

A Hybrid Quantum Key Distribution Algorithm Integrating BB84 and Twin-Field QKD for Enhanced Security and Efficiency

YAHIA JAZYAH
Faculty of Computer Studies,
Arab Open University,
KUWAIT

Abstract: - Quantum Key Distribution (QKD) represents a revolutionary advancement in secure communication. It leverages principles of quantum mechanics to establish cryptographic keys between parties with theoretically unbreakable security. Among the various QKD protocols, BB84 (Bennett and Brassard, 1984) and Twin-Field QKD are prominent due to their foundational simplicity and advanced key generation efficiency, respectively. The BB84 protocol, as the first QKD protocol, uses quantum bits (qubits) in different bases to securely generate shared keys, while Twin-Field QKD enhances the key generation rate by exploiting quantum interference between distant entangled states, making it more suitable for long-distance communication. This work explores the integration of BB84 and Twin-Field QKD into a hybrid algorithm, aiming at combining the robustness of BB84 with the high key generation rate and entropy of Twin-Field QKD. The hybrid algorithm alternates between the two protocols, leveraging their individual strengths to optimize key generation performance. Simulation results indicate that the hybrid algorithm can effectively balance the robustness and simplicity of BB84 with the high efficiency and entropy of Twin-Field QKD. Specifically, the hybrid algorithm demonstrated an error rate of 8.9%, a key generation rate of 50%, and an entropy of 0.999 bits, which outperforms the compared algorithms.

Key-Words: - BB84, Qubit, Twin-Field, Key Distribution, QKD, Quantum.

Received: April 16, 2026. Revised: June 2, 2026. Accepted: July 8, 2026. Published: September 24, 2026.

1 Introduction

Quantum Key Distribution (QKD) stands at the forefront of modern cryptography, offering a path towards secure communication that is impervious to the threats posed by quantum computers. Among the QKD protocols, two prominent approaches, BB84 and Twin-Field QKD, have emerged as the most important part of quantum secure communication. Additionally, the fusion of these protocols into a hybrid algorithm holds the promise of advancing state-of-the-art in quantum key generation, [1], [2].

The BB84 protocol, conceived by Bennett and Brassard in 1984, revolutionized cryptography by utilizing the principles of quantum mechanics. At its core, BB84 leverages the inherent randomness and uncertainty of quantum states to assist secure key exchange between two parties. By encoding information into qubits and exchanging them over

a quantum channel, the two parties can establish a shared secret key while detecting any potential eavesdropping attempts.

In parallel, Twin-Field QKD has emerged as a cutting-edge approach to quantum key generation, offering enhanced security and efficiency compared to traditional protocols. Introduced by Boström and Felbinger in 2002, Twin-Field QKD exploits interference of weak coherent states between two parties at a central, possibly untrusted, node.

While BB84 and Twin-Field QKD represent distinct approaches to quantum key distribution, the hybridization of these protocols holds great promise for advancing the capabilities of quantum cryptography. By merging elements from both BB84 and Twin-Field QKD, a hybrid algorithm can leverage their respective strengths to enhance

security, efficiency, and resilience in key generation.

BB84 has proven its robustness in theoretical and practical settings, its key generation rate decreases exponentially with distance, posing limitations for long-range quantum communication. To overcome this, Twin-Field QKD was proposed, utilizing single-photon interference and phase-matching techniques to enable linear scaling of key rates with distance, achieving secure transmission over distances exceeding 500 km without the need for quantum repeaters.

In pursuit of combining the advantages of multiple QKD strategies, hybrid QKD algorithms have emerged. These approaches integrate features from protocols like BB84 and Twin-Field QKD, aiming to balance efficiency, error tolerance, and entropy performance. Hybrid models are particularly promising for next-generation quantum networks, offering flexible deployment and improved resilience to noise.

This study compares BB84, Twin-Field QKD, and a hybrid QKD protocol in terms of error rate, key generation rate, and entropy through a simulation-based approach, providing insights into their practical performance and applicability in real-world quantum-secure communications.

The hybrid algorithm aims at achieving a balance between the robust security of BB84 and the high key generation rate and entropy of Twin-Field QKD. The goal is to enhance the overall performance of QKD systems, making them more suitable for practical and secure long-distance communication.

2 Literature Review

Practical implementations of QKD often rely on weak coherent pulses rather than ideal single photons, making them vulnerable to the photon-number-splitting (PNS) attack.

Decoy-state QKD dramatically improves security and performance by varying pulse intensities, enabling accurate estimation of the single-photon fraction and allowing secure transmission over long distances, [3], [4].

Measurement device independent QKD (MDI-QKD) was introduced to address the detector-side

vulnerabilities common in practical QKD systems, [3].

Twin-Field QKD overcomes the limitations of MDI-QKD, which includes limited key rates at long distances, by introducing a novel interference-based architecture. It achieves a key rate that scales as $\sqrt{\eta}$. Later refinements, such as Phase-Matching QKD (PM-QKD), simplified the implementation and strengthened security proofs, [4].

