Proceedings of the 4th International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/86/2025.20340

A Study on Security in Mode-Pairing and Sending-or-Not-Sending Quantum Key Distribution Protocols

Yaping Wang[1,a,*]

[1]*Ziyang Yanjiang No.1 Middle School, Ziyang, 641300, China*
a. Granate_@outlook.com
**corresponding author*

Abstract: In recent years, quantum key distribution (QKD) protocols have undergone rapid evolution, thus significantly advancing the field of quantum communications. The exploitation of quantum properties enables quantum communication to achieve superior security, yet many traditional protocols still face challenges in terms of stability and practicality. Since 2019, two new QKD protocols have emerged: mode-pairing QKD and sending-or-not-sending TF-QKD. In this paper, through an in-depth analysis of the existing literature, a simple mathematical derivation of the quantum uncertainty relation is provided, along with a systematic summary of the process for proving the security of these two new protocols. The results demonstrate that sending-or-not-sending TF-QKD can still effectively ensure the security of information in the presence of large bit error rates, showing its potential application in quantum communication. In addition, the paper explores future research directions, including experimental validation in diverse real-world environments, performance optimization, and the development of robust error correction techniques. These studies provide a critical foundation for the practicalization of QKD and promote the further development of quantum communication technology.

Keywords: Quantum Communication, Quantum Key Distribution (QKD), Mode-Pairing QKD, Sending-or-Not-Sending TF-QKD

1. Introduction

The quantum communication, as an emerging method of information transmission, employs the core principles of quantum mechanics to achieve greater security compared to conventional communication methods. The theoretical foundation of quantum communication has progressively developed since Stephen Wisner proposed the concept of multiplexed channels with quantum currency and conjugate coding in 1969 [1]. The BB84 (Bennett-Brassard 1984) protocol, one of the earliest proposed quantum key distribution (QKD) protocols, lays down the theoretical framework for quantum communication [2]. However, despite the ongoing introduction of various QKD protocols, many traditional protocols still encounter significant challenges related to stability and practical implementation. In recent years, two new QKD protocols, mode-pairing QKD and sending-or-not-sending TF-QKD, have emerged as a result of in-depth research and technological advances. These two protocols excel in the security and practicality of quantum communication, and especially demonstrate their unique advantages in coping with high bit error rates. Nonetheless, the relevant research on these two protocols is still limited, and the theoretical and experimental data are not yet

DOI: 10.54254/2753-8818/86/2025.20340

sufficient. Therefore, this paper aims to examine the security of these two new QKD protocols, provide mathematical derivation of the quantum uncertainty relation, and summarize the process of security proof through comprehensive analysis of the existing literature. In addition, future research directions are explored, especially the need for experimental validation and performance optimization of these protocols in real-world applications. By analyzing the security of two new QKD protocols, this paper helps to understand future experimental validation and protocol optimization.

2. Foundations of Quantum Secure Communication and Classical Cryptography

2.1. Basics of Classical Cryptography

The main goal of cryptography is to protect the confidentiality and security of information against spoofing and forgery [3]. The theoretical foundation of modern cryptography was laid down by the publication of *Communication Theory of Secrecy Systems* by Claude Elwood in 1949. And modern cryptography is divided into two main types, e.g., symmetric encryption and asymmetric encryption. The symmetric encryption uses the same key during encryption and decryption, while the asymmetric encryption employs a public key for encryption and a private key for decryption. The RSA algorithm, a classic example of asymmetric encryption, relies for its security on the complexity of factorization of large numbers. Specifically, the time to factorize a 400-digit number is about 10^{10} years [4]. However, the emergence of quantum computers presents a significant threat to the RSA algorithm. Therefore, there is an urgent need for cryptographers to develop new algorithms to ensure the security of key generation and distribution and to meet the challenges posed by quantum computing, especially in the context of evolving quantum communication and quantum key distribution technologies.

