Check for updates

Received: 1 December 2023 | Revised: 17 February 2024 | Accepted: 1 March 2024

IET Quantum Communication

DOI: 10.1049/qtc2.12092

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

# Entanglement and teleportation in quantum key distribution for secure wireless systems

**Md. Ferdous Ahammed** | **Mohammad Ismat Kadir**

Electronics and Communication Engineering, Khulna University, Khulna, Bangladesh

**Correspondence**

Mohammad Ismat Kadir, Electronics and Communication Engineering, Khulna University, Khulna 9208, Bangladesh.
Email: ismat.kadir@ece.ku.ac.bd

**Abstract**

Entanglement-assisted quantum key distribution (QKD) has attracted significant attention for its ability to provide highly secure wireless systems. This work explores the employment of quantum teleportation and the quantum Fourier transform (QFT) in entanglement-assisted QKD to enhance security. By integrating the concepts of entanglement, teleportation, and QFT, the key distribution strategy is significantly improved, leading to more secure communication. The system has been thoroughly tested for quantum bit error rate, secure key rate, and reconciliation efficiency. The results show that this technique outperforms the standard BB84 protocol. Based on their simulations, this protocol appears to be a promising technique for providing quantum-level security to next-generation wireless communication systems.

**KEYWORDS**

quantum communication, quantum cryptography, quantum entanglement, teleportation

## 1 | INTRODUCTION

As wireless communication technologies grow, the need for secure and reliable communication channels becomes increasingly important. The fifth-generation (5G) wireless communication standard offers faster data transfer rates, lower latency, and increased capacity compared to its predecessors [1]. However, these advancements also pose new security challenges, such as interception, malware, and trojans, and many can interrupt the communication of sensitive information [2]. In contrast, classical cryptographic techniques can be easily defeated by exploiting immense computing power [3]. To overcome these challenges, researchers are investigating many cryptographic techniques, such as quantum cryptography, that utilise the principles of quantum physics due to the increasing significance of data security [4]. For instance, quantum key distribution (QKD) is the most well-known cryptographic protocol for acquiring absolute security in communication [5, 6]. By utilising the idea of uncertainty derived by Stephen Wiesner in the early 1970s [7] and photon polarisation, QKD ensures the information is transmitted only to the receiver. In the QKD protocol, secure keys are generated and shared between two parties that are only known to them, and if the eavesdropper tries to access the keys, that will be identified [8]. Hence, QKD offers unconditional security for communication by preventing any eavesdropping attempts [9]. Bennett and Brassard published the most well-known QKD protocol (BB84) [10] in 1984, which utilises the idea of the no-cloning theorem [11] and Heisenberg's uncertainty principle [4]. In the BB84 protocol, classical random bits are encoded as single-photon polarisation with four random polarisation states. The first QKD protocol (E91) based on entanglement was presented by Ekert in 1991 [12]. Quantum entanglement offers several distinctive properties that can enhance the robustness of entanglement-aided QKD systems. Specifically, it assures a higher level of security in QKD by detecting the presence of an intruder. Entanglement assists in maintaining correlations over long distances, and entangled pairs can establish secure channels between distant parties. Entangled states can perform error correction and reconciliation, enabling the recovery of secret keys shared between distant parties. In the E91 protocol [12], two parties could efficiently share entangled polarised photons. BBM92 and BB84 protocols employ the concept of privacy amplification, raw key exchange, and key sifting [13]. In

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2024 The Authors. *IET Quantum Communication* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

the same year, Bennett proposed the B92 protocol [14]. This system utilises only two non-orthogonal states, with each state representing a one-bit value.

Muller, Breguet, and Gisin showed fibre-based QKD over 1.1 km using polarisation coding in 1993 [15]. In a separate development, Townsend, Rarity, and Tapster proposed fibre-based QKD over 10 km using phase coding [16]. Over the years, with development, the transmission distance has surpassed 120 km [17]. Another new experimental outcome of long-distance continuous-variable QKD (CV-QKD) was reported, which successfully transmitted quantum information up to 202.81 km over an ultralow-loss optical fibre [18]. In the experiment, excess noise was controlled efficiently, and effective reconciliation techniques were employed. Vactor Zapatero et al. presented a review of device-independent QKD (DI-QKD), which enables the secure exchange of secret keys [19, 20]. DI-QKD eliminates quantum hacking threats to which non-DI-QKD protocols are vulnerable. The major QKD protocols in the literature and their main features are listed in Table 1.

The quantum Internet is another unique concept of quantum communication networks, which promise improved security, faster communication speed, and vast network capacity [28]. The quantum Internet paves the way for various new applications. As quantum Internet fulfils the requirements of 6G communication networks, it is expected to work in tandem with 6G networks [29, 30].

A quantum repeater plays a critical role in transmitting quantum information over long distances [31]. In quantum channels, quantum repeaters help to mitigate loss and noise, which are crucial to building a quantum network. Quantum repeaters are important to the development of the quantum Internet. In a recent review, Azuma, Koji, et al. presented the designs and conceptual frameworks of quantum repeaters [32, 33]. They proposed new kinds of repeaters, such as memoryless, error-corrected, and all-photonic repeaters, and categorised the repeaters according to the processes employed to reduce losses and mistakes.

Another quantum concept, namely quantum teleportation, evolved as an outstanding technique for transferring qubits without physically moving the particles [34]. It requires both the classical and the quantum resources. Bits are the classical components, whereas qubits are the quantum components. Classical resources are transmitted over the classical channel and quantum resources over the quantum channel [35]. The study in Ref. [36] demonstrates that quantum teleportation can transmit qubits up to 500–1400 km of distance [37, 38]. In the context of QKD, teleportation might help in establishing entanglement and securely transmitting quantum states between distant parties.

Despite the potential benefits of entanglement-assisted QKD, there is still a lack of understanding about how it can be effectively implemented and integrated into existing communication systems. The main idea behind this work is the incorporation of quantum entanglement and teleportation in the BB84 QKD protocol. We propose an effective and efficient entanglement-assisted QKD protocol, which can be used to strengthen the security of 5G and beyond wireless communication techniques. There are some recent review articles, for example, [37, 39–41], on how QKD and other quantum mechanical concepts can enhance the security of next-generation wireless systems.

This work explores the theoretical underpinnings of entanglement-assisted QKD, develops practical implementation strategies, and evaluates the performance of the proposed protocol in realistic communication scenarios. We investigate the effectiveness of using entanglement-assisted QKD protocol for secure next-generation wireless communication systems. Furthermore, we compare the proposed protocol with the existing ones based on metrics such as the secure key rate, security against attacks, and resistance to noise and errors.

The contributions of this work can be summarised as follows:

1. We propose an entanglement-assisted QKD protocol using quantum teleportation and quantum Fourier transform (QFT) for the quantum channel. This technique can enhance the efficiency of entanglement manipulation and information processing for the proposed cryptographic protocol.
2. We consider a classical frequency-selective channel and employ conventional OFDM-based communication over the classical channel.
3. We evaluate the performance of the proposed protocol in terms of key generation rate, error rate, and mutual information between Alice and Bob or Alice and Eve and the expected number of bits to be spilled in the post-processing operations.

The rest of this paper is organised as follows. Section 2 outlines the background materials related to quantum communication and QKD. Specifically, it describes QKD, measurements, and entanglement-aided QKD. Section 3 provides an overview of the proposed design. This section also outlines the ideas of quantum Fourier transform, quantum teleportation, and Eve's interception and re-transmission incorporated in the proposed design. The performance metrics of the proposed system are described in Section 4, and Section 5 provides the simulation results and discussion. Section 6 outlines the challenges and limitations of implementing the proposed protocol in real-world scenarios. Finally, Section 7 concludes the article.

## 2 | BACKGROUND

In this section, we provide a brief introduction to some basic but useful concepts related to quantum computation, quantum information theory, and quantum communications. These preliminaries are essential for understanding the concept of entanglement-aided QKD systems.

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

**TABLE 1** Existing quantum key distribution (QKD) protocols.

| Protocol's name | Year | Core principle | Description |
|---|---|---|---|
| BB84 [10] | 1984 | Quantum superposition, No-cloning theorem | This protocol uses single-photon polarisation with four random polarisation states to encode information. It also uses two bases—a rectilinear basis and a diagonal basis. |
| E91 [12] | 1991 | Quantum entanglement, violation of Bell's inequality | This scheme uses entangled polarised photon pairs shared between two parties. |
| BBM92 [13] | 1992 | Quantum entanglement, violation of Bell's inequality | It is also an entanglement-based protocol like E91. It also employs privacy amplification, raw key exchange, and key sifting. |
| B92 [14] | 1992 | No-cloning theorem, use of non-orthogonal states | It is a modified version of the BB84 protocol. However, it uses two polarisation states (0 ° and 45 ° ) instead of four states. |
| SSP [21] | 1999 | Prepare-and-measure, use of six non-orthogonal states | It is also another modified version of the BB84 protocol. It employs six polarisation states rather than four to represent the bits. |
| SARG04 [22] | 2004 | Remote state preparation | It is also another modified version of the BB84 protocol. It uses laser pulses instead of a single photon source. It provides an unconditional security at a higher quantum bit error rate (QBER) under a photon-number-splitting (PNS) attack. |
| COW [23, 24] | 2004 | Key generation by weak coherent pulses, detection of Eve's interference by interferometer | It performs at higher data rates with weak coherent pulses. It can provide higher efficiency in the presence of a PNS attack. |
| KMB09 [25] | 2009 | Index transmission error rate (ITER) calculation, long-distance communication | The KMB09 protocol employs two orthogonal, mutually unbiased bases, each encoding either '0' or '1'. |
| S13 [26] | 2013 | Quantum key swapping | It is also an improved version of the BB84 protocol. However, it employs private reconciliations and asymmetric cryptography. The main idea behind the protocol is that the final key length never changes during key exchange. |
| AK15 [27] | 2015 | Utilisation of EPR theory in QKD | This protocol uses Einstein, Podolsky, and Rosen (EPR) theory, quantum, and public channels in its four phases of authentication, transformation, exchanging, and reconciliation. |

