北海道大学大学院情報科学院

２０２４年度

博士論文

Study on measurement-device-independent quantum key distribution with time synchronization

測定装置に依存しない量子鍵配送における時間同期に関する研究

葛　皓波

Ge　Haobo

Contents

List of Figures

Chapter 2

Chapter 3

Chapter 4

Chapter 5

List of Tables

Chapter 2

Chapter 3

Chapter 1

Overview

1.1 Research background

Nowadays we live in an information society. The importance of information security is self-evident. The application of secure communication is increasingly involved in all aspects of our lives. So, the research on cryptography and the development of secure and efficient encryption technology become particularly important.

The most basic application of cryptography is to hide the meaning of information in the process of transmission to avoid eavesdropping by others. The sender converts the identifiable plaintext into unidentifiable ciphertext through encryption, while the receiver uses decryption to obtain the sender's information while ensuring that the eavesdropper cannot obtain the information. In the modern information society, cryptography has become an indispensable part of our daily life, providing necessary security for our network access, e-commerce and other activities.

1.1.1 Modern cryptography

Classical cryptography can be divided into transposition cipher and substitution cipher according to the encryption and decryption methods used. The most famous example of a transposition cipher is the Scytale of Ancient Greek. And the most famous examples of substitution cipher include the Caesar cipher and the Enigma cipher machine of Germany.

After World War II, with the rapid increase in the demand for cryptography and the development of computer and electronics technology, cryptography gradually became a systematic discipline. Modern cryptography is divided into symmetric cryptography and asymmetric cryptography according to whether the keys held by the sender and receiver are the same [1].

Symmetric cryptography is that sender and receiver hold the same key, so it is also called a private key password. DES (Data Encryption Standard) [2] proposed in 1976 and AES (Advanced Encryption Standard) proposed in 2001 are typical examples of symmetric cryptography. In addition, One-Time Pad method is considered to be the only theoretically unconditional secure encryption at present [3].

Asymmetric cryptography is also known as public key cryptography [4], whose key is divided into public key and private key. The public key is a public part, while the private key is kept secret by the receiver. The typical representative of this kind of cipher is RSA (Rivest–Shamir–Adleman)

encryption proposed in 1978. If you have both the public and private keys, the decryption process is simple, but if you have only the public key and no private key, the decryption time at the level of current computer is much longer than the effective time of encryption. It is easy to see the security of public key cryptography mainly benefits of the limit of current computer computing speed.

In the 1980s, the concept of quantum computer [5], [6] was proposed, which means the computing speed could be greatly improved. Shor algorithm [7] and Grover algorithm [8] based on quantum computer have also brought great threats to modern cryptography.

Although the security of the One-Time Pad method is unbreakable in theory, due to the large consumption of highly random keys, which require timely and safe distribution, strict storage, and timely destruction after using, the scheme is difficult to be applied in practice.

The threat posed by the development of quantum computers to secure communications will eventually be solved by quantum mechanics. Quantum cryptography, a secure communication guaranteed by physical principles, offers new possibilities for the ideal security scheme of One-Time Pad.

1.1.2 Quantum cryptography

One-Time Pad method is the only encryption that has been proved to be unconditional secure. However, in the practical implementation of classical cryptography, there are two insurmountable challenges: the generation of true random numbers and the unconditional secure distribution of keys in non-secure channels. The deterministic nature of classical physics precludes the generation of random numbers, while basic quantum processes can produce genuinely random numbers. Simultaneously, classical cryptographic theory lacks a secure model to describe the key distribution process in non-secure channels, primarily because classical physics allows information to be copied.

Quantum uncertainty theorem implies that if a quantum system Ψ is not in one of the eigenstates of an observable F, but rather exists as a linear combination of multiple eigenstates, then prior to measuring Ψ with respect to F, the observer cannot deterministically know the measurement outcome. Instead, the observer can only obtain different measurement outcomes along with their corresponding probabilities. Furthermore, once a measurement is performed on the quantum state, the original state is disturbed, effectively losing information about the coefficients of the superposition among different eigenstates.

In classical cryptography, information can be precisely cloned because various states in the classical domain are mutually orthogonal. As long as the original state can be completely measured, it is possible to copy an identical state, achieving information cloning. On the contrary, the quantum no-cloning theorem asserts that there is no universal transformation capable of accurately cloning arbitrary unknown quantum states. If a quantum system is measured to obtain some information, generally, the original quantum system will be disturbed unless the states in the original quantum system are known to be mutually orthogonal in advance. In a system where the states are non-

orthogonal, an eavesdropper, Eve, cannot completely and precisely clone the unknown quantum states exchanged between Alice and Bob. Any attempt to gain information about the quantum states through measurement will disrupt the original quantum states, thereby revealing Eve's presence. Communication parties can share unconditionally secure cryptographic keys.

In 1984, Bennett and Brassard proposed the concept of quantum key distribution at the IEEE academic conference held in Kolkata, India, and published the first academic paper on the quantum key distribution (QKD) protocol BB84 whose security was strictly proved [9]. Based on the fundamental principles of quantum physics, QKD enables the distribution of unconditionally secure random keys through non-secure channels. The generated secure keys can be used in the One-Time Pad mechanism to achieve true One-Time Pad security. With the development of quantum mechanics, it is possible to generate and distribute provable true random numbers. Quantum cryptography is an important step towards the quantum era from modern cryptography, because its security is based on the physical principles of quantum mechanics, no matter how strong the attacker's computing power is, it cannot be cracked.

1.2 Research purpose

The actual QKD systems may have various security loopholes due to the inevitable errors and defects of the equipment. Security certification on actual QKD system should handle the loopholes properly. One scheme is to fix existing security loopholes. Loopholes due to device imperfection must be carefully tested, accurately modeled, and then modified for security analysis and key rate estimation. However, if all loopholes are accurately modeled, it costs additional measurement device and time. Moreover, there is no guarantee that all loopholes have been fixed.

Another scheme is to relax the requirement for the device in practical systems. This scheme is known as device-independent quantum key distribution (DI-QKD) protocol [10]-[12], proposed by Acin et al. However, DI-QKD has very strict requirements. These requirements are difficult to achieve with the existing technology in experiment.

Among the elements of the QKD system, detectors are unreliable, because they may be attacked by any inputs Eve designs. Several attacks such as detection efficiency mismatching attack [13] and time-shift attack attacks [14], etc. Against these attacks, Lo et al. proposed measurement-device-independent quantum key distribution (MDI-QKD) protocol [15]. It is based on the assumption that the source device is reliable. This scheme can be implemented with currently available optical devices. Since MDI-QKD can be regarded as the time-reversal of the entanglement-based QKD, the security proof is the same in the ideal case. Moreover, MDI-QKD is immune to all attacks against detector loopholes.

According to Lo et al. [10], it is critical for the photons emitted by two independent lasers to be indistinguishable. Since MDI-QKD protocol is based on the photon bunching effect of two

indistinguishable photons at a 50:50 beam splitter (BS), stable HOM interference [16][17] should be observed. The validity of the HOM test was probed in principle. However, the fiber channel is susceptible to disturbances in real-world environments, and the effect of non-ideal visibility becomes particularly pronounced in long-distance transmission. Therefore, it is imperative to elucidate the relationship between HOM interference visibility and the final key rate, and to establish methods for improving visibility. In practical compensation of the disturbance, it is of utmost importance to determine the desired accuracy to maintain the final key rate.

Thus far, a few studies have explored this issue, with exceptions including the study by Curty et al. [18], which calculated only the effect of misalignment error in the limit of zero distance. The effects of imperfect visibility become serious for long distance transmission, because the fiber channel is exposed to perturbations in practical conditions. Precise control of the channel would be necessary to compensate the perturbation. However, the precise control may raise the cost for implementation. It is important to determine the target of the precision to maintain the final key rate in practice.

Tang, et al. [19] and Valivarthi et al. [20] demonstrated disturbance compensation schemes; however, these schemes rely on long-distance feedback channels, which may introduce unnecessary errors. Even when the signal source is compensated and corrected, errors generated in long-distance fiber channels may still be overlooked.

We explore the acceptable indistinguishability of the MDI-QKD. We calculate the key generation rate of a three-intensity decoy-state MDI-QKD protocol with a finite key length. Then, we calculate the effect of the visibility of the two-photon interference on the key generation rate. Finally, we calculate the acceptable time delay of the two Gaussian pulses at a 50:50 BS. We also propose a novel synchronization scheme for MDI-QKD aimed at mitigating the effect of temporal indistinguishability. We introduce a time synchronization scheme through disturbance compensation at the receiver, Charlie.

1.3 Chapter outlines

In this study, the effect of two-photon temporal distinguishability of MDI-QKD is studied and an improved time synchronization scheme is proposed. Chapter outlines are shown as follows.

- **Chapter 1:** We review the development of quantum cryptography and quantum key distribution (QKD) and introduce the research background and the purpose of this study.
- **Chapter 2**: We mainly introduce the principle of several common protocols for QKD. First, we introduce the first proposed BB84 protocol, which has been proved to be theoretically unconditionally secure. Subsequently, we introduce the realistic vulnerabilities of QKD systems and lead to some improved protocols for these problems
- **Chapter 3**: To address side-channel loopholes in QKD systems, we primarily focus on introducing the measurement-device-independent quantum key distribution (MDI-QKD) protocol. This section

provides a detailed overview of the principles behind the MDI-QKD protocol. Additionally, we supplement this discussion with several commonly used encoding methods in practice.

- **Chapter 4**: We emphasize a hitherto overlooked issue within MDI-QKD, involving the indistinguishability requirement for photons emitted by two independent laser sources at the measurement device in the middle, necessitating the observation of stable Hong-Ou-Mandel (HOM) interference. This section provides a detailed analysis of the effects of temporal distinguishability on MDI-QKD protocols during two-photon interference and derives the acceptable range of time delays under Gaussian photon conditions.
- **Chapter 5**: We propose a novel synchronization scheme for MDI-QKD to address the temporal distinguishability effects described in the preceding sections. Our approach ingeniously leverages optical frequency comb (OFC) technology, installing each component of the synchronization system at the detection end, thereby mitigating errors introduced by long-distance optical fiber transmission. Experimental results indicate the high feasibility and exceptional cost-effectiveness of our proposed scheme.
- **Chapter 6**: We summarize the research results of this study and describe the prospects of our research.

References

[1] M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information”, American Journal of Physics 70, 471 (2002).

[2] X.-B. Wang, T. Hiroshima, A. Tomita and M. Hayashi, “Quantum information with Gaussian states”, Physics Reports, 2007, 448(1):1-111.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev.Mod.Phys.74.145 (2002).

[4] N. Gisin and R. Thew, “Quantum communication”, Nature Photonics, 1, 165-171 (2007).

[5] M. Dusek, N. Lutkenhaus and M. Hendrych, “Quantum Cryptography”, Progress in Optics, 2006, 49:381-454, arXiv: quant-ph/0601207.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, “The security of practical quantum key distribution”, Rev.Mod.Phys.81, 1301 (2009).

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental quantum cryptography”, Journal of Cryptology, 1992, 5(1): 3-28.

[8] P. D. Townsend, “Quantum cryptography on optical fiber networks”, European Conference on Parallel Processing, 1998, 35-46.

[9] C. H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Theoretical Computer Science, 2014, 560(1): 7-11.

[10] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, “Device-Independent

Security of Quantum Cryptography against Collective Attacks", Phys. Rev. Lett. 98, 230501 (2007).

[11] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography", Phys. Rev. Lett. 94, 230503 (2005).

[12] D. Gottesman, H.-K. Lo, N. Lutkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices", International Symposium on Information Theory, 2004. ISIT 2004. Proceedings, DOI:10.1109/ISIT.2004.1365172.

[13] V. Makarov, A. Anisimov and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems", Phys. Rev. A. 74, 022313 (2006).

[14] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Phys. Rev. A. 78, 042333 (2008).

[15] H.-K. Lo, M. Curty and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Phys. Rev. Lett. 108, 130503 (2012).

[16] P. D. Townsend, "Quantum cryptography on optical fiber networks", European Conference on Parallel Processing, 1998, 35-46.

[17] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard and H.Zbinden, "Fast and user-friendly quantum key distribution", Journal of Modern Optics, 2000, 47(2-3): 517-531.

[18] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," Nat Commun 5, 3732, 2014. DOI: 10.1038/ncomms4732

[19] Y.-L. Tang, H.-L. Yin, S.-J. Chen, et al., "Measurement-Device-Independent Quantum Key Distribution over 200 km," Phys. Rev. Lett. 113, 190501(2014).

[20] R. Valivarthi, Q. Zhou, C. John, et al., "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," Quantum Sci. Technol. 2,04LT01 (2017).

Chapter 2

Quantum key distribution

2.1 Introduction

In 1984, Bennett and Brassard proposed the concept of quantum key distribution at the IEEE academic conference held in Kolkata, India, and published the first academic paper on the quantum key distribution (QKD) protocol whose security was strictly proved [1].

The security of Quantum Key Distribution (QKD) is guaranteed by three principles of quantum mechanics: the Heisenberg uncertainty principle, the theory of wavefunction collapse, and the no-cloning theorem.

Heisenberg uncertainty principle: This principle states that non-commuting observables cannot be simultaneously measured to arbitrary precision. Measuring one observable to a precise degree means that the uncertainty of the other will be infinite. For instance, it's impossible to simultaneously know the position and momentum of a quantum state in the same direction. Once the momentum is precisely determined, its position becomes unknowable, and vice versa. In the context of the BB84 protocol, the essence of its security lies in using two sets of non-orthogonal bases for encoding and decoding, meaning states from these two bases are non-commuting. Consequently, an eavesdropper cannot determine the polarization with a single measurement.

Wavefunction collapse theory: This theory suggests that measuring a quantum state not in an eigenstate of the measurement basis will lead to the quantum state collapsing into one of the basis' eigenstates with a certain probability. Taking the horizontal and vertical basis as an example, where the eigenstates are $|H\rangle$ and $|V\rangle$, a quantum state described by $(|H\rangle+|V\rangle)/\sqrt{2}$ will collapse to either $|H\rangle$ or $|V\rangle$ with a 50% probability upon measurement. In the BB84 protocol, if an eavesdropper attempts to measure a quantum state, unless the state is an eigenstate of their measurement basis, they will inevitably alter the original state, thus leaving a trace.

No-cloning theorem: This theorem asserts that it is impossible to create a perfect copy of an arbitrary unknown quantum state. The above two principles ensure that a single measurement cannot obtain complete information about a state and that observing it leaves a mark. The No-Cloning Theorem further ensures that an eavesdropper cannot gain information about the quantum state through replication.

Quantum key distribution establishes a set of keys rather than sending plain text encrypted

directly. This is because the basis of the security is the measurement of quantum states, and the measurement behavior of wave functions is a process of quantum randomization. According to One-Time Pad method, as long as the key is not reused, then when the key is secure, the communication is also secure. Encrypted text itself, even if uses a public channel, there is no security issue.