2.2. Uncertainty Relation

The uncertainty relation is a fundamental concept in quantum mechanics that refers to the fact that the position and momentum of a particle cannot be measured precisely at the same time. This principle reflects the intrinsic properties of quantum systems and reveals the effect of the measurement process on the state of the system. There are various methods for deriving the uncertainty relation. This section presents a derivation based on the fundamental postulates of quantum theory, which aids in a deeper understanding of the essential characteristics of quantum measurement [4].

Based on the De Broglie relation $\lambda = \frac{h}{p}$ and the energy equation E=hf , it can be observed that as the accuracy of the measurement of position is increased, the wavelength λ decreases while the momentum p increases, thus decreasing the accuracy of the momentum measurement. Specifically, the following relationship can be considered:

$$\lambda \Delta p + \Delta \lambda p = 0 \tag{1}$$

The actual “wave packet” can be viewed as a superposition of many monochromatic plane sine waves with the following mathematical expression:

$$\varphi(x,t) = \int_{\Delta\lambda}^{-} C\varphi_\lambda d_\lambda \tag{2}$$

where $\Delta\lambda$ must be a multiple of the wavelength λ, that is $n\lambda$. By combining this equation with the quantization characteristics, the uncertainty relation between position and momentum can be derived, with the proof processes for other uncertainty relations following a similar structure. These derivations not only enhance the understanding of quantum measurement but also provide a crucial theoretical foundation for subsequent research [5].

DOI: 10.54254/2753-8818/86/2025.20340

3. Discussion of Two Quantum Key Distribution Protocols

3.1. Mode-Pairing QKD

The protocol, proposed in 2022, can achieve the key rate of $R = O\sqrt{\eta}$ without the need for global phase locking, where η represents the channel transmittance [6]. The main steps of the security proof are based on the decoy states technique, beginning with i rounds of quantum state preparation ($i \in \{1,2,3,\ldots N\}$), where pulse intensities are drawn from the set $\{0, v, \mu\}$ ($\mu > v > 0$), and the phases $\theta_i^{\alpha}$are randomly selected from the interval [0, 2π). Thus, Alice's coherent state is expressed as $|\sqrt{\mu_i^{\alpha}} exp(i\theta_i^{\alpha})\rangle$, while Bob's state is represented by $\left|\sqrt{\mu_i^{\beta}} exp\left(i\theta_i^{\beta}\right)\right\rangle$. They transmit their pulses to Charlie for single-photon interference measurements, iterating this process *N* times, after which Charlie reports the measurement outcomes. Subsequently, Alice and Bob formulate a pairing strategy based on these results. Given the exceedingly low energy of single photons in the visible spectrum, the optical path and detector precision requirements are stringent, potentially leading to invalid detection events [7]. Therefore, they define the maximum pairwise interval between detection C_i as L. If the pulse interval between the first and second valid detection results does not exceed *L*, the corresponding event pair is recorded; otherwise, the first detection result is discarded, and pairing proceeds. Ultimately, they achieve mode pairing, although the associated programming output process remains unspecified. The essence of this methodology lies in ensuring accurate pairing of valid detection results, thereby safeguarding the security and robustness of the quantum key distribution process.

Based on the intensity differences in the pairing results, Alice (Bob) marks the basis vectors of the data pairs in terms of pairing rules, angle corrections and final key formation. In pairing rules, Z pair means one intensity is 0 and the other is not 0; X pair is two intensities equal and neither of them is 0; 0 pair is two intensities both of them are 0 while discarded pair is two intensities unequal and neither of them is 0, as shown in Table 1. Then Alice and Bob announce the basis vectors of every position pair (i, j) and the sum of intensities $\left(\mu_{ij}^{\alpha} + \mu_{ij}^{\beta}\right)$.