## 2.1 | Quantum bits

Information is expressed differently in classical and quantum computing. In classical computing, the bit is the fundamental unit of information with two basic states '0' and '1' to build up all data. In quantum computing, 'quantum bit' or 'qubit' is the fundamental unit of quantum information. One qubit has two possible states ($|0\rangle$ and $|1\rangle$), where the notation $|\psi\rangle$, often referred to as the 'ket', denotes the quantum states. The general representation of a single qubit on any state can be expressed [35, 42] as follows:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{1}$$

where $|\psi\rangle$ represents the superposition or linear combination of both $|0\rangle$ and $|1\rangle$ states [43], $\alpha$ and $\beta$ are complex numbers that represent the probability of locating a qubit in state $|0\rangle$ and $|1\rangle$, and they satisfy $|\alpha|^2 + |\beta|^2 = 1$, and $\alpha, \beta \neq 0$. A single qubit of any state can also be represented using a spherical coordinate system ($r$, $\theta$, $\varphi$) which is denoted as the Bloch sphere. Any single qubit strategy can be depicted geometrically on a Bloch sphere. The representation of $\alpha$ and $\beta$ in Bloch sphere [44] can be expressed by

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{pmatrix} \cos\dfrac{\theta}{2} \\ e^{i\varphi}\sin\dfrac{\theta}{2} \end{pmatrix} \tag{2}$$

where $\theta$ and $\varphi$ are real numbers. The integers $\theta$ and $\varphi$ denote a point on the Bloch sphere, which is a three-dimensional sphere. The angle $\theta\epsilon[0, \pi]$ stands for latitude, and $\varphi\epsilon[0, 2\pi]$ stands for longitude on the Bloch sphere. Using (2), we can rewrite (1) as follows [35]:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)\left|0\right\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)\left|1\right\rangle. \tag{3}$$

Substituting the values of $\theta = \frac{\pi}{2}$ and $\varphi = 0$ in (3), we obtain the probability of finding a qubit in state $|+\rangle$ as follows:

$$|\psi\rangle = \cos\left(\frac{\pi}{4}\right)\left|0\right\rangle + e^{i.0}\sin\left(\frac{\pi}{4}\right)\left|1\right\rangle \tag{4}$$

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{5}$$

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \tag{6}$$

Again, substituting the values of $\theta = \frac{\pi}{2}$ and $\varphi = \pi$ in (3), the probability of finding a qubit in state $|-\rangle$ can be obtained as follows:

$$|\psi\rangle = \cos\left(\frac{\pi}{4}\right)\Big|0\rangle + e^{i.\pi}\sin\left(\frac{\pi}{4}\right)\Big|1\rangle \tag{7}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{8}$$

$$|\psi\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \tag{9}$$

The graphical representation of a single qubit state's Bloch sphere is depicted in Figure 1. A single-qubit register of a quantum information system can be modelled [35] as follows:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{and } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \tag{10}$$

For a two-bit classical system, we will have four states denoted by 00, 01, 10, and 11. By contrast, in a two-qubit quantum information system, there will also be four possible states represented by $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. These four possible states can be expressed [45] by the tensor products of $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$.

## 2.2 | Quantum key distribution

QKD employs the principles of quantum mechanics, for example, the Heisenberg uncertainty principle and the quantum no-cloning theorems, to ensure the unconditional security of quantum cryptography for two communicating parties, for example, Alice and Bob [46, 47]. The fundamental requirement of the QKD protocol is that qubits be transmitted using a public quantum channel with an error rate less than a given threshold. It is a promising technology for exchanging private keys securely and mitigating communications against security threats like eavesdroppers [5]. Therefore, eavesdroppers cannot obtain the quantum information from qubits without disturbing their states. Some existing QKD protocols include BB84 [10], E91 [12], B92 [14], SARG04 [22], and others.

BB84 is the first and most widely used QKD protocol proposed by Bennett and Brassard in 1984 [10]. Rectilinear basis ( + ) and diagonal basis ( × ) are two basis sequences used in the BB84 protocol. A rectilinear basis ( + ) consists of horizontal polarisation (0 °) and vertical polarisation (90 °). Besides, diagonal basis also consists of diagonal polarisation (45 °) and anti-diagonal polarisation (135 °). The four states of polarisation are shown in Figure 2a, and two types of basis polarisation-coding are shown in Figure 2b.

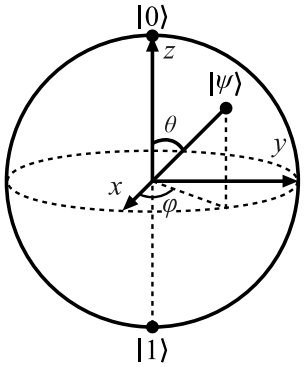


**FIGURE 1** Bloch sphere-based representation of a single qubit state from (3) [35]. The qubit vector is represented by $|\psi\rangle$, while the polar and the azimuthal angles are denoted by $\theta$ and $\varphi$, respectively. Each qubit's state is expressed in terms of $x$, $y$, and $z$ coordinates.

Bit-wise representation for polarisation-coding of the BB84 protocol is depicted in Figure 3b.

A basic representation of the BB84 protocol is illustrated in Figure 3a. The BB84 protocol has two phases—the quantum channel phase and the classical channel phase. The basic working procedure of BB84 is as follows where points $(1-3)$ are quantum channel phase and $(4-6)$ are classical channel phase:

1. Alice generates two random bit strings—basis sequence bits and key bits.
2. She picks each key bit as the $\{|0\rangle, |1\rangle\}$ state if the respective basis sequence bit is 0 otherwise, she picks the state in $\{|+\rangle, |-\rangle\}$.
3. She transmits the encoded states to Bob. Bob generates his basis sequence bits string. As he does not know about Alice's basis sequences, Bob measures each qubit in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ using his basis sequence bits string.
4. Bob and Alice share their basis sequences.
5. When Bob's estimated basis is different than Alice's basis, they both scrap key bit from that location.
6. Alice and Bob both check and compare the key bits with each other. The communication will be aborted if disagreements exceed the threshold number.

## 2.3 | Heisenberg's uncertainty principle

Heisenberg's uncertainty principle is a fundamental concept in quantum mechanics. Werner Heisenberg first formulated the uncertainty principle in 1927 [48]. It states that two physical properties such as position and momentum cannot be estimated simultaneously. The principle can be mathematically expressed [48] as follows:

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License


**FIGURE 2** (a) Four states of polarisation (*i*) horizontal polarisation, 0 ° (*ii*) vertical polarisation, 90°, (*iii*) diagonal polarisation, 45°, and (*iv*) anti-diagonal polarisation, 135°. (b) Two types of the basis for encoding purpose (*i*) rectilinear basis ( + ), and (*ii*) diagonal basis ( × ).

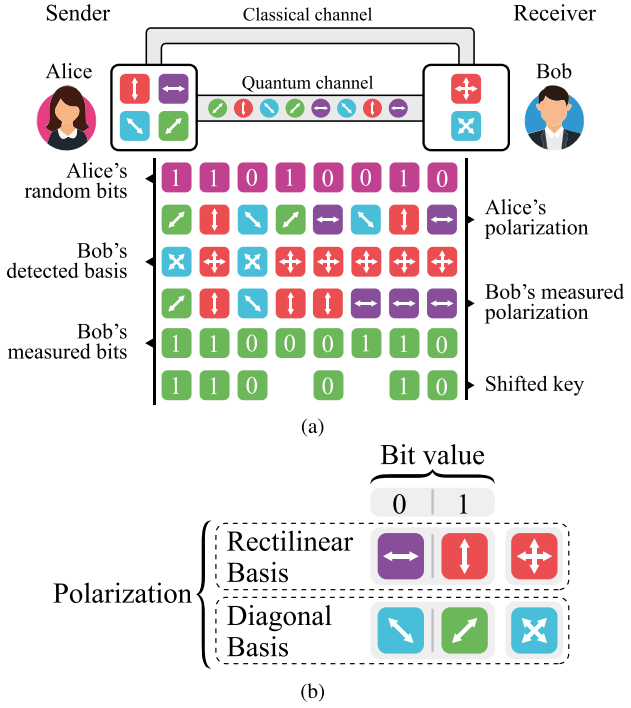


**FIGURE 3** (a) Illustration of the principles of the BB84 quantum key distribution (QKD) protocol [10]. (b) Bit-wise representation for polarisation-coding of the BB84 protocol.

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \tag{11}$$

where $\Delta x$ and $\Delta p$ denote the uncertainties in position and momentum, respectively, and $\hbar$ refers to the reduced Planck's constant. In quantum communications, the uncertainty principle provides the insight that an observer cannot be certain about what will happen to a closed quantum system—it can just predict with some probability about some potential outcomes. This probability is related to the probability associated with the superposition states mentioned earlier. The principle has also the significance that, upon measurement, the quantum state of a particle collapses [39].

## 2.4 | No-cloning theorem

No-cloning theorem is a fundamental concept in quantum mechanics [11]. According to the theorem, it is impossible to create an exact copy of an arbitrary unknown quantum state to its linearity and unitarity. Therefore, any eavesdropper cannot create a clone of the quantum state to explore data during transmission.

The phenomenon that the linear combination of all possible states of a quantum system is also a quantum state of the system is the underlying cause of the no-cloning theorem. To illustrate this, let us consider the two states $|0\rangle$, $|1\rangle$, and their superposition state given by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. If cloning is possible, that is, $|0\rangle$ can be cloned to $|00\rangle = |0\rangle|0\rangle$ and $|1\rangle$ to $|11\rangle = |1\rangle|1\rangle$, then $|\psi\rangle$ should be cloned to $\alpha|00\rangle + \beta|11\rangle$, where $|00\rangle = |0\rangle \otimes |0\rangle$. However, we have $|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|00\rangle$. This shows that cloning is not possible [39].

