Software Security and Quantum Communication: A Long-distance Free-space Implementation Plan of QSDC Without Quantum Memory

YEW KEE WONG*, YIFAN ZHOU*, ZI YAN LI*, YAN SHING LIANG*, and XINLIN ZHOU*, BASIS International School Guangzhou, China

Software security is crucial to ensuring the confidentiality, integrity, and availability of software systems and applications. However, conventional cryptographic methods based on mathematical assumptions are vulnerable to various attacks, especially in the era of quantum computing. Therefore, there is a need for a new paradigm of software security that can resist quantum threats. This paper proposes a novel approach to using Long-Distance Free-Space Quantum Secure Direct Communication (LF QSDC) to enhance software security. LF QSDC is a quantum communication protocol that enables two parties to exchange secret messages directly without relying on a pre-shared key or quantum error correction. Our research delves into integrating LF QSDC into software security, emphasizing its practicality for long-distance communication through the use of memory DL04 protocol, Machine Learning Enhanced JEEC, and PAT Technologies. By adopting this approach, we reinforce security for global software security and ensure their sustainability in an era where both quantum and advanced classical threats coexist side by side. Thus, LF QSDC emerges as a future-proof security mechanism highly applicable to software security systems.

Additional Key Words and Phrases: Quantum Cryptography, Software Security, Quantum Secure Direct Communication, Software Engineering

ACM Reference Format:
Yew Kee Wong, Yifan Zhou, Zi Yan Li, Yan Shing Liang, and Xinlin Zhou. 2024. Software Security and Quantum Communication: A Long-distance Free-space Implementation Plan of QSDC Without Quantum Memory. 1, 1 (February 2024), 23 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The fields of software and software engineering are in constant flux, driven by the need to adapt to societal and environmental shifts. As software becomes increasingly integral across various sectors—including communication, education, entertainment, business, and governance—its complexity, diversity, and ubiquity escalate. Software engineering, which applies rigorous engineering principles to software design, development, testing, and maintenance, seeks to bolster software quality, reliability, and efficiency. It endeavors to meet the diverse needs and expectations of stakeholders and end-users.

*Yew Kee Wong, Yifan Zhou, Zi Yan Li, Yan Shing Liang, and Xinlin Zhou shares co-first authorship to this work.

Authors' address: Yew Kee Wong, yewkeewong.eric@gmail.com; Yifan Zhou, yifan.zhou11882-bigz@basischina.com; Zi Yan Li, ziyan.li11716-bigz@basischina.com; Yan Shing Liang, yanshing.liang40486-bigz@basischina.com; Xinlin Zhou, xinlin.zhou13495-bigz@basischina.com, BASIS International School Guangzhou, 8, Jiantashan Lu, Guangzhou, Guangdong, China.

XXXX-XXXX/2024/2-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Nevertheless, software and software engineering also face many threats and risks, especially in terms of security. Security is a paramount concern in software engineering, entailing the safeguarding of systems and applications against unauthorized interventions, alterations, or destruction. It covers the protection of data and information's confidentiality, integrity, and availability throughout storage, processing, or transmission phases. Ensuring security is vital for maintaining software functionality, performance, and usability, in addition to protecting user privacy, rights, and societal interests.

However, software security and the broader field of software engineering face significant threats from a variety of sources: the escalating complexity, diversity, and interconnectedness of software systems; the intensifying sophistication and frequency of cyberattacks; and the introduction of disruptive technologies and paradigms. Among these, quantum computing emerges as a critical challenge. By harnessing quantum mechanics, quantum computing has the potential to solve problems far more efficiently than traditional computing methods, posing a direct threat to current security protocols and undermining the foundational assumptions of software security. Quantum computing poses a serious threat to the security of software and software engineering, as it can potentially break the current cryptographic systems that are widely used to protect the data and information on networks software systems, and applications [1][2]. Several quantum-resistant cryptographic methods have been proposed, such as Lattice-based cryptography, Multivariate cryptography, and Hash-based cryptography. Still, they are not immune to classical attacks, such as lattice reduction algorithms, differential cryptanalysis, and collision attacks [3][4][5].

Quantum communication is a promising technology that can improve the security and performance of networks. However, it requires a new protocol that can overcome the challenges of long-distance free-space quantum communication for practical software security applications. We propose Long-distance Free-space Quantum Secure Direct Communication (LF QSDC) as a potential solution.

LF QSDC is superior to other quantum communication methods, such as Quantum Key Distribution (QKD), because it can directly transmit data without the need for key exchange, which is essential for QKD. This direct transmission approach reduces the vulnerability points and enhances security, which is vital for the decentralized and trustless nature of blockchain networks [11][12]. Moreover, LF QSDC is compatible with long-distance free-space communication, which matches the nature of long-range, bulk communication in software security. QKD, on the other hand, has security advantages but also has drawbacks such as the dependence on key exchange and the limitations in communication distance, which make it less suitable for the expansive and interconnected blockchain networks that are integral to Web 3.0 applications [7][8].

LF QSDC also outperforms other quantum direct communication methods, because it can enable reliable quantum communication over long distances in free-space environments [9][10]. This is especially important for applications that involve transactions happening over large distances. Conventional QSDC methods are more suited for short distances or within fiber channels, but they face challenges when applied on a larger scale due to signal loss and difficulties in transmitting through free-space environments [11][13-14].

LF QSDC is based on the memory-free DL04 protocol [15] and enhanced with Machine Learning enhanced Joint Encryption and Error Control coding (ML JEEC) [16]and Pointing, Acquisition, and Tracking (PAT) technologies [17], which can address these limitations. The memory-free nature of the DL04 protocol reduces the complexity of quantum state storage and management, making the system more practical and robust for real-world applications [15]. The addition of PAT technologies and a ML JEEC coding scheme mitigates the issues related to atmospheric turbulence and alignment errors, which are significant challenges in free-space quantum communication [16,18,19].

Table 1. Comparison of Types of Quantum Secure Communication Protocols

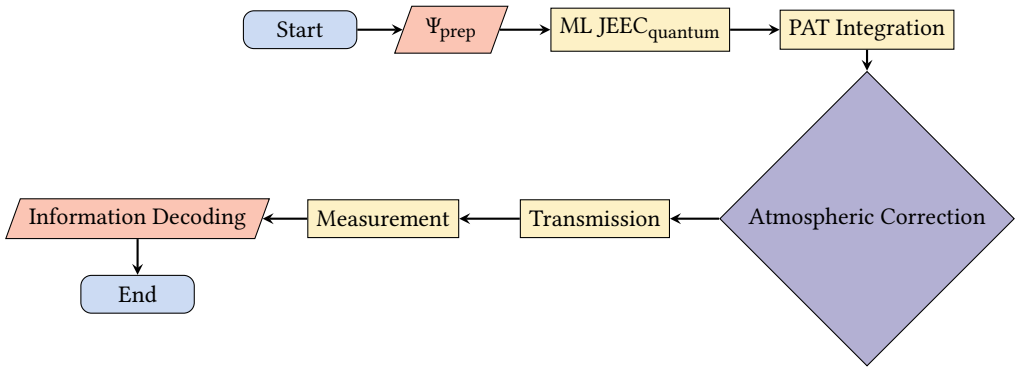
Category	**Type of Protocol**			
	LF QSDC	***DL04 Protocol***	***Memory-Free DL04***	***QKD***
Communication Distance	**Long-distance (intercontinental)**	Moderate distance	Moderate distance	Short to moderate distance
Security Level	High (no key exchange required)	High (key exchange involved)	High (key exchange involved)	**Very High (key exchange fundamental)**
Implementation Complexity	**Moderate (enhanced by PAT technologies)**	High (requires quantum memory)	**Moderate (no quantum memory required)**	High (requires sophisticated setup)
Suitability for Globalized Blockchain	**Highly suitable**	Moderately suitable	Moderately suitable	Less suitable for global scale
Resistance to Atmospheric Disturbances	**Strong (mitigated by adaptive optics)**	Moderate (susceptible to some atmospheric effects)	Moderate (susceptible to some atmospheric effects)	Weak (highly susceptible to atmospheric effects)

In this paper, we will also explore an integration plan of LF QSDC into software security systems to address both quantum and conventional threats while ensuring its practicality and efficiency. The technical integration of LF QSDC with software requires a novel approach. Software protocols would need to be adapted to accommodate the direct transmission capabilities of LF QSDC. This integration will involve modifying the software's transaction validation mechanisms to include verification processes that are compatible with the quantum-secured data from LF QSDC. Additionally, ensuring that the ledger can record and reconcile quantum-secured communication is crucial. This necessitates not only advancements in quantum communication technologies but also developments in software architecture that can support such integration.