Author in [5] proposed an efficient key sifting scheme, which requires less time to build the sifted key compared to the sifted key in the conventional BB84 protocol. [6] used the quantum scissors in the receiver of a discrete-modulation Gaussian-modulated continuous-variable quantum key distribution (CV-QKD) protocol to achieve positive secret key rates at high loss and high excess noise regimes of operation. [7] proposed a continuous-variable quantum key distribution (CVQKD) scheme based on the atmosphere-to-seawater channel. [8] presented a concrete 3-key combiner system implemented on a Field Programmable Gate Arrays (FPGA) platform. [9] proposed a hybrid integration of ultra-low-loss silicon nitride waveguides with indium phosphide electro-optic modulators to produce high-performance quantum key distribution transceiver chips to achieve high performance in decoding of photonic qubits on-chip at GHz speeds. [10] introduced an authenticated hybrid key exchange protocol that incorporates post-quantum cryptography (PQC) and QKD in a modular and information-theoretically secure architecture. [11] combined PQC and QKD to securely exchange a key that remains secure even if only one of the three key exchange methods is secure. [12] presented the development and implementation of a versatile ad-hoc metropolitan-range QKD network which integrated various types of physical channels and QKD protocols, and a mix of trusted and untrusted nodes.

Time-multiplexed hybrid QKD architectures have been widely explored as a means of combining multiple quantum communication protocols within a shared physical infrastructure. By allocating different QKD schemes to separate temporal modes, time-multiplexing enables efficient hardware reuse, mitigates cross-protocol

interference, and supports adaptive switching between protocols based on channel conditions, [13], [14].

Next, is providing insight into details about the BB84 and Twin Field algorithms.

2.1 BB84 Protocol

BB84 uses the polarization states of single photons to encode bits and employs quantum principles to detect eavesdropping attempts. It serves as the foundation for many subsequent QKD protocols.

Qubits can become entangled, meaning the state of one qubit is dependent on the state of another, regardless of the distance between them. This phenomenon forms the basis of many quantum protocols, including BB84, [1].

2.2 Principles of BB84

1) Encoding

Where the sender wants to securely transmit a key to the receiver. The sender randomly encodes each bit of the key into one of four possible states: horizontal (0°), vertical (90°), diagonal (45°), or anti-diagonal (-45°), $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, respectively.

Mathematically, a qubit can be represented as a quantum state vector using (1).

2) Transmission

The sender sends these qubits to the receiver over a quantum channel, which could be fiber optic cable or even free space.

3) Measurement

The receiver receives the qubits and randomly measures each qubit's polarization state, choosing one of two bases: either the rectilinear (horizontal/vertical) or diagonal (diagonal/anti-diagonal) basis. Mathematically, the rectilinear basis $\{|H\rangle, |V\rangle\}$ or the diagonal basis $\{|D\rangle, |A\rangle\}$.

4) Discussion

After transmission, the sender and receiver publicly compare which bases they used for each qubit. They keep only the bits where they used the same basis.

5) Security Check

To ensure no eavesdropping, both sender and receiver sacrifice a portion of their key to

compare. Any discrepancy between their keys indicates potential interference and the need to abort the protocol.

The security of BB84 relies on the principles of quantum mechanics. Any attempt by an eavesdropper to intercept or measure the qubits will disturb the sender and receiver's states, thus revealing the eavesdropper's presence.

Once they've verified the absence of eavesdropping, they discard the bits used for comparison and retain the rest as a shared secret key. This key can then be used for secure communication using classical cryptographic methods.

2.3 Twin-Field Protocol

Twin-Field QKD is an advanced quantum communication protocol that enhances the security and efficiency of QKD compared to earlier protocols like BB84, [15], [16].

2.4 Principles of Twin-Field

1) Photon Encoding

Sender encodes each bit of the key into quantum states of photons. The sender uses two different degrees of freedom (DOFs) to encode the information. These could be, for instance, the polarization and the time-bin of the photons as shown in (1).

$$|\psi\rangle = |\psi_{\text{polarization}}\rangle \otimes |\psi_{\text{time-bin}}\rangle \quad (1)$$

2) Transmission

The sender sends these encoded photons to the receiver through a quantum channel.

3) Measurement

The receiver receives the photons and measures them using compatible detectors. The receiver must measure both degrees of freedom used by the sender, which adds an extra layer of security.

4) Security Verification

Both sender and receiver perform security checks to detect any eavesdropping attempts. This involves comparing a subset of their key bits to check for discrepancies that could indicate interception.

Twin-Field QKD employs a dual-basis encoding scheme, where the sender randomly chooses one of two bases for each degree of

freedom when encoding the photons. This adds complexity for any potential eavesdropper trying to intercept the key.