No-cloning theorem has significant implications for quantum information processing and quantum cryptography, including QKD. The security of QKD relies on the fact that any attempt by an eavesdropper to clone the transmitted quantum states would inevitably introduce errors that can be detected. The no-cloning theorem contributes to the information-theoretic security of QKD. It provides a way to detect the presence of an eavesdropper with high confidence, making QKD a promising method for secure communication.

## 2.5 | Entanglement

Entanglement is probably the most important concept that can provide enhanced security to a quantum mechanical system. The idea of 'entanglement' dates back to 1935. The predictions of Einstein, Podolsky, and Rosen (EPR) [49] about the EPR pair and the concurrent contributions of Erwin Schrödinger [50, 51] introduced the idea of entanglement. The 'spooky action at a distance' of Einstein or the 'Verschränkung' of Schrödinger is such a powerful idea that the 2022 Nobel Prize in Physics was awarded to Alain Aspect, John Clauser, and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science" [52].

Entanglement is a property in quantum mechanics where two or more particles become intrinsically correlated, even when they are spaced far apart. These entangled particles exhibit a specific property—if one particle's state is measured, the state of the other(s) instantly correlates, regardless of the distance separating them. This phenomenon helps detect any eavesdropping attempts in QKD because any interception or measurement attempt on an entangled particle will alter its state, indicating tampering [12, 53]. Entanglement is a widely studied area of research for providing enhanced security in quantum physics, quantum communication, and quantum computing.

## 2.6 | Quantum measurement

Measurement plays a significant role in determining the security effectiveness of the key exchange between Alice and Bob. It is the final step of the QKD protocol, where Bob performs

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

measurements of the received quantum states to measure the bits. The received quantum states are encoded with two orthogonal bases, namely the rectilinear basis ($|0\rangle$ and $|1\rangle$) and the diagonal basis $\{|+\rangle, |-\rangle\}$.

After receiving the transmitted bases of Alice from the quantum channel, Bob will try to decode the state and retrieve the actual key bits from the transmitted bases. For this procedure, Bob randomly generates the basis selection bits as Alice has generated for obtaining maximally entangled states. Bob is unaware of whether measurements are deterministic or made using the same methodology as Alice's. Bob selects the bases at random to measure the quantum states. In the rectilinear basis, Bob measures quantum states using the $\{|0\rangle, |1\rangle\}$ basis. On the other hand, on a diagonal basis, he measures quantum states using the $\{|+\rangle, |-\rangle\}$. Bob will, on average, be fortunate and choose the same quantum state as Eve. In this instance, the bits obtained from his measurement will match the bits Alice supplied. But the other half of the time, he will be unlucky and select the state that Alice did not use. In this instance, only 50% of the time, the bit produced by his measurement will match the bit transmitted by Alice. If he selects the correct basis, the measured bits will be decoded with the highest probability. Bob currently possesses a binary sequence of key bits resulting from all these measurements [54].

## 2.7 | Entanglement-assisted quantum key distribution

An entangled qubit is one whose quantum states cannot be represented independently and separately. Entanglement has been broadly used in QKD. Entanglement has been used to identify the existence of eavesdroppers and generate a secret key. In the entanglement-based QKD version, Alice and Bob share a special entangled state that allows them to obtain perfectly correlated bits upon measuring their half of the state. We will see how they can construct such a state, how they can check whether they were successful, and how they can detect Eve's attempted attack.

In the entanglement-based protocol [12, 13], Alice and Bob create a special entangled state by sharing between two-qubit resisters, which is a superposition of states, also called Bell state, for example, ($|00\rangle$ and $|11\rangle$). In a Bell state, one qubit is correlated with another such that the state of another qubit can dictate one qubit. John Bell investigated the concept of entanglement in 1964 [55], and 'Bell State' was named to commemorate his contribution. The concept of the Bell states and the relevant quantum information processing are essential for the QKD system. There are four maximally entangled Bell states that form an orthogonal basis of quantum states [56] as given by

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{12}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{13}$$

where $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ are called the Einstein, Podolsky, and Rosen (EPR) pairs [49], which are the most widely used system that provides entanglement between two qubits. Alice first randomly generates two bits sequences, that is, ("0" and "1"). One is the generated key sequence and another is the Alice basis selection sequence. Alice then generates maximally entangled quantum states using those basis selection and key sequences. For instance, if the basis selection sequence is 0 and the key sequence is 0, then the maximally entangled state $|B_{s_{00}}\rangle$ can be written as follows:

$$|B_{s_{00}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{14}$$

Similarly, the maximally entangled states corresponding to the other basis and key sequences can be expressed as follows:

$$|B_{s_{01}}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{15}$$

$$|B_{s_{10}}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{16}$$

$$|B_{s_{11}}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{17}$$

In the above-mentioned equations, maximally entangled states $|B_{s_{00}}\rangle$, $|B_{s_{10}}\rangle$, and $|B_{s_{01}}\rangle$, $|B_{s_{11}}\rangle$ are conjugate pairs.

We note at this point that entanglement-assisted QKD requires an appropriate access technology as well as appropriate physical channels [39, 57].

## 2.8 | Quantum decoherence and fidelity

Quantum decoherence refers to the loss of quantum coherence in the quantum states of particles used for encoding information. Due to environmental factors, gradual decay of the states of a quantum system occurs which is defined as decoherence. Usually, the state of a quantum system is represented by its density matrix $\rho$ and the matrix is crucial for describing mixed states and quantum operations. Quantum decoherence influences the evolution of the density matrix over time, [35].

The degree of quantum decoherence can be quantified in terms of the 'fidelity' of the system. Fidelity measures the similarity between the ideal quantum state and the actual state, as described by the density matrix. It is calculated as the overlap between the states and ranges from 0 to 1, with higher values indicating better fidelity.

Mathematically, the fidelity between two quantum states whose density matrices are $\rho$ and $\sigma$ can be expressed [35, 58] as follows:

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

$$F(\rho,\sigma)=\left[\mathrm{tr}\left(\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)\right]^2, \tag{18}$$

where tr (·) represents the trace operator.

The fidelity defined by (18) can be seen as a measure of the overlap between the initial quantum state $|\psi_i\rangle\langle\psi_i|$ and the decoherent state $|\psi\rangle\langle\psi|$ of an entangled system. Considering the states as pure states, the fidelity is given [58] by $F=\left|\langle\psi_i|\psi\rangle\right|^2$. In a QKD protocol, environmental interactions result in decoherence, which negatively impacts the fidelity of quantum states.

## 3 | PROTOCOL DESIGN

This section provides an overview of the proposed teleportation-based and entanglement-aided QKD protocol. The proposed entanglement-assisted QKD protocol has the potential to provide secure wireless communications between two participants, Alice and Bob. The system is intended to guarantee the confidentiality and integrity of data transmission in next-generation wireless systems. The overall block diagram of the entanglement-assisted QKD is shown in Figure 4, and the block diagram of the post-processing operations is depicted in Figure 5. The proposed protocol is similar to the BB84 protocol—however, it employs the entanglement as used by Ekert [12] and follows the ideas of Bennett et al. [13].

As illustrated in Figure 4, Alice encodes quantum states using basis and key sequences. She employs a teleportation-inspired strategy for the encoding [57]. She utilises half of the third-party-distributed entangled particles (e.g., EPR pairs) as a resource for quantum communication. Alice applies the quantum Fourier transform (QFT) to the encoded quantum states. After that, Alice teleports the entangled states to Bob. This can be for a long distance without requiring the transmission of physical components, albeit the environmental imperfections are modelled by a quantum channel. We note that faster-than-light communication is still not possible because the communication of basis and the measurement outcomes occur over the classical channel.

Bob, on the other side, has the Alice-teleported quantum entangled states. He first employs channel equalisation on the teleported quantum states. The quantum channel equalisation [59] differs significantly from the classical channel equalisation. Following quantum channel equalisation, he uses inverse QFT (IQFT) operations to transform the basis back into the original basis. This step ensures that both Alice and Bob are using the same basis for further processing. Then, he measures the received quantum states and records the measurement outcomes. After that, both Alice and Bob perform a post-processing operation on the classical channel.

The post-processing strategy is shown in Figure 5, which is essential for improving the security and dependability of the shared key. It is carried out over a classical channel to verify the protocol's security. The postprocessing operation is composed of several key components, such as key sifting, error correction, reconciliation, and security analysis [60]. First, key-sifting

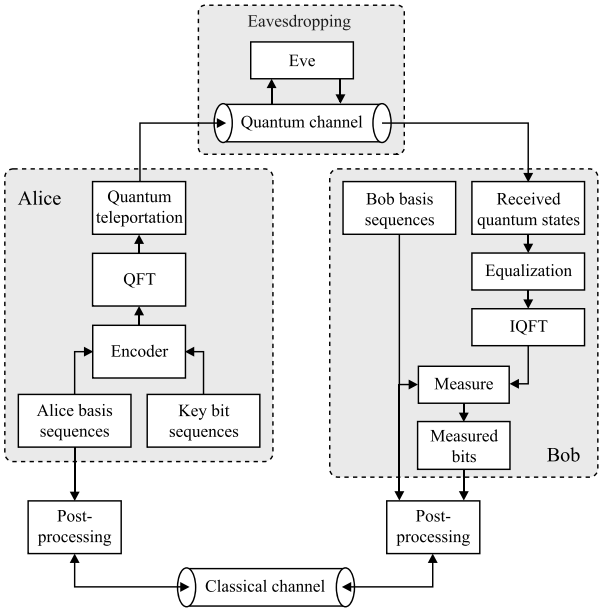


**FIGURE 4** Overall block diagram of the proposed entanglement-assisted quantum key distribution (QKD) protocol. Alice prepares and teleports quantum information to Bob. Quantum Fourier transform (QFT) and inverse quantum Fourier transform (IQFT)-based basis transformation are employed for strengthening security. During transmission over the quantum channel, Eve tries to access the information. Bob measures Alice's quantum information and shares the measurement outcomes over a classical channel. Mismatch in measurement outcomes alerts the interception of Eve.