2 LONG-DISTANCE, FREE-SPACE QSDC OVERVIEW

This section introduces Quantum Secure Direct Communication over long distances in free space, an advanced method allowing secure information exchange without the need for intermediate transmission of the encryption key. We explore how cutting-edge technologies can overcome current limitations, making QSDC feasible for practical use across vast distances in the open air and throughout space via satellite communication. The next section will detail these innovations, highlighting their potential to revolutionize software secure communication on a global scale.

Here is a flowchart of LF QSDC:



2.1 State Preparation

The sender, Alice, prepares a sequence of single photons in one of the four time-bin states:

$$|T_0\rangle = |0\rangle, \quad |T_1\rangle = |1\rangle, \quad |T_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |T_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ denote the early and late time bins, respectively [7]. Alice randomly chooses two bits, a_0 and a_1, to encode each photon. The encoding rule is as follows [20]:

$$(a_0, a_1) \rightarrow \begin{cases} |T_0\rangle, & \text{if } (a_0, a_1) = (0, 0), \\ |T_1\rangle, & \text{if } (a_0, a_1) = (0, 1), \\ |T_2\rangle, & \text{if } (a_0, a_1) = (1, 0), \\ |T_3\rangle, & \text{if } (a_0, a_1) = (1, 1). \end{cases} \tag{2}$$

Alice also randomly chooses another bit, a_2, to determine the phase of each photon. The phase modulation rule is as follows [11]:

$$a_2 \rightarrow \begin{cases} \phi = 0, & \text{if } a_2 = 0, \\ \phi = \pi, & \text{if } a_2 = 1. \end{cases} \tag{3}$$

Alice applies a phase modulator (PM) to each photon according to the value of a_2. The PM shifts the phase of the late time bin by ϕ, resulting in the following four phase states [11]:

$$|P_0\rangle = |0\rangle, \quad |P_1\rangle = |1\rangle, \quad |P_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle), \\ |P_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi}|1\rangle). \tag{4}$$

The phase states are related to the time-bin states by the following transformation [13]:

$$|P_i\rangle = \frac{1}{\sqrt{2}}(|T_i\rangle + e^{i\phi}|T_{i\oplus 2}\rangle), \tag{5}$$

where $\oplus$ denotes addition modulo 4. Alice records the values of a_0, a_1, and a_2 for each photon, and sends the photons to the receiver, Bob, through a free-space channel.

2.2 State Transmission

The photons travel through the free-space channel, which introduces various disturbances, such as atmospheric turbulence, beam wandering, scintillation, and background noise. These disturbances affect the coherence and fidelity of the quantum states and may cause errors or losses during transmission. To overcome these challenges, LF QSDC employs an enhanced ML JEEC coding scheme, an integration of PAT Technologies, and an Atmospheric Quantum Correction Algorithm.

In a research paper context, expanding on the techniques for Long-Distance Free-Space Quantum Secure Direct Communication (LF QSDC) with a focus on their synergy and suitability for Web 3.0 and blockchain security:

(1) ML JEEC Coding: ML-JEEC integrates machine learning with JEEC [15] to optimize quantum communication encryption and error correction, enhancing security and reliability in changing channel conditions.
(2) PAT Technologies: These technologies, essential for aligning quantum signals and maintaining a stable communication link, are critical for the continuous operation of decentralized blockchain networks [17].

(3) Atmospheric Quantum Correction Algorithms: Addressing disturbances like turbulence ($\Delta\Phi_{turbulence}$), these algorithms preserve the coherence of quantum states, ensuring the reliability of long-distance transmissions crucial for global blockchain networks [6].

This combination of schemes and algorithms ensures a secure, reliable, and efficient quantum communication system, aligning perfectly with the requirements of blockchain in the Web 3.0 era. We will discuss the design and integration of these methods in detail in the next section.

2.3 State Measurement

Bob receives the photons from Alice and measures them using an interferometer and a single-photon detector (SPD). The interferometer consists of a beam splitter (BS), two PMs, and two mirrors (M). The BS splits each photon into two paths, corresponding to the early and late time bins. The PMs shift the phases of the two paths by θ and $\theta + \pi$, respectively. The mirrors reflect the photons back to the BS, where they recombine and interfere.

The measurement outcome depends on the phase state of the photon and the phase difference θ between the two paths. The probability of detecting a photon at the output port is given by

$$P(\theta) = \frac{1}{2}(1 + \cos(\phi - 2\theta)), \tag{6}$$

where ϕ is the phase of the photon[20]. Bob randomly chooses the value of θ for each photon and records the detection results. Bob then announces the values of θ publicly and discards the results that correspond to $\theta = \frac{\pi}{4}$ or $\theta = \frac{3\pi}{4}$, since these values do not provide any information about the phase of the photon.

2.4 Information Extraction

Alice and Bob extract the information from the transmitted and measured photons, using the following steps:

(1) Alice and Bob perform sifting, where they compare the values of a_2 and θ, and keep only the results that satisfy $a_2 \oplus \theta = 0$ or $a_2 \oplus \theta = 1$. This ensures that Bob's measurement basis is aligned with Alice's encoding basis and that the phase information is preserved [7].
(2) Alice and Bob perform error correction, where they apply the error-correcting codes to correct the bit errors and phase errors in the sifted data. They also perform privacy amplification, where they apply a hash function to reduce the information leakage to Eve [22].
(3) Alice and Bob perform information reconciliation, where they compare the values of a_0 and a_1, and extract the common bits as the final secret message. They also perform authentication, where they verify the integrity of the message using a secret key shared beforehand [23].

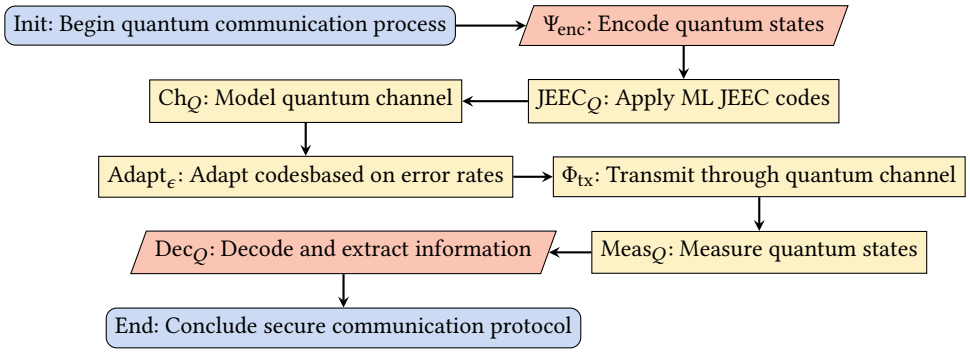
The LF QSDC protocol can achieve secure and direct communication over long distances and free-space channels, without the need for quantum memory or quantum repeaters. The base of LF QSDC, Memrory Free QSDC, has been experimentally demonstrated over a 19-km urban atmospheric channel and has the potential to be extended to satellite-based QSDC in the future [15].

3 PRACTICAL LONG-DISTANCE, FREE-SPACE SECURE TRANSMISSION TECHNIQUES

This section explores groundbreaking methods for transmitting information securely and without loss across vast distances through air or space. It emphasizes technologies that ensure data sent from one point arrives intact and entirely private at another, despite the challenges of physical distance and potential interference. Upcoming discussions will explore innovative solutions that make such futuristic communication feasible and reliable.

3.1 Machine Learning Enhanced JEEC Coding

In this section, we will elaborate on integrating machine learning with traditional joint encryption and error-control coding techniques to form ML-JEEC, focusing on enhancing quantum communication systems. We will describe the application of machine learning algorithms to dynamically adjust encryption and error correction in quantum channels, addressing the challenges posed by eavesdropping and noise. Then we will outline the methodology for implementing ML algorithms to predict channel conditions and optimize communication strategies, thereby ensuring robust and efficient transmission of quantum information.