2.2 QKD system

In practical applications, the system configurations of different QKD protocols vary, but generally, they should include the following components: light source, modulation module, demodulation module, detection, post-processing module, and random number generator (RNG). As illustrated in Figure 2.1: the light source, after being modulated by the encoding module controlled by the random number generator, is sent into the channel. Upon receiving the optical pulse signal, the receiver carries out decoding operations under the control of the random number generator and proceeds with detection. Finally, a secure key is generated after post-processing.

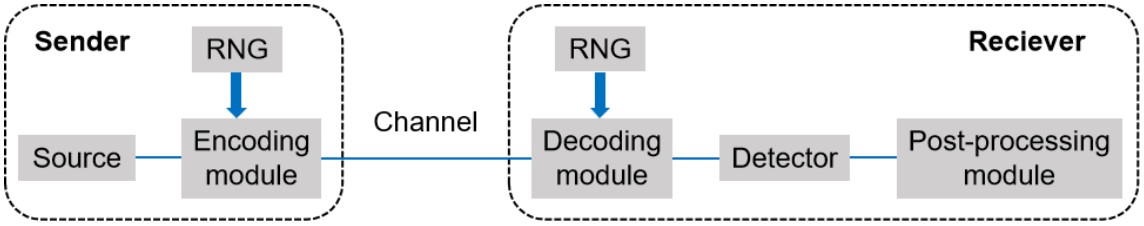


Figure 2.**错误!文档中没有指定样式的文字。**1. General components of a QKD System.

(a) Light source:

Photons, as the carriers of encoding compared to commonly used electrons, atoms, electromagnetic waves, etc., can have a higher information capacity. Moreover, there are no electromagnetic crosstalk or charge interactions between photons. Therefore, photons have better spatial adaptability and parallelism, making them more suitable for transmission. Hence, they are the optimal choice for information carriers in QKD systems.

In QKD theory, the ideal light source is a single-photon source. Due to practical device limitations, an ideal single-photon source is essentially unattainable. Currently, the mainstream approaches to generating approximate single-photon sources are divided into two categories. The first category is deterministic single-photon sources. These sources produce single photons through the transition from an excited state to the ground state. Common schemes include quantum dot schemes and NV (Nitrogen-Vacancy) center schemes. The second category is probabilistic single-photon sources. These sources utilize the higher-order nonlinear effects produced by photons in various materials to probabilistically generate a pair of photons. By detecting the presence or absence of one photon, the existence of the other photon can be inferred. This type of probabilistic

source is commonly generated through parametric down-conversion (PDC) processes and four-wave mixing (FWM) processes. In current practical QKD systems, the commonly used approximation for a single-photon source is attenuated coherent light, i.e., a weak coherent source (WCS). This type of source has a good single-photon component and, generally speaking, its photon number follows a Poisson distribution:

$$P_n(\mu) = \frac{\mu^n}{n!} e^{-\mu}. \tag{2.1}$$

where n represents the number of photons and μ represents the average light intensity. In addition to the single-photon component, this type of light source also contains a small amount of multi-photon components. In section 2.4, we will analyze the risks posed by these multi-photon components in QKD.

As a light source, quantum entangled sources are also an important resource. This type of light source embodies some of the most peculiar properties of quantum mechanics. Entangled light sources are generally generated through parametric down-conversion processes, where the resulting two photons can be entangled in dimensions such as time, wavelength, and polarization. The common E91 protocol utilizes such entangled sources for the transmission of encoded information between parties. Additionally, entangled sources find applications in quantum communication such as quantum teleportation and entanglement swapping.

(b) Encoding and decoding Devices:

The selection of encoding and decoding devices for a system depends on the overall system implementation scheme and the characteristics of the channel. In two-dimensional space, common encoding methods include polarization encoding and phase encoding. For transmission environments such as free space, where light attenuation is relatively low around 800nm, and photon polarization is minimally affected by the atmosphere, polarization encoding is typically used. However, for systems transmitting through optical fibers, both encoding methods have their advantages, with phase encoding generally being more suitable for fiber-optic transmission.

Common polarization encoding methods include two approaches: active modulation and passive modulation. The active modulation method utilizes the optoelectronic effects of certain polarization control devices for polarization state modulation, such as Pockels cells, lithium niobate crystals, potassium dihydrogen phosphate (KDP) crystals, etc. Additionally, polarization modulation can be achieved using a combination of phase modulators and Sagnac interferometers. The passive modulation method involves using multiple lasers at the light source end, preset to specific polarizations, and selecting polarization through optical switches for polarization choice.

For phase encoding, the initially used Mach-Zehnder (MZ) interferometer with equal arms transmitted light pulses through two optical fibers. However, environmental disturbances had a significant impact on the lengths of the two fibers, rendering this interferometer impractical [2].

Subsequently, the use of a pair of unequal-arm MZ interferometers gradually became mainstream. This structure can transmit light through a single optical fiber, with the phase difference encoded on the leading and trailing pulses through unequal-arm MZ interferometers. The receiver utilizes the same interferometer to interfere with pulses encoded by both parties, completing the decoding operation. However, the visibility of unequal-arm MZ interferometers may be affected by changes in fiber polarization characteristics during long-distance transmission, affecting overall stability. Later, the unequal-arm Faraday-Michelson (FM) interferometer scheme was proposed [3]. This type of interferometer utilizes the round-trip structure formed by Faraday mirrors, eliminating the influence of polarization disturbances on the transmission fibers and long and short arms of the interferometer. Additionally, it eliminates the requirement for lithium niobate phase modulators to select polarization. Therefore, the interferometer structure of the FM scheme achieves environmental independence and better stability compared to the MZ interferometer. Furthermore, considering high-speed modulation, this interferometer structure was improved to the Faraday-Sagnac-Michelson (FSM) interferometer [4]. In the FM interferometer, the same pulse undergoes phase modulation twice, which leads to overly complex phase encoding in systems with higher repetition rates. In the new FSM interferometer, different polarizations of the same light pulse can reach the phase modulator simultaneously, enhancing the adaptability of high-speed systems while retaining the original stability advantages of the FM interferometer. Additionally, by controlling the on-off state of the long and short arms, these unequal-arm interferometers can realize the timestamp-phase encoding scheme.

(c) Detector:

The choice of detector varies among different QKD protocols. For discrete-variable QKD protocols, single-photon detectors are commonly used devices. Parameters of single-photon detectors include detection efficiency, dark count rate, timing jitter, afterpulsing, maximum count rate, etc.

Commonly used detectors include:

1. Avalanche photodiode detectors (APD): These detectors operate in Geiger mode, where the reverse bias applied to the P-N junction is greater than the avalanche voltage. At this point, the generated carriers in the depletion layer gain sufficient energy to undergo impact ionization with the lattice, creating electron-hole pairs and triggering an avalanche effect, resulting in a detectable current. After detection, an artificial quenching process is performed to suppress the avalanche effect and transition to a linear operating mode. Materials for these detectors can include silicon (wavelength range: near-infrared, efficiency: 60%~70%), germanium (wavelength range: except for the long wavelength of 1550nm), indium gallium arsenide (wavelength range: 1550nm, efficiency: 5%~30%).

2. Superconducting nanowire single-photon detectors (SNSPD): In this type of detector, photons

are absorbed by the superconducting nanowire, disrupting Cooper pairs and creating a hot spot. This hot spot alters the local critical current density of the adjacent region, forming a resistive barrier spanning the nanowire, effectively transitioning from a superconducting to a resistive state. At this point, a voltage signal detectable at the ends of the nanowire is generated, completing the conversion from photon to voltage signal. These detectors have very high detection efficiency (can exceed 90%) and can achieve extremely low dark count rates. Due to their short dead time, their maximum count rate can approach 100MHz, but they operate at temperatures around 2K, requiring certain specifications for the entire system.

(d) Post-processing module:

After the detector obtains response events, a series of post-processing operations are required to obtain secure and consistent keys. The entire process generally includes error correction, privacy amplification, and classical channel authentication.

Error correction is aimed at correcting inconsistent keys generated by QKD. Common error correction methods include the Cascade error correction protocol in interactive error correction and LDPC coding in one-way error correction. To measure the performance of error correction, the error correction efficiency $f(e)$ is defined in the key rate function as the ratio of the consumed information $I(e)$ during error correction to the ideally consumed information $H_2(e)$, where e is the measured error rate.

Privacy amplification compresses the amount of key shared between legitimate users while reducing the information obtained by eavesdroppers to a negligible level. For example, compressing m bits to n bits can be achieved by sharing a consistent $m \times n$ random matrix. Commonly used matrices include Toeplitz matrices, which require only a small number of random numbers $m+n-1$ to construct a random matrix, reducing the system's demand for random numbers. Additionally, the complexity of the matrix can be reduced, and calculations accelerated using the fast Fourier transform algorithm.

In QKD systems, in addition to the quantum channel, a classical channel authenticated by hashing functions is also required. Eavesdroppers can obtain information from both parties through the classical channel but cannot modify the exchanged information. The authentication process can be handled using hash functions as authentication algorithms: the sender attaches the hash value generated from the message to be transmitted as authentication information and sends it to the receiver through the classical channel. The receiver uses the same hash function to calculate the hash value and compares it with the authentication information to check for modifications by eavesdroppers. This authentication technique is well-established in classical communication. Common methods include Toplitz matrix authentication based on LFSR.

(e) Random number generator:

Ideally, QKD protocols require the use of true random numbers in addition to perfect light

sources and encoding/decoding mechanisms. During the encoding/decoding process, random numbers determine the selection of states preparation and measurement bases. At this point, if an eavesdropper can obtain some information about the random numbers, the security of the entire QKD system is compromised.

For ideal random numbers, they must meet requirements such as uniform distribution and unpredictability. If the random numbers are not uniformly distributed or exhibit periodic patterns, an eavesdropper can use known information to predict preceding or subsequent random numbers. Currently, widely used random numbers are pseudo-random numbers, which are generated from short seeds using deterministic random number algorithms to produce longer random sequences. This approach can also generate uniformly distributed random numbers and offers high speed. However, these random numbers are fundamentally derived from deterministic algorithms. Once these algorithms and seeds are cracked, the security of these random numbers is compromised as they can be replicated.

In addition to pseudo-random numbers, physical random numbers are generated from random physical processes. These random numbers exhibit higher randomness and are closer to ideal true random numbers. However, some physical processes can theoretically be predicted, so while these random numbers have higher randomness than pseudo-random numbers, their security still has vulnerabilities.

So far, quantum random number generators (QRNGs) based on the intrinsic randomness of quantum mechanics are the only theoretically true random number generators. For example, in an ideal scenario, a single photon passing through a 50:50 beam splitter generates uniformly distributed, unpredictable true random numbers based on the detection events at the two outputs. This process appears similar to flipping a coin to get heads or tails, but the fundamental difference lies in the fact that while the entire process of coin flipping can be accurately calculated through modeling the forces acting on the coin, the process of generating random detection results through a beam splitter includes the randomness introduced by measurement collapse and is unpredictable.

2.3 QKD protocols

2.3.1 BB84 protocol

The Discrete Variable Quantum Key Distribution (DV-QKD) is the longest-standing and most extensively studied category of protocols in quantum key distribution. In this class of protocols, the Hilbert space used for encoding is finite-dimensional. Examples include using specific polarization states or specific phase information of photons as the encoding space. The first historically significant DV-QKD protocol is the BB84 protocol. It can use the characteristics of quantum state and quantum measurement to realize unconditional secure key distribution. Here is a brief overview

of this protocol.

In quantum communication, the communicating parties are generally denoted as Alice and Bob. BB84 is a one-way communication protocol in which the sender is Alice and the receiver who receives and measures the signal is Bob. A protocol can be designed to share the same, randomly generated string of key bits between Alice and Bob.

(1) Quantum State Preparation

The polarization encoding BB84 protocol utilizes four polarization states of a single photon. Alice has two orthogonal bases for preparing polarized photons. The two states in each group of orthogonal bases represent the information of 0 or 1 respectively, and the corresponding relationship is shown in Table 2.1.

Bit value	Z basis	X basis
0	$\|0\rangle$	$\|+\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$
1	$\|1\rangle$	$\|-\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$

Table 2.1 Basis encoding of BB84 protocol

Here |0> and |1> correspond to the horizontal and vertical polarization states of photons, which are two states of Z basis that are perpendicular to each other. |+> and |-> correspond to the 45° and 135° polarization states, respectively, which are two states of the X basis that are perpendicular to each other. By calculation, it is easy to know that these four polarizations conform to the following relationship

$$\begin{aligned} \langle 0|1\rangle = \langle +|-\rangle = 0 \\ \langle 0|0\rangle = \langle 1|1\rangle = \langle +|+\rangle = \langle -|-\rangle = 1 \\ |\langle 0|+\rangle|^2 = |\langle 0|-\rangle|^2 = |\langle 1|+\rangle|^2 = |\langle 1|-\rangle|^2 = \frac{1}{2} \end{aligned} \quad . \tag{2.2}$$

From Eq.(2.2) we can see that polarization states belonging to same basis are orthogonal to each other. But polarization states that do not belong to the same basis are not orthogonal to each other, and the overlap probability is 1/2. Then Alice sends prepared quantum state to Bob through a non-secure channel.

(2) Quantum State Measurement

Bob also has two sets of orthogonal bases as same as Alice's. Bob randomly selects a set of bases to measure the photons from Alice, and records measurement results and the basis used. Now Alice and Bob each have a Key A and Key B which called Raw Key.

According to theory of wave function collapse, quantum state will collapse to the eigenstate of

the measurement operator after being measured. If Z basis is used to measure |0> and |1>, a definite result will be obtained. So |0> and |1> are the eigenstate of Z basis. However, if Z basis is used to measure |+> and |->, since Z basis and X basis are not orthogonal, the measurement results will collapse randomly to the eigenstate of Z basis. So, there's no way to determine the polarization state of the output. Similar results will be obtained by using X basis.

(3) Basis comparing

Alice and Bob disclose the used bases through classical channels and compare them to each other. Only the cases that Bob successfully measured, and Alice and Bob used the same basis were retained, while the others were discarded. The key compared and sifted is called Sift Key. According to the selection of basis, different measurement results are shown in Table 2.2.

Bob \ Alice		Z basis		X basis	
		$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Z basis	$\|0\rangle$	1	0	1/2	1/2
	$\|1\rangle$	0	1	1/2	1/2
X basis	$\|+\rangle$	1/2	1/2	1	0
	$\|-\rangle$	1/2	1/2	0	1

Table 2.2 Depending on the basis of Alice's and Bob's choices, there are 16 outcomes and their probabilities. Where 1 means it must happen, 0 means it must not happen, 1/2 means it has a 50% chance to get result.

Because only the basis used and the sequence number of correct matching pulses are disclosed, the classical channel does not reveal any information about the key. A single photon pulse is indivisible. Even if an eavesdropper named Eve intercepts a photon pulse, she cannot know in advance which basis to use. According to the no-cloning theorem, Eve cannot get any useful information from them.