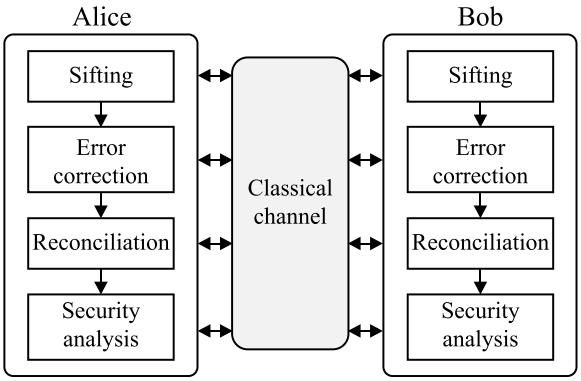


**FIGURE 5** Block diagram of the post-processing operations. Proposed post-processing operations include sifting, error correction, reconciliation, and security analysis. These operations are conducted over a classical channel.

enhances the security of the protocol by bit-sifting the raw key [61]. Then, error correction fixes transmission errors and guarantees the accuracy of the key. After that, Alice and Bob perform reconciliation to align their keys. In the reconciliation process, the difference between keys is identified and fixed, along with any mistakes or eavesdropping [60]. The protocol's security is evaluated in the final step of the process to determine whether the communication is secure or not for further improvement.

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

### 3.1 | Quantum teleportation and its use in the proposed protocol

Quantum teleportation is a technique to transfer a qubit's quantum state without physically moving it. In teleportation, two particles set apart share the same quantum state even at a long distance. Entanglement is essential in quantum teleportation. The basic working procedure of quantum teleportation [62] may be briefly described as follows:

- Alice has a qubit, $|\psi\rangle$, and she teleports the qubit to Bob which is entangled with the state, for instance, $B_{s_{00}}$ and

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{19}$$

where $\alpha$ and $\beta$ are two complex numbers, and they satisfy the relation $|\alpha|^2 + |\beta|^2 = 1$. We have

$$|\psi\rangle = |\psi\rangle \otimes |B_{s_{00}}\rangle \tag{20}$$

This may come from an EPR source, and Alice may share this with Bob.

- Bob receives the entangled qubits shared by Alice. He does not know the quantum state of the qubits.
- Bob adopts Bell state measurement based on the received qubit and classical information sent by Alice over the classical channel. Bob checks which state collapses with the measurement.

The graphical representation of the quantum teleportation circuit or (20) is illustrated in Figure 6.

We have adopted the basic procedure of the quantum teleportation technique in our entanglement-assisted QKD. Kronecker tensor product is applied to a maximally entangled state and randomly generated qubit which produces a density matrix [39]. After that, the controlled-NOT gate or CNOT gate is adopted on our density matrix. CNOT is a quantum gate that can entangle two qubits, and their state will be correlated. CNOT gate is applied to the density matrix, resulting in entangled qubits:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{21}$$

After that, the Hadamard gate is applied to our resulting density matrix. The Hadamard gate is also a quantum gate that can perform a Hadamard transform (a unitary operation that creates superpositions of states) on a qubit.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{22}$$

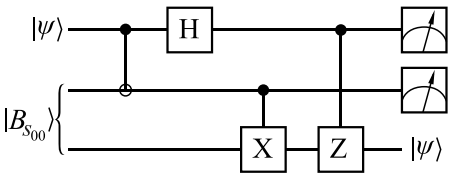


**FIGURE 6** Quantum teleportation circuit [35], comprising Hadamard gates $H$, Pauli-$X$ and $Z$ gates, the input Bell state $|B_{s_{00}}\rangle$ and input quantum state $|\psi\rangle$.

### 3.2 | Quantum Fourier transform in the proposed scheme

Quantum Fourier transform (QFT) is a fundamental quantum technique that is used in a variety of quantum methods, including Shor's algorithm for integer factoring and the quantum phase estimation algorithm. As already mentioned before, the Bell state is a maximally entangled two-qubit state that is useful in quantum communication and quantum computation such as factoring large numbers and searching unsorted databases [63]. Depending on the situation, applying the QFT to a Bell state can have numerous advantages. One possible advantage is that it can construct a superposition of all conceivable values of the Bell state's entanglement parameter. This superposition can subsequently be employed in quantum algorithms such as quantum teleportation and quantum error correction [64, 65]. Therefore, we have applied QFT to the entangled Bell state and passed it across the quantum channel. We can express the QFT [66, 67] by

$$|q\rangle \rightarrow \frac{1}{\sqrt{2^d}} \left( \sum_{c=0}^{2^d-1} \right) \left( e^{\frac{2\pi i}{2^d}} \right)^{u.c} |x\rangle \tag{23}$$

where input quantum states are $|x\rangle = |x_1 x_2 \ldots x_d\rangle$, output quantum states are $|q\rangle = |q_1 q_2 \ldots q_d\rangle$, and number of qubits is $d$, and $u = 0, 1, 2, \ldots, (2^d - 1)$.

Equation (23) can be rewritten [68] as follows:

$$|q_1 q_2 . q_d\rangle \rightarrow \frac{\left(|0\rangle + e^{2\pi i 0.q_d}|1\rangle\right)}{2^{\frac{d}{2}}} \otimes \ldots \otimes \frac{\left(|0\rangle + e^{2\pi i 0.q_1 q_2 \ldots q_d}|1\rangle\right)}{2^{\frac{d}{2}}} \tag{24}$$

Equation (24) defines that $\Theta(n^2)$ quantum gates are required for implementing a QFT circuit. For each qubit, a Hadamard gate is implemented to induce phase at 0 or $\pi$. The phase shift is controlled according to the prior qubits. Furthermore, the IQFT is executed by reversing each quantum gate. The protocol's primary structure remains intact for utilising QFT instead of random $\frac{\pi}{2}$ phase shift as an encryption technique [68]. The predetermined sequence of execution helps to ensure the security of our proposed system.

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

QFT enhances the efficiency of entanglement manipulation and information processing in the proposed system, aiding in the implementation of more advanced cryptographic protocols [69]. QFT can be used as a building block of entanglement in a QKD system [70]. As shown in Figure 4, QFT in the sender (Alice) and IQFT in the receiver (Bob) can utilise basis transformation, thereby providing more resilience to eavesdropping. QFT is also capable of mitigating the error in a noisy channel [69]. In the proposed scheme, QFT is used for detecting basis mismatches, thereby improving the security of the QKD system.

## 3.3 | Quantum channel employed in the scheme

A quantum channel is used for transmitting quantum information. In classical communication, classical information expressed by '0' or '1' is transmitted through the classical channel, whereas quantum information in terms of qubits is sent over the quantum channels. The qubits can also be of multiple states.

### 3.3.1 | Depolarising channel

A depolarising channel can lead to a quantum state, typically to a mixed state. This means that it has a classical probability distribution over pure states. It is typically some sort of noise imposed in the quantum domain and may be mathematically represented as a perfectly positive, trace-preserving map from one density matrix to another. In a depolarising channel, a bit-flip error, phase-flip error, or bit-phase-flip error can occur at equal probabilities. The noise arises due to the climate changes in the free space [71]. The depolarising quantum channel can be mathematically expressed [35] as follows:

$$D_\rho = (1-r)\rho_d + \frac{r}{3}\left(\boldsymbol{X}\rho_d\boldsymbol{X} + \boldsymbol{Y}\rho_d\boldsymbol{Y} + \boldsymbol{Z}\rho_d\boldsymbol{Z}\right) \tag{25}$$

where $\rho_d = |\psi\rangle\langle\psi|$ is the probability density operator and $r$ denotes the depolarising parameter or error probability. The $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{Z}$ are three Pauli gates. The operator $\boldsymbol{X}$ is a NOT gate. A phase shift of $\pi$ radian is applied by the $\boldsymbol{Z}$ operator, and the operator $\boldsymbol{Y}$ is the combination of $\boldsymbol{X}$ and $\boldsymbol{Z}$. Each of the operators $\boldsymbol{X}$, $\boldsymbol{Y}$ and $\boldsymbol{Z}$ is applied with a probability of $\frac{r}{3}$.

$$\boldsymbol{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \boldsymbol{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \boldsymbol{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{26}$$

We can redefine the quantum depolarising channel for our proposed system [35] according to (25) as follows

$$D_\rho = (1-r)\rho_d + \frac{rI_8}{2} \tag{27}$$

where $I_8$ is a $8 \times 8$ unit matrix, $\rho_d$ denotes the original states of Alice, $r$ denotes the depolarisation probability, and $(1-r)$ represents the probability of unchanged states.

## 3.4 | Classical channel

The classical channel in QKD is used for public communication between Alice and Bob for transmitting classical information—measurement outcomes, corrections, control, or synchronisation signals. Alice and Bob need to establish a connection to share their basis even in the presence of Eve. This exchange of information is essential for establishing a secure link.

Bob obtains the measured key bits after measuring the received qubit states. After that, Alice and Bob share their basis sequences. When Bob's basis is different from Alice's basis, they both sift the measured key bit. In this step, various types of classical channels can be adopted [72]. In the proposed protocol, various wireless or optical communication strategies may be adopted. We have considered the orthogonal frequency division multiplexing (OFDM)-based Rayleigh fading channel for our investigations. However, other modulation methods, for example, universal filtered multi-carrier (UFMC), generalised frequency division multiplexing (GFDM) etc., or an optical communication method can be adopted.