3.1.1 *Channel and Measurement Model.*

- Quantum Channel Model:
  - Let P_{loss} represent the probability of photon loss in the quantum channel.
  - Dark count probability is denoted as P_{dark}.
  - Quantum Bit Error Rate (QBER) is represented by $QBER$.
  - The quantum channel can be modeled as [6]:

$$C_Q = \alpha \cdot P_{loss} + \beta \cdot P_{dark} + \gamma \cdot QBER \tag{7}$$

    where α, β, γ are weighting factors for each component.
- Quantum Measurement Model:
  - Measurements in quantum communication are subject to basis mismatch and detector inefficiencies.
  - Let $P_{mismatch}$ denote the probability of basis mismatch. The effective measurement model, M_Q, can be expressed as [24]:

$$M_Q = (1 - P_{mismatch}) \cdot \text{Efficiency of the detector} \tag{8}$$

3.1.2 Encryption and Error-Control Coding Strategy. In this subsection, we present our proposed scheme for combining encryption and error-control coding in a single process. The main idea is to use a secret key to generate a random codebook of codewords, each of which is a linear combination of a message and a parity vector. The parity vector is computed using a linear error-correcting code, such as a Reed-Solomon code or a low-density parity-check code. The secret key is also used to select a codeword from the codebook for each message and to encrypt the index of the codeword using a symmetric cipher, such as AES or ChaCha20. The encrypted index and the codeword are then transmitted over the channel. The receiver, who shares the same secret key with the sender, can decrypt the index, retrieve the corresponding codeword from the codebook, and decode the message using the error-correcting code. This scheme provides both data secrecy and data reliability in one step, without requiring any additional overhead or complexity.

Encryption Function. Let M be the set of all possible messages, each of which consists of k bits. Let C be the set of all possible codewords, each of which consists of n bits, where $n > k$. Let K be the set of all possible secret keys, each of which consists of l bits. We define the encryption function as follows:

$$E_k(M) = (C, E_k(i)) \tag{9}$$

where $k \in K$ is the secret key, $M \in M$ is the message, $C \in C$ is the codeword, $i \in \{1, 2, \ldots, |C|\}$ is the index of the codeword in the codebook, and $E_k(i)$ is the encryption of the index using the secret key. The encryption function can be implemented as follows:

(1) Generate a random codebook $B = \{C_1, C_2, \ldots, C_{|C|}\}$ using the secret key k as a seed for a pseudorandom number generator. Each codeword C_i is a linear combination of the message M and a parity vector P_i, which is computed using a linear error-correcting code. That is,

$$C_i = M \oplus P_i \tag{10}$$

where $\oplus$ denotes the bitwise exclusive-or operation.

(2) Select a codeword C from the codebook B using a pseudorandom function $F_k(M)$, which takes the secret key k and the message M as inputs and outputs an index $i \in \{1, 2, \ldots, |C|\}$. That is,

$$C = C_{F_k(M)} \tag{11}$$

(3) Encrypt the index i using the secret key k and a symmetric cipher $E_k(i)$. The cipher can be any secure and efficient algorithm, such as AES or ChaCha20.

(4) Output the pair $(C, E_k(i))$ as the ciphertext.

Error Correction Code. Let C' be the set of all possible received codewords, each of which may contain some errors due to the channel noise. Let M' be the set of all possible decoded messages, each of which may differ from the original message due to the decoding errors. We define the decoding function as follows:

$$D(C') = M' \tag{12}$$

where $C' \in C'$ is the received codeword, and $M' \in M'$ is the decoded message. The decoding function can be implemented as follows:

(1) Decrypt the index i using the secret key k and the inverse cipher $D_k(E_k(i))$. The inverse cipher can be the same algorithm as the encryption cipher but with the opposite operation mode, such as AES-decrypt or ChaCha20-decrypt.

(2) Retrieve the corresponding codeword C from the codebook B using the decrypted index i. That is,

$$C = C_i \tag{13}$$

(3) Decode the message M' from the codeword C using the linear error-correcting code. That is,

$$M' = C \oplus P_i \tag{14}$$

where P_i is the parity vector associated with the codeword C_i.

(4) Output the message M' as the decoded message.

3.1.3 Machine Learning Integration. In this section, we present our proposed scheme for integrating machine learning techniques with the encryption and error-control coding strategy. The main idea is to use a machine learning algorithm to predict the future channel condition based on the current and historical data and to optimize the encryption and coding parameters according to the prediction and the security requirement. This scheme can adapt to the dynamic and uncertain channel environment and achieve a trade-off between data secrecy and data reliability.

Adaptive Learning Algorithm for Channel Prediction. We use a machine learning algorithm to model the channel condition as a stochastic process and to predict the future channel state based on current and historical observations. The predictive model is given by:

$$P_t = ML(C_t, H_t) \tag{15}$$

where P_t is the prediction at time t, C_t is the current channel condition, and H_t is the historical data. The machine learning algorithm can be any supervised or unsupervised learning method, such as neural networks, support vector machines, or hidden Markov models. The prediction can be either deterministic or probabilistic, depending on the algorithm and the data.

Here is a Pseudocode demonstration of our design:

```
# Import required libraries
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.svm import SVC
from sklearn.ensemble import AdaBoostClassifier
from sklearn.metrics import accuracy_score

# Load and prepare the dataset
df = pd.read_csv("channel_data.csv")
X = df.drop(columns='channel') # Using 'drop(columns=...)' for clarity
y = df['channel']

# Split dataset into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Define and configure the machine learning models
svc = SVC(probability=True, kernel='linear')
abc = AdaBoostClassifier(base_estimator=svc, n_estimators=50, learning_rate=1.0)

# Train the AdaBoost model
abc.fit(X_train, y_train)

# Make predictions and evaluate the model
predictions = abc.predict(X_test)
accuracy = accuracy_score(y_test, predictions)

print(f"Accuracy: {accuracy}")
```

Optimization of Encryption and Coding Parameters. We use an optimization function to determine the optimal encryption and coding parameters for each message based on the prediction and the security requirement. The optimization function is given by:

$$O(P_t, S) = (k', r') \tag{16}$$

where O is the optimization function, P_t is the prediction, S is the security requirement, k' is the optimized key, and r' is the optimized coding rate. The optimization function can be any mathematical or heuristic method, such as linear programming, genetic algorithms, or simulated annealing. The security requirement can be any metric or constraint that measures the level of data secrecy, such as the entropy, the mutual information, or the bit error rate. The optimization function aims to maximize the security requirement while minimizing the coding rate, subject to the channel condition and the error-correction capability.

Here is a Pseudocode demonstration of our design:

```
import numpy as np
from scipy.optimize import linprog
```

```
def optimize_channel(P_t, S):
    # Objective: minimize the coding rate
    c = [0, 1] # Only coding rate contributes to the cost

    # Constraints: Security requirement and coding rate feasibility
    A = [[-S, -P_t]]
    b = [-S * P_t]

    # Bounds for the key (k') and coding rate (r')
    bounds = [(0, 255), (0, 1)]

    # Solve the linear programming problem
    result = linprog(c, A_ub=A, b_ub=b, bounds=bounds, method='highs')

    # Extract the optimized key (as integer) and coding rate
    k_prime, r_prime = int(result.x[0]), result.x[1]

    return k_prime, r_prime
```

3.1.4 *Security Enhancement Techniques.*

- Decoy State Method:
  - Employ decoy states with varying intensities to estimate channel parameters.
  - Use statistical methods to analyze the difference in detection rates between signal and decoy states to estimate P_{loss} and detect eavesdropping.
  - The estimation can be formulated as solving a set of linear inequalities derived from decoy state intensities and detection rates [20]. The general form of these linear inequalities can be represented as follows:
    For a set of decoy states with different intensities μ_i (where i indexes the different decoy states), and corresponding detection rates Y_i, the inequalities can be structured to estimate the parameters like photon loss (P_{loss}) and single-photon detection rates Y_1. The estimation typically aims to bind the yield of the single-photon states Y_1 and the quantum bit error rate (QBER) for single-photon states.
    The set of inequalities:
    (1) $Y_1 \geq g(\mu_i, Y_i, \ldots)$ - Lower bound for single-photon yield.
    (2) $Y_1 \leq h(\mu_i, Y_i, \ldots)$ - Upper bound for single-photon yield.
    (3) $QBER_1 \geq f(\mu_i, Y_i, \ldots)$ - Lower bound for single-photon QBER.
    (4) $QBER_1 \leq j(\mu_i, Y_i, \ldots)$ - Upper bound for single-photon QBER.
    Here, g, h, f, and j are functions derived from the intensities of the decoy states and the observed detection rates [20]. These functions are constructed based on the statistical behavior of quantum channels and detectors, taking into account factors like dark counts and basis mismatch.
- Privacy Amplification:
  - After decoding, apply a hash function H to the key to reduce its length and eliminate partial information.
  - The process can be represented as [21-22]:

$$K_{final} = H(K_{decoded}) \tag{17}$$

  - The choice of H and the length of K_{final} are critical and depend on the estimated QBER and eavesdropping probabilities.