(4) Post-processing

The probability that Alice and Bob use different polarization basis is 50%. In addition, there is also channel noise. And Eve may send false pulses to Bob after intercepting them. Therefore, Sift Key needs to be post-processed. In general, Alice and Bob randomly select a part of Sift Key and disclose them by classical channel to compare with each other and estimate bit error rate and information obtained by Eve. If bit error rate is bigger than a certain threshold, the current round of

the protocol is terminated. They discard all remaining bits and restart the protocol.

If the protocol continues, Alice and Bob perform error correction and error verification. After correcting the inconsistent part of the key, Alice and Bob have the same key sequence. This key is called raw key. Then, Alice and Bob implement privacy amplification to reduce the information obtained by Eve to zero. Then they can get Final Key.

We make a brief analysis of its security proof. When there is no channel loss or eavesdropper, Alice and Bob perform perfect quantum state preparation and measurement. At this moment, sift keys of both sides shall be completely the same, with bit error rate of 0.

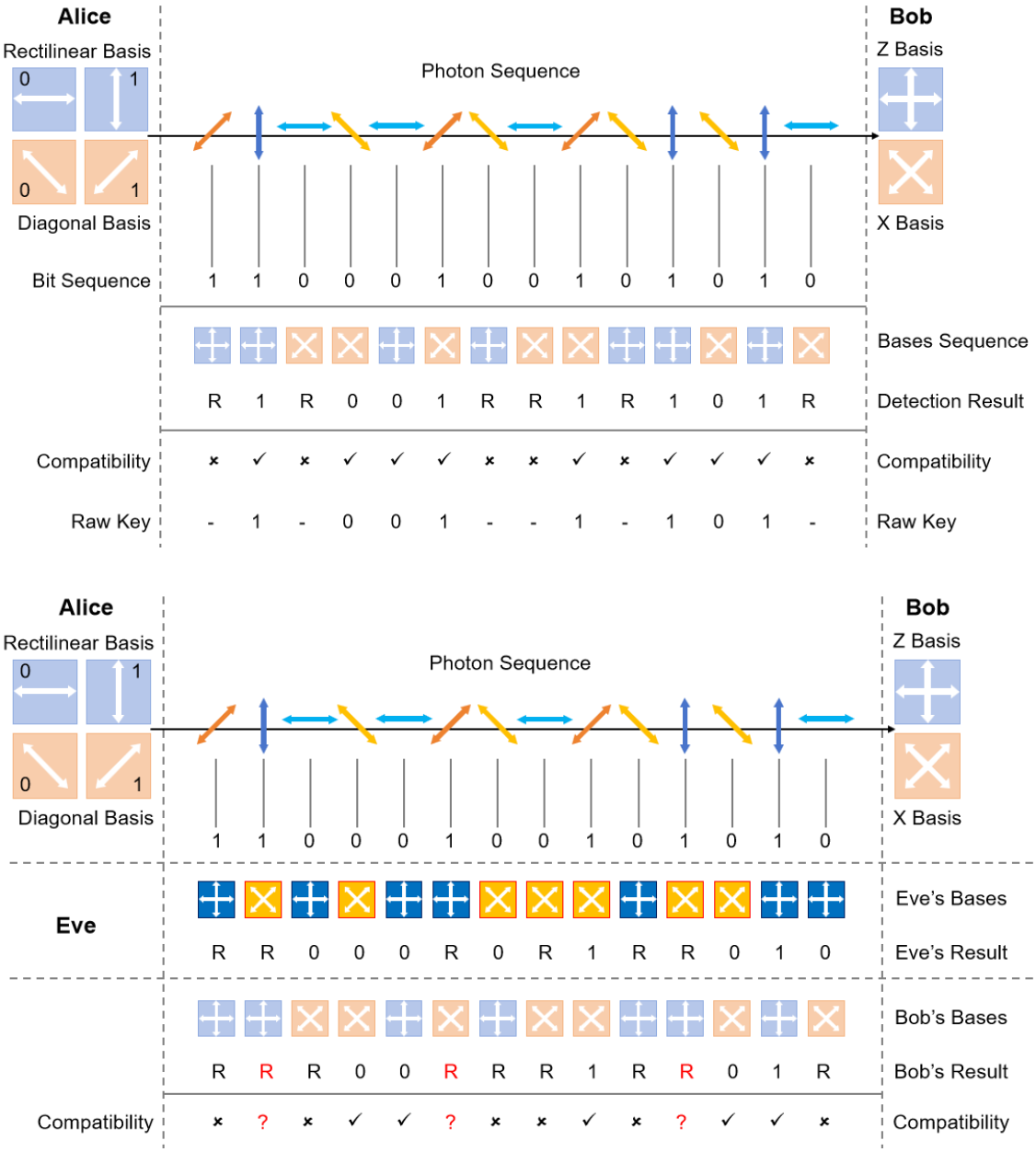


Figure 2.2 Process of BB84 protocol without and with Eve.

The communication process of BB84 protocol is shown in Fig 2.2. Suppose that Eve uses Intercept-resend Attack to eavesdrop on the system. Eve will measure the photon before it reaches Bob, then reprepare the photon based on the measurement result and resend it to Bob. Eve cannot accurately obtain the real information of the quantum state sent by Alice, so she can only randomly select the basis for projection measurement. There is a 50% probability that Eve and Bob use different basis for measurement, then the quantum state that Eve resends to Bob is no longer same as Alice's original quantum state. Since there is a 50% probability that the basis used by Alice and Bob are different, according to this analysis, a bit error rate of 25% will be generated if Eve eavesdrops on all qubits. Alice and Bob judge whether there is an eavesdropper based on bit error rate analysis of system. Then they perform Error Correction and Privacy Amplification to reduce the information obtained by Eve.

In addition to polarization coding, BB84 protocol can also be implemented by phase coding [5]. This idea was first proposed by Bennett in 1992, who pointed out that the phase difference between front and rear pulses could be used to create states required by BB84 protocol. Figure 2.3 is a typical Mach-Zehnder interferometer-based phase-coding BB84 protocol QKD system. Table 2.3 shows

Bob \ Alice		Z basis		X basis	
		0	π	$\frac{\pi}{2}$	$\frac{3\pi}{2}$
Z basis	0	D_0	D_1		
X basis	$\frac{\pi}{2}$			D_0	D_1

Table 2.3 Results with different selection of basis of phase encoding BB84 protocol.

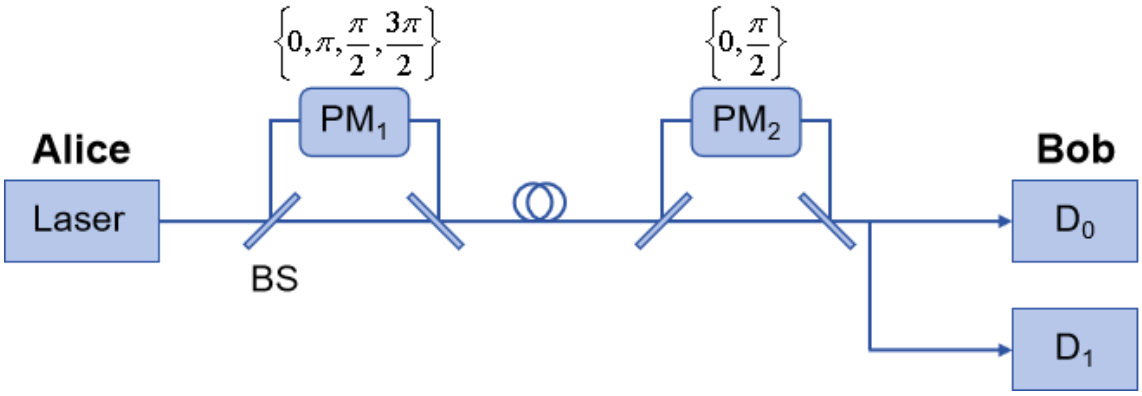


Figure 2.3. Mach-Zehnder interferometer-based phase-coding BB84 protocol. BS: beam splitter, PM: phase modulator, D: single-photon detector

The unconditional security of BB84 protocol has been proved mathematically and physically, but as described above, its security proof is based on idealized conditions. For practical QKD system, due to a variety of unsatisfactory factors including noise, channel loss and device (laser, detector) performance limitations [5][9], its security and efficiency issues have not been resolved.

2.3.2 Security proof

Next, we demonstrate the unconditional security of the BB84 protocol at the information-theoretical level using the method of entanglement distillation [10], [11], derived from the monogamy of entanglement [12], [13]. In measurement-device-independent protocols proposed in subsequent chapters, we also use this method to prove their security. In this approach, the security of a prepare-and-measure QKD protocol is equivalent to the security of an entanglement distillation protocol. As illustrated in Figure 2.4, in this protocol, Alice first prepares a maximally entangled state

$$|\phi_1\rangle = \frac{\sqrt{2}}{2}\left(|00\rangle_{AB} + |11\rangle_{AB}\right), \tag{2.3}$$

where the two particles are respectively denoted as particles A and B. Alice randomly performs a Hadamard operation (represented by the H gate in Figure 2.4) on particle B before sending it to Bob. Bob then randomly performs a Hadamard operation on the particle he receives. We consider the most general Pauli channel, where the identity matrix corresponding to the two-dimensional quantum state prepared by Alice is denoted by I, the bit error matrix is denoted by X, the phase error matrix by Z, and the bit-phase error matrix by $Y = XZ$. From this, we can construct a basis in the two-dimensional Hilbert space, and any quantum bit displacement can be attributed to these

three types of errors. The Hadamard operation can be represented by the Hadamard operator:

$$H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The bit error matrix, phase error matrix, and bit-phase error matrix are respectively denoted as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

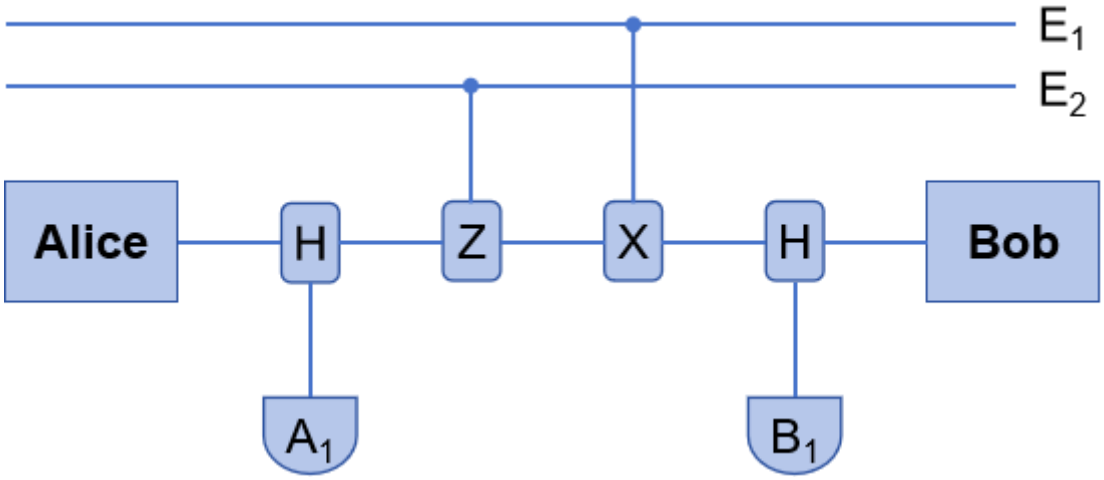


Figure 2.4. Diagram of the entanglement distillation protocol, considering the most general Pauli channel model. H represents the Hadamard operation. X and Z represent the introduction of bit errors and phase errors by the eavesdropper in the channel, respectively. A_1 and B_1 are auxiliary particles at the Alice and Bob ends, respectively. When Alice and Bob establish a maximally entangled state, they can negotiate an unconditionally secure key.

Considering that the eavesdropper Eve can perform arbitrary operations on the quantum states in the channel, the joint quantum state of Alice, Bob, and Eve can be described as

$$\sum_{u,v,i,j} \sqrt{P_u P_v Q_i Q_j}\left(I_A \otimes H_{B_1}^{i} X_{E_1}^{u} Z_{E_2}^{v} H_{A_1}^{j} |\phi_1\rangle |u\rangle_{E_1} |i\rangle_{B_1} |j\rangle_{A_1}\right), \tag{2.4}$$

where $u, v, i, j \in \{0,1\}$, $j(i)$=0 or 1 can equivalently be considered that Alice (Bob) has chosen the Z-basis (the eigenstates of the Pauli matrix σ_Z, simply called the Z-basis) or the X-basis (the eigenstates of the Pauli matrix σ_X, simply called the X-basis), while $u(v)$=0 or 1 respectively represent the occurrence of a bit error or a phase error in the channel. P_u and P_v represent the probabilities of Eve introducing the operators $X_{E_1}^{u}$ and $Z_{E_2}^{v}$, while Q_i and Q_j respectively represent the probabilities of Bob and Alice introducing operations $H_{B_1}^{i}$ and $H_{A_1}^{j}$. Without loss of

generality, we can assume that Alice and Bob choose the Z and X bases with equal probabilities, i.e., for $i, j \in \{0,1\}$ both $Q_i = \frac{1}{2}$ and $Q_j = \frac{1}{2}$.