Table 1: Pairing Rules

	Alice	0	X	Z
Bob				
0		0 pair	X pair	Z pair
X		X pair	X pair	discard
Z		Z pair	discard	Z pair

For example, in a random Z pair, if μ_i^{α}=0, Alice sets the key $K_{\alpha} = 0$, and if μ_j^{α}=0, then sets $K_{\alpha} = 1$. And in an X pair, Alice extracts the key using the relative phase with the equation $K_{\alpha} = \left(\left(\theta_j^{\alpha} - \theta_i^{\alpha}\right)/\pi mod2\right)$. During the angle calibration, Alice and Bob compute their alignment angles δ^{α} and δ^{β}, retaining them if conditions are satisfied. In the final key formation process, they select valid Z pairs to generate key strings Z and Z′, utilizing the decoy states method to estimate the lower bound of effective single-photon detection and the upper bound of phase error rates in the raw key [8]. The security factor ε_{cor} indicates the maximum tolerable error. If $\mathrm{P}(\mathrm{Z} \neq \mathrm{Z}') \leq \varepsilon_{\mathrm{cor}}$ is satisfied, the protocol is considered secure and feasible [8,9]. In error correction and hash functions, Alice computes the hash value of key Z using a random hash function, with a length of $\log_2(2/\varepsilon_{\mathrm{cor}})$,

DOI: 10.54254/2753-8818/86/2025.20340

and Bob performs the same operation, ensuring the final key's security through collision resistance and properties of the hash function. The key equation for the security protocol condition is as follows:

$$L \leq n_L^{z1}[1 - h(e_{z1}^{ph,U})] - \gamma_{EC} - log_2(2/\varepsilon_{cor}) - 2\,log_2 \frac{1}{\sqrt{2}\hat{\epsilon}\epsilon PA} \tag{3}$$

where h(x)is the binary Shannon Entropy Function, n_L^{zl} denotes the lower limit of effective single-photon detection in the raw key, and $e_{zl}^{ph,U}$ represents the upper limit of phase error rates. Moreover, the formula takes into account various factors that may affect the security of the key and provides a further derivation of security [8].

3.2. Sending-or-Not-Sending TF-QKD

This protocol was first proposed by Lucamarini et al [10,11], and its key rate was shown to be proportional to $\sqrt{\eta}$, relying on single-photon interference instead of two-photon interference. The newly proposed sending-or-not-sending TF-QKD protocol allows for the direct use of the traditional decoy-state method, while ensuring security automatically, which can effectively handle the high loss caused by long-distance single-photon interference [11].

In any given time window *i*, Alice and Bob independently decide whether it is a signal window or a decoy window. They perform random phase shift $\delta a(\delta b)$ on the coherent state and send it to Charlie. The core of the sending-or-not-sending TF-QKD protocol is as follows: in a signal window, Alice (or Bob) sends a signal to Charlie with probability μ, and does not send with probability $(1-\mu)$. In the signal window , if Alice (Bob) sends a coherent state with intensity M, then the two-mode state in any case of this window can be obtained. And if they both choose to send a coherent state of the same intensity in the decoy window at the same time, the two-mode coherent state can still be obtained at this time. Charlie performs phase compensation on the result and then measures all two-fields with a Beam-splitting Measure and announces the measurement results. Alice and Bob subsequently announce their decoy windows, signal windows, and pulse intensities. The time window which both Alice and Bob are determined to be signal windows is defined as Z windows, and the state from them are referred to Z pair. The effective events occurring in the Z-basis are named as Z-bits. The subset of the Z-window is defined as the Z1 window, and the effective event occurring in it is the Z1-bits. In the Z1-window, when only one of Alice and Bob decides and actually sends a single photon state, The photon state can only be in the state $|z0\rangle = |01\rangle$ or $|z1\rangle = |10\rangle$. This is referred to as a Z1 pair. Similarly, the definition of Z1-bits follows the same criteria. At the same time, a A time window that satisfies the conditions in which both Alice and Bob select the decoy window, send signals with the same coherent state intensity, and the random phase satisfies a specific equation is defined as an X window. The corresponding definitions remain consistent with the previous descriptions. Subsequently, Z bits are randomly selected for error testing to determine the bit error rate in the Z basis. After discarding the test bits, the remaining Z bits are refined into the final key. The announced data of X pairs is utilized to calculate the count rate s_1 of the X1 windows, followed by the calculation of relevant parameters for the Z1 bits, such as the phase flip rate. The final key is refined according to the following formula [11-14].