Table 1 (Appendix) provides a summary of the pros and cons of both protocols with respect to the proposed algorithm.

Before going through the details of the proposed algorithm. The following summarizes the necessity of QKD as it addresses the critical shortcomings of classical cryptography by offering a method of secure key exchange rooted in the fundamental laws of quantum mechanics, rather than assumptions about computational hardness. Unlike RSA or ECC, which are threatened by the advent of quantum computers, QKD protocols like BB84 and Twin-Field QKD enable two parties to generate a shared secret key while detecting any eavesdropping attempts through quantum phenomena like the no-cloning theorem and measurement-induced disturbances. These protocols ensure forward secrecy, provide resistance to quantum attacks, and allow detection of intrusion through increased error rates. But still suffers from several weak points related to error rates and scalability.

Twin-Field QKD has emerged as one of the most significant advancements in long-distance quantum communication, offering a realistic and reproducible simulation framework supported by mathematically rigorous definitions and comprehensive security analyses. The original TF-QKD proposal introduced a novel interference-based architecture that achieves a key rate scaling proportional to $\sqrt{\eta}$. Since its introduction, it has been accompanied by well-defined mathematical models that describe phase interference, decoy-state estimation, and the characterization of single-photon and multi-photon contributions. Furthermore, subsequent variants, such as PM-QKD, have provided rigorous, composable security proofs under realistic device imperfections, channel noise, and finite-key conditions. Together, these developments provide a complete theoretical and simulation foundation that supports reproducible experiments, accurate numerical modelling, and secure deployment in practical quantum networks.

To represent the System Model of Twin Field QKD, consider Alice and Bob use phase-randomized weak coherent states (2):

$$|\alpha k\rangle, |\sqrt{\mu}e^{i\phi k}\rangle, |\beta l\rangle, |\sqrt{\mu}e^{i\theta l}\rangle \quad (2)$$

Where μ is the mean photon number (intensity), $\phi k, \theta l \in \{0, \pi\}$ for key encoding.

Central interference measurement is when Charlie performs a 50:50 beam splitter transformation (3):

$$U_{BS}: H_A \otimes H_B \rightarrow H_C \quad (3)$$

Where H_A and H_B are Hilbert spaces representing Alice and Bob's optical modes, H_C is the joint measurement space of Charlie

which acts on creation operators as (4):

$$a^\dagger \rightarrow \frac{a^\dagger + b^\dagger}{\sqrt{2}}, b^\dagger \rightarrow \frac{a^\dagger - b^\dagger}{\sqrt{2}} \quad (4)$$

Charlie performs threshold detection with two detectors: D0 and D1.

A twin-field detection event occurs when exactly one detector clicks (5).

$$E \in \{D0, D1\} \quad (5)$$

Key-encoding and sifted key is when Alice chooses a raw bit $x \in \{0, 1\}$ by selecting (6):

$$\phi_x = \begin{cases} 0, & x = 0, \\ \pi, & x = 1 \end{cases} \quad (6)$$

And the Twin Field QKD achieves ϵ -secure key generation under the composable security framework if:

$$\|\rho_{KE} - \rho_U \otimes \rho_E\|_1 \leq \epsilon \quad (7)$$

Where K is the final key, E is the adversary's quantum system, U is a uniform distribution, $\|\cdot\|_1$ and 1 is the trace distance.

3 Proposed Algorithm

Merging BB84 and Twin-Field QKD in one algorithm involves integrating the key components of both protocols to leverage their respective advantages. The hybrid algorithm divides the total number of bits into segments and alternates between using BB84 and Twin-Field QKD for each segment. This ensures that the benefits of both protocols are incorporated into the final key. Then each protocol segment generates its own raw key and associated error

rate. The error rates from both protocols are combined proportionally based on the length of the keys generated in each segment. A measure of the randomness of the key is calculated for each protocol segment and combined to assess the overall entropy of the hybrid key. Finally, the raw keys generated by both protocols are merged into a single key.

Algorithm 1 presents the approach to merge BB84 and Twin-Field QKD into a single hybrid algorithm:

Algorithm 1. The proposed hybrid QKD

Initial Setup

- Alice generates random bit sequences for qubits and measurement bases for both BB84 and Twin-Field QKD.
- Bob generates random measurement bases for both protocols.

1) Entanglement Generation

- Alice creates entangled qubits using the Twin-Field QKD technique.
- Alice sends one half of each entangled pair to Bob, while keeping the other half.

2) Measurement and Basis Selection

- Alice and Bob both measure the received qubits using their respective measurement bases for Twin-Field QKD.
- Alice and Bob also measure the qubits using their respective measurement bases for BB84.

3) Error Correction:

- Alice and Bob perform error correction separately for BB84 and Twin-Field QKD using appropriate techniques.

4) Key Generation:

- Alice and Bob extract raw keys separately for BB84 and Twin-Field QKD based on matching measurement bases and outcomes.
- The raw keys obtained from both protocols are combined to form a hybrid key.