## 3.5 | Eve's interception and re-transmission in the proposed protocol

In QKD, it is very important to exchange keys between parties without any intrusion. In QKD, including the BB84 protocol, eavesdroppers, also known as 'Eve', are one of the most significant security threats. Eavesdroppers intrude during transmission and gather information about quantum states without detection. As a result, it disrupts the process of distributing keys [73]. Eve can employ various types of techniques to intrude, including photon absorption, re-transmission, and the creation of replicas of the intercepted photons for future measurement [74, 75].

### 3.5.1 | Eve's measurement

After intercepting the quantum states, Eve measures Alice's states in the quantum channel first before sending them to Bob to extract encoded information from quantum states. Eve can select to measure the intercepted photons on either a rectilinear or diagonal basis. Since Eve is unaware of Alice's qubit states, the basis sequences are generated [75], and the probability of correctly predicting the states is 25%.

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

### 3.5.2 | Detection of Eve's presence

As already mentioned above, Eve selects the basis randomly based on Heisenberg's uncertainty principle and no-cloning theorem, and the measurements disrupt the quantum states and introduce errors in communication [73, 75, 76]. As a result, Eve's intrusion will be detected or identified in the reconciliation process. If the error rate exceeds the threshold value, then the intrusion can be ascertained. Under these circumstances, the compromised key will be discarded, and the communication will be aborted.

## 3.6 | The proposed method for secure wireless systems

The proposed QKD protocol offers a promising solution for providing enhanced security to next-generation wireless systems. As wireless communication systems evolve, quantum technologies such as entangled QKD with teleportation can play a crucial role in securing the information exchanged over these networks. Quantum security mechanisms provide a future-proof solution against potential threats posed by quantum computers, which could compromise classical cryptographic systems.

As a key enabler of the sixth generation (6G) wireless system, quantum communication will harness the properties of entangled photons to provide secure communication across any distance [37, 40]. Mainly, three types of quantum-secured communication systems are envisioned for 6G and beyond wireless systems—quantum-secured direct communication (QSDC), quantum-secured indirect communication (QSIC), and QKD [37, 39, 77]. Among the three, QKD is the most-researched type of the communication method, where the secret key allocated by QKD is used to encrypt the classical information, and the resulting ciphertext is transmitted to the receiver.

QKD protocols differ based on the principles, techniques, and resources they use. The proposed protocol provides security for next-generation wireless systems through a combination of quantum principles and cryptographic techniques. Specifically, entanglement forms the foundation for quantum communication. Entangled particles exhibit correlations that are stronger than any classical correlations, allowing for the creation of secure quantum keys. Additionally, quantum teleportation enables the secure transfer of quantum states over long distances without physically transmitting the particles. This is crucial for next-generation wireless systems where communication spans large geographical areas. Furthermore, QFT provides an efficient way to perform basis transformations in the quantum domain. In the context of QKD, QFT facilitates the conversion of quantum states between different bases, enhancing the security of the key distribution process. The performance of the QKD protocol is improved in a noisy channel due to the employment of QFT because QFT provides increased robustness against all types of operational errors—bit-flip, phase-flip, and phase-change error [69].

With the increasing number of users and to cater to the user demands, new enabling technologies for the 6G are being developed at a breathtaking speed. The proposed QKD protocol offers a powerful and secure method for exchanging cryptographic keys in the context of 6G technologies incorporating terahertz (THz) communication, reconfigurable intelligent surfaces (RIS), joint sensing and communications, multi-carrier modulation, and non-orthogonal multiple access (NOMA) [40]. The designs of the QKD algorithms proposed for these systems can be found in Refs. [37, 78–81]. Exploiting entanglement with the aid of the proposed design may also ensure the security of the key exchange process. Thus, the proposed QKD protocol remains a vital component in safeguarding the integrity of communication channels against emerging cyber threats. Since the proposed protocol allows users to share quantum information without observing it, a quantum Internet might be useful for establishing global cooperation in quantum computation [57].

# 4 | PERFORMANCE METRICS

In this section, we provide a brief description of the performance metrics used for the investigation of the proposed quantum communication scheme. Specifically, the performance metrics are the quantum bit error rate (QBER), secure key rate (SKR), reconciliation efficiency, the lower bound of security, and the conventional bit error rate (BER) of classical communication systems.

## 4.1 | Quantum bit error rate

In a QKD-based quantum communication system, QBER refers to the transmission quality of the signal received. QBER is the ratio of error qubits to the total number of qubits sent [82]. Lower QBER implies that the transmission is reliable and the receiver receives transmitted quantum information correctly. By contrast, higher QBER represents significant errors during communication which may result in corrupted and incorrect information. Therefore, the conservation of lower QBER is of utmost importance [83] for the successive communication of quantum information.

Following the measurement of received states in a QKD system, Bob responds to Alice over a classical channel to be sure that his measured key sequences are the same as those of Alice. By computing QBER, it can be detected whether eavesdropping has occurred. If the QBER is higher than the maximum accepted rate, the communication will terminate. The QBER in the presence of Eve's interception can be expressed [84] as follows:

$$Q_{\mathrm{BER}} = e_{\mathrm{Eve}}(1 - e_{ch}) + e_{ch}(1 - e_{\mathrm{Eve}}), \tag{28}$$

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

where $e_{cb}$ denotes the error probability of the channel and $e_{\text{Eve}}$ represents the error probability due to Eve's interception. When there is no interception of Eve, Eve's attack level can be expressed by $\Im = 0$, and the $Q_{\text{BER}}$ will be $e_{cb}$.

In our proposed system, we have computed $Q_{\text{BER}}$ for simulating QBER performance for various parameters and also done numerical analysis. $Q_{\text{BER}}$ is calculated in the post-processing scheme. Several processes take place in our system, such as sifting, discarding missed matches, error counting, and finally $Q_{\text{BER}}$ calculation.

## 4.2 | Secure key rate

The secure key rate (SKR) of a quantum information system can be defined by the ratio of the secret key length to the number of signals sent through the channel while two parties are communicating in the presence of eavesdroppers. That means that SKR can be expressed as the proportion of secure key length to the number of signals that pass through the channel [85]. The secure key rate without Eve's attack can be computed in terms of the QBER in an asymptotic scenario [86] as follows:

$$K_{sr} = 1 - H(Q_{\text{BER}}), \tag{29}$$

where $K_{sr}$ denotes the SKR, and $H$ refers to the binary entropy function.

## 4.3 | Lower bound of security and reconciliation efficiency

The lower bound of security is a security measure of QKD when the mutual information of Alice and Bob $I(\text{Alice}\,;\,\text{Bob})$ is higher than the mutual information of Alice and Eve $I(\text{Alice}\,;\,\text{Bob})$ [86, 87].

The mutual information of Alice and Bob [84] is given by

$$I(\text{Alice}\,;\,\text{Bob}) = H(\text{Alice}) - H(\text{Alice}\,|\text{Bob}), \tag{30}$$

where $H(\text{Alice}) = 1$ and $H(\text{Alice}\,|\,\text{Bob})$ are the Shannon entropy between Alice and Bob which is the $Q_{\text{BER}}$ from (28). Therefore, substituting the value of $H(\text{Alice})$ in (30), we have

$$I(\text{Alice}\,;\,\text{Bob}) = 1 - H(Q_{\text{BER}}). \tag{31}$$

Accordingly, the mutual information of Alice and Eve may be written as follows:

$$I(\text{Alice}\,;\,\text{Eve}) = 1 - H\left(\frac{1}{2} - e_{\text{Eve}}\right). \tag{32}$$

Hence, the lower bound of security can be expressed as [86] follows:

$$L_{bs} : I(\text{Alice}\,;\,\text{Eve}) < I(\text{Alice}\,;\,\text{Bob}) \tag{33}$$

$$L_{bs} : 1 - H(Q_{\text{BER}}) > 1 - H\left(\frac{1}{2} - e_{\text{Eve}}\right) \tag{34}$$

$$L_{bs} : H(Q_{\text{BER}}) < H\left(\frac{1}{2} - e_{\text{Eve}}\right) \tag{35}$$

Equation (35) can be further simplified as [84] follows:

$$L_{bs} : r < \frac{4(1-\Im)}{3(2-\Im)}. \tag{36}$$

It is apparent from (36) that by decreasing the depolarising parameter $r$, the lower bound of security can be obtained.

On the other hand, reconciliation refers to the error correction operation carried out through a public channel. In reconciliation, the error between the generated key and the received keys is resolved. Reconciliation efficiency or the error correction capability directly impacts the overall performance of the QKD system in terms of both key generation rate and error rate [35]. Several factors including the QBER, Eve's attack level, target SKR, and security level influence the lower bound of reconciliation efficiency. To calculate the lower bound of reconciliation efficiency $\eta_{lb}$, we need to compute the target SKR $K_{tr}$ and the theoretical SKR $Kth$ first.

The theoretical secret key rate $Kth$ is the difference between $I$(Alice; Bob) and $I$(Alice; Eve) [84].

$$K_{th} = H\left(\frac{1}{2} - e_{\text{Eve}}\right) - H(Q_{\text{BER}}). \tag{37}$$

If the theoretical secret key rate is greater than the user-defined target secret key rate, we can obtain the reconciliation efficiency. Otherwise, the depolarisation parameter will need to be decreased. The lower bound of reconciliation efficiency can be expressed [84] as follows:

$$\eta_{lb} = H(Q_{\text{BER}})\frac{\frac{1}{2} - e_{\text{Eve}}}{K_{tr}}. \tag{38}$$

For post-processing reconciliation protocols, the value of $\eta_{lb}$ is less than 1.

## 4.4 | Bit error rate of classical channel

The classical communication channel is used to transmit the measured bits. For our investigations, we have used an OFDM-based communication system over a Rayleigh fading wireless channel for the transmission of the measured bits. We have also simulated the BER performance of the classical channel as a function of the channel's signal-to-noise ratio (SNR).

