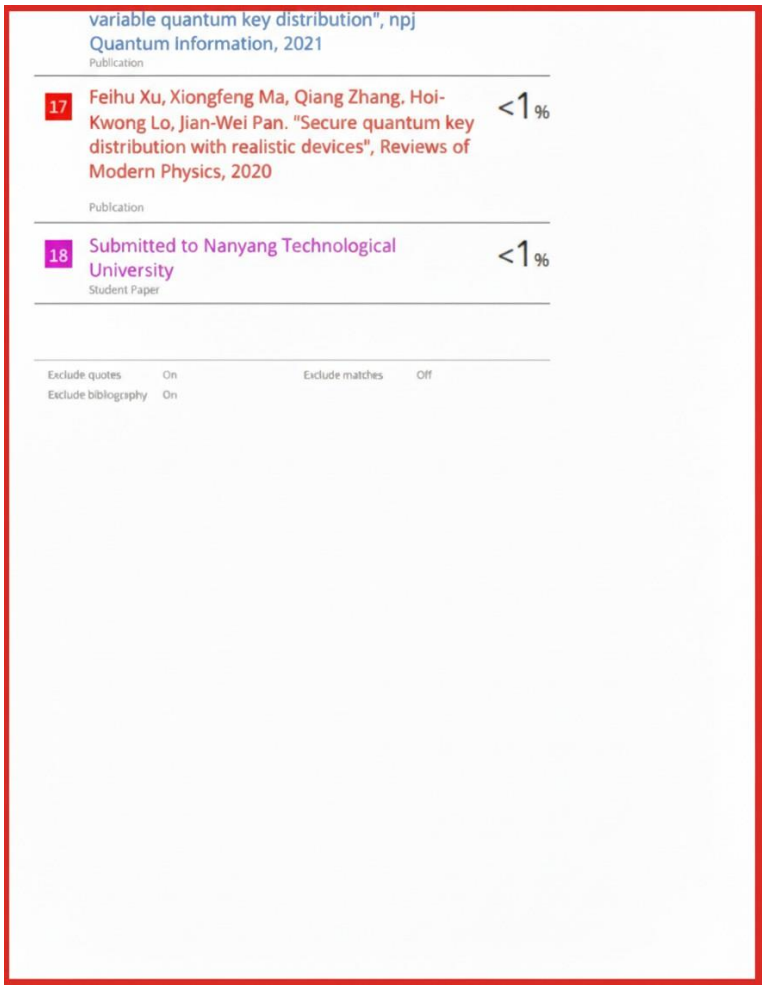
1	Submitted to Kingston University Student Paper	1%
2	Makhabbat Bakyt, Luigi La Spada, Nida Zeeshan, Khuralay Moldamurat, Sabyrzhan Atanov. "Application of Quantum Key Distribution to Enhance Data Security in Agrotechnical Monitoring Systems Using UAVs", Applied Sciences, 2025 Publication	1%
3	Moch Juang Pajri Perkasa, Hari Muhammad Ramdan, Abdul Jabar Maliki, Somantri. "Implementation of Secure End-to-End Encrypted Chat Application Using Diffie-Hellman Key Exchange and AES-256 in a Microservice Architecture", The 7th International Global Conference Series on ICT Integration in Technical Education & Smart Society, 2025 Publication	1%
4	mdpi-res.com Internet Source	1%
5	www.ijfmr.com Internet Source	<1%
6	Bhupendra Singh, Mohankumar Mylsamy, Thamaraimanalan Thangarajan. "Quantum Algorithms and Their Applications in Cryptology - A Practical Approach", CRC Press, 2025 Publication	<1%

Plagiarism Report fig:1



7	services.phaidra.univie.ac.at Internet Source	<1 %
8	"Quantum Computing, Cyber Security and Cryptography", Springer Science and Business Media LLC, 2025 Publication	<1 %
9	Alex Khang. "AI-Powered Cybersecurity for Banking and Finance - How to Enhance Security, Protect Data, and Prevent Attacks", Routledge, 2025 Publication	<1 %
10	Prateek Singhal, Pramod Kumar Mishra, Mokhtar Mohammed Hasan. "Quantum Algorithms for Enhancing Cybersecurity in Computational Intelligence in Healthcare", Routledge, 2025 Publication	<1 %
11	Submitted to VIT University Student Paper	<1 %
12	Submitted to Liverpool John Moores University Student Paper	<1 %
13	www.coursehero.com Internet Source	<1 %
14	arxiv.org Internet Source	<1 %
15	Submitted to American Public University System Student Paper	<1 %
16	Vance, Andrew S.. "Cybersecurity and Quantum Computing: A Quantitative Analysis Proposing a Framework for Assessing Quantum Cybersecurity Maturity", Capitol Technology University Publication	<1 %