5) Security Analysis:

- Perform security analysis to evaluate the secrecy and robustness of the hybrid key against various attacks.

6) Final Key Generation:

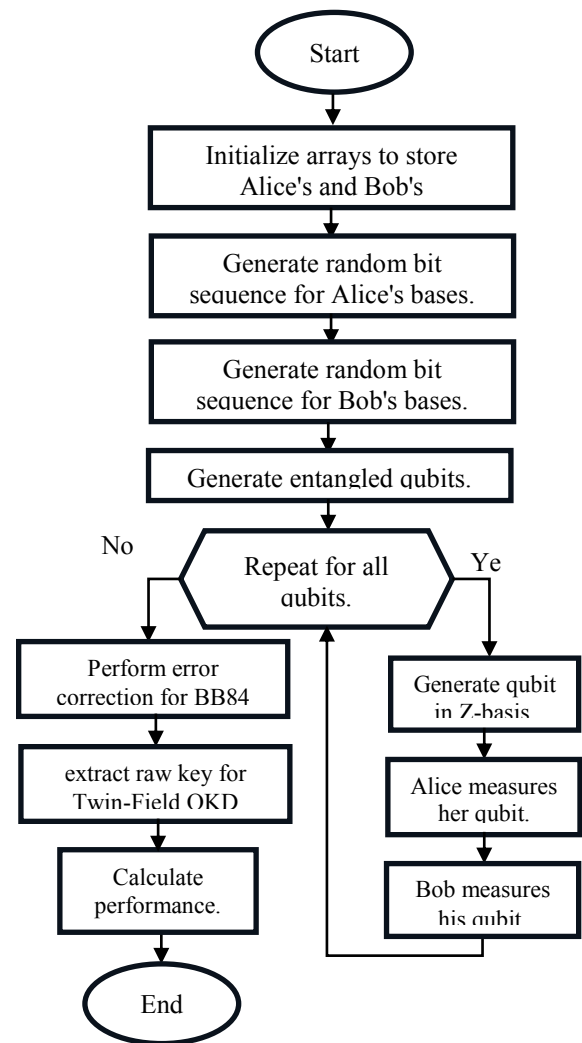


Fig. 1: Flowchart of the proposed algorithm. Source: created by the authors

- Generate the final secure key by processing the hybrid key obtained from both BB84 and Twin-Field QKD.

7) Performance Evaluation:

- Evaluate the error rate, key generation rate, and other performance metrics of the hybrid algorithm to assess its effectiveness compared to the individual protocols.

Figure 1 shows the flowchart of the proposed hybrid algorithm. While Figure 2 shows the process of measurements by Alice and Bob, who measure the qubit in the specified basis and return measurement outcome (0 or 1).

The performance of the proposed algorithm is measured by calculating:

- Error rate, which is the frequency of errors that occur during the transmission and measurement of qubits exchanged between sender and receiver. These errors can arise due to various factors, including noise in the communication channel, imperfections in the quantum devices, and interference from external sources. In QKD protocols such as BB84 and Twin-Field QKD, error rates are typically evaluated by comparing the measurement outcomes obtained by the sender and receiver for a subset of qubits. If the measurement outcomes do not match, it indicates an error in the transmission or measurement process. The error rate is then calculated as the ratio of the number of mismatched measurement outcomes to the total number of qubits exchanged. It is calculated using (8).

$$ER = N_{error}/N_{total} \quad (8)$$

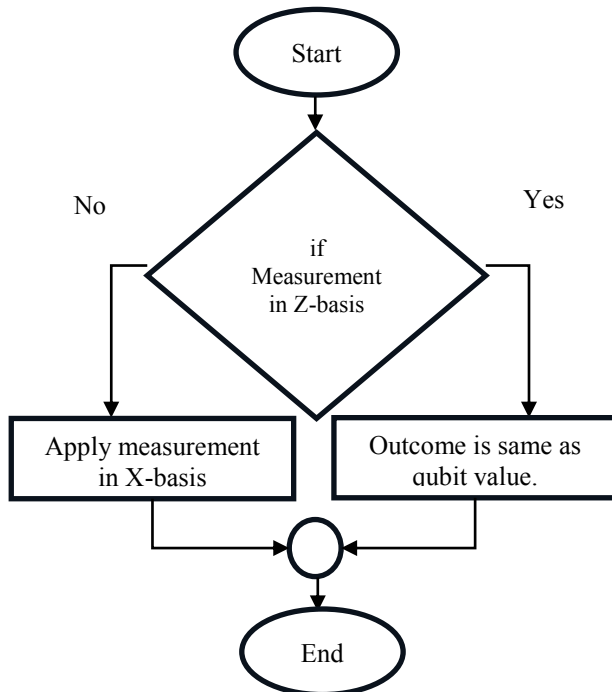


Fig. 2: Measuring of qubit.
Source: created by the authors

where N_{error} is the number of mismatched measurement outcomes, and N_{total} is the total

number of qubits exchanged between sender and receiver.