After the "basis comparison and sifting" operations, cases where $i \neq j$ will be discarded. Since Alice and Bob do not know Eve's particles, we can take the trace over the three-party quantum system to obtain the density matrix

$$\begin{aligned}\rho_{AB} = \sum_{u,v} P_u P_v \Bigg(& \frac{1}{2} I_A \otimes X_{E_1}^{u} Z_{E_2}^{v} \left|\phi_1\right\rangle\left\langle\phi_1\right| Z_{E_2}^{v} X_{E_1}^{u} \otimes I_A \\ & + \frac{1}{2} I_A \otimes H_{B_1}^{i} X_{E_1}^{u} Z_{E_2}^{v} H_{A_1} \left|\phi_1\right\rangle\left\langle\phi_1\right| H_{A_1} Z_{E_2}^{v} X_{E_1}^{u} H_{B_1}^{i} \otimes I_A \Bigg).\end{aligned} \tag{2.5}$$

After passing through the quantum channel, the corresponding quantum states transform into the following four states:

$$\begin{aligned}\left|\phi_1\right\rangle &= \frac{\sqrt{2}}{2}\left(\left|00\right\rangle_{AB} + \left|11\right\rangle_{AB}\right), \\ \left|\phi_2\right\rangle &= \frac{\sqrt{2}}{2}\left(\left|01\right\rangle_{AB} + \left|10\right\rangle_{AB}\right), \\ \left|\phi_3\right\rangle &= \frac{\sqrt{2}}{2}\left(\left|00\right\rangle_{AB} - \left|11\right\rangle_{AB}\right), \\ \left|\phi_4\right\rangle &= \frac{\sqrt{2}}{2}\left(\left|01\right\rangle_{AB} - \left|10\right\rangle_{AB}\right),\end{aligned} \tag{2.6}$$

where

$$\begin{aligned}\left|\phi_2\right\rangle &= X_{E_1}\left|\phi_1\right\rangle, \\ \left|\phi_3\right\rangle &= Z_{E_2}\left|\phi_1\right\rangle, \\ \left|\phi_4\right\rangle &= X_{E_1}^{u} Z_{E_2}^{v}\left|\phi_1\right\rangle.\end{aligned} \tag{2.7}$$

Based on equations (2.6) and (2.7), we can rewrite the density matrix in equation (2.5) as:

$$\rho_{AB} = p_1\left|\phi_1\right\rangle\left\langle\phi_1\right| + p_2\left|\phi_2\right\rangle\left\langle\phi_2\right| + p_3\left|\phi_3\right\rangle\left\langle\phi_3\right| + p_4\left|\phi_4\right\rangle\left\langle\phi_4\right|. \tag{2.8}$$

Both bit errors and phase errors in the Pauli channel can be considered introduced by the eavesdropper Eve. From equation (2.7), it can be observed that the initially shared quantum state $\left|\phi_1\right\rangle$ transforms into $\left|\phi_2\right\rangle$, $\left|\phi_3\right\rangle$, and $\left|\phi_4\right\rangle$, corresponding to Eve introducing bit errors, phase errors, and bit-phase errors in the channel, respectively. Therefore, the final bit error rate and phase error rate can be respectively expressed as:

$$\begin{aligned}e_b &= \left\langle\phi_2\right|\rho_{AB}\left|\phi_2\right\rangle + \left\langle\phi_4\right|\rho_{AB}\left|\phi_4\right\rangle = p_2 + p_4, \\ e_p &= \left\langle\phi_3\right|\rho_{AB}\left|\phi_3\right\rangle + \left\langle\phi_4\right|\rho_{AB}\left|\phi_4\right\rangle = p_3 + p_4,\end{aligned} \tag{2.9}$$

where e_b and e_p represent the bit error rate and the phase error rate, respectively. It is noteworthy

that $HZH = X$, substituting into equation (2.5), we obtain:

$$e_p - e_b = p_2 - p_3 = 0. \tag{2.10}$$

Therefore, we can observe that the bit errors under the *Z* basis are equal to the phase errors under the *X* basis, while the bit errors under the *X* basis are equal to the phase errors under the *Z* basis. The secure key rate after error correction and privacy amplification, eliminating the errors and mutual information with the eavesdropper Eve, can be expressed as:

$$R = \frac{1}{2}\left(1 - H_2\left(e_b\right) - H_2\left(e_p\right)\right). \tag{2.11}$$

Although researchers have provided unconditional security proofs for the BB84 protocol at the information-theoretic level, it is evident that this security proof implicitly assumes that "Alice and Bob's source and detection ends are ideal, physically secure areas where eavesdroppers cannot intrude" and "Alice and Bob have ideal, trusted devices for preparing and measuring quantum states." In theoretical proofs, these assumptions seem reasonable; however, unfortunately, real devices possess numerous non-ideal characteristics, making it difficult for users to prepare the ideal quantum states required for security proofs, while Eve can exploit these non-ideal characteristics to intrude into the source and detection ends. The introduction of BB84-QKD has not put an end to the struggle between encryption and eavesdropping [14].

2.3.3 Other protocols

After the proposal of the BB84 protocol, its security was rigorously proven [15], [17]. Researchers have also attempted to design QKD protocols from different principles and perspectives. These protocols can mainly be classified into two categories based on the spatial dimensions of the signal source encoding: discrete variable (DV) and continuous variable (CV). The mainstream discrete variable protocols include:

Proposed by Ekert in 1991, the E91 protocol was the first to use the concept of entanglement for key generation [18]. Both parties share an entangled pair and use different basis vectors for measurement to achieve the generation of correlated keys and security verification. In this protocol, the violation of Bell inequalities or equivalent CHSH inequalities is used to detect the presence of eavesdroppers.

Proposed by Bennett in 1992, the B92 protocol requires only two non-orthogonal states compared to the BB84 protocol to complete the entire process, reducing the implementation complexity [19]. However, due to its low efficiency, it did not replace BB84 and become a mainstream protocol.

The BBM92 protocol is similar to the E91 protocol, using entangled light sources and testing for

Bell state correlations [20]. In terms of security, it uses methods similar to the BB84 protocol for error detection. Therefore, the BBM92 protocol is also known as an equivalent entanglement protocol of BB84.

The SARG04 protocol is designed to counter Photon Number Splitting (PNS) attacks [21]. In this protocol, two pre-agreed non-orthogonal quantum state sets are used to resist eavesdroppers' PNS attacks. When generating keys, both single-photon and two-photon components are secure. However, due to its efficiency being only half that of the BB84 protocol, it only has certain advantages when the light intensity is strong and there are many multi-photon components.

Phase-encoded distribution protocol encodes information based on the relative phase difference between two pulses and includes several variations such as differential phase shift (DPS) protocol [22], coherent one-way (COW) protocol [23], and Round-Robin differential phase shift (RRDPS) protocol [24]. Among them, the DPS protocol-based high-speed experimental system is relatively easy to implement, but its complete security proof is still lacking. The RRDPS protocol can eliminate error monitoring and demonstrates good research value.

The measurement device independent QKD (MDI-QKD) protocol places the measurement terminal in an untrusted third party [25]. Both communicating parties send prepared encoded states to the measurement terminal, where Bell state measurements are performed, and the measurement results are announced. This setup can immunize against attacks on the measurement terminal, with security guaranteed by entanglement swapping.

The twin-field QKD (TF-QKD) protocol is a special type of measurement device independent protocol [26]. In this protocol, both users prepare twin-field states sent to the measurement terminal, where single-photon interference measurements are conducted. This scheme is similar to the original MDI-QKD protocol in terms of apparatus but based on single-photon interference, significantly improving the transmission distance.

Additionally, common discrete variable protocols also include the six-state protocol [27] and the Ping-Pong protocol [28], among others.

CV QKD protocols utilize the canonical components of optical field states to carry information, often in the form of continuous distributed Gaussian random numbers. These protocols mainly include squeezed state protocols [29], coherent state protocols [30], and entanglement state protocols. As this paper primarily focuses on DV QKD protocols, these CV QKD protocols will not be further discussed.

2.4 Loopholes of practical QKD system

QKD protocols assume certain characteristics about the actual devices used in their security proofs, yet no real-world system is flawless. During an attack, an eavesdropper will attempt to acquire more information than the communicating parties believe is possible. Since the theoretical security

of QKD is based on quantum mechanics, the only way to obtain more information is when the assumptions about the user devices do not hold. Below, we will discuss some common practical vulnerabilities and corresponding attack methods.

2.4.1 PNS attack

The theoretical security of the BB84 protocol has been proven by researchers from both an information-theoretic and physical perspective. However, the protocol theoretically employs an ideal single-photon source, which is difficult to realize in practice. The commonly used weak coherent source (WCS) [24-26] contains multiphoton components: for example, under Eq.2.1 with $\mu = 0.5$, the probability of sending zero photons $P_0(0.5) = 0.607$, sending a single photon $P_1(0.5) = 0.303$, and the probability of sending more than two photons ($n \geq 2$) is 0.09. In this case, an eavesdropper can perform what is known as the photon number splitting (PNS) attack [31]. The basic idea of the PNS attack is as follows: Eve performs a non-destructive measurement on the pulses, and if she finds more than one photon, she will separate one photon and send the remaining photons to Bob. In such a scenario, Bob cannot detect the presence of eavesdropping, and Eve only needs to wait for Alice to announce her basis choice before measuring the separated photon, thereby obtaining the same information as Bob. Here, we assume that the eavesdropper, Eve, is omnipotent under the premise of not violating the laws of physics or any axioms. That is, in this attack, the eavesdropper can perform the PNS attack using a lossless channel and quantum storage.

Eve can analyze the number of photons per pulse and intercept all single-photon pulses. Then she separates all of the multi-photon pulses, keeps one photon of them, and sends the rest pulses to Bob. This makes Eve's photons the same quantum state as Bob's photons. She can wait for Alice and Bob to disclose the basis, and then measure her own photons. Finally, Eve can get exactly the same key as Bob.

Notice that when Eve intercepts all single photon pulses, although it seems to result in a significant reduction in the number of pulses that Bob can receive to make eavesdropping to be detected, channel losses due to the practical long distance QKD system is very large. These losses are mixed in with channel losses and cannot be easily distinguished.

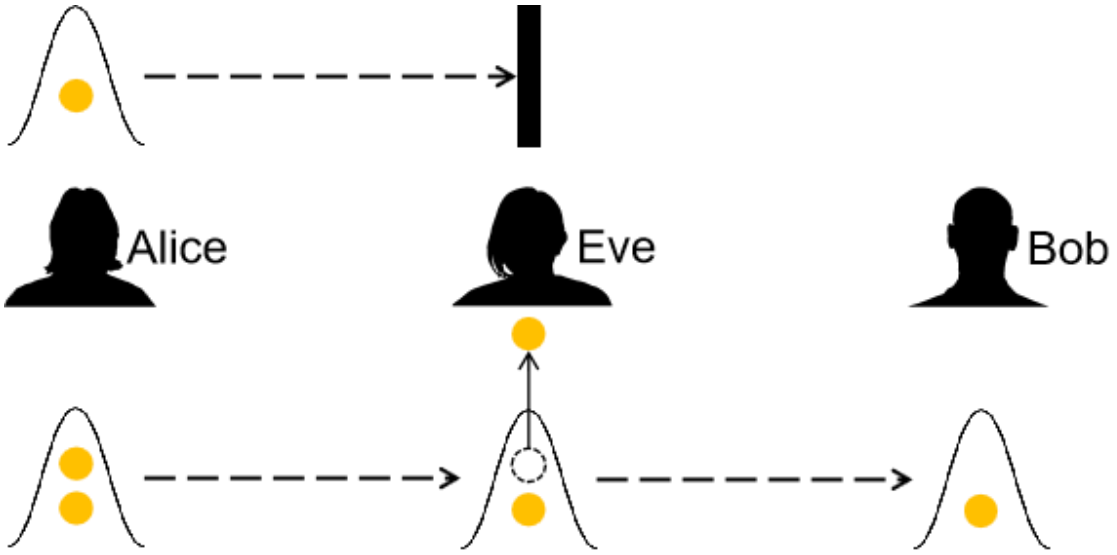


Figure 2.5. A schematic diagram illustrating the principle of PNS attack.

Under the PNS attack, QKD can still generate secure keys. In 2004, Gottesman and others proposed the "GLLP" analysis method, which is based on the theory of entanglement purification and provides a secure key rate for the BB84 protocol under a PNS attack [32]. In this theory, the security analysis is based on the worst-case assumption that all multiphoton pulses are controlled by Eve. Let the probability of multiphoton pulses be P_{multi}, and the probability of a light pulse being received be Q. Then, the probability of Eve eavesdropping is defined as $\Delta = P_{multi}/Q$. In this scenario, the portion of the pulses that can be used to generate keys is reduced to $1-\Delta$. Furthermore, under the worst-case assumption, all errors are considered to be caused by single photons. If the observed error rate is δ, then the error rate for single photons is given by $\tilde{\delta}_p = \frac{\delta}{1-\Delta} + \varepsilon$ (where $\varepsilon > 0$). The final secure key rate formula can be derived from these considerations:

$$R = Max\left[(1-\Delta) - H_2(\delta) - (1-\Delta)H_2\left(\frac{\delta}{1-\delta}\right), 0\right], \tag{2.12}$$

where $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

In the case of using WCS, when the intensity $\xi \ll 1$, the probability of a pulse being a single photon is $P_1 = \mu + O(\mu^2)$, and the probability of it being a multiphoton pulse is $P_{multi} = \frac{1}{2}\mu^2 + O(\mu^3)$. In this scenario, the probability of a photon being detected by Bob is $Q = \eta(\mu + \mu^2)$. Consequently, the probability of Eve eavesdropping can be expressed as:

$$\Delta = \frac{P_{multi}}{Q} = \frac{\mu + O(\mu^2)}{2\eta}. \tag{2.13}$$

where η represents the channel transmittance. In this case, the post-sifting key rate can be expressed as $\frac{1}{2}Q \approx \frac{1}{2}\eta\mu \approx \eta^2\Delta$, where the coefficient $\frac{1}{2}$ represents the basis efficiency of the BB84 protocol. It can be observed that the final rate is approximately proportional to the square of the channel transmittance, i.e., $R \sim O(\eta^2)$.

2.4.2 Decoy state method

Under the PNS attack, the key rate is significantly reduced due to the broad estimation of the error rate and yield for single photons. In the absence of practical single-photon technologies, researchers have proposed the decoy state method [33]-[35]. With this method, light sources containing multiphoton components can also be used securely and efficiently in practical applications.

The key point of the decoy state method lies in modulating decoy states $(\nu_1, \nu_2, ...)$ in addition to preparing the original signal intensity μ. When the decoy states and signal states have similar characteristics (such as timing information and wavelength), the eavesdropper can only obtain information about the photon number in the pulses, unable to distinguish which pulse comes from which source. Therefore, the yield Y_n and quantum bit error rate (QBER) e_n of both states are only dependent on the photon number and are independent of the source intensity. In other words:

$$\begin{aligned} Y_n(signal) &= Y_n(decoy) = Y_n, \\ e_n(signal) &= e_n(decoy) = e_n. \end{aligned} \tag{2.14}$$

After communication, Alice and Bob can statistically obtain the corresponding gains and error rates for the chosen post-selection. These two quantities can be represented as weighted averages of the probabilities of events with *n* photons:

$$\begin{aligned} &Q_\mu = \sum_{n=0}^{\infty} P_n(\mu) Y_n, E_\mu Q_\mu = \sum_{n=0}^{\infty} P_n(\mu) e_n Y_n, \\ &Q_\nu = \sum_{n=0}^{\infty} P_n(\nu) Y_n, E_\nu Q_\nu = \sum_{n=0}^{\infty} P_n(\nu) e_n Y_n, \nu \in \{\nu_1, \nu_2, ...\}. \end{aligned} \tag{2.15}$$

When the number of decoy states ν is infinitely large, the values of Y_n and e_n can be accurately solved. However, in practice, the number of decoy states is finite. Wang [35] utilized three intensities and modulated the signal state μ, decoy state ν, and vacuum state *o*. By using analytical methods, it is possible to solve for the response rate Y_1 and error rate e_1 for single photons. Finally, the key rate formula inheriting the GLLP ideology can be expressed as [34]:

$$R \geq q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{2.16}$$

where *q* depends on the implementation (1/2 for the BB84 protocol, because half the time Alice and Bob basis are not compatible, and if we use the efficient BB84 protocol [32], we can have *q*=1). Q_μ and E_μ are the gain and quantum bit error rate (QBER) of the signal state, respectively. Here, the gain means the ratio of the number of Bob's detection events (where Bob chooses the same basis as

Alice) to Alice's number of emitted signals. QBER means the error rate of Bob's detection events for the case that Alice and Bob use the same basis. And $f(E_\mu)$ is the error correction efficiency [36].