3.2 PAT Technologies

The LF QSDC system integrates advanced PAT technologies to enhance the reliability and efficiency of quantum communication over long distances in free space. PAT systems are critical for maintaining the alignment and stability of quantum signals, which are susceptible to atmospheric disturbances and alignment errors.

3.2.1 Design Principles of PAT Systems. The PAT system is designed to automatically adjust the direction and position of quantum signal transmission and reception equipment, ensuring optimal alignment between communicating parties. This is crucial for minimizing signal loss and maintaining high fidelity of the quantum state during transmission.

The PAT system consists of three main components: a pointing device, a tracking device, and a control device. The pointing device is responsible for directing the quantum signal beam toward the intended receiver, using a combination of mechanical and optical elements, such as mirrors, lenses, and motors. The tracking device is responsible for detecting the incoming quantum signal beam from the transmitter, using a photodetector or a camera. The control device is responsible for coordinating the pointing and tracking devices, using feedback loops and algorithms, to achieve the desired alignment and stability.

The PAT system operates in two modes: a coarse mode and a fine mode. The coarse mode is used to establish the initial alignment between the transmitter and receiver, using a wide-angle beam and a low-resolution detector. The fine mode is used to refine the alignment and maintain stability, using a narrow-angle beam and a high-resolution detector.

3.2.2 Mathematical Equations. The performance of the PAT system can be quantified by several metrics, such as alignment error, signal acquisition probability, and pointing stability. These metrics can be formulated by mathematical equations, as follows:

(1) **Alignment Error Correction:**
The alignment error (e_a) is modeled as a function of the angular misalignment (θ_m) and the distance (d) between the transmitter and receiver:

$$e_a = f(\theta_m, d) \tag{18}$$

where $f(\cdot)$ represents the functional relationship, which is determined empirically or through simulation. The alignment error measures the deviation of the quantum signal beam from the ideal optical axis, which can result in signal loss or state degradation. The PAT system aims to minimize the alignment error by adjusting the pointing and tracking devices accordingly. The alignment error correction algorithm (AEC) can be expressed as:

$$AEC = \arg\min_{\theta_p, \theta_t} e_a(\theta_p - \theta_t, d) \tag{19}$$

where θ_p and θ_t are the pointing and tracking angles, respectively. The AEC algorithm finds the optimal pointing and tracking angles that minimize the alignment error, using methods such as gradient descent or Newton's method.

(2) **Signal Acquisition:**
The probability of successful signal acquisition (P_a) depends on the signal-to-noise ratio (SNR) and the alignment precision (σ):

$$P_a = g(SNR, \sigma) \tag{20}$$

with $g(\cdot)$ encapsulating the acquisition algorithm's efficiency under varying SNR conditions and alignment precisions. The signal acquisition probability measures the likelihood of establishing a quantum link between the transmitter and receiver, which can be affected by

noise sources, such as background light, thermal noise, and dark counts. The PAT system aims to maximize the signal acquisition probability by optimizing the SNR and the alignment precision.

The signal acquisition algorithm (SAC) can be expressed as:

$$SAC = \arg \max_{SNR,\sigma} P_a(SNR, \sigma) \tag{21}$$

where SNR and σ are the signal-to-noise ratio and the alignment precision, respectively. The SAC algorithm finds the optimal SNR and alignment precision that maximize the signal acquisition probability, using methods such as thresholding or Bayesian inference.

(3) **Pointing Stability:**

The pointing stability requirement (S_p) to maintain the quantum link can be expressed as:

$$S_p < \frac{\lambda}{D_{eff}} \tag{22}$$

where λ is the wavelength of the quantum signal, and D_{eff} is the effective aperture diameter of the transmitter/receiver system. The pointing stability requirement measures the maximum allowable angular deviation of the quantum signal beam from the optical axis, which external factors, such as wind, vibration, and turbulence can cause. The PAT system aims to satisfy the pointing stability requirement by stabilizing the pointing and tracking devices against these factors.

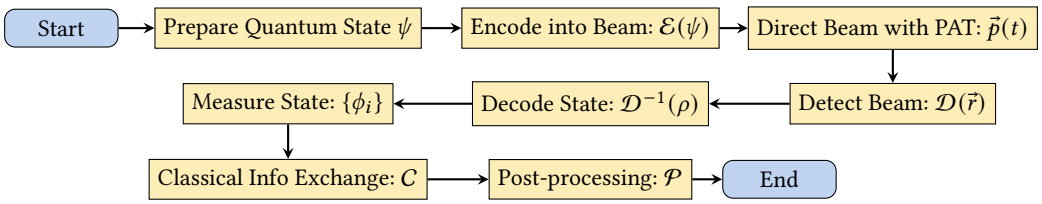
The pointing stability algorithm (PSA) can be expressed as:

$$PSA = \arg \min_{\Delta\theta_p, \Delta\theta_t} S_p(\Delta\theta_p, \Delta\theta_t) \tag{23}$$

where $\Delta\theta_p$ and $\Delta\theta_t$ are the pointing and tracking angular deviations, respectively. The PSA algorithm finds the optimal pointing and tracking angular deviations that minimize the pointing stability requirement, using methods such as PID control or Kalman filter.

3.2.3 Integration with QSDC Protocol. The integration of PAT technologies with the QSDC protocol involves the synchronization of quantum state preparation, signal transmission, and reception processes with the dynamic adjustments made by the PAT system. This ensures that the quantum signals are accurately pointed, acquired, and tracked, thereby reducing transmission errors and enhancing communication security.

The integration process can be summarized by the following steps:



(1) The transmitter prepares the quantum state to be encoded and transmitted, using a quantum source, such as a single-photon source or an entangled photon pair source.
(2) The transmitter encodes the quantum state into the quantum signal beam, using a quantum modulator, such as a phase modulator or a polarization modulator.
(3) The transmitter directs the quantum signal beam toward the receiver, using the pointing device of the PAT system.
(4) The receiver detects the incoming quantum signal beam, using the tracking device of the PAT system.

(5) The receiver decodes the quantum state from the quantum signal beam, using a quantum demodulator, such as a phase demodulator or a polarization demodulator.
(6) The receiver measures the quantum state, using a quantum detector, such as a single-photon detector or a coincidence detector.
(7) The transmitter and receiver exchange classical information, such as basis choices, error correction codes, and privacy amplification keys, using a classical channel, such as a radio or optical link.
(8) The transmitter and receiver perform post-processing steps, such as error correction, privacy amplification, and authentication, to ensure the security and reliability of the quantum communication.

3.3 Atmospheric Quantum Correction Algorithm

3.3.1 Introduction. The LF QSDC system is designed to enable secure quantum communication over long distances in free space. A critical component enhancing this capability is the Atmospheric Quantum Correction Algorithm (AQCA), which mitigates the adverse effects of atmospheric conditions on quantum signal fidelity.

3.3.2 Design and Implementation. The AQCA is integrated within the LF QSDC framework to address challenges such as atmospheric turbulence, absorption, and scattering. These phenomena can degrade the quantum state of photons, leading to increased quantum bit error rates (QBER) and reduced communication security and reliability.

The AQCA consists of four main modules: a disturbance modeler, a quantum error corrector, an adaptive optics system, and a signal enhancer and recoverer. The disturbance modeler is responsible for estimating the atmospheric parameters and their impact on the quantum signal. The quantum error corrector is responsible for applying QEC techniques to the quantum signal. The adaptive optics system is responsible for adjusting the quantum signal's path in real time. The signal enhancer and recoverer are responsible for processing the quantum signal to improve the SNR and recover the original quantum state.

3.3.3 Mathematical Formulation. The AQCA leverages advanced mathematical models and algorithms to correct for atmospheric distortions. Key components of the algorithm include:

(1) **Modeling Atmospheric Disturbances:**
Disturbances are modeled using statistical methods that account for the variability in atmospheric conditions. This involves quantifying the impact of turbulence, absorption, and scattering on photon states.
The atmospheric turbulence is modeled by the Kolmogorov theory, which assumes that the refractive index fluctuations follow a power-law spectrum. The strength of the turbulence is characterized by the Fried parameter (r_0), which represents the coherence length of the wavefront. The effect of the turbulence on the quantum signal is quantified by the scintillation index (σ_I^2), which measures the intensity fluctuations of the signal. The scintillation index can be approximated by the Rytov approximation, which is valid for weak to moderate turbulence regimes. The Rytov approximation is given by:

$$\sigma_I^2 \approx 1.23 C_n^2 k^{7/6} L^{11/6} \tag{24}$$

where C_n^2 is the refractive index structure constant, k is the wave number, and L is the propagation distance.
The atmospheric absorption is modeled by the Beer-Lambert law, which assumes that the intensity of the quantum signal decreases exponentially with the propagation distance. The

effect of the absorption on the quantum signal is quantified by the transmittance (T), which measures the fraction of the signal that reaches the receiver. The transmittance is given by:

$$T = e^{-\alpha L} \tag{25}$$

where α is the absorption coefficient, which depends on the wavelength and the atmospheric composition.