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

## 5 | SIMULATION RESULTS AND DISCUSSION

In this section, we discuss the simulated performances of the proposed system and compare it to the existing methods. We have used MATLAB 2019a for our simulations to measure the performance.

Figure 7 shows the QBER performance of the entanglement-assisted QKD system with and without Eve's interception. The QBER performance of the proposed protocol is also shown in Figure 7, where the QBER is measured with different depolarising parameters, $r$ using (28). We also compare the QBER of the proposed protocol with that of the EnQuad [84] system. According to Figure 7, the QBER decreases significantly as the SNR of the classical increases in both scenarios. Furthermore, we also observe that the proposed protocol outperforms EnQuad. As expected, the QBER performance without the presence of Eve's interception is better than that with Eve's interception.

Figure 8 shows both SKR and QBER performance of the proposed scheme for different Eve attack levels $\Im$. SKR is evaluated using (29) and (37), where QBER is required for obtaining a value of the corresponding SKR. In Figure 8 the SKR and QBER performance is shown for the proposed protocol and that of the EnQuad. As observed from Figure 8, there is an inverse relationship between the SKR and the QBER performances. That means that as the QBER increases, the SKR decreases significantly in both scenarios.

To investigate the SKR versus QBER performance as depicted in Figure 8, we use the binary entropy-related equations (29) and (37). As another theoretical benchmark, the achievable SKR can be expressed for the BB84 protocol with two equiprobable states as [86]:

$$K_{sr} = -\log_2\left[\frac{1}{2}\left(1 + 2\sqrt{(1 - Q_{\mathrm{BER}})Q_{\mathrm{BER}}}\right)\right], \qquad (39)$$

where $K_{sr}$ and $Q_{\mathrm{BER}}$ denote the SKR and QBER, respectively. This analytical performance is also shown in Figure 8 as a benchmark for this performance results. We see that the numerical results for the proposed scheme have a similar relationship to the BB84 protocol. However, the SKR of the proposed protocol as dictated by (29) and (37) has a higher value than that of the BB84 given by (39) for all the QBER values.

Figure 9 depicts the SKR and the QBER performance against the signal-to-noise ratio (SNR) of the proposed scheme in a single plot. As expected, when the SNR of the classical channel increases, the SKR also increases and, QBER decreases. This is because a higher SNR means that the quantum information is less likely to be corrupted by noise. Therefore, QBER will decrease and SKR will increase. A higher QBER refers to more detection errors, which indicates that secure key extraction becomes more complicated.

Figure 10 depicts the BER performance for transmitting basis sequences between Alice and Bob over a Rayleigh fading

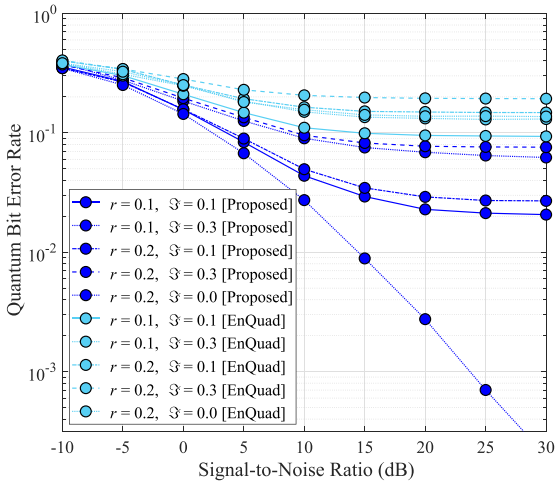


**FIGURE 7** Quantum bit error rate (QBER) performance of entanglement-assisted quantum key distribution (QKD) system for various levels of Eve's attack and different depolarising parameters.

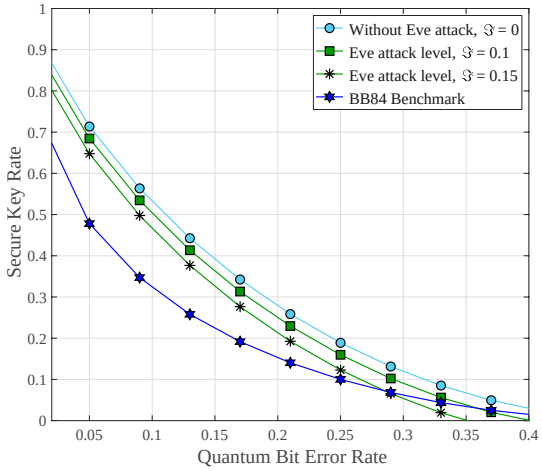


**FIGURE 8** Performance between secure key rate (SKR) and quantum bit error rate (QBER) for different Eve attack levels.

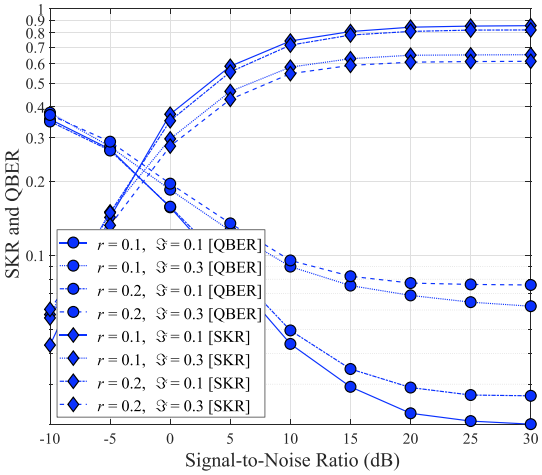


**FIGURE 9** The secure key rate (SKR) and quantum bit error rate (QBER) performance of the proposed protocol in a single plot.

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

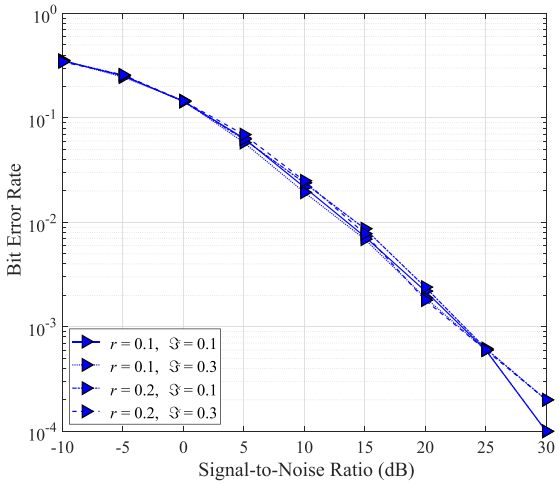


**FIGURE 10** Bit error rate (BER) performance for transmitting basis sequences over the classical channel for different depolarising parameters and Eve's attack levels.

channel for different depolarising parameters $r$ and Eve attack levels $\Im$. Figure 10 shows that BER decreases as SNR increases. The BER performance is consistent across all depolarising parameters and Eve attack levels since the basis sequences are sent through the same classical channel parameters. It is plausible that the BER performance of the classical channel indicated by Figure 10 will remain unaffected by Eve's attack and the quantum channel parameters.

Table 2 shows the numerical results for the proposed entanglement-assisted QKD system. Table 2 also compares the performance of the proposed protocol with that of the BB84 protocol simulator EnQuad [84]. The number of photons, depolarising parameters, and Eve's attack levels of the proposed scheme have been considered. The security level represents whether the scheme is secure from Eve's interception or not. If the communication is secure, the post-processing scheme is continued—otherwise, the communication is terminated.

In a nutshell, our simulations compare the entanglement- and teleportation-aided protocol with the relevant QKD protocols regarding SKR, QBER, security against attacks, and resistance to noise and errors. The results promise improved SKR, increased security against attacks, and improved resilience against noise.

## 6 | CHALLENGES AND LIMITATIONS OF THE PROPOSED PROTOCOL

The proposed QKD protocol offers remarkable security promises—however, its implementation in real-world scenarios poses a range of significant challenges. The major challenges and limitations are outlined below.

1. Decoherence and noise: It is technically challenging to generate and distribute fully entangled qubit pairs over a long distance due to environmental noise and decoherence. As already described in Section 2.8, decoherence refers to the phenomenon of the quantum system's interaction with its environment and the consequent collapse of its quantum state and loss of its entanglement. Moreover, QKD is more sensitive to noise [88]; therefore, the entangled state's fidelity can be reduced significantly due to quantum channel noise. Additionally, the practical implementation of teleportation-aided QKD will face challenges, such as various imperfections, scattering, background noise, temperature fluctuations, vibrations, etc [89]. The proposed protocol employs quantum teleportation, which might reduce these deleterious effects. However, it remains susceptible to external noise and interference, particularly during the creation of entangled states and measurement processes. Mitigating these effects is crucial for maintaining the fidelity of the quantum states [37].
2. Typical Distance: Optical fibre is the primary medium for QKD and a measurement-device-independent fibre-based QKD is shown to support a 404 km distance [90]. Advanced quantum repeaters may be used to increase the distance [32]. Entanglement-aided QKD is demonstrated to provide wireless security up to a distance of 1000 km [37]. However, the proposed protocol uses quantum teleportation and QFT. Consequently, key distribution at a longer distance might be possible—however, considering the limited distance due to the classical channel communication, enormously long-distance communication might not be feasible.
3. Device miniaturisation: The miniaturisation of quantum devices is a real-world challenge for the proposed scheme. Chip-scale miniaturisation is a requirement to provide quantum security for next-generation smartphones, wristwatches, and tablets [37]. Low-cost mass production of the chip-scale QKD relying on the proposed protocol is a practical challenge [91].
4. Quantum memory: Efficient and reliable quantum memories can store entangled quantum states for a long time [92]. However, according to the requirement, there is a scarcity of appropriate quantum memories to develop QKD protocols. Moreover, existing quantum memories have issues with narrow storage times for essential processing. For this reason, quantum communication systems cannot be feasible.
5. Synergy between Classical and Quantum communications: For the proper functioning of the protocol, the quantum and the classical system must co-exist. The quantum operations must require assistance from classical communication for sharing important information. Quantum operations are comparatively more fragile, and a quantum-classical synergy is essential to protect the system from attacks against, for example, quantum repeaters [39, 93].