- Key generation rate, which is the rate at which a shared secret cryptographic key is generated between the sender and the receiver over a quantum communication channel. It is represented mathematically using (9).

$$KR = k_- / n_- \times f \quad (9)$$

where k is the number of raw key bits obtained after error correction and privacy amplification, n is the total number of qubits exchanged between sender and receiver, and f is the efficiency factor, representing the fraction of qubits that contribute to the final key after error correction and privacy amplification.

Achieving a high key generation rate is crucial for practical QKD implementations, as it determines the speed and efficiency of secure key establishment. Maximizing the key generation rate involves optimizing various aspects of the QKD system, such as error correction techniques, privacy amplification methods, and channel characteristics, to ensure reliable and efficient key generation in real-world communication scenarios.

- Entropy, which refers to the measure of randomness or uncertainty associated with the generated cryptographic key. It quantifies the degree of unpredictability of the key, which is crucial for ensuring its security against cryptographic attacks. In QKD protocols such as BB84 and Twin-Field QKD, entropy is typically evaluated based on the distribution of measurement outcomes obtained from the exchanged qubits. The entropy of the key is directly related to the randomness of these measurement outcomes, with higher entropy indicating a more random and unpredictable key.

The entropy of a cryptographic key can be mathematically expressed using Shannon entropy, which is defined in (10).

$$H = \sum_i p_i \log_2 p_i \quad (10)$$

where p_i is the probability distribution of possible outcomes i .

4 Mathematical Representation

Sender generates pairs of entangled qubits using a quantum entanglement source (Twin-Field QKD), the entangled qubits can be represented in equation 11.

$$|\psi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle) \quad (11)$$

where $|00\rangle$ and $|11\rangle$ represent the two possible states of the entangled qubits.

The sender prepares qubits in one of two possible bases: the Z-basis or the X-basis. Where each qubit prepared can be represented using (12) or (13).

$$q_i = \begin{cases} |0\rangle \text{ with propability } 1/2 \\ |1\rangle \text{ with propability } 1/2 \end{cases} \quad (12)$$

Or

$$q_i = \begin{cases} |+\rangle \text{ with propability } 1/2 \\ |-\rangle \text{ with propability } 1/2 \end{cases} \quad (13)$$

The sender sends one qubit from each entangled pair, along with one qubit prepared in the BB84 protocol, to the receiver over a quantum communication channel. Then, the receiver randomly chooses one of the two bases (Z-basis or X-basis) to measure each received qubit. The measurement outcomes obtained by the receiver can be represented using (14) and (15).

$$m_i = \begin{cases} |0\rangle \text{ with propability } p_{00} \\ |1\rangle \text{ with propability } p_{11} \end{cases} \quad (14)$$

Or

$$m_i = \begin{cases} |+\rangle \text{ with propability } p_{++} \\ |-\rangle \text{ with propability } p_{--} \end{cases} \quad (15)$$

This mathematical representation captures the key steps involved in the hybrid QKD algorithm, which combines elements from both the BB84 and Twin-Field QKD protocols to achieve enhanced security and efficiency in quantum key distribution.

Considering the case when Alice and Bob encode qubits in one of four BB84 states using (16):

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (16)$$

In the hybrid model, these states are prepared locally by Alice and Bob, then sent to an intermediate node (Charlie) for interference.

The interference visibility at Charlie's station is critical, depending on the relative phase between

Alice and Bob's weak coherent states, as shown in (17)

$$|\alpha e^{i\varphi A}\rangle, |\alpha e^{i\varphi B}\rangle \quad (17)$$

where φA and φB are random global phases chosen from a discrete set. The interference term (I) is used to determine detector clicks at Charlie in (18).

$$I = |\alpha A e^{i\varphi A} + \alpha B e^{i\varphi B}|^2 \quad (18)$$

where the Interference is constructive or destructive based on the phase difference in (19).

$$\Delta\varphi = \varphi A - \varphi B \quad (19)$$

The probability of a successful detector click and error rates for different intensity levels are represented in (20) and (21).

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \quad (20)$$

$$E_\mu = \frac{e_o Y_0 + e_d(1 - e^{-\eta\mu})}{Q_\mu} \quad (21)$$

where Q_μ is the gain for signal intensity μ , Y_0 is the background/dark count yield, η is the total transmission efficiency, e_d is the misalignment error, and e_o is the error from background noise, which is adapted to a twin-field measurement setup.

The hybrid rate, which combines BB84-style security analysis with Twin-Field distance scaling, is in (22)

$$R \geq P_{pass} \cdot [Q1 \cdot (1 - H_2(e1)) - Q_\mu \cdot f(E_\mu) H_2(E_\mu)] \quad (22)$$

where P_{pass} is the probability that interference is successful (Charlie), $Q1$ is the gain of a single-photon state, $e1$ is the error rate of a single-photon state, $f(E_\mu)$ is the error correction inefficiency, $H_2(x)$ is the binary entropy function.