In practical system, Q_μ and E_μ can be directly measured experimentally. In addition, Q_1 is the gain and e_1 is the bit error rate of single photon in the signal state. They can be calculated by using the decoy state method. The lower bound of the gain of single-photon Q_1 is

$$Q_1 \geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right). \tag{2.17}$$

Similarly, Q_ν represents the gain of decoy state. And Y_0 represents yield of vacuum state, representing the probability that Bob's detector responds when it receives vacuum state pulse. Then the upper bound of single photon bit error rate e_1 is

$$e_1 \leq \frac{E_\nu Q_\nu e_\nu - e_0 Y_0}{\min(Y_1)\nu}, \tag{2.18}$$

where e_0 means the bit error rate of vacuum state, and Y_1 means the detection rate of single photon by Bob's detector, whose lower bound is

$$Y_1 \geq \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right). \tag{2.19}$$

Here, E_ν, Q_ν and Y_0 can also be directly measured by experiments. With decoy state method, the limit transmission distance of QKD system can reach 142 km by simulation [37]. BB84 protocol can be applied practically without perfect single photon source. So, decoy state method has been widely used.

Figure 2.3 illustrates the difference in key rates before and after using the decoy state method. It can be observed that, based on the GLLP formula, the decoy state method significantly enhances both transmission distance and key rate. As mentioned earlier, without using decoy states, the GLLP key rate is proportional to the square of the channel transmittance. However, with the use of decoy state method, it returns to the level comparable to schemes using single-photon sources, i.e., proportional to the first power of the transmittance.

When employing the decoy state method, researchers have proposed a passive decoy state method in addition to the active modulation of decoy states [38]-[40]. Unlike the active decoy state method, which uses intensity modulators and other devices to actively adjust the light intensity, the passive decoy state method utilizes statistical probabilities of trigger and non-trigger events detected by Alice's local detectors, equivalent to the probability distributions of photon numbers obtained under different intensities. This passive approach can be immune to imperfections introduced by intensity modulators or some side-channel vulnerabilities, thus offering practical value.

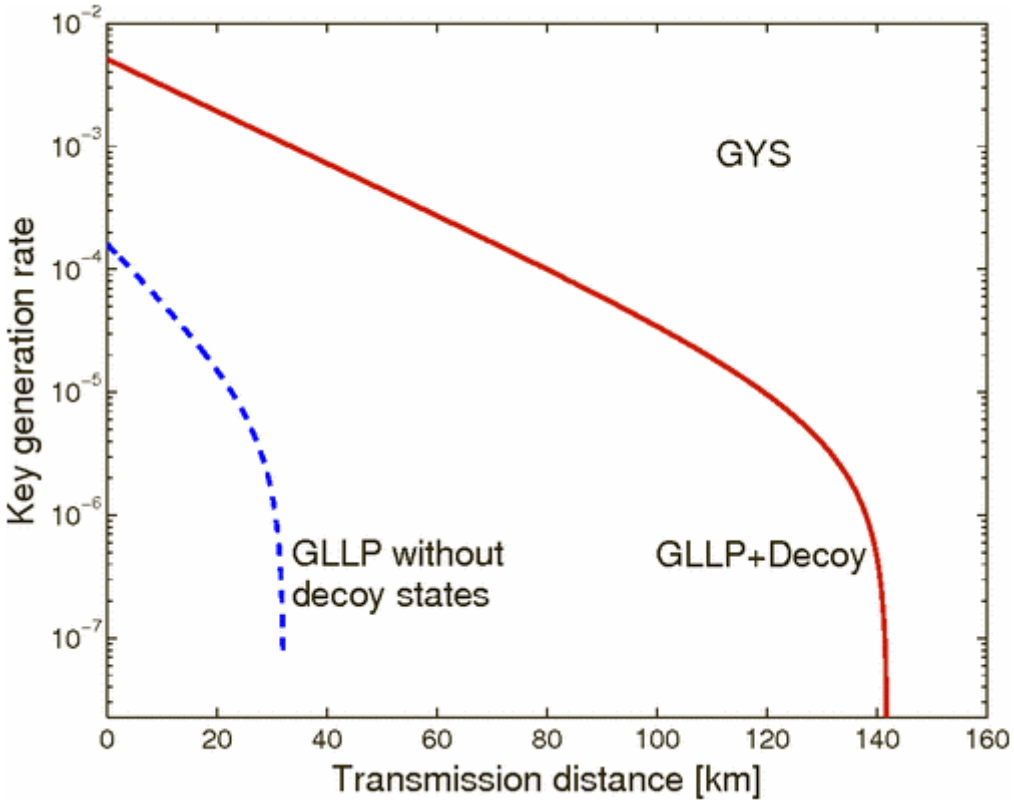


Figure 2.6. The variation of the key rate with transmission distance under the GLLP formula for both the scenarios with and without using decoy states [34].

2.4.3 Other common attack methods

In the preceding two sections, we focused on introducing the PNS attack and the corresponding countermeasure, the use of decoy states. Now, we will briefly introduce other common attacks targeting QKD.

Trojan Horse Attack: In QKD, the Trojan horse attack is a method of obtaining user information by emitting light pulses. Vakhitov et al. [41] targeted the BB84 and B92 protocols, where strong light pulses are sent into the user's channel, and by measuring the light emitted back, they gain knowledge about the legitimate user's preparation and measurement basis choices. In this way, eavesdroppers can obtain the same bit information as the legitimate users without introducing errors. Additionally, eavesdroppers can use Trojan horse attacks to target intensity modulators to steal Alice's modulation information. If eavesdroppers can distinguish decoy states from signal states, they can continue to use PNS attacks to obtain information even when users employ the decoy state method. Generally, defenses against Trojan horse attacks include increasing isolators, fiber loop mirrors, attenuators, etc., to filter or increase attenuation, thereby increasing the difficulty for eavesdroppers to obtain information.

Time-shift Attack: Systems such as polarization coding and phase coding typically use two

detectors, with the avalanche photodiode detector (APD) being commonly used in the 1550 nm band. In security analysis and theoretical assumptions, the performance parameters of the two detectors are often assumed to be the same. However, in practical applications, the detection efficiency of different detectors varies over time [42]. The time-shift attack proposed by Lo et al. [43] exploits the inconsistency in detection efficiency over time to control the arrival time of light pulses at the receiver, increasing the eavesdropper's probability of correctly guessing the results. The greater the difference between the two detectors, the higher the probability of successful eavesdropping.

Strong Light Blinding Attack: The strong light blinding attack [44], proposed by the Makarov group against the flaws of APD, operates in linear mode and Geiger mode. The strategy of the strong light blinding attack is to lower the reverse bias or increase the reverse breakdown voltage of APD by incident light, causing the APD to not operate in Geiger mode. When operating in linear mode, eavesdroppers can use the fake-state attack [45] to control the receiver's information without increasing the error rate, thus obtaining all the information without alerting the user.

Phase Remapping Attack: Ideally, the function of a phase modulator is to add a given additional phase to the pulse. However, in practical use, the phase modulator is controlled by non-ideal square waves. For "plug-and-play" systems, eavesdroppers can control the time of light pulse incidence on the sender to reach the moment of rising edge of the phase modulator control voltage, causing the corresponding loaded phase not to be the value pre-set by the sender [46]. Eavesdroppers can then optimize the incidence time through measurement to reduce errors, thereby avoiding detection by the user.

2.4.4 Side-channel loopholes

Side-channel loopholes, also known as side-channel vulnerabilities, refer to vulnerabilities caused by the additional characteristics such as performance, power consumption, radiation, etc., that can be detected when devices perform encryption and decryption operations. In an ideal protocol, such loopholes would not exist. However, in practice, imperfections in encoding/decoding or detection devices may leak relevant information.

In the first BB84 experiment, Bennett et al. utilized polarization encoding to achieve spatial transmission of 32 cm [47]. However, during the entire experiment, emitting different polarization states would produce noise at different frequencies. That is to say, if the eavesdropper knows which polarization state corresponds to this sound, then the entire system is completely in an unsafe environment. In 2001, German researchers found that detectors emit fluorescence after detecting photons, and eavesdroppers can detect the leaked fluorescence to identify which detector corresponds to the response [48]. This loophole is actually quite deadly, as eavesdroppers can obtain critical response information without introducing any errors during the attack, without interfering with the states and measurements of the sending parties. In 2007, Kurtsiefer et al. discovered that different detectors have different average response times [49]. At this time, there would be a

correlation between the publicly disclosed response times of the communication parties and the detection results. In addition, in some early experimental systems, multiple lasers were used to prepare different polarization states [50]. Researchers found that pulses of different polarization states produced by these lasers have differences in the time domain, space domain, and frequency domain. Therefore, eavesdroppers can extract encoding information by targeting detection of light, thereby completing eavesdropping.

The main reason for the above side-channel vulnerabilities is that there is a certain correlation between the encoding state or measurement results and some other dimensional information. Eavesdroppers can eavesdrop on encoding and decoding information based on side-channels, thus further obtaining the final key.

2.5 Summary

This chapter introduces the components of QKD systems and common QKD protocols, with a focus on the BB84 protocol. It then emphasizes the photon number splitting (PNS) attack. In response to this attack, QKD protocols, combined with the decoy state method, can achieve secure and efficient key transmission. This lays the groundwork for the subsequent chapters' discussion on practical system implementations.

References

[1] C. H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, Theoretical Computer Science, 2014, 560(1): 7-11.

[2] X Mo. "Experimental Research on Quantum Cryptography," University of Science and Technology of China (USTC), 2006.

[3] X-F Mo, B Zhu, Z-F Han, Y-Z Gui, and G-C Guo, "Faraday–Michelson system for quantum cryptography," Opt. Lett. 30, 2632-2634 (2005).

[4] S Wang, W Chen, Z-Qiang Yin, D-Y He, C Hui, P-L Hao, G-J Fan-Yuan, C Wang, L-J Zhang, J Kuang, S-F Liu, Z Zhou, Y-G Wang, G-C Guo, and Z-F Han, "Practical gigahertz quantum key distribution robust against channel disturbance," Opt. Lett. 43, 2030-2033 (2018).

[5] X.-B. Wang, T. Hiroshima, A. Tomita and M. Hayashi, “Quantum information with Gaussian states”, Physics Reports, 2007, 448(1):1-111.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev.Mod.Phys.74.145 (2002).

[7] N. Gisin and R. Thew, “Quantum communication”, Nature Photonics, 1, 165-171 (2007).

[8] M. Dusek, N. Lutkenhaus and M. Hendrych, “Quantum Cryptography”, Progress in Optics, 2006, 49:381-454, arXiv:quant-ph/0601207.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev,

"The security of practical quantum key distribution", Rev.Mod.Phys.81, 1301 (2009).

[10] Shor, P. W., Preskill, J. "Simple proof of security of the BB84 quantum key distribution protocol," Physical Review Letters, 2000, 85(2): 441–444.

[11] Li, H. "Research on quantum cryptography security." Hefei: University of Science and Technology of China, 2012.

[12] Coffman, V., Kundu, J., Wootters, W. K. "Distributed entanglement," Physical Review A, 2000, 61(5): 052306.

[13] Koashi, M., Winter, "A. Monogamy of quantum entanglement and other correlations," Physical Review A, 2004, 69(2): 022309.

[14] Xu, F., Ma, X., Zhang, Q., et al. "Secure quantum key distribution with realistic devices," Reviews of Modern Physics, 2020, 92(2): 025002.

[15] Lo H K, Chau H F. "Unconditional security of quantum key distribution over arbitrarily long distances," Science, 1999, 283(5410): 2050-2056.

[16] Shor P W, Preskill J. "Simple proof of security of the BB84 quantum key distribution protocol," Physical Review Letters, 2000, 85(2): 441.

[17] Mayers D. "Unconditional security in quantum cryptography," Journal of the ACM (JACM), 2001, 48(3): 35 1-406.

[18] Ekert A K. "Quantum cryptography based on Bell's theorem," Physical Review Letters, 1991, 67(6): 661.

[19] Bennett C H. "Quantum cryptography using any two nonorthogonal states," Physical Review Letters, 1992, 68(21): 3 121.

[20] Bennett C H, Brassard G, Mermin N D. "Quantum cryptography without Bell's theorem," Physical Review Letters, 1992, 68(5): 557.

[21] Scarani V, Acin A, Ribordy G, et al. "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Physical Review Letters, 2004, 92(5): 057901.

[22] Inoue K, Waks E, Yamamoto Y. "Differential phase shift quantum key distribution," Physical Review letters, 2002, 89(3): 037902.

[23] Stucki D, Brunner N, Gisin N, et al. "Fast and simple one-way quantum key distribution," Applied Physics Letters, 2005, 87(19): 194108.

[24] Sasaki T, Yamamoto Y, Koashi M. "Practical quantum key distribution protocol without monitoring signal disturbance," Nature, 2014, 509(7501): 475-478.

[25] Lo H K, Curty M, Qi B. "Measurement-device-independent quantum key distribution," Physical Review Letters, 2012, 108(13): 130503.

[26] Lucamarini M, Yuan Z L, Dynes J F, et al. "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature, 201 8, 557(7705): 400-403.

[27] Bruß D. “Optimal eavesdropping in quantum cryptography with six states,” Physical Review Letters, 1998, 8 1(14): 301 8.

[28] Boström K, Felbinger T. “Deterministic secure direct communication using entanglement,” Physical Review Letters, 2002, 89(1 8): 1 87902.

[29] Cerf N J, Levy M, Van Assche G. “Quantum distribution of Gaussian keys using squeezed states,” Physical Review A, 2001, 63(5): 0523 1 1.

[30] Grosshans F, Grangier P. “Continuous variable quantum cryptography using coherent states,” Physical Review Letters, 2002, 88(5): 057902.

[31] Brassard G, Lütkenhaus N, Mor T, et al. “Limitations on practical quantum cryptography,” Physical Review Letters, 2000, 85(6): 1330.

[32] Gottesman D, Lo H K, Lutkenhaus N, et al. “Security of quantum key distribution with imperfect devices,” International Symposium on Information Theory, 2004. ISIT 2004. Proceedings. IEEE, 2004: 136.

[33] Hwang W Y. “Quantum key distribution with high loss: toward global secure communication,” Physical Review Letters, 2003, 91(5): 057901.

[34] Lo H K, Ma X, Chen K. “Decoy state quantum key distribution,” Physical Review Letters, 2005, 94(23): 230504.

[35] Wang X B. “Beating the photon-number-splitting attack in practical quantum cryptography,” Physical Review Letters, 2005, 94(23): 230503.

[36] H.-K. Lo, H. F. Chau and M. Ardehali, “Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security”, Journal of Cryptology, 2005, 18(2):133-165.

[37] X. Ma, “Quantum cryptography: theory and practice”, University of Toronto, arXiv:0808.1385.