In addition to the above-mentioned practical challenges and limitations, there are some other implementation challenges of the proposed scheme. For example, the generation of entangled qubits or EPR pais, the reduction of the complexity associated with the QFT and IQFT implementation, and the

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

**TABLE 2** Numerical results for various parameters of entanglement-assisted quantum key distribution (QKD).

| Depolarising parameter, $r$Eve attack level, $\Im$ | Scheme | Theoretical key rate, $Kth$ | Asymptotic secure key rate, $K_{sr}$ | QBER, $Q_{BER}$ | Leakage bits, $l_b$ | Reconciliation efficiency, $\eta_{lb}$ | Security level |
|---|---|---|---|---|---|---|---|
| $r = 0.1$ | Proposed | 0.382 | 0.854 | 0.020 | 3314.6 | 0.969 | Secure |
| $\Im = 0.1$ | EnQuad | 0.382 | 0.552 | 0.093 | 3102.8 | 0.940 | |
| $r = 0.1$ | Proposed | 0.285 | 0.651 | 0.062 | 3615.6 | 0.961 | Secure |
| $\Im = 0.3$ | Enquad | 0.285 | 0.441 | 0.130 | 3529.8 | 0.963 | |
| $r = 0.2$ | Proposed | 0.145 | 0.821 | 0.026 | 4289.8 | 0.963 | Secure |
| $\Im = 0.1$ | EnQuad | 0.145 | 0.441 | 0.147 | 4275.8 | 0.991 | |
| $r = 0.2$ | Proposed | 0.100 | 0.395 | 0.075 | 4540.7 | 0.960 | Secure |
| $\Im = 0.3$ | EnQuad | 0.100 | 0.292 | 0.193 | 4470.9 | 0.995 | |
| $r = 0.2$ | Proposed | 0.163 | 0.997 | $0.197e^{-03}$ | 1972.0 | 0.982 | Secure |
| $\Im = 0$ | EnQuad | 0.163 | 0.443 | 0.129 | 2227.6 | 0.977 | |
| $r = 0.2$ | Proposed | - | - | 0.173 | - | - | Insecure |
| $\Im = 0.7$ | EnQuad | - | - | 0.261 | - | - | |

cost-effectiveness are some of the potential challenges. The standardisation of the associated protocols, components, and infrastructure has to be promoted to facilitate interoperability and scalability [91, 94].

## 7 | CONCLUSION

An entanglement-assisted and teleportation-inspired QKD system has been conceived to provide security in wireless systems. By leveraging the unique properties of quantum entanglement and quantum teleportation, this system combines classical and quantum technologies to enhance its efficacy and practicality. The proposed system incorporates OFDM modulation in the classical channel to exchange measured data. The system has been thoroughly evaluated using numerical simulations to examine key metrics such as QBER, BER, SKR, and reconciliation efficiency. The simulation results have been compared with those using the BB84 protocol simulator EnQuad [84]. The results have demonstrated the system's robustness against quantum noise and classical interference. To further enhance the system's efficiency and security, extensive experiments and exploration of alternative quantum channels can be conducted. Additionally, more sophisticated error correction techniques can be developed to improve reconciliation efficiency. Overall, this study has significant potential in ensuring the confidentiality and integrity of data transmission in an increasingly interconnected world.

## AUTHOR CONTRIBUTIONS

**Md. Ferdous Ahammed**: Conceptualisation; investigation, methodology; software; writing – original draft. **Mohammad Ismat Kadir**: Conceptualisation; investigation; methodology; supervision; writing – review and editing.

## ACKNOWLEDGEMENTS

The authors acknowledge helpful suggestions from the anonymous reviewers.

## CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflict of interest.

## DATA AVAILABILITY STATEMENT

Data sharing is not applicable—no new data is generated.

## ORCID

*Mohammad Ismat Kadir* https://orcid.org/0000-0003-2828-6808

## REFERENCES

1. Boccardi, F., et al.: Five disruptive technology directions for 5G. IEEE Commun. Mag. 52(2), 74–80 (2014)
2. Khan, R., et al.: A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. IEEE Commun. Surv. Tutorials 22(1), 196–248 (2020). https://doi.org/10.1109/comst.2019.2933899
3. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994)
4. Gisin, N., et al.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145–195 (2002). https://doi.org/10.1103/revmodphys.74.145
5. Lo, H.K., Curty, M., Tamaki, K.: Secure quantum key distribution. Nat. Photon. 8(8), 595–604 (2014). https://doi.org/10.1038/nphoton.2014.149
6. Imre, S.: Quantum communications: explained for communication engineers. IEEE Commun. Mag. 51(8), 28–35 (2013). https://doi.org/10.1109/mcom.2013.6576335
7. Wiesner, S.: Conjugate coding. ACM Sigact. New. 15(1), 78–88 (1983). https://doi.org/10.1145/1008908.1008920
8. Martinez, J.E.: Decoherence and Quantum Error Correction for Quantum Computing and Communications (2022). arXiv:220208600
9. Peev, M., et al.: A novel protocol-authentication algorithm ruling out a man-in-the-middle attack in quantum cryptography. Int. J. Quant. Inf. 03(01), 225–231 (2005). https://doi.org/10.1142/s0219749905000797

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

10. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, p. 175. India (1984)
11. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299(5886), 802–803 (1982). https://doi.org/10.1038/299802a0
12. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67(6), 661–663 (1991). https://doi.org/10.1103/physrevlett.67.661
13. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. 68(5), 557–559 (1992). https://doi.org/10.1103/physrevlett.68.557
14. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121–3124 (1992). https://doi.org/10.1103/physrevlett.68.3121
15. Muller, A., Breguet, J., Gisin, N.: Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. Europhys. Lett. 23(6), 383 (1993)
16. Townsend, P.D., Rarity, J., Tapster, P.: Single photon interference in 10 km long optical fibre interferometer. Electron. Lett. 7(29), 634–635 (1993)
17. Gobby, C., Yuan, a, Shields, A.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. 84(19), 3762–3764 (2004)
18. Zhang, Y., et al.: Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys. Rev. Lett. 125, 010502 (2020)
19. Zapatero, V., et al.: Advances in device-independent quantum key distribution. NPJ Quan. Inf. 9(1) (2023)
20. Acín, A., et al.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. 98(23) (2007). https://doi.org/10.1103/physrevlett.98.230501
21. Bechmann-Pasquinucci, H., Gisin, N.: Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phys. Rev. 59(6), 4238 (1999)
22. Scarani, V., et al.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. 92(5), 057901 (2004)
23. Gisin, N., et al.: Towards Practical and Fast Quantum Cryptography (2004). quant-ph/0411022
24. Stucki, D., et al.: Fast and simple one-way quantum key distribution. Appl. Phys. Lett. 87(19), 194108 (2005)
25. Khan, M.M., Murphy, M., Beige, A.: High error-rate quantum key distribution for long-distance communication. New J. Phys. 11(6), 063043 (2009)
26. Serna, E.H.: Quantum Key Distribution from a Random Seed (2013). arXiv:13111582
27. Abushgra, A., Elleithy, K.: Initiated decoy states in quantum key distribution protocol by 3 ways channel. In: 2015 Long Island Systems, Applications and Technology, pp. 1–5 (2015)
28. Kimble, H.J.: The quantum internet. Nature 453(7198), 1023–1030 (2008). https://doi.org/10.1038/nature07127
29. Rozenman, G.G., et al.: The quantum internet: a synergy of quantum information technologies and 6G networks. IET Quan. Commun. 4(4), 147–166 (2023). https://doi.org/10.1049/qtc2.12069
30. Chowdhury, M.Z., et al.: 6G wireless communication systems: applications, requirements, technologies, challenges, and research directions. IEEE Open J. Commun. Soc. 1, 957–975 (2020). https://doi.org/10.1109/ojcoms.2020.3010270
31. Boone, K., et al.: Entanglement over global distances via quantum repeaters with satellite links. Phys. Rev. A. 91(5), 052325 (2015). https://doi.org/10.1103/physreva.91.052325
32. Azuma, K., et al.: Quantum repeaters: from quantum networks to the quantum internet. Rev. Mod. Phys. 95(4), 045006 (2023). https://doi.org/10.1103/revmodphys.95.045006
33. Bloom, Y., et al.: Quantum cryptography: a simplified undergraduate experiment and simulation. Physics 4(1), 104–123 (2022). https://doi.org/10.3390/physics4010009
34. Cacciapuoti, A.S., et al.: Quantum internet: networking challenges in distributed quantum computing. IEEE Netw. 34(1), 137–143 (2019). https://doi.org/10.1109/mnet.001.1900092
35. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2010)
36. Bennett, C.H., et al.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993). https://doi.org/10.1103/physrevlett.70.1895
37. Zhou, X., et al.: Towards Quantum-Native Communication Systems: New Developments, Trends, and Challenges (2023). ArXiv. 2023;abs/2311.05239
38. Ren, J.G., et al.: Ground-to-satellite quantum teleportation. Nature 549(7670), 70–73 (2017). https://doi.org/10.1038/nature23675
39. Li, Z., et al.: Entanglement-assisted quantum networks: mechanics, enabling technologies, challenges, and research directions. IEEE Commun. Surv. Tutor. 25(4), 2133–2189 (2023). https://doi.org/10.1109/comst.2023.3294240
40. Ali, M.Z., et al.: Quantum for 6G communication: a perspective. IET Quan. Commun. 4(3), 112–124 (2023). https://doi.org/10.1049/qtc2.12060
41. Hasan, S.R., et al.: Quantum communication systems: vision, protocols, applications, and challenges. IEEE Access 11, 15855–15877 (2023). https://doi.org/10.1109/access.2023.3244395
42. Saad, H.M., et al.: Quantum-inspired genetic algorithm for resource-constrained project-scheduling. IEEE Access 9, 38488–38502 (2021). https://doi.org/10.1109/access.2021.3062790
43. Amiri, P.K.: Quantum computers. IEEE Potentials 21(5), 6–9 (2003). https://doi.org/10.1109/mp.2002.1166617
44. Wie, C.R.: Two-qubit Bloch sphere. Physics 2(3), 383–396 (2020). https://doi.org/10.3390/physics2030021
45. Broadbent, A., Schaffner, C.: Quantum cryptography beyond quantum key distribution. Des. Codes Cryptogr. 78(1), 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4
46. Maeda, W., et al.: Technologies for quantum key distribution networks integrated with optical communication networks. IEEE J. Sel. Top. Quant. Electron. 15(6), 1591–1601 (2009). https://doi.org/10.1109/jstqe.2009.2032664
47. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. science 283(5410), 2050–2056 (1999). https://doi.org/10.1126/science.283.5410.2050
48. Heisenberg, W.: Physics and Philosophy: The Revolution in Modern Science. Harper Collins (1958)
49. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. 47(10), 777–780 (1935). https://doi.org/10.1103/physrev.47.777
50. Schrödinger, E.: Discussion of probability relations between separated systems. Math. Proc. Camb. Phil. Soc. 31(4), 555–563 (1935). https://doi.org/10.1017/s0305004100013554
51. Schrödinger, E.: Probability relations between separated systems. Math. Proc. Camb. Phil. Soc. 32(3), 446–452 (1936). https://doi.org/10.1017/s0305004100019137
52. Press release: NobelPrize.org. Nobel Prize Outreach AB 2024 2022. Sat (2024)
53. Gupta, M., Nene, M.J.: Quantum computing: an entanglement measurement. In: 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), pp. 1–6 (2020)
54. Singh, H., Gupta, D.L., Singh, A.K.: Quantum key distribution protocols: a review. J. Comput. Eng. 16(2), 1–9 (2014). https://doi.org/10.9790/0661-162110109
55. Bell, J.S.: On the Einstein Podolsky rosen paradox. Phys. Physique Fizika 1(3), 195–200 (1964). https://doi.org/10.1103/physicsphysiquefizika.1.195
56. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85(2), 441–444 (2000). https://doi.org/10.1103/physrevlett.85.441
57. Shannon, K., Towe, E., Tonguz, O.K.: On the Use of Quantum Entanglement in Secure Communications: A Survey (2020). arXiv.07907
58. Jozsa, R.: Fidelity for mixed quantum states. J. Mod. Opt. 41(12), 2315–2323 (1994). https://doi.org/10.1080/09500349414552171