The atmospheric scattering is modeled by the Mie theory, which assumes that the quantum signal is scattered by spherical particles that are comparable in size to the wavelength. The effect of the scattering on the quantum signal is quantified by the scattering cross section (σ_s), which measures the probability of the signal being scattered by a particle. The scattering cross section is given by:

$$\sigma_s = \frac{2\pi^5 d^6}{3\lambda^4} \left(\frac{n^2 - 1}{n^2 + 2} \right)^2 Q_{ext} \tag{26}$$

where d is the particle diameter, λ is the wavelength, n is the refractive index of the particle, and Q_{ext} is the extinction efficiency factor, which depends on the size parameter and the refractive index ratio of the particle and the medium.

(2) **Quantum Error Correction (QEC):**

The AQCA employs QEC techniques tailored to atmospheric conditions. These techniques are designed to identify and correct errors induced by the atmosphere, enhancing the resilience of quantum communication.

The QEC techniques are based on the use of quantum codes, which are mathematical structures that encode quantum information into larger quantum systems, such as qubits or qumodes. Quantum codes can protect quantum information from errors by exploiting the properties of quantum entanglement and superposition. Quantum codes can be classified into two types: discrete-variable (DV) codes and continuous-variable (CV) codes. DV codes use discrete quantum systems, such as qubits, to encode quantum information. CV codes use continuous quantum systems, such as qumodes, to encode quantum information.

The AQCA selects the appropriate type of quantum code based on the quantum signal's modulation scheme. For phase-modulated signals, such as coherent states or squeezed states, the AQCA uses CV codes, such as Gaussian codes or non-Gaussian codes. For polarization-modulated signals, such as single photons or entangled photons, the AQCA uses DV codes, such as stabilizer codes or non-stabilizer codes.

The QEC process consists of three steps: encoding, syndrome measurement, and decoding. Encoding is the process of applying a quantum code to the quantum signal before transmission. Syndrome measurement is the process of measuring the quantum signal after transmission to detect errors. Decoding is the process of applying a quantum code to the quantum signal after syndrome measurement to correct the errors.

(3) **Adaptive Optics System:**

An adaptive optics system is integrated to dynamically adjust the quantum signal's path in real time, countering the effects of atmospheric turbulence. The system uses feedback from the quantum signal itself to optimize the transmission path.

The adaptive optics system consists of three main components: a *wavefront sensor*, a *deformable mirror*, and a *control unit*. The wavefront sensor is responsible for measuring the phase distortions of the quantum signal caused by the turbulence. The deformable mirror is responsible for compensating the phase distortions by applying a conjugate phase profile to the quantum signal. The control unit is responsible for coordinating the wavefront sensor

and the deformable mirror, using feedback loops and algorithms, to achieve the optimal wavefront correction.

The adaptive optics system operates in two modes: a *closed-loop mode* and an *open-loop mode*. The closed-loop mode is used when the quantum signal is strong enough to provide sufficient feedback for the wavefront sensor. The open-loop mode is used when the quantum signal is too weak to provide sufficient feedback for the wavefront sensor. In this case, the system uses a reference beam, such as a laser beam, to provide the feedback for the wavefront sensor, and applies the same correction to the quantum signal.

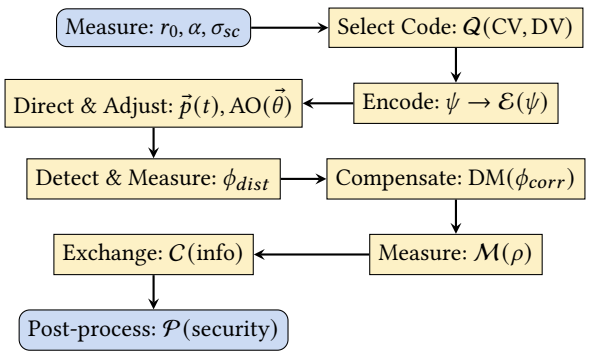
(4) **Signal Enhancement and Recovery:**
Signal processing algorithms are applied to enhance the signal-to-noise ratio (SNR) and recover the original quantum state. This involves sophisticated filtering and estimation techniques that leverage the known properties of quantum signals.

The signal enhancement algorithms are based on the use of filters, such as Kalman filters or Wiener filters, which are designed to reduce the noise and interference in the quantum signal. The optimal filters use a mathematical model of the quantum signal and the noise to compute the optimal estimate of the quantum state. The optimal filters can also incorporate the information from the syndrome measurement and the QEC to improve the estimation accuracy.

The signal recovery algorithms are based on the use of maximum likelihood estimation (MLE) or Bayesian inference, which are designed to infer the most probable quantum state from the quantum signal. The MLE or Bayesian inference use a probability distribution of the quantum state and the quantum signal to compute the most likely quantum state. The MLE or Bayesian inference can also incorporate the information from the QEC to improve the inference accuracy.

3.3.4 Integration with LF QSDC Protocol. The AQCA is seamlessly integrated with the LF QSDC protocol, ensuring that atmospheric corrections are applied efficiently during the transmission phase. This integration involves real-time monitoring of atmospheric conditions and dynamic adjustment of the quantum signal to maintain high fidelity and security.

The integration process can be summarized by the following steps:



(1) The transmitter and the receiver measure the atmospheric parameters, such as the Fried parameter, the absorption coefficient, and the scattering cross section, using the disturbance modeler module of the AQCA.

(2) The transmitter and the receiver select the appropriate quantum code, such as a CV code or a DV code, based on the quantum signal's modulation scheme and the atmospheric parameters, using the quantum error corrector module of the AQCA.

(3) The transmitter encodes the quantum state into the quantum signal, using a quantum source and a quantum modulator, and applies the quantum code to the quantum signal, using the encoding step of the QEC process.
(4) The transmitter directs the quantum signal toward the receiver, using the pointing device of the PAT system, and adjusts the quantum signal's path in real-time, using the adaptive optics system module of the AQCA.
(5) The receiver detects the incoming quantum signal, using the tracking device of the PAT system, and measures the quantum signal's phase distortions, using the wavefront sensor of the adaptive optics system.
(6) The receiver compensates the quantum signal's phase distortions, using the deformable mirror of the adaptive optics system, and enhances the quantum signal's SNR, using the signal enhancer and recoverer module of the AQCA.
(7) The receiver measures the quantum signal, using a quantum detector, and applies the quantum code to the quantum signal, using the syndrome measurement and decoding steps of the QEC process, to recover the original quantum state.
(8) The transmitter and the receiver exchange classical information, such as basis choices, error correction codes, and privacy amplification keys, using a classical channel, such as a radio or optical link.
(9) The transmitter and the receiver perform post-processing steps, such as error correction, privacy amplification, and authentication, to ensure the security and reliability of the quantum communication.

4 LF QSDC SIMULATION PLAN AND ANALYSIS

In the forthcoming research phase, our primary objective is to meticulously simulate and evaluate the performance of our ML JEEC codes, PAT Technologies, and Atmospheric Quantum Correction Algorithm. Given our current constraints, which include the absence of experimental quantum communication hardware, our focus will be exclusively on theoretical models and software simulations. This approach enables us to predict and optimize the protocol's performance under various conditions, laying the groundwork for future experimental validation once the necessary equipment becomes accessible.