For channel loss and detector modeling (23) is used.

$$\eta = 10^{-\alpha L/10} \quad (23)$$

where L is the total distance (Km), and α is fiber loss (dB/km).

The finite-key analysis framework quantifies the security of the protocol when only a finite number of signals (N) are exchanged. In the hybrid algorithm, Alice and Bob alternate between BB84

mode (used for robust bit generation and error estimation) and Twin-Field mode (used for efficient phase-based key generation), as illustrated in (24):

$$R_{finite} = \frac{1}{N} \left[S1^{TF} (1 - h(e_{ph}^{TF})) + S1^{BB84} (1 - h(e_{ph}^{BB84})) - leak_{EC} - \Delta_{finite} \right] \quad (24)$$

where $S1^{TF}$ is the number of Twin Field single-photon effective events, $S1^{BB84}$ is the number of BB84 single-photon events, e_{ph}^{TF} is the Twin Field phase error rate, e_{ph}^{BB84} is the BB84 bit error rate, $leak_{EC}$ is error-correction leakage, and Δ_{finite} finite-size correction using smooth min-entropy calculated in (25)

$$\Delta_{finite} = 7 \sqrt{\frac{\log(2/\varepsilon_{sec})}{N}} + \frac{2\log(1/\varepsilon_{PA})}{N} \quad (25)$$

where ε_{sec} is the overall secrecy parameter, ε_{PA} is the failure probability of privacy amplification, N is the total uses of the channel calculated in (26):

$$N = NB + NTF \quad (26)$$

NB is the number of BB84 rounds, NTF is the number of Twin Field QKD rounds.

Privacy amplification of the Hybrid Algorithm removes potential information that an eavesdropper may have gained during interference-based Twin Field events, BB84 basis-matched events, and classical error-correction exchanges represented by the privacy amplification model in (27):

$$f: \{0,1\}^n \rightarrow \{0,1\}^l \quad (27)$$

where l is the length of the final secret key that satisfies (28):

$$l \leq H_{min}^{\varepsilon}(K|E) - leak_{EC} - 2\log \frac{1}{\varepsilon_{PA}} \quad (28)$$

where $H_{min}^{\varepsilon}(K|E)$ is the smooth min-entropy of the joint key over Eve's information measured in (29), ε_{PA} is the privacy amplification failure probability.

$$H_{min}^{\varepsilon}(K|E) = H_{min}^{\varepsilon}(K_{TF}|E) + H_{min}^{\varepsilon}(K_{BB84}|E) \quad (29)$$

Thus, the privacy amplification compresses the combined hybrid key, ensuring composable security.

Error correction leakage for the information that Eve gains through classical reconciliation is measured in (30):

$$leak_{EC} = f_{EC} n_{raw} h(e_{bit}^{hybrid}) + \log\left(\frac{2}{\varepsilon_{EC}}\right) \quad (30)$$

where $f_{EC} \geq 1$ inefficiency of the reconciliation code, n_{raw} is the combined raw key length from both protocols, e_{bit}^{hybrid} is the effective bit error rate combining BB84 and Twin Field contributions calculated in (31), ε_{EC} is the allowed failure probability of error correction.

$$(e_{bit}^{hybrid} = \frac{n_{BB84} e_{bit}^{BB84} + n_{TF} e_{bit}^{TF}}{n_{BB84} + n_{TF}} \quad (31)$$

For Twin Field-QKD Phase Error Bound, decoy-state Field-QKD yields an estimate in (32):

$$e_{ph}^{TF} \leq \frac{E_{1,1}^{TF} + \delta_{PE}}{Y_{1,1}^{TF}} \quad (32)$$

where $E_{1,1}^{TF}$ is the phase-error yield from single-photon interference, $Y_{1,1}^{TF}$ is the single-photon twin-field yield, δ_{PE} is the deviation from finite-size parameter estimation.

This ensures the Twin Field contribution is secure even under phase noise and finite samples.

While for BB84 Phase Error Bound in the Z/X bases is given in (33):

$$e_{ph}^{BB84} = e_{bit}^x \quad (33)$$

where e_{bit}^x is the observed X-basis error rate.

And the hybrid algorithm's phase error is in (34):

$$e_{ph}^{hybrid} = \frac{S_1^{TF} e_{ph}^{TF} + S_1^{BB84} e_{ph}^{BB84}}{S_1^{TF} + S_1^{BB84}} \quad (34)$$

This provides a rigorous, composable upper bound on Eve's information about the hybrid key.

5 Simulation Results

After applying the previous algorithm with parameters in Table 2, Table 3 presents the calculated results of the hybrid algorithm, in addition to the results of BB84 and Twin-Field QKD.