[38] Adachi Y, Yamamoto T, Koashi M, et al. “Simple and efficient quantum key distribution with parametric down-conversion,” Physical Review Letters, 2007, 99(1 8): 1 80503.

[39] Curty M, Ma X, Qi B, et al. “Passive decoy-state quantum key distribution with practical light sources,” Physical Review A, 2010, 8 1(2): 0223 10.

[40] Wang Q, Zhang C H, Wang X B. “Scheme for realizing passive quantum key distribution with heralded single-photon sources,” Physical Review A, 2016, 93(3): 0323 12.

[41] Vakhitov A, Makarov V, Hjelme D R. “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography,” Journal of Modern Optics, 2001, 48(13): 2023-2038.

[42] Makarov V, Anisimov A, Skaar J. “Effects of detector efficiency mismatch on security of quantum cryptosystems,” Physical Review A, 2006, 74(2): 0223 13.

[43] Qi B, Fung C F, Lo H, et al. “Time-shift attack in practical quantum cryptosystems,” Quantum Information & Computation, 2007, 7(1): 73-82.

[44] Makarov V. “Controlling passively quenched single photon detectors by bright light,” New Journal

of Physics, 2009, 1 1(6): 065003.

[45] Makarov V, Hjelme D R. “Faked states attack on quantum cryptosystems,” Journal of Modern Optics, 2005, 52(5): 691-705.

[46] Fung C H F, Qi B, Tamaki K, et al. “Phase-remapping attack in practical quantum-key-distribution systems,” Physical Review A, 2007, 75(3): 0323 14.

[47] Bennett C H, Bessette F, Brassard G, et al. “Experimental quantum cryptography,” Journal of Cryptology, 1992, 5(1): 3-28.

[48] Kurtsiefer C, Zarda P, Mayer S, et al. “The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks,” Journal of Modern Optics, 2001, 48(13): 2039-2047.

[49] Lamas-Linares A, Kurtsiefer C. “Breaking a quantum key distribution system through a timing side channel,” Optics Express, 2007, 1 5(1 5): 9388-9393.

[50] Nauerth S, Fürst M, Schmitt-Manderb ach T, et al. “Information leakage via side channels in free space BB84 quantum cryptography,” New Journal of Physics, 2009, 1 1(6): 065001.

Chapter 3

Measurement-device-independent quantum key distribution

3.1 Introduction

Quantum key distribution enables distant parties to securely exchange keys. While the security of QKD protocols has been theoretically proven, ensuring the security of practical QKD systems still faces significant challenges. Before security proofs can be applied in practical scenarios, vulnerabilities arising from imperfections in various devices must be carefully tested. For instance, mismatches in detector efficiency can be exploited by eavesdroppers to carry out efficiency mismatch attacks [1] or time-shift attacks [2]. Other imperfections, such as detector dead times, can also be exploited by attackers, posing threats to the security of practical systems [3]. Despite countermeasures being proposed for these attacks, completely eliminating them requires addressing the root cause - detector efficiency vulnerabilities. The security vulnerabilities of QKD systems stem from issues in current Bell inequality tests, primarily consisting of three types of vulnerabilities corresponding to the three assumptions of Bell inequality tests.

1. Spatial Leakage [4], corresponding to the assumption that the two parties appear spatially separated.

2. Efficiency Leakage [5], corresponding to the fair sampling assumption.

3. Random Leakage, corresponding to the assumption that measurement bases are randomly chosen.

In QKD, some of these leaks have been proven to be more dangerous. For instance, it can be reasonably assumed that the information of legitimate parties Alice and Bob is protected from being known to eavesdropper Eve. Therefore, spatial leakage is unlikely to lead to attack behavior. With the development of quantum random number generators [6], random leakage may also no longer pose security issues. However, efficiency leakage creates opportunities for many attack methods, all of which exploit efficiency leakage.

Summarizing some of the attack methods from the previous chapter, it can be observed that certain attacks targeting the source end are relatively easier to address, such as the decoy state method and the addition of isolators for necessary protection. However, attacks exploiting

imperfections in detectors have become a more serious problem. To address this issue, one approach is to patch existing vulnerabilities by precisely characterizing the leaks or discrepancies, and then making corresponding modifications in security analysis and rate estimation. For example, in response to the previously mentioned bright light blinding attack, Z. Yuan et al. proposed adding strong light detection devices at the receiver end and adjusting the load resistance of detectors to prevent eavesdropping [7]. While this "patching leaks" approach can sometimes be effective, accurately modeling all vulnerabilities may require additional monitoring equipment and time, and there is no guarantee that all leaks have been patched.

Another solution is to relax the requirement for trusted devices in practical systems, a protocol known as Device-Independent (DI) QKD protocol. A prominent DI protocol proposed by Acin et al. [8]-[10] involves sending entangled states to both Alice and Bob, who then perform Bell state measurements to calculate the violation of the CHSH inequality, quantifying the amount of information obtained by Eve:

$$\langle S \rangle = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle . \tag{3.2}$$

In this protocol, there is no longer a requirement for trusted devices; instead, ensuring flawless Bell state testing guarantees the security of the system. However, achieving flawless Bell state testing is not straightforward. It requires ensuring that locality loopholes and detection loopholes are not exploited by eavesdroppers, with a total detection efficiency requirement exceeding 82.8%. This implies that even if the detection efficiency of single-photon detectors reaches 100%, the secure transmission distance of the system is only about 4 kilometers. Moreover, the current practicality of DI-QKD is limited, as the efficiency of commonly used InGaAs/InP infrared single-photon avalanche photodiodes is in the order of 20%, and silicon-based visible light single-photon avalanche photodiodes is only around 65% ($\lambda \approx 700$nm). These requirements are difficult to achieve with the existing technology in experiment. Therefore, the implementation of DIQKD is challenging under current conditions, and its practicality is limited.

In this scenario, researchers have proposed the concept of Measurement Device Independent Quantum Key Distribution (MDI-QKD) [11], [12]. This method is based on the idea of entanglement swapping, where both communicating parties send optical pulses to an untrusted third party (UTP) for measurement. This third party can be either secure or controlled by an eavesdropper. In this case, since there is no requirement for the security of the measurement side, the protocol can resist attacks against the detection side.

In major QKD protocol such as BB84 protocol, one party prepares the quantum state, and the other party receives and measures the quantum state. The MDI-QKD protocol does not follow this process at all. The quantum state is measured by a third party with no requirements for security. Eve can even control the measuring device.

3.2 MDI-QKD protocols

The most significant advantage of MDI-QKD systems is their ability to withstand all detector-side channel attacks, whether they are known attacks or potential security threats. In MDI-QKD systems, users can outsource the most challenging part of QKD—the photon detection system—to an untrusted third party without compromising the overall system security. This means that we can achieve the ideal mode of communication: even with completely untrusted network nodes (created by an adversarial third party), secure communication can still be achieved between two communicating nodes.

First, Alice and Bob each prepare random pulse sequences and then send the pulses to the third party located in the middle: the detector. No assumptions are made about the detector, and it can even be an untrusted eavesdropper like Eve. The detector performs Bell state measurements on the two input photons. In the detector, the two photons first undergo interference at a beamsplitter (BS), and then they are sent to two detectors to detect the quantum state of the photons. If Alice and Bob's photons interfere to form a Bell state, the measurement is successful.

Once the quantum communication steps are completed, the third party utilizes a public channel to announce the measurement results and informs Alice and Bob of the successful measurement times. Alice and Bob then select the bit information of their respective successful measurement times as their raw key and discard the data from other times. The public announcement of measurement results means that even if there is an eavesdropper present, their eavesdropping is meaningless—all measurement terminal information is not hidden but disclosed to the outside world. Therefore, Eve does not need to employ any eavesdropping means to obtain all the information from the measurement terminal. Even if Eve alters the measurement results at the detection moment, Alice and Bob can still detect Eve's tampering behavior based on the broadcast measurement results, rendering Eve's eavesdropping behavior non-covert.

MDI-QKD systems are entirely feasible in practice. The scheme can utilize standard optical devices and operate over high-loss channels. For example, the scheme only requires attenuated laser pulses instead of ideal single-photon sources, and low-efficiency detectors can be used. Alice and Bob can also estimate the probability of successful measurement and the quantum bit error rate for different input photon numbers.

The security of MDI-QKD relies on the time-reversed EPR (Einstein-Podolsky-Rosen) QKD protocol. The EPR-QKD protocol involves the preparation party initially preparing entangled pairs and then sending one photon from the entangled pair to Alice and the other to Bob to share key information. The process of MDI-QKD is exactly the reverse process of EPR-QKD, where Alice and Bob first prepare single photons separately and then send them to the measurement terminal to form entangled pairs. Therefore, the security proof of MDI-QKD is equivalent to the security of EPR-QKD.

3.2.1 Polarization encoding MDI-QKD protocol

Refer to polarization coding MDI-QKD [11] proposed by Lo et al in 2012. In the case of single photon, Alice and Bob randomly prepare quantum states |0> and |1> (Z basis) and |+> and |-> (X basis) in two-dimensional Hilbert space. Then Alice and Bob send the photons simultaneously to Charlie, an untrusted third party. Charlie performs the Bell state measurement after receiving the photons sent by Alice and Bob. This causes the photons to collapse into one of the four complete Bell states $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$. Then Charlie discloses the results to Alice and Bob through classical channel. According to the measurement results, Alice and Bob keep the events in successful Bell state measurement and discard the unsuccessful events. After basis reconciliation through classical channel, Alice and Bob need to perform post-processing such as error correction and privacy amplification to extract the final key.

Disclosed measurement results provide no information on the key, though Eve can get all the information on detector side. Even if Eve changes the measurement results, Alice and Bob can still find eavesdropping behavior based on the broadcasted measurement results. Therefore, Eve's eavesdropping behavior will not be covert.

The security proof of MDI-QKD depends on the time reversal EPR-QKD protocol. In EPR-QKD protocol, entangled photons pair is first prepared by the sender. Then one photon of the entangled pair is sent to Alice and another to Bob. In MDI-QKD, Alice and Bob first prepare single photons, and send them to the detector side to generate entanglement between Alice and Bob. The process is exactly the time inverse process of EPR-QKD protocol. Therefore, the security proof of MDI-QKD is equivalent to that of EPR-QKD.

MDI-QKD system is completely feasible. This scheme can be implemented with standard optical devices and high loss channels. For example, detectors with low detection efficiency can be used. Applying decoy state method, MDI-QKD can also use non-ideal single-photon sources (such as weakly coherent sources as in BB84 protocol). Our research is mainly based on the three-intensity decoy state method MDI-QKD containing vacuum state.

The schematic diagram of the decoy state MDI-QKD based on polarization encoding is shown in Fig 3.1. Alice and Bob use weak coherent pulses source (WCP) with random phase. The emitted pulses are prepared by polarization modulator (Pol-M) into one of the four polarization states used in BB84 protocol. The intensity modulator (IM) is used to generate pulses with different intensities for decoy state method. Then Alice and Bob send the photons to Charlie, an untrusted relay, for Bell state measurements. Decoy state method can be used to estimate the yield that means the probability of successful measurement events and phase error at detector side under different input photon numbers.

At the receiver side, photons are interfered by a 50:50 beam splitter (BS). Two outputs of BS connect to a polarizing beam splitter (PBS), respectively. With PBS, photons are transformed into a

horizontal or vertical polarization state. The outputs of each PBS connect to a single-photon detector. A successful Bell state measurement corresponds to the response of two detectors. If the probes D_{10} and D_{21} or D_{11} and D_{20} response at the same time, it means two photons projected into Bell state $|\Psi^-\rangle$. If D_{10} and D_{11} or D_{20} and D_{21} response, Bell state $|\Psi^+\rangle$.

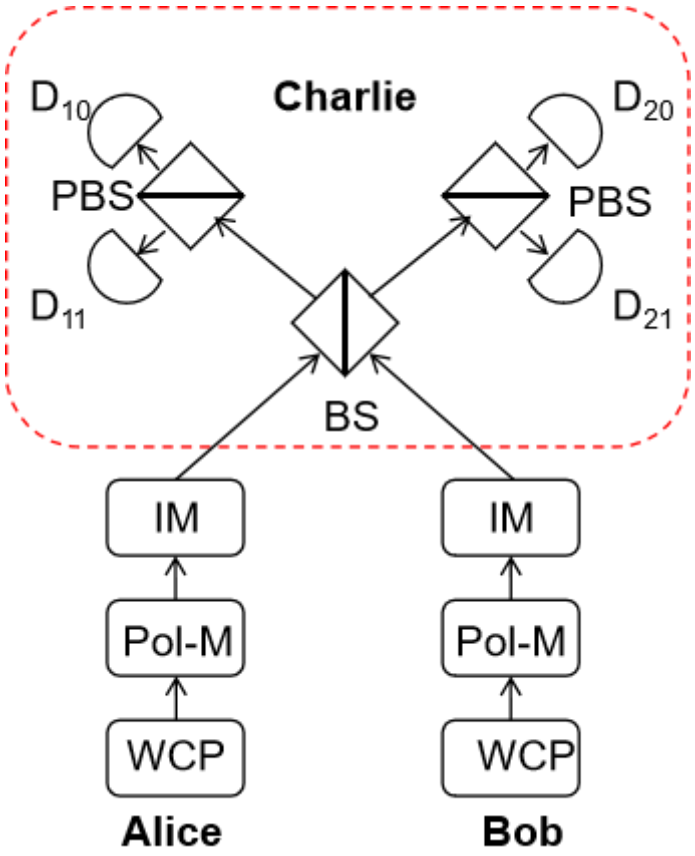


Figure.3.1 A schematic diagram of polarization encoding MDI-QKD.

Decoy state MDI-QKD protocol based on polarization coding has the steps as follows:

(1) Alice and Bob select the basis from $\omega \in \{x, z\}$ with probability p_ω (where $\sum p_\omega = 1$). Then, they randomly assign bit values from $\{0, 1\}$. For the polarization-encoding scheme, the four states are $z_0 = 0°$, $z_1 = 90°$, $x_0 = 45°$, and $x_1 = 135°$.

(2) Alice and Bob randomly generate three types of pulses with different intensities μ_i and ν_j $(i, j = 0, 1, 2)$ with probabilities p_{μ_i} and p_{ν_j} (where $\sum p_{\mu_i} = 1$ and $\sum p_{\nu_j} = 1$), respectively. Here, μ_2 and ν_2 represent the signal state, μ_1 and ν_1 represent the decoy state, and $\mu_0 = \nu_0 = 0$ represents the vacuum state. We assume that $\mu_2 > \mu_1 > 0$ and $\nu_2 > \nu_1 > 0$.

(3) Alice and Bob send pulses via a quantum channel to Charlie, whose device may be under the control of eavesdropper Eve. The total number of pulses is recorded as *N*.

(4) Charlie performs the BSM. Successful results are announced to Alice and Bob via an authenticated classical channel.