26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

59. Li, Y., James, M.: Equalization for linear quantum channels. In: 2017 IEEE 56th Annual Conference on Decision and Control (CDC);, pp. 6161–6164 (2017)
60. Ma, X., Lütkenhaus, N.: Improved Data Post-Processing in Quantum Key Distribution and Application to Loss Thresholds in Device Independent QKD (2011). arXiv:11091203
61. Li, Q., et al.: Efficient bit sifting scheme of post-processing in quantum key distribution. Quant. Inf. Process. 14(10), 3785–3811 (2015). https://doi.org/10.1007/s11128-015-1035-8
62. Bouwmeester, D., et al.: Experimental quantum teleportation. Nature 390(6660), 575–579 (1997). https://doi.org/10.1038/37539
63. Song, X., et al.: Bell's measure and implementing quantum Fourier transform with orbital angular momentum of classical light. Sci. Rep. 5(1), 14113 (2015). https://doi.org/10.1038/srep14113
64. Kitaev, A.Y.: Quantum Measurements and the Abelian Stabilizer Problem (1995). quant-ph/9511026
65. Gottesman, D.: Stabilizer Codes and Quantum Error Correction. California Institute of Technology (1997)
66. Mastriani, M.: Quantum Fourier transform is the building block for creating entanglement. Sci. Rep. 11(1), 22210 (2021). https://doi.org/10.1038/s41598-021-01745-x
67. Tan, X., et al.: Quantum key distribution protocol using quantum fourier transform. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, pp. 96–101 (2015)
68. Nagy, M., Akl, S.G.: Coping with decoherence: parallelizing the quantum Fourier transform. Parallel Process. Lett. 20(03), 213–226 (2010). https://doi.org/10.1142/s012962641000017x
69. Mastriani, M.: Entanglement parallelization via quantum fourier transform. Adv. Quan. Tech. 6(10), 2300022 (2023). https://doi.org/10.1002/qute.202300022
70. Mastriani, M.: Quantum Fourier transform is the building block for creating entanglement. Sci. Rep. 11(1), 22210 (2021). https://doi.org/10.1038/s41598-021-01745-x
71. Jeong, Y.C., Kim, Y.S., Kim, Y.H.: Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols. Laser Phys. 21(8), 1438–1442 (2011). https://doi.org/10.1134/s1054660x11150126
72. Adu-Kyere, A., Nigussie, E., Isoaho, J.: Quantum key distribution: modeling and simulation through BB84 protocol using Python3. Sensors 22(16), 6284 (2022). https://doi.org/10.3390/s22166284
73. Lütkenhaus, N.: Security against eavesdropping in quantum cryptography. Phys. Rev. 54(1), 97–111 (1996). https://doi.org/10.1103/physreva.54.97
74. Elboukhari, M., Azizi, M., Azizi, A.: Quantum key distribution protocols: a survey. Int. J. Universal Comput. Sci. 1(2) (2010)
75. Ekert, A.K., et al.: Eavesdropping on quantum-cryptographical systems. Phys. Rev. A. 50(2), 1047–1056 (1994). https://doi.org/10.1103/physreva.50.1047
76. Huttner, B., Ekert, A.K.: Information gain in quantum eavesdropping. J. Mod. Opt. 41(12), 2455–2466 (1994). https://doi.org/10.1080/09500349414552301
77. Chandra, D., et al.: Direct quantum communications in the presence of realistic noisy entanglement. IEEE Trans. Commun. 70(1), 469–484 (2022). https://doi.org/10.1109/tcomm.2021.3122786
78. Kundu, N.K., et al.: MIMO terahertz quantum key distribution under restricted eavesdropping. IEEE Trans. Quan. Eng. 4, 1–15 (2023). https://doi.org/10.1109/tqe.2023.3264638
79. Bahrani, S., Razavi, M., Salehi, J.A.: Orthogonal frequency-division multiplexed quantum key distribution. J. Lightwave Technol. 33(23), 4687–4698 (2015). https://doi.org/10.1109/jlt.2015.2476821
80. Kisseleff, S., Chatzinotas, S.: Trusted reconfigurable intelligent surface for multi-user quantum key distribution. IEEE Commun. Lett. 27(8), 2237–2241 (2023). https://doi.org/10.1109/lcomm.2023.3291052
81. Yu, X., et al.: A NOMA-Based quantum key distribution system over Poisson atmospheric channels. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2019)
82. Kumar, P., Prabhakar, A.: Bit error rates in a frequency coded quantum key distribution system. Opt Commun. 282(18), 3827–3833 (2009). https://doi.org/10.1016/j.optcom.2009.06.030
83. Scarani, V., et al.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301–1350 (2009). https://doi.org/10.1103/revmodphys.81.1301
84. Abdelgawad, M.S., Shenouda, B.A., Abdullatif, S.O.: EnQuad: a publicly-available simulator for quantum key distribution protocols. Cybern. Inf. Technol. 20(1), 21–35 (2020). https://doi.org/10.2478/cait-2020-0002
85. Cai, R.Y.Q., Scarani, V.: Finite-key analysis for practical implementations of quantum key distribution. New J. Phys. 11(4), 045024 (2009). https://doi.org/10.1088/1367-2630/11/4/045024
86. Bratzik, S., et al.: Min-entropy and quantum key distribution: Nonzero key rates for "small" numbers of signals. Phys. Rev. 83(2), 022330 (2011). https://doi.org/10.1103/physreva.83.022330
87. Diffie, W., Hellman, M.E.: New directions in cryptography. In: Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pp. 365–390. Association for Computing Machinery (2022)
88. Wilde, M.M.: 4. in: The Noisy Quantum Theory, pp. 97–140. Cambridge University Press (2013)
89. Oh, S., Lee, S., Lee, Hw: Fidelity of quantum teleportation through noisy channels. Phys. Rev. A. 66(2), 022316 (2002). https://doi.org/10.1103/physreva.66.022316
90. Yin, H.L., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. 117(19), 190501 (2016). https://doi.org/10.1103/physrevlett.117.190501
91. Diamanti, E., et al.: Practical challenges in quantum key distribution. Npj Quan. Inf 2(1), 16025 (2016). https://doi.org/10.1038/npjqi.2016.25
92. Simon, C., et al.: Quantum memories: a review based on the European integrated project 'Qubit Applications (QAP). The Eur. Phys. J. D 58(1), 1–22 (2010). https://doi.org/10.1140/epjd/e2010-00103-y
93. Cacciapuoti, A.S., et al.: When entanglement meets classical communications: quantum teleportation for the quantum internet. IEEE Trans. Commun. 68(6), 3808–3833 (2020). https://doi.org/10.1109/tcomm.2020.2978071
94. Liu, R., et al.: Towards the industrialisation of quantum key distribution in communication networks: a short survey. IET Quant. Commun. 3(3), 151–163 (2022). Portico. https://doi.org/10.1049/qtc2.12044


**How to cite this article:** Ahammed, M.F., Kadir, M.I.: Entanglement and teleportation in quantum key distribution for secure wireless systems. IET Quant. Comm. 5(4), 551–566 (2024). https://doi.org/10.1049/qtc2.12092

26328925, 2024, 4, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12092, Wiley Online Library on [06/01/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License