4.1 Simulation Plan

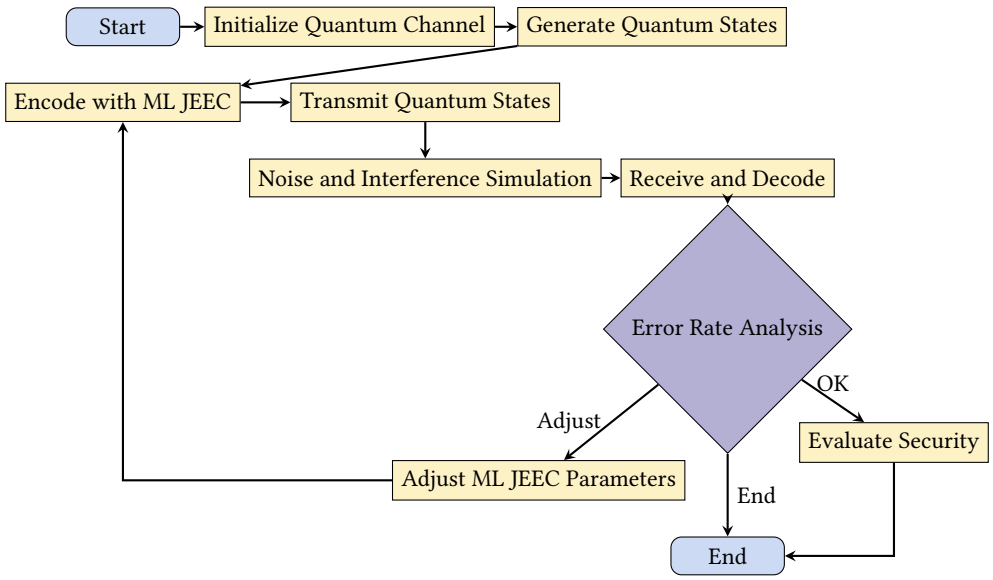
The testing framework for the LF QSDC system meticulously evaluates its operational efficacy, commencing with the initialization of the quantum channel ($\mathcal{Q}_C$), a conduit essential for the transmission of entangled photons (Ψ_{ent}). This phase sets the groundwork for secure quantum communication by establishing a pathway for encoded quantum states (Ψ_{enc}) utilizing ML JEEC coding ($C_{\text{ML JEEC}}$). Such encoding is pivotal, aiming to bolster error correction capabilities without undermining the quantum states' coherence and security.

The protocol then progresses to the transmission phase (Φ_{transmit}), where encoded quantum states are dispatched through the free-space medium, encountering environmental noise ($\mathcal{N}$), simulating real-world atmospheric conditions. The subsequent reception and decoding phase is critical, employing $C_{\text{ML JEEC}}$ to ameliorate errors introduced during transmission, highlighted by the quantum channel's intrinsic error characteristics ($\epsilon_{\text{quantum}}$). An in-depth error rate analysis (η_{error}) ensues, assessing the integrity of the received quantum information against the original transmission. This analysis is instrumental in driving the iterative optimization of ML JEEC parameters (Θ_{opt}), with the goal of minimizing error rates and maximizing system fidelity (F_{system}).

Concluding the protocol, a rigorous security evaluation (Σ_{security}) is conducted to ensure the system's robustness against potential eavesdropping attempts, affirming the LF QSDC system's

capacity to maintain the confidentiality and integrity of the transmitted information. This comprehensive assessment confirms the system's technical viability and underscores its practical applicability in secure quantum communication networks, marking a significant leap forward in the domain of quantum communication technologies.

Here is a summary flowchart for the simulation plan:

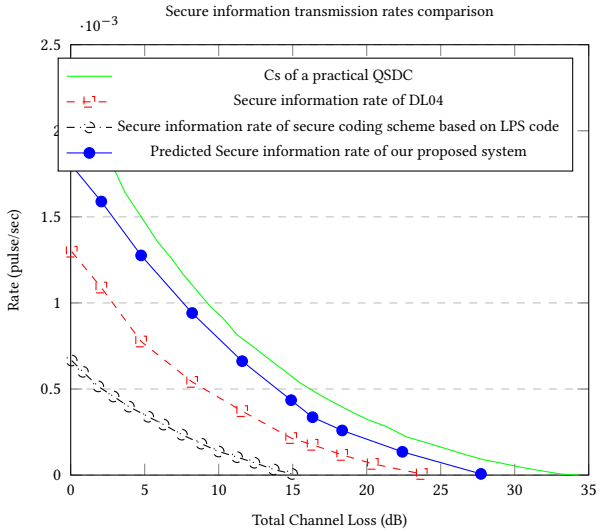


4.2 Predicted Results and Analysis

In this subsection, we intend to evaluate the theoretical performance of our proposed lossless free space, and long-distance transmission techniques which consist of ML JEEC, PAT Technologies, and Atmospheric Quantum Correction Algorithm. By drawing comparisons with existing JEEC codes and other ML JEEC variants, we aim to demonstrate superior reliability and secure information rates offered by our framework.

Due to constraints on accessing advanced quantum testing equipment and limitations in funding, our results are derived from a comprehensive suite of computer simulations. These simulations incorporate stochastic models of quantum channels and sophisticated error patterns, which are emblematic of practical quantum communication environments. They allow us to extrapolate the performance of our system and estimate their operational capabilities, providing a theoretical yet convincing argument for their potential efficacy in real-world applications.

The following graph shows the predicted secure information transmission rates of the proposed transmission scheme, the secure coding based on DL04 Coding [15], the secure coding based on LPS codes, and Cs for a practical QSDC system, without the consideration of the loss caused by the delayed fiber [26].

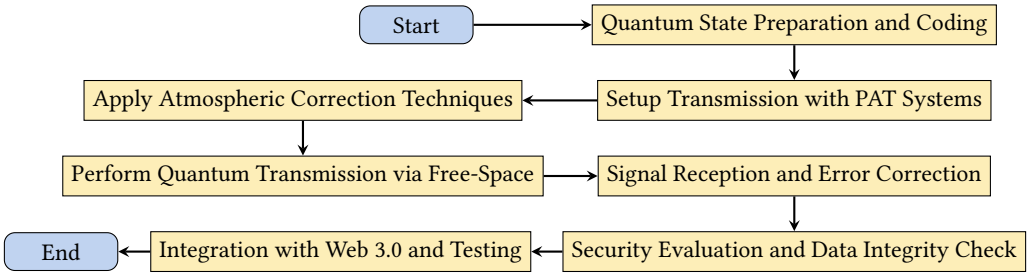


These predictions show that our system will enhance the practical threshold for QSDC systems by demonstrating its potential to sustain higher secure information rates even in conditions of significant channel loss. However, the current iteration of our system is still unable to achieve practical long-distance QSDC communications.

Nevertheless, our future iterations and enhancements to our system coding will focus on further optimizing the error correction capabilities and adapting to the specific challenges of quantum channels, such as quantum noise and decoherence. These improvements will bring our system to meet the stringent requirements of practical QSDC.

5 IMPLEMENTATION PLAN FOR LF QSDC

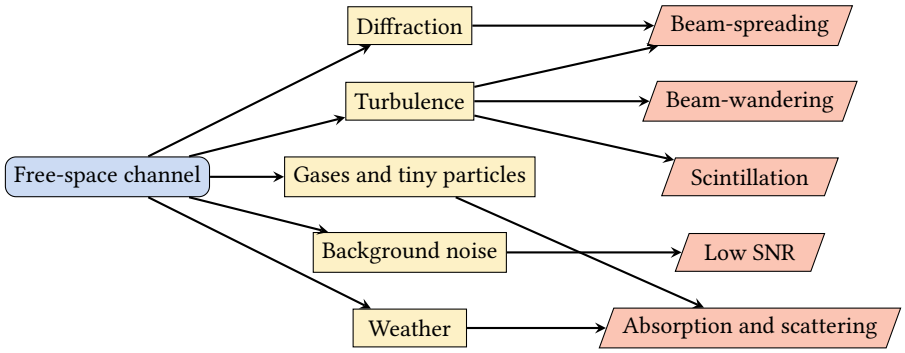
This section outlines a comprehensive approach to integrating LF QSDC into various practical frameworks, highlighting its versatility and potential across different domains, here is an overview of our plan:



5.1 Technical Implementation of LF QSDC

5.1.1 One-Way Transmission Protocols in Free-Space Channel. For free-space communication, protocols designed for one-way transmission, such as the RECON and QKPC protocols, may present advantages over bidirectional methods due to the complexity of the free-space environment affecting signal conveyance over long distances [25]. The transmission of information through a free-space channel encounters numerous challenges including beam divergence, atmospheric disturbances, absorption, scattering, interference from natural light, geometric diminution, and

climatic impacts, which all could impede communication [26,27,28]. The diagram below encapsulates these primary factors of the free-space channel and their influence on the propagation of optical signals [26].



Therefore, employing one-way transmission protocols like RECON or QKPC could prove to be more advantageous than the bidirectional techniques utilized in quantum secure direct communication (QSDC) due to the intrinsic properties of the free-space channel [29]. The advantage of one-way transmission lies in its straightforwardness, eliminating the need for signals to be sent back to the originator for further processing, thereby minimizing the distance quantum states must travel [30]. Such one-directional protocols can be specifically designed to be more resilient against natural light and atmospheric interferences, thus reducing susceptibility to ambient noise and improving the precision of channel estimation [31]. Streamlining the communication process can additionally enhance security by reducing the required level of interaction between the communicating parties [29].