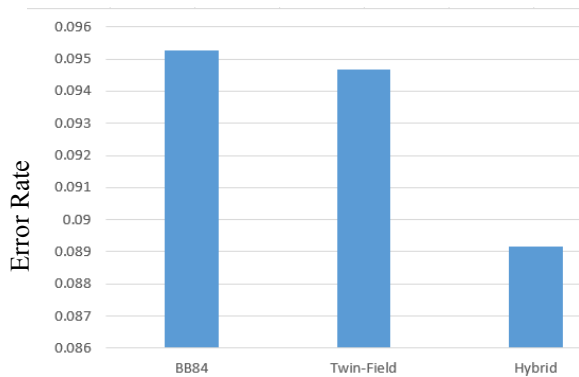


Fig. 3: Comparisons of error rates.

Source: created by the authors

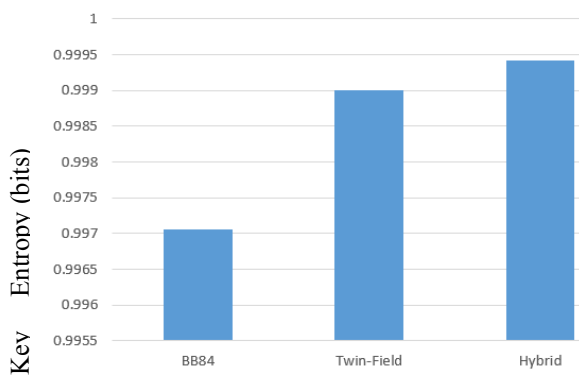


Fig. 5: Comparisons of Entropy

Source: created by the authors

The previous results are the average of several attempts to calculate the metrics.

The error rates are represented visually as shown in Figure 3.

The error rate of the hybrid algorithm is lower compared to both BB84 and twin-field. This reduction in error rate can be attributed to the error correction techniques employed in both BB84 and Twin-Field QKD, which are effectively combined

Table 3 Simulation Results

Protocol	Error Rate	Key Generation Rate	Entropy (bits)
BB84	0.095254	0.49675	0.997058
Twin-Field	0.094668	0.49375	0.999005
Hybrid Algorithm	0.089152	0.5065	0.999415

in the hybrid approach.

Figure 4 presents the key generation rates of the proposed algorithm in comparison to the BB84 and Twin-Field algorithms.

The alternating usage of BB84 and Twin-Field QKD ensures efficient resource utilization. By dividing the total number of bits evenly between the two protocols, the hybrid approach optimizes key generation efficiency. And Figure 5 presents the entropy.

The hybrid algorithm dynamically switches between BB84 and Twin-Field QKD based on the communication requirements. This adaptive protocol selection optimizes entropy generation by ensuring that the most suitable protocol is used for each segment of the communication channel.

Table 2. Simulation Parameters

Symbol	Value
N	10^8
pTF=pB	0.5
α	0.2 dB/Km
LA=LB	100Km
μ_s	0.4
μ_{d1}	0.1
μ_{d2}	0.01
η_d	0.6
Pd	10^{-6}
$\sigma\phi$	0.8
fEC	1.15
$\epsilon_{sec} = \epsilon_{PA}$	10^{-10}

Source: created by the authors

It is clear from the figures that the proposed algorithm outperforms the compared algorithms. The proposed algorithm specifies the generation of entangled qubit pairs using a quantum entanglement source, a characteristic feature inherited from Twin-Field QKD. It specifies the preparation of qubits in two orthogonal bases, typically the Z-basis and X-basis, as in BB84.

The receiver randomly measures the received qubits in either the Z-basis or X- basis, and publicly compares the measurement bases with the sender. This step is crucial for determining which measurement outcomes to retain for further processing.

The algorithm extracts a raw key by retaining matching measurement outcomes, following principles from both BB84 and Twin-Field QKD.

6 Conclusion

By integrating specifications and operational aspects from BB84 and Twin-Field, the proposed algorithm offers a comprehensive approach to quantum key distribution, combining the strengths of each protocol while mitigating their individual limitations. This approach results in enhanced key generation rate and entropy, as proved by simulation results. For future work, optimizing the hybrid parameters, such as adaptive switching ratios, intensity selection, and pulse allocation, could be considered to maximize key rate and efficiency, especially in finite-key scenarios. A hybrid algorithm could be combined with dynamic routing and quantum repeaters to support long-distance secure communication.

Acknowledgement:

I would like to thank the Arab Open University in Kuwait for support and help.