$$R = 2\varepsilon(1-\varepsilon)\left[Me^{-M}S_1\left(1 - H\left(e_1^{ph}\right) - S_z f H(E^z)\right)\right] \tag{4}$$

where S_z is the count rate observed in z window. calculating with fixed numerical value, the protocol still has obvious advantages in the case of a large error rate [11].

DOI: 10.54254/2753-8818/86/2025.20340

4. Practical Applications and Future Developments

4.1. Practical Applications of Mode-Pairing QKD

Mode-Paring QKD technique has multiple advantages in practical applications. Utilizing quantum interference effects, its core mechanism is based on second-order interference, effectively avoiding the complexities of global phase locking, especially in situations with minimal local phase fluctuations. This flexibility makes the mode-paring QKD particularly suitable for non-laboratory environments, reducing reliance on high-precision equipment and increasing the feasibility and cost-effectiveness of implementation. In practical applications, the financial sector and government communications have illustrated the substantial advantages of Mode-Paring QKD. In the financial sector, the protection of assets and information is of paramount importance, particularly during the processing of high-value transactions and the transfer of sensitive data. A prominent financial institution employs Mode-Paring technique across its distributed network, enabling the rapid generation of millions of secure keys per second. This has led to a notable enhancement in transaction security and customer confidence. Also, the bank employs optical multiplexing technology to transmit multiple keys over the same optical fiber, greatly improving system efficiency. In government communications, the confidentiality and integrity of information are critically important. A national government has deployed Mode-Paring QKD in its classified communications network to ensure absolute security of intergovernmental communications. In this system, the Mode-Paring QKD is highly resistant to interference in the face of ambient noise and photon loss, dynamically adjusting signal strength and transmission paths under a variety of external conditions to ensure efficient and secure key distribution. And the technological compatibility of Mode-Paring QKD allows for seamless integration with existing optical components, supporting various fiber and laser configurations, thereby lowering the technical barriers for system construction. This feature not only simplifies the expansion process for enterprises and organizations but also lays the groundwork for the future construction of large-scale quantum networks. The application cases of Mode-Paring QKD in the financial sector and government communications fully show its potential for achieving efficient and secure quantum communication in the real world, promoting the widespread application of quantum technology.

4.2. Practical Applications of Sending-or-Not-Sending QKD

The sending-or-not-Sending TF-QKD technique significantly improves the security and flexibility of quantum communication via its innovative signaling strategy. In this protocol, TF-QKD effectively reduces the possibility of eavesdroppers obtaining information by selectively sending and receiving signals. Its core lies in utilizing the uncertainty in the transmission process to force the eavesdropper to face the risk of information loss. This mechanism can enhance key security, and provide a powerful tool for monitoring and detecting eavesdropping behavior. TF-QKD shows robust performance in high-interference environments, making it particularly well-suited to complex scenarios such as urban communications. For example, it is used to protect the data transmission of vehicle networking in the intelligent transportation system of a large city. By dynamically adjusting the signal transmission strategy, the system maintains a high key generation rate under low signal-to-noise ratio conditions, effectively solving the limitations of traditional QKD in long-distance transmission. In addition, it can also maintain stable key generation in dense urban environments to meet the increasing security requirements of modern communications [10]. And it extends the maximum distance of quantum key distribution, overcoming the limitations of the effectiveness of traditional protocols in long-distance communication. For example, an experiment demonstrated that TF-QKD successfully achieved key distribution over 100 km in an urban fiber optic network, significantly improving the feasibility of