(5) If a successful result is reported, Alice and Bob compare their basis and intensities via an authenticated classical channel. If Alice and Bob use the same basis, Bob (or Alice) performs a bit flip according to Charlie's result (as shown in Table 3.1) to match with the other. They then keep these bits as a sift key. The remaining bits are discarded.

Result / Basis	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$
Z basis	Bit flip	Bit flip
X basis	Bit flip	No bit flip

Table 3.1 Rule of Alice and Bob's post-selection

(6) Alice and Bob calculate the overall gain $S^{\omega}_{\mu i \nu_j}$, which is defined as the probability of a successful BSM when Alice and Bob send pulses with intensities of μ_i and ν_j, respectively, in the basis of x or z.

(7) Alice and Bob disclose the sift key sent with basis x to estimate error rate $E^{\mathrm{x}}_{\mu i \nu_j}$. They disclose part of the sift key with basis z to estimate $E^{\mathrm{z}}_{\mu i \nu_j}$. Then, they use the rest of the sift key with basis z of signal states μ_2 and ν_2 to generate the final key.

(8) Alice and Bob correct these errors to generate an error-corrected key. Then, they determine the number of sacrificed bits from the yield and error rate based on the decoy method and perform privacy amplification to obtain the final key.

3.2.2 Phase encoding MDI-QKD protocol

Due to the difficulty in maintaining polarization direction in optical fiber channels, which is greatly affected by channel characteristics, scholars have proposed an MDI QKD scheme based on phase encoding [13], as shown in Figure 3.2.

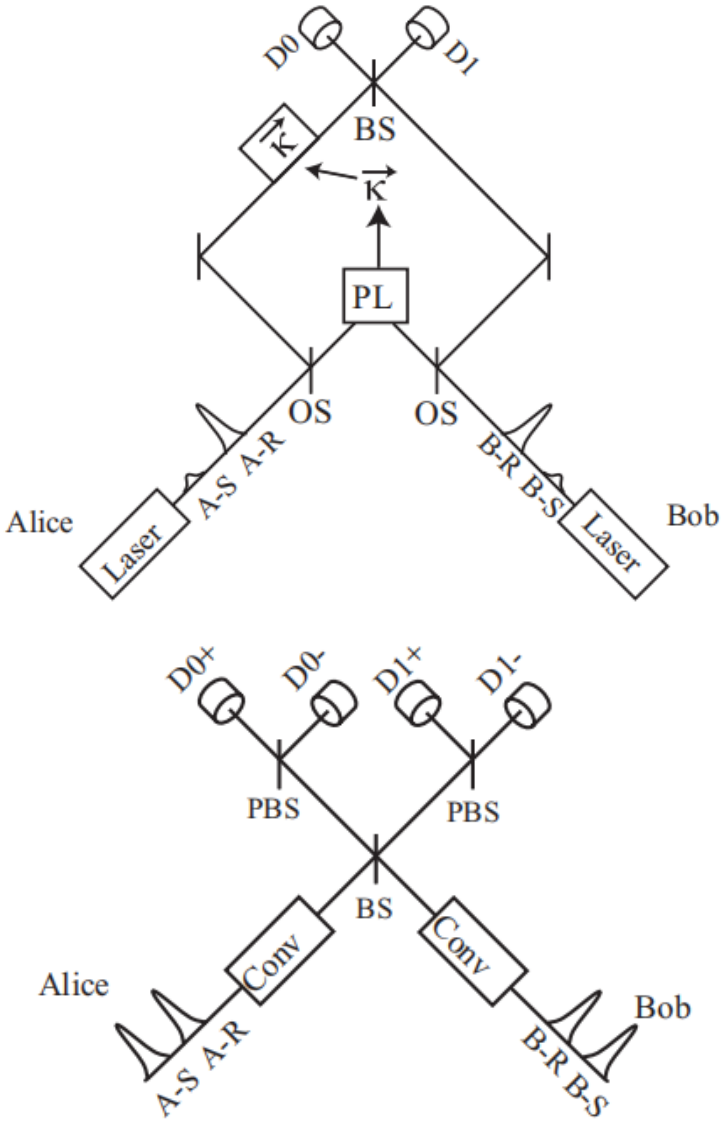


Figure.3.2. Two schematic diagrams of phase encoding MDI-QKD.

In Figure 3.2, A-S (B-S) and A-R (B-R) represent Alice's (Bob's) signal pulses and reference pulses, respectively. The phase of the signal pulse is modulated to be one of 0, π/2, 3π/2, or π according to the random choices of Alice and Bob. In this structure, we assume that the intensities of Alice's signal (reference) pulse and Bob's signal (reference) pulse are matched. In order to lock the relative phase, we use strong pulses as reference pulses. OS represents an optical switch, which allows the reference pulses and signal pulses to be transmitted or reflected separately. PL represents a measurement unit to measure the phase difference between the two signals in mutually orthogonal polarization modes and outputs the phase difference of the two pulses, denoted as K. K will be used as a parameter to modulate Alice's input signal. Then, Alice's and Bob's signal pulses enter a 50:50

beam splitter, and the output of the beam splitter is connected to single-photon detectors. If only one detector responds, D0 or D1, the protocol is successful. When only D1 responds, Bob performs a bit flip to obtain the filtered raw key.

3.2.3 Path-phase encoding MDI-QKD protocol

The MDI QKD implementation scheme based on path-phase encoding requires high-speed optical switches. If path-phase encoding is adopted, it can reduce the requirements for devices. The MDI QKD implementation scheme based on path-phase encoding is illustrated in the figure below [14].

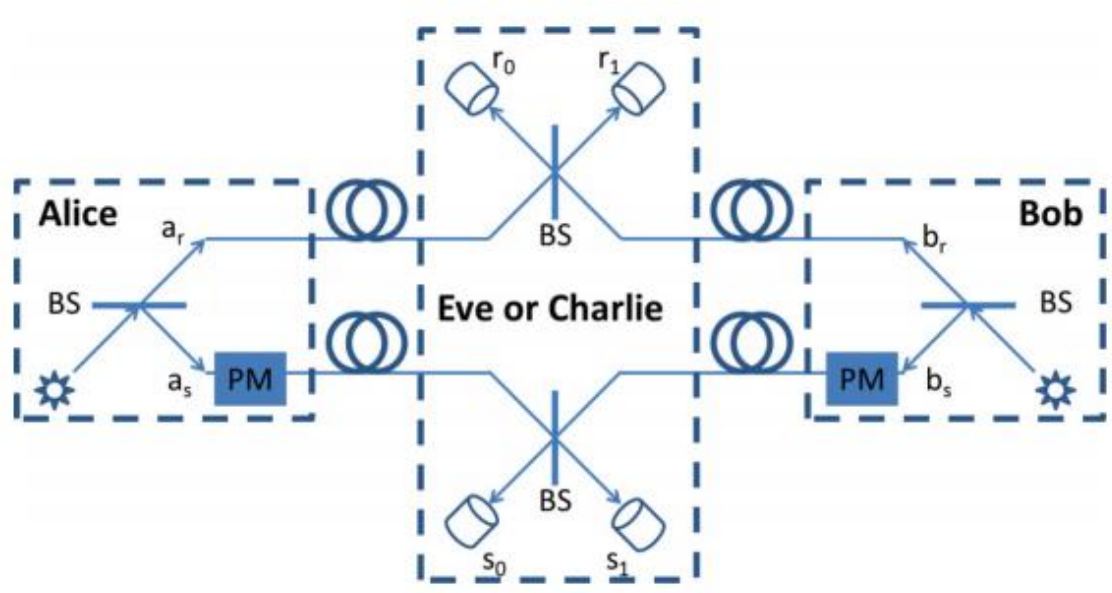


Figure.3.3. A schematic diagram of path-phase encoding MDI-QKD.

In this scheme, Alice and Bob prepare single-photon states and send them through a 50:50 beam splitter (BS). After passing through the beam splitter, photons are outputted through two different paths, which are respectively considered as the reference mode and the signal mode. In the reference mode, there is no phase modulation on the corresponding path, while in the signal mode, the path undergoes phase modulation (PM). At the Alice side, the two modes are labeled as *ar* and *as*, while at the Bob side, they are labeled as *br* and *bs*. Photons passing through as and bs undergo a relative phase shift with respect to the reference mode, generated by the PM, with a phase offset of 0, π/2, π, or 3π/2. The relative phase shifts at the Alice and Bob sides are denoted as θ_a and θ_b, respectively. The resulting states are then as follows:

$$\left(|1\rangle_{ar}|0\rangle_{as}+e^{i\theta_a}|0\rangle_{ar}|1\rangle_{as}\right)\otimes\left(|1\rangle_{br}|0\rangle_{bs}+e^{i\theta_b}|0\rangle_{br}|1\rangle_{bs}\right). \tag{3.2}$$

The photons are sent to the measurement terminal, where Charles or even Eve conducts the same Bell state measurement as in the previous scheme. The successful measurement results in one

response from detector r_0 or r_1 and one response from detector s_0 or s_1. Bits corresponding to unsuccessful instances are discarded. At the moment of successful Bell state measurement, the joint state of Alice and Bob is:

$$|1\rangle_{ar}|0\rangle_{as}|0\rangle_{br}|1\rangle_{bs}+e^{i(\theta_a-\theta_b)}|0\rangle_{ar}|1\rangle_{as}|1\rangle_{br}|0\rangle_{bs}. \tag{3.3}$$

The joint state described above, after passing through a 50:50 beamsplitter, will yield:

$$\begin{aligned}&|01+10\rangle_{r0r1}|01-10\rangle_{s0s1}\\&+e^{i(\theta_a-\theta_b)}|01-10\rangle_{r0r1}|01+10\rangle_{s0s1}\\&=|0101-0110+1001-1010\rangle_{r0r1s0s1}\\&+e^{i(\theta_a-\theta_b)}|0101+0110-1001-1010\rangle_{r0r1s0s1}\end{aligned}. \tag{3.4}$$

If $\theta_a-\theta_b=0$, then the above expression will become:

$$|0101-1010\rangle_{r0r1s0s1} \tag{3.5}$$

which implies that r_0 and s_0 respond simultaneously, or r_1 and s_1 respond simultaneously.

If $\theta_a-\theta_b=\pm\pi$, the expression will become

$$|0110-1001\rangle_{r0r1s0s1} \tag{3.6}$$

which means that either r_0 and s_1 respond simultaneously, or r_1 and s_0 respond simultaneously.

Thus, based on the detector response outcomes, one can infer the phase difference between Alice and Bob's phase modulations and determine which instances allow the formation of correlated bit strings for Alice and Bob's secret key bits.

Similar to the single-photon case of the original MDI-QKD scheme [11], the key rate formula for path-phase encoding MDI-QKD scheme follows Shor-Preskill's result [15], [16]

$$R\geq Y_{11}\left[1-fH\left(e_{11}\right)-H\left(e_{11}\right)\right], \tag{3.7}$$

where Y_{11} is the successful detection (trigger in the relay) rate provided that Alice and Bob send out single photons; e_{11} is the quantum bit error rate (QBER); f is the error correction inefficiency (see, e.g, [17]).

The scheme in Figure 3.3 relies on single-photon states to ensure its proper operation. In practice, on-demand single-photon sources can be implemented using parametric down-conversion processes [18], or by relying on quasi-atomic systems such as quantum dots [19]. In these scenarios, one must consider the impact of multi-photon states on system performance. With recent advancements in compact, cost-effective single-photon sources, reliance on single-photon states in our scheme is not necessarily a setback, especially when considering the simplicity of the BSM module compared to those proposed in [11][20].

3.2.4 Time-bin encoding MDI-QKD protocol

The scheme depicted in Figure 3.3 relies on single-photon states for proper operation. In practice, on-demand single-photon sources can be achieved through parametric down-conversion processes [18] or utilizing quasi-atomic systems such as quantum dots [19]. In these scenarios, the impact of multi-photon states on system performance must be considered. With recent advancements in compact, cost-effective single-photon sources, dependence on single-photon states in our scheme is not necessarily a drawback, particularly when considering the simplicity of the BSM module compared to those proposed in [11], [20].

The setup in Figure 3.3 requires two optical channels for each user, which may seem redundant and necessitates maintaining relative phase coherence between the two channels. By employing a simple time-multiplexing technique, however, both issues can be addressed.

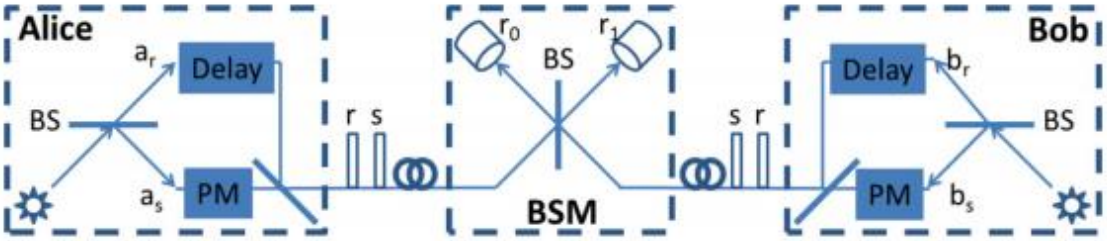


Figure.3.4. A schematic diagram of time-bin encoding MDI-QKD.

Unlike using path-phase encoding, Alice and Bob can employ time multiplexing to separate their reference and signal modes. This can be achieved by utilizing Mach-Zehnder interferometers at the transmitter, as illustrated in Figure 3.4. This results in both reference and signal pulses propagating along the same physical channel. Additionally, if the time delay between the two modes is sufficiently short, it can be reliably assumed that the relative phase between the reference and signal modes remains well preserved along the channel, as shown in Figure 3.3. The BSM module in Figure 3.4 is also simpler compared to that in Figure 3.3, as it only utilizes two single-photon detectors instead of four. Furthermore, it is simpler than the proposed BSM modules in [11][20], as it does not require optical switches or phase-to-polarization converters. Like any other schemes, time synchronization is necessary to ensure that the corresponding reference and signal modes arrive at the correct time and effectively interfere with each other.

The time-bin encoding scheme must address the main issue of dead time in single-photon detectors. After detection, a detector will be non-responsive (dead) for a period of time until it resets. The dead time of a detector is caused by the after-pulse effect in avalanche photodiode single-photon detectors. In the time-multiplexing scheme, detectors are required to detect photons in two consecutive pulses, whose time difference could be short. The dead time of detectors

ultimately limits the repetition rate of the proposed scheme. Here, we propose appropriate postselection methods to address the dead-time issue.

Regarding the postselection events of the BSM module in Figure 3.4, we consider two scenarios. In the first scenario, we assume that the dead time of single-photon detectors is shorter than the delay in Mach-Zehnder interferometers. In this case, for the time slot corresponding to signal pulses, detectors r_0 and r_1 in Figure 3.4 are similar to detectors s0 and s1 in Figure 3.3. To achieve a higher repetition rate, a delay possibly shorter than the detector's dead time must be utilized [21][22]. From the discussion of Equations (3.5) and (3.6), we observe that the dead-time issue becomes problematic only when Alice and Bob's results are correlated (i.e., they use the same phase). To address this issue, Alice and Bob can further filter out those detection events resulting from the terms in Equation (3.5). In other words, by accepting a 1/2 loss in the final key rate, we will only retain measurement results in which both r_0 and r_1 are triggered in different time slots (corresponding to the arrival of the reference or signal beams).