5.1.2 Experimental Implementation. In 2020, a successful experimental demonstration was conducted for the DL04 quantum secure direct communication (QSDC) protocol in a free-space environment. The experiment achieved a notable data transmission speed of 500 bits per second over a 10-meter distance, with an impressively low Quantum Bit Error Rate (QBER) of $0.49\% \pm 0.27\%$, as depicted in Figure 1 [32].

The achievement of such a low QBER is critical for assessing the reliability and robustness of QSDC systems in free-space communication, suggesting the protocol's effectiveness in accurately transmitting quantum information—a key factor for secure communications [33,34]. This low error rate underscores the protocol's potential to mitigate errors from environmental factors or unauthorized interception, thereby ensuring data integrity [35].

The reported data rate of 500 bits per second over a 10-meter distance highlights the protocol's efficiency in transmitting data under the tested conditions. Although the test covered a relatively short distance, it signifies the potential for scaling up the technology to cover longer distances, paving the way for future enhancements and optimizations in the field [32].

The experimental setup utilized a phase-encoding scheme to manage quantum states through a vacuum, as shown in Figure 2 [32]. In this setup, Bob modifies the phase of each pulse through a longer optical path with one of four phase values 0, $\pi/2$, π, $3\pi/2$, creating distinct phase-encoded quantum states. Alice, on her part, uses two optical paths—one for security verification and the other for data encoding. She employs phase modulation to detect eavesdropping and to encode binary information, demonstrating a sophisticated method for secure quantum communication [32].

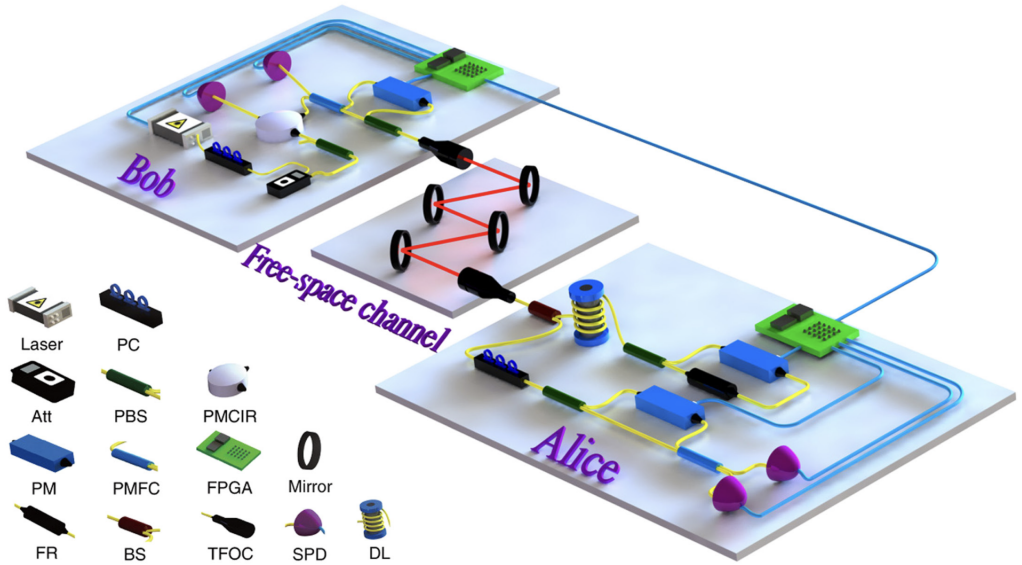


Fig. 1. The main characteristics of the free-space channel and their impacts on optical signal transmission

This phase-encoding technique illustrates the practical application of advanced quantum communication strategies in open-air conditions and highlights the protocol's capacity for effective data processing and scalability for long-distance communication [32].

Furthermore, the experiment incorporated mechanisms for eavesdropping detection, emphasizing the protocol's effectiveness in ensuring the confidentiality and integrity of communications. This capability is especially critical for QSDC protocols, where protecting against unauthorized interception is paramount [32].

Despite the limited 10-meter range of this experiment, its successful execution reinforces the feasibility of extending such technologies to greater distances. Technological advancements, such as more sensitive detectors, adaptive optics, and improved error correction strategies, could address long-range communication challenges, including signal loss, beam spreading, and atmospheric disturbances.

The experimental outcomes affirm the viability of QSDC for accurate and secure quantum data transmission via free-space channels. The progress in reducing QBER, increasing transmission speeds, implementing sophisticated encoding methods, and enhancing security measures lays a solid foundation for future research and development in practical, long-range quantum communication systems.

5.2 Feasibility and Adaptability of Satellite-based QSDC

5.2.1 Feasibility of Satellite Communication with LF QSDC. Previous research into the transmission of quantum states from satellites to Earth has shown promising results, with Quantum Bit Error Rates (QBERs) staying within acceptable margins for secure quantum communications [36,37,38]. The successful transmission of quantum information over distances ranging from 2,200 km to beyond 36,000 km, with link losses between 100 and 110 dB, confirms the feasibility of quantum communications over the vast distances required for satellite-based networks [38,39]. Integrating FL QSDC approach into satellite communications could further improve this capability, providing a

simpler and more secure method of communication that avoids the vulnerabilities associated with traditional key exchange methods [35].

The memory-less DL04 protocol is pivotal in LF QSDC for streamlining the storage and management of quantum states, particularly suitable for satellite communication due to its adaptability in free-space conditions. This adaptability makes it an excellent candidate for overcoming the challenges associated with transmitting quantum signals through Earth's atmosphere. However, achieving high interference visibility, as seen in related experiments, remains crucial. Improving the visibility in DL04 QSDC emphasizes the necessity for advancements in the protocol or its supporting technologies to mitigate QBERs influenced by atmospheric conditions and other noise sources [40].

Incorporating ML JEEC coding into LF QSDC significantly boosts the system's ability to correct errors, addressing the challenges posed by long-distance transmission and atmospheric factors [40,41]. ML JEEC coding thus improves the feasibility of satellite-based LF QSDC by enhancing error correction capabilities, ensuring the integrity and security of transmitted data.

PAT technologies play an essential role in maintaining a stable and accurate communication link between satellites and ground stations [42]. These technologies compensate for satellite movement and atmospheric variations, reducing signal loss and increasing the viability of LF QSDC for satellite communications.

5.2.2 Expanding Feasibility with LF QSDC. Improving the practicality of lightweight and flexible quantum secure direct communication (LF QSDC) involves a series of strategic developments, such as enhancing beam transmission methods, strengthening phase and polarization encoding techniques, incorporating quantum repeaters and relay satellites, improving operation in daylight conditions, integrating with current satellite infrastructures, fostering standardization and interoperability, and formulating appropriate regulatory and policy measures.

Adjustments in adaptive optics and beam focusing are pivotal for increasing the accuracy and efficiency of quantum signal exchanges between satellites and ground stations. These advancements help counteract atmospheric interferences, reducing beam dispersion and drift, which is vital for maintaining high communication precision over long distances.

Developing more robust encoding methods for phase and polarization that withstand atmospheric and environmental disruptions is essential. These methods are crucial for ensuring the reliable transmission of quantum states through the Earth's atmosphere, maintaining low quantum bit error rates (QBER) in satellite-based QSDC systems.

The deployment of quantum repeaters and relay satellites could extend the reach of QSDC systems, enabling a global quantum communication network. Quantum repeaters facilitate the entanglement of quantum states across multiple nodes, overcoming the distance limitations of direct quantum communications.

For QSDC systems to be effective in daylight, addressing the challenge of solar radiation is necessary. This may involve the development of more sensitive detectors and the use of narrowband filters to improve the signal-to-noise ratio.

Integrating LF QSDC with existing satellite communication frameworks necessitates compatibility in terms of payload, energy requirements, and the potential for upgrading current satellites with quantum communication capabilities.

Establishing standardized protocols and ensuring interoperability among different quantum communication systems are essential for creating a cohesive and scalable global quantum communication network. This includes standardizing encoding methods, error-correction techniques, and security protocols.

Furthermore, developing specific regulatory and policy frameworks to govern the use and security of satellite-based quantum communications is crucial to address legal, privacy, and security concerns. By focusing on these areas for improvement and adaptation, the viability and effectiveness of satellite-based LF QSDC can be significantly advanced, setting the stage for a secure and efficient worldwide quantum communication network.

6 CONCLUSION

In this research, we delve into the integration of Long-Distance Free-Space Quantum Secure Direct Communication with secure software communication frameworks, proposing a theoretical framework aimed at enhancing the security attributes of software systems in the quantum computing epoch. This manuscript delineates the capability of LF QSDC to reinforce software infrastructures against a broad array of cryptographic challenges, encompassing both quantum and classical threats, through the employment of direct quantum communication mechanisms that bypass traditional key exchange methodologies. Furthermore, LF QSDC is elucidated as a significant advancement over existing QSDC methodologies, given its proficiency in facilitating lossless communication across free space and extended distances via satellite technology.