DOI: 10.54254/2753-8818/86/2025.20340

information transmission. Through precise algorithm and protocol optimization, TF-QKD not only ensures key security but also significantly increases the distance of information transmission, laying a solid theoretical and practical foundation for the future development of quantum communication. This feature demonstrates the prospect of the wide application of quantum technology in the field of information security. The sending-or-not-sending TF-QKD technique significantly improves the security and flexibility of quantum communication with its innovative signaling strategy. In this protocol, TF-QKD can effectively reduce the possibility of eavesdroppers obtaining information by selectively sending and receiving signals. Its core lies in utilizing the uncertainty inherent in the transmission process to force eavesdroppers to face the risk of information loss. This mechanism not only enhances key security, but provides a powerful tool for monitoring and detecting eavesdropping behavior [15]. TF-QKD is especially suitable for high interference and complex communication environments, and thus has great potential in practical applications. By dynamically adjusting the signaling strategy, TF-QKD is able to maintain a high key generation rate with a low signal-to-noise ratio, addressing the limitations of traditional QKD for long-distance transmission.

5. Conclusion

This paper provides proof of security for two new quantum key distribution protocols, and the results show that both protocols have good security under ideal conditions. However, these protocols still have some limitations due to the relatively small amount of relevant research and experimental data. Mode-pairing QKD protocols need to ensure small local phase fluctuations to maintain high key rates, but the complexity of real communication environments makes it difficult to consistently maintain the ideal state. The sending-or-not-sending QKD protocols remain susceptible to the finite key effect in long-distance transmission, thus resulting in the inaccuracy of the pertinent parameters and an adverse impact on the key rate. In addition, long-distance key distribution is hindered by signal attenuation. Future research should focus on experimental validation in diverse real-world environments, thereby optimizing the performance of these protocols under different conditions, and developing robust error correction techniques. Exploring hybrid approaches combining elements of these two protocols can help improve their adaptability and practicality in quantum communication networks.

References

[1] *Wiesner, S. (1983) Conjugate coding. SIGACT News, 15, 78-88.*

[2] *Bennett, C.H. and Brassard, G. (2014) Quantum Cryptography: Public Key Distribution and Coin Tossing. Theoretical Computer Science, 560(11): 7-11.*

[3] *Menezes, A.J. Oorschot, P.C. and Vanstone, S.C. (1997) Handbook of Applied Cryptography. Boca Raton.*

[4] *Nielsen, M.A. and Chuang, I.L. (2010) Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press.*

[5] *Jiang, Y.C. (2007) A Brief Derivation of the Uncertainty Relation. Journal of Sichuan University of Arts and Sciences, 17(2): 2.*

[6] *Zeng, P., et al. (2022) Mode-pairing quantum key distribution. Nat Commun 13, 3903*

[7] *Wu, Q.L., et al. (2010) Single Photon Detection Technology. Progress in Physics, 2010(3): 11.*

[8] *Wang, Z.H., et al. (2023) Tight finite-key analysis for mode-pairing quantum key distribution. Commun Phys 6, 265*

[9] *Li, Z.M. (2010) The Design and Analysis of Hash Functions. Beijing University of Posts and Telecommunications.*

[10] *Lucamarini, M., et al. (2018) Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 557(7705):400-403.*

[11] *Twin-field quantum key distribution with large misalignment error (Xiangbin Wang, Zongwen Yu , Xiaolong Hu*

[12] *Liu, Y., et al. (2023) 1002 km twin-field quantum key distribution with finite-key analysis. Quantum Front 2, 16.*

[13] *Jiang, C., et al. (2020) Zigzag approach to higher key rate of sending-or-not-sending twin field quantum key distribution with finite-key effects.*

[14] *Jiang, C., et al. (2021) Composable security for practical quantum key distribution with two way classical communication.*

DOI: 10.54254/2753-8818/86/2025.20340

[15] Liu, Y., et al. (2023) Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys Rev Lett 130(21):210801