References:

- [1] Nurhadi, A.I. and Syambas, N.R., 2018, July. Quantum key distribution (QKD) protocols: A survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)* (pp. 1-5). IEEE. DOI:10.1109/ICWT.2018.8527822.
- [2] Fung, C.H.F., Tamaki, K. and Lo, H.K., 2006. Performance of two quantum-key-distribution protocols. *Physical Review A*, 73(1), p.012337. <https://doi.org/10.1103/PhysRevA.73.012337>
- [3] Lo, Hoi-Kwong, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution." *Physical review letters* 94, no. 23 (2005): 230504. <https://doi.org/10.1103/PhysRevLett.94.230504>.
- [4] Ma, Xiongfeng, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. "Practical decoy state for quantum key distribution." *Physical Review A—Atomic, Molecular, and Optical Physics* 72, no. 1 (2005): 012326. <https://doi.org/10.1103/PhysRevA.72.012326>
- [5] Biswas, C., Haque, M.M. and Gupta, U.D., 2022. A modified key sifting scheme with artificial neural network-based key reconciliation analysis in quantum cryptography. *IEEE Access*, 10, pp.72743-72757. <https://doi.org/10.1109/ACCESS.2022.3188798>.
- [6] Ghalaii, M., Ottaviani, C., Kumar, R., Pirandola, S. and Razavi, M., 2020. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. *IEEE Journal on Selected Areas in Communications*, 38(3), pp.506-516. <https://doi.org/10.1109/JSAC.2020.2969058>.
- [7] Guo, Y., Peng, Q., Liao, Q. and Wang, Y., 2021. Trans-media continuous-variable quantum key distribution via untrusted entanglement source. *IEEE Photonics Journal*, 13(2), pp.1-12. <https://doi.org/10.1109/JPHOT.2021.3064057>.
- [8] Ricci, S., Dobias, P., Malina, L., Hajny, J. and Jedlicka, P., 2024. Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2024.3364520>.
- [9] Dolphin, J.A., Paraïso, T.K., Du, H. "A hybrid integrated quantum key distribution transceiver chip". *npj Quantum Inf* 9, 84 (2023). <https://doi.org/10.1038/s41534-023-00751-3>.
- [10] L. Garms, T. K. Paraïso, N. Hanley, A. Khalid, C. Rafferty, J. Grant, J. Newman, A. J. Shields, C. Cid, M. O'Neill, "Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem". *Adv Quantum Technol.* 2024, 7, 2300304. <https://doi.org/10.1002/qute.202300304>.
- [11] N. Aquina, S. Rommel and I. T. Monroy, "Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution," *2024 24th International Conference on Transparent Optical Networks (ICTON)*, Bari, Italy, 2024, pp. 1-4. <https://doi.org/10.1109/ICTON62926.2024.10648124>.

- [12] M. Goy, J. Krause, Ö. Bayraktar, " Ad-hoc hybrid-heterogeneous metropolitan-range quantum key distribution network", 2024. <https://doi.org/10.48550/arXiv.2412.07473>.
- [13] Verdier, Pierre-Enguerrand, Romain Alléaume, and Thomas Rivera. "Investigating Raman backscattering decay and the perspective of time-multiplexed quantum communications." *Optics Express* 33, no. 15 (2025): 31029-31041. <https://doi.org/10.1364/OE.561961>.
- [14] Sabatini, Mattia, Tommaso Bertapelle, Paolo Villoresi, Giuseppe Vallone, and Marco Avesani. "Hybrid encoder for discrete and continuous variable QKD." *Advanced Quantum Technologies* (2025): 2400522. <https://doi.org/10.1002/qute.202400522>.
- [15] Zhou, F., Qu, W., Wang, J., Dou, T., Li, Z., Yang, S., Sun, Z., Miao, G. and Ma, H., 2020. Twin-field quantum key distribution with heralded single-photon source. *The European Physical Journal D*, 74, pp.1-6. <https://doi.org/10.1140/epjd/e2020-10219-0>.
- [16] Curty, M., Azuma, K. and Lo, H.K., 2019. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information*, 5(1), p.64. <https://doi.org/10.1038/s41534-019-0175-6>.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

This work is done completely by a single author.

Sources of Funding for Research Presented in a Scientific Article or the Scientific Article Itself

This research has no funds.

Conflict of Interest

The authors have no conflicts of interest to declare.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US

APPENDIX

Table 1. Comparisons Between BB84, Twin-Field, and the Proposed Hybrid Algorithm

Aspect	BB84 Protocol	Twin-Field QKD	Proposed Hybrid Algorithms
Error Rates	Sensitive to errors from photon loss, detector inefficiencies, and noise.	More robust against errors over long distances, better noise resilience due to interference techniques.	Minimized error rate
Key Generation Rates	Decays exponentially with distance.	Linear decay with distance, enabling higher rates over long distances.	Performance depends on algorithm and quantum-classical integration efficiency.
Entropy	Generates high entropy for short distances but degrades rapidly over longer distances.	Maintains higher entropy over long distances due to improved photon utilization.	Entropy not directly relevant to QKD; applies to problem-specific randomness in optimization or simulations.
Scalability	Limited scalability due to exponential key rate decay.	High scalability for large networks and long distances.	Scalable for specific problems.

Source: created by the authors