The conceptual foundation of LF QSDC is anchored in the memory-free DL04 protocol, operationalized through the synergistic integration of machine learning-optimized JEEC codes, state-of-the-art pointing, acquisition, and tracking (PAT) technologies, in conjunction with algorithms for atmospheric quantum correction. These components are crucial for overcoming the environmental and technical barriers currently limiting the effective deployment of quantum communication technologies, especially in the realm of long-distance free-space transmissions. Additionally, this work proposes a comprehensive strategic framework that includes the evolution of quantum communication technologies, their integration with current software infrastructures, and the resolution of both environmental and technical challenges to establish a secure and efficient conduit for data exchange. Our approach underscores the importance of collaborative efforts among quantum researchers and technological innovators to refine and ensure the interoperability of LF QSDC protocols with existing software standards, thereby fostering a robust, quantum-secure network environment capable of confronting the diverse cybersecurity threats of today and tomorrow.

It is imperative to recognize that the discourse presented herein is predominantly theoretical. The practical implementation of LF QSDC within software systems presents significant engineering challenges and necessitates considerable advancements in quantum communication technologies. Prospective research avenues may encompass the development of more sophisticated quantum error correction methods to improve the fidelity of quantum information transfer. Investigating innovative PAT systems for enhanced stability and precision in quantum signal alignment could markedly augment the practicality of LF QSDC. Moreover, a critical exploration into scalable quantum network architectures that can be seamlessly integrated with conventional software infrastructures, ensuring that enhancements in quantum security do not detrimentally affect the network's functionality or accessibility, represents another vital direction for future research.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annu. Symp. Foundations of Computer Science. IEEE, 1994, pp. 124–134.

[2] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett., vol. 79, no. 2, pp. 325–328, 1997.

[3] I. B. Djordjevic, O. Milenkovic, and B. Vasic, "Generalized low-density parity-check codes for optical communication systems," J. Lightw. Technol., vol. 23, no. 5, pp. 1939–1946, 2005.

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, 2007.

[5] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," J.Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptogra- phy," Rev. Mod. Phys., vol. 74, no. 1, p. 145, 2002.
[7] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in IEEE Int. Conf. Computers, Systems, Signal Processing., 1984.
[8] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. Long, "Implementation and security analysis of practical quantum secure direct communication," Light Sci. Appl., vol. 8, no. 1, p. 22, 2019.
[9] C. Wang, F. Deng, Y. Li, X. Liu, and G. L. Long, "Quantum secure di- rect communication with high-dimension quantum superdense coding," Phys.Rev. A, vol. 71, no. 4, p. 044305, 2005.
[10] L. Yin, C. Jiang, C. Jiang, N. Ge, L. Kuang, and M. Guizani, "A communication framework with unified efficiency and secrecy," IEEE Wirel. Commun., vol. 26, no. 4, pp. 133–139, 2019.
[11] F. Deng and G. Long, "Secure direct communication with a quantum one-time pad," Phys.Rev. A, vol. 69, no. 5, p. 052319, 2004.
[12] F. Deng, G. Long, and X. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," Phys.Rev. A, vol. 68, no. 4, p. 042317, 2003.
[13] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device– independent quantum secure direct communication," EPL (Eurpphys Lett.), vol. 125, no. 4, p. 40004, 2019.
[14] W. Zhang, D. Ding, Y. Sheng, L. Zhou, B. Shi, and G. Guo, "Quantum secure direct communication with quantum memory," Phys. Rev. Lett., vol. 118, no. 22, p. 220501, 2017.
[15] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, L. Hanzo. "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," IEEE Transactions on Communications, 68(9), 5778-5792, 2020.
[16] I. B. Djordjevic, O. Milenkovic, and B. Vasic, "Generalized low-density parity-check codes for optical communication systems," J. Lightw. Technol., vol. 23, no. 5, pp. 1939–1946, 2005.
[17] M. Bailly, E. Perez. "Pointing, acquisition, and tracking system of the European SILEX program: a major technological step for intersatellite optical communication," Free-Space Laser Communication Technologies III, Vol. 1417, pp. 142-157, 1991.
[18] G. Yue, L. Ping, and X. Wang, "Generalized low-density parity-check codes based on Hadamard constraints," IEEE Trans. Inf. Theory, vol. 53, no. 3, pp. 1058–1079, 2007.
[19] Z. Sun, R. Qi, Z. Lin, L. Yin, G. Long, and J. Lu, "Design and implementation of a practical quantum secure direct communication system," in Proc. IEEE GlobeCom Conf. Wkshps. IEEE, 2018, pp. 1–6.
[20] C. Wang, F. Deng, G., and G. L. Long. "Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state," Optics Communications, 253(1-3), 15–20, 2005.
[21] P. Maunz, D. Moehring, S. Olmschenk, et al. "Quantum interference of photon pairs from two remote trapped atomic ions," Nature Phys 3, 538–541, 2007.
[22] C. Bennett, H., G. Brassard, C. Crépeau, and U. M. Maurer. "Generalized privacy amplification," IEEE Transactions on Information Theory, 41(6), 1915-1923, 1995.
[23] J. Carter, L., and M. N. Wegman. "Universal classes of hash functions," Journal of Computer and System Sciences, 18(2), 143-154, 1979.
[24] J. Hu, B. Yu, M. Jing, L. Xiao, S. Jia, G. Qin, and G. L. Long. "Experimental quantum secure direct communication with single photons," Light: Science and Applications, 5(9), e16144, 2016.
[25] S. Zafar and H. Khalid, "Free space optical networks: applications, challenges and research directions," Wireless Personal Communications, vol. 121, no. 1, pp. 429-457, 2021.
[26] H. Kaushal, V. K. Jain and S. Kar, "Free-space optical channel models," in Free Space Optical Communication, New Delhi, India: Springer, 2017, pp. 9-41.
[27] A. M. Al-Kinani, A. A. Al-Habash, A. A. Al-Habash and A. A. Al-Habash, "A survey of hybrid free space optics communication networks to overcome atmospheric turbulence," Entropy, vol. 24, no. 11, p. 1573, 2022.
[28] A. Avella et al., "Characterization of free-space quantum channels," arXiv preprint arXiv:1810.05700, 2018.
[29] T. Ye, and Z. Ji, "Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states", arXiv preprint arXiv:2205.04631, 2021.
[30] M.Xiao, and C. Ma, "Fault-tolerant quantum private comparison protocol", International Journal of Theoretical Physics, vol. 61, no. 1, p. 41, 2022.
[31] J. Liu, Q. Wang, Y. Yang, and Q. Wen, "Quantum private comparison protocol based on high-dimensional quantum states", Quantum Information Processing, vol. 13, no. 11, pp. 2391-2404, 2014.
[32] D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Lin, G. Long, "Experimental free-space quantum secure direct communication and its security analysis," Photonics Res, 8(9), 1522–1531, 2020.
[33] R. Qi, Y. Zhang, S. Wang, H. Li, Z. Wang, S. Wang, X. Chen, and J.-W. Pan, "Experimental demonstration of free-space quantum secure direct communication with single photons", Light: Science and Applications, vol. 9, no. 1, p. 28, 2020.

[34] G. Vallone, D. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels", arXiv preprint arXiv:1404.1272, 2014.
[35] R. Qi et al., "Implementing a practical quantum secure direct communication system," Light: Science and Applications, vol. 8, no. 1, p. 21, 2019.
[36] J.-G. Ren et al., "Ground-to-satellite quantum teleportation," Nature, vol. 549, no. 7670, pp. 70-73, 2017.
[37] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, no. 7670, pp. 43-47, 2017.
[38] A. V. Khmelev et al., "Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers," Entropy, vol. 25, no. 4, p. 670, 2023.
[39] P. Panteleev and G. Kalachev, "Degenerate Quantum LDPC Codes With Good Finite Length Performance," Quantum, vol. 5, p. 585, 2021.
[40] P. Panteleev and G. Kalachev, "Layered Decoding of Quantum LDPC Codes," IEEE Transactions on Information Theory, vol. 66, no. 8, pp. 5198-5209, 2020.
[41] J. Roffe, "Towards practical quantum LDPC codes," Quantum Views, vol. 5, p. 63, 2021.
[42] M. T. Toledo, "Process Analytical Technology (PAT) - Enhance Quality and Efficiency," 2021. [Online].