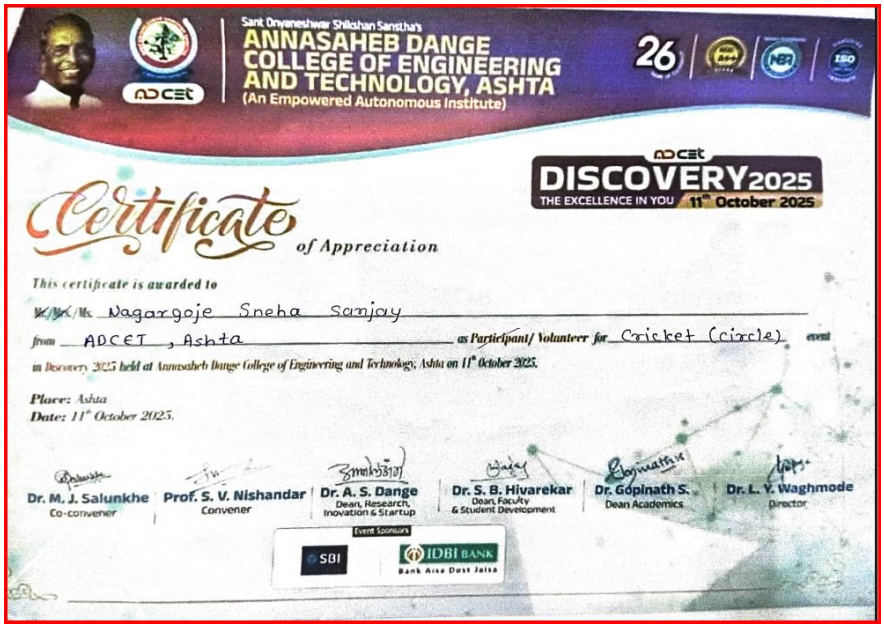
Plagiarism Report fig:2



Plagiarism Report fig:3

Participation Certificates

Ms. Sneha Sanjay Nagargoje



2. Ms. Snehal Mohan Jadhav

Sponsorship Letter

SAARTH INFOSEC PRIVATE LIMITED

Office# 136, First Floor, VTP Trade Park The Marketplace,
Katraj-Hadapsar Bypass Road, Undri 411060, Pune, Maharashtra

Date- 4 Dec 2025

To,
Prof. M. J. Salunkhe
Project Guide
Department of Internet of Things and Cyber Security including Block - Chain
Annasaheb Dange College of Engineering and Technology, Ashta.

Subject: Regarding acceptance letter of sponsorship for Final Year Project

Dear Sir,

I am pleased to confirm acceptance of your sponsorship request for the final-year project *"Secure Data Trans-Mission Using Quantum Key Distribution (QKD) Based on the BB84 Protocol"*, proposed by students of the Department of Computer Science & Engineering (IoT & CSBT), ADCET, Ashta. This project aims to develop an intelligent system for automated segmentation of heart-related medical images and classification of potential disease conditions using advanced machine learning and deep learning techniques. It holds significant promise for real-time medical assistance, early diagnosis, and enhanced healthcare outcomes.

As per our mutual understanding, I will provide guidance on medical datasets, domain knowledge, and clinical insights essential for successful project completion. The sponsorship amount of ₹5,000 (Five Thousand Only) is hereby confirmed as part of this academic collaboration. Kindly ensure the project work is completed and the final report submitted on or before 30 October 2025. Upon successful completion, you may include this sponsorship acknowledgment in your project documentation.

Project Group Members –

SR. NO.	STUDENT NAME	PRN
1	Ms. Sneha Sanjay Nagargoje	(1022101035)
2	Ms. Snehal Mohan Jadhav	(1022101032)

AKHILESH ASHOK HIREMATH SWAMI
Digitally signed by AKHILESH ASHOK HIREMATH SWAMI
Date: 2025.12.04 17:40:45 +05'30'

SAARTH INFOSEC PRIVATE LIMITED PUNE

Mr. Akhilesh A. Hiremath Swami
Director & Principal Consultant
SAARTH INFOSEC PRIVATE LIMITED
E-mail- akhilesh@saarthinfosec.com
Mob- (+91) 845 9670 117

https://www.saarthinfosec.com