The setup in Figure 3.4 can be easily modified to implement encoding in all three Pauli bases. If we represent the standard basis vectors, i.e., eigenvectors of the Z operator, by a single-photon state in the reference mode and a single-photon state in the signal mode, the encodings implemented by the setup of Figure 3.4 are those of X and Y bases. If one replaces the first beam splitter in the encoder with a polarizing beam splitter and uses horizontally or vertically polarized light at the source [23], the same setup can be used for Z-basis encoding as well. For single-photon sources, the choice of which basis to use for the QKD protocol is arbitrary. However, the QBER values of X and Y bases are more susceptible to influence compared to the Z basis, hence Z and X basis encoding are used in the experimental setup of [24], [25].

3.3 Decoy state MDI-QKD

3.3.1 Three intensities MDI-QKD protocol

We use a symmetric protocol with three intensities to each basis as shown in Section 3.2.1. The final key rate can be estimated by Alice and Bob as follow [14], [23], [27]:

$$R \geq p_{\mu_2} p_{\nu_2} p^{\mathrm{Z}}_{\mu_2} p^{\mathrm{Z}}_{\nu_2} \left\{ \mu_2 \nu_2 e^{-\mu_2-\nu_2} s^{\mathrm{Z}}_{11} \left[1 - H\left(e^{\mathrm{X}}_{11} \right) \right] - S^{\mathrm{Z}}_{\mu_2\nu_2} f H\left(E^{\mathrm{Z}}_{\mu_2\nu_2} \right) \right\}, \tag{3.8}$$

where $S^{\omega}_{\mu i \nu j} = n^{\omega}_{\mu i \nu j} / N^{\omega}_{\mu i \nu j}$ is the counting rate of the pulse pairs of intensity $\mu_i \nu_j$ in basis ω, f is the error correction inefficiency and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. The probability that Alice (Bob) chooses intensity μ_i (ν_j) is $p_{\mu i}$ ($p_{\nu j}$) and the probability that Alice (Bob) chooses basis ω is $p^{\omega}_{\mu i}$ ($p^{\omega}_{\nu j}$). The yield s^{Z}_{11} and phase error rate e^{X}_{11} on z-

basis are defined for the pulses when Alice and Bob send those containing a single photon. The detail of decoy method is given in appendix. The other parameters are also defined.

The yield Y_{nm}^{ω} are defined by the probability of successful measurement event, when Alice and Bob send *n*-photon pulse and *m*-photon pulse, respectively, in basis X or Z. The phase error rate e_{nm}^{ω} is defined similarly. When the phases of the weak coherent states used by Alice and Bob are randomized, the quantum channel can be modeled as a photon-number channel model [26]. That means Alice and Bob randomly choose quantum channels with Poisson distribution. The overall gain $S_{\mu i\nu j}^{\omega}=n_{\mu i\nu j}^{\omega}/N_{\mu i\nu j}^{\omega}$ and quantum bit error rate (QBER) $E_{\mu i\nu j}^{\omega}=m_{\mu i\nu j}^{\omega}/n_{\mu i\nu j}^{\omega}$ are related to the counting rate and error rate by [37-39]:

$$\begin{aligned} S_{\mu_1\nu_1}^{\omega} &= \sum_{n,m=0}^{\omega} \frac{\mu_i^n \nu_i^m}{n!m!} e^{-\mu_i-\nu_j} s_{nm}^{\omega}, \\ E_{\mu_1\nu_1}^{\omega} S_{\mu_1\nu_1}^{\omega} &= \sum_{n,m=0}^{\omega} \frac{\mu_i^n \nu_i^m}{n!m!} e^{-\mu_i-\nu_j} s_{nm}^{\omega} e_{nm}^{\omega}. \end{aligned} , \tag{3.9}$$

where $N_{\mu i\nu j}^{\omega}$ is the total number of pulse pairs with intensity μ_i and ν_j in basis ω, $n_{\mu i\nu j}^{\omega}$ ($m_{\mu i\nu j}^{\omega}$) is the number of effective (wrong) events from $N_{\mu i\nu j}^{\omega}$. The counting rate s_{nm}^{ω} is defined by the probability of a successful measurement event when Alice and Bob send pulses containing *m* and *n* photons, respectively. The error rate e_{nm}^{ω} is defined in a similar manner.

The total gain $S_{\mu_1\nu_1}^{\omega}$ can be written as

$$\begin{aligned} e^{\mu_i+\nu_j} S_{\mu_i\nu_j}^{\omega} &= \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} s_{nm}^{\omega} \\ &= \sum_{m=0}^{\infty} \frac{\nu_j^m}{m!} s_{0m}^{\omega} + \mu_i \left(s_{10}^{\omega} + \nu_j s_{11}^{\omega} + \sum_{m=2}^{\infty} \frac{\nu_j^m}{m!} s_{1m}^{\omega} \right) \\ &\quad + \sum_{n=2}^{\infty} \frac{\mu_i^n}{n!} \left(s_{n0}^{\omega} + \nu_j s_{n1}^{\omega} + \sum_{m=2}^{\infty} \frac{\nu_j^m}{m!} s_{nm}^{\omega} \right) \\ &= e^{\nu_j} S_{0\nu_j}^{\omega} + e^{\mu_i} S_{\mu_i 0}^{\omega} - S_{00}^{\omega} + \mu_i \nu_j s_{11}^{\omega} \\ &\quad + \sum_{m=2}^{\infty} \frac{\mu_i \nu_j^m}{m!} s_{1m}^{\omega} + \sum_{n=2}^{\infty} \frac{\mu_i^n \nu_j}{n!} s_{n1}^{\omega} + \sum_{n,m=2}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} s_{nm}^{\omega} \end{aligned} . \tag{3.10}$$

Then we will get

$$
\begin{aligned}
& e^{\mu_2+\nu_2}S^{\omega}_{\mu_2\nu_2}-e^{\mu_1+\nu_1}S^{\omega}_{\mu_1\nu_1} \\
&= g_1^{\omega}+\left(\mu_2\nu_2-\mu_1\nu_1\right)s^{\omega}_{11}+\sum_{m=2}^{\infty}\frac{\mu_2\nu_2^{m}-\mu_1\nu_1^{m}}{m!}s^{\omega}_{1m} \\
&+\sum_{n=2}^{\infty}\frac{\mu_2^{n}\nu_2-\mu_1^{n}\nu_1}{n!}s^{\omega}_{n1}+\sum_{m=2}^{\infty}\frac{\mu_2^{n}\nu_2^{m}-\mu_1^{n}\nu_1^{m}}{n!m!}s^{\omega}_{nm} \\
&\geq g_1^{\omega}+\left(\mu_2\nu_2-\mu_1\nu_1\right)s^{\omega}_{11}+a\sum_{m=2}^{\infty}\frac{\mu_2\nu_2^{m}+\mu_1\nu_1^{m}}{m!}s^{\omega}_{1m} \\
&+b\sum_{n=2}^{\infty}\frac{\mu_2^{n}\nu_2+\mu_1^{n}\nu_1}{n!}s^{\omega}_{n1}+c\sum_{m=2}^{\infty}\frac{\mu_2^{n}\nu_2^{m}+\mu_1^{n}\nu_1^{m}}{n!m!}s^{\omega}_{nm} \\
&\geq g_1^{\omega}+\left(\mu_2\nu_2-\mu_1\nu_1\right)s^{\omega}_{11} \\
&+\xi\left(\sum_{m=2}^{\infty}\frac{\mu_2\nu_1^{m}+\mu_1\nu_2^{m}}{m!}s^{\omega}_{1m}+\sum_{n=2}^{\infty}\frac{\mu_2^{n}\nu_1+\mu_1^{n}\nu_2}{n!}s^{\omega}_{n1}+\sum_{n,m=2}^{\infty}\frac{\mu_2^{n}\nu_1^{m}+\mu_1^{n}\nu_2^{m}}{n!m!}s^{\omega}_{nm}\right) \\
&= g_1^{\omega}+g_2^{\omega}+g_3^{\omega}-\left(\mu_1\nu_1-\mu_2\nu_2+\xi\mu_2\nu_1+\xi\mu_1\nu_2\right)s^{\omega}_{11}
\end{aligned}
\quad . \tag{3.11}
$$

For any n, $m\geq 2$, the following inequalities always hold :

$$
\begin{aligned}
\frac{\mu_2\nu_2^{m}-\mu_1\nu_1^{m}}{\mu_2\nu_1^{m}+\mu_1\nu_2^{m}} &\geq \frac{\mu_2\nu_2^{2}-\mu_1\nu_1^{2}}{\mu_2\nu_1^{2}+\mu_1\nu_2^{2}}\equiv a\geq 0 \\
\frac{\mu_2^{n}\nu_2-\mu_1^{n}\nu_1}{\mu_2^{n}\nu_1-\mu_1^{n}\nu_2} &\geq \frac{\mu_2^{2}\nu_2-\mu_1^{2}\nu_1}{\mu_2^{2}\nu_1-\mu_1^{2}\nu_2}\equiv b\geq 0 \\
\frac{\mu_2^{n}\nu_2^{m}-\mu_1^{n}\nu_1^{m}}{\mu_2^{n}\nu_1^{m}+\mu_1^{n}\nu_2^{m}} &\geq \frac{\mu_2^{2}\nu_2^{2}-\mu_1^{2}\nu_1^{2}}{\mu_2^{2}\nu_1^{2}+\mu_1^{2}\nu_2^{2}}\equiv c\geq 0
\end{aligned}
\quad , \tag{3.12}
$$

where g_1^{ω} , g_2^{ω} , g_3^{ω} with $\xi=\min\left(a,b,c\right)$ can be written as follows :

$$
\begin{aligned}
g_1^{\omega} &= e^{\nu_2}S^{\omega}_{0\nu_2}+e^{\mu_2}S^{\omega}_{\mu_2 0}-e^{\nu_1}S^{\omega}_{0\nu_1}-e^{\mu_1}S^{\omega}_{\mu_1 0} \\
g_2^{\omega} &= \xi\left(e^{\mu_2+\nu_1}S^{\omega}_{\mu_2\nu_1}-e^{\nu_1}S^{\omega}_{0\nu_1}-e^{\mu_2}S^{\omega}_{\mu_2 0}+S^{\omega}_{00}\right) \\
g_3^{\omega} &= \xi\left(e^{\mu_1+\nu_2}S^{\omega}_{\mu_1\nu_2}-e^{\nu_2}S^{\omega}_{0\nu_2}-e^{\mu_1}S^{\omega}_{\mu_1 0}+S^{\omega}_{00}\right)
\end{aligned}
\quad . \tag{3.13}
$$

Also, according to Eqs.(3.9) and (3.10), we can get

$$
\begin{aligned}
e^{\mu_1+\nu_1}S^{\omega}_{\mu_1\nu_1}E^{\omega}_{\mu_1\nu_1} &= g_4^{\omega}+\mu_1\nu_1 s^{\omega}_{11}e_{11} \\
&+\sum_{m=2}^{\infty}\frac{\mu_1\nu_1^{m}}{m!}s^{\omega}_{1m}e_{1m}+\sum_{n=2}^{\infty}\frac{\mu_1^{n}\nu_1}{n!}s^{\omega}_{n1}e_{n1}+\sum_{n,m=2}^{\infty}\frac{\mu_1^{n}\nu_1^{m}}{n!m!}s^{\omega}_{nm}e_{nm}
\end{aligned}
\quad , \tag{3.14}
$$

where

$$g_4^{\omega} = e^{\nu_1} S_{0\nu_1}^{\omega} E_{0\nu_1}^{\omega} + e^{\mu_1} S_{\mu_1 0}^{\omega} E_{\mu_1 0}^{\omega} - S_{00}^{\omega} E_{00}^{\omega}. \tag{3.15}$$

Then the lower bound of s_{11}^{ω} and upper bound of e_{11}^{ω} can be written as :

$$s_{11}^{\omega} \geq \underline{s_{11}^{\omega}} = \frac{g_1^{\omega} + g_2^{\omega} + g_3^{\omega} - e^{\mu_2+\nu_2} S_{\mu_2\nu_2}^{\omega} + e^{\mu_1+\nu_1} S_{\mu_1\nu_1}^{\omega}}{\mu_1\nu_1 - \mu_2\nu_2 + \xi\mu_2\nu_1 + \xi\mu_1\nu_2}. \tag{3.16}$$

and

$$e_{11}^{\omega} \leq \overline{e_{11}^{\omega}} = \frac{e^{\mu_1+\nu_1} S_{\mu_1\nu_1}^{\omega} E_{\mu_1\nu_1}^{\omega} - g_4^{\omega}}{\mu_1\nu_1 s_{11}^{\omega}}. \tag{3.17}$$

The protocol model can be considered a photon-number channel model when the phase of pulses is fully randomized [37], and the overall counting rate and error rate QBER on the x basis and z basis are shown as [37-39]:

$$\begin{aligned} S_{\mu_i\nu_j}^{\mathrm{x}} &= 2y^2\left[1+2y^2-4yI_0(s)+I_0(2s)\right] \\ S_{\mu_i\nu_j}^{\mathrm{x}} E_{\mu_i\nu_j}^{\mathrm{x}} &= e_0 S_{\mu_i\nu_j}^{\mathrm{x}} - 2(e_0-e_d)y^2\left[I_0(2s)-1\right] \\ S_{\mu_i\nu_j}^{\mathrm{z}} &= S_C + S_E \\ S_{\mu_i\nu_j}^{\mathrm{z}} E_{\mu_i\nu_j}^{\mathrm{z}} &= e_d S_C + (1-e_d) S_E \end{aligned}. \tag{3.18}$$

where

$$\begin{aligned} S_C &= 2(1-p_d)^2 e^{-\mu'/2}\left[1-(1-p_d)e^{-\eta_a\mu_i/2}\right] \\ &\quad \times\left[1-(1-p_d)e^{-\eta_b\nu_j/2}\right] \\ S_E &= 2p_d(1-p_d)^2 e^{-\mu'/2}\left[I_0(2s)-(1-p_d)e^{-\mu'/2}\right] \end{aligned}. \tag{3.19}$$

In Eqs. (3.18) and (3.19), $I_0(s)$ is the modified Bessel function of the first kind, p_d is the dark count rate of the photon detector, e_0 is the error rate of the background, and e_d is the error rate due to two-photon distinguishability. The transmittance from Alice or Bob to Charlie is given by $\eta_a = \eta_b = \eta_d 10^{-\alpha l/20}$, where α is the loss coefficient of the standard fiber link, η_d is the detection efficiency, and *l* is the total distance between Alice and Bob. The other parameters are given by [37-39]

$$\begin{aligned} \mu' &= \eta_a\mu_i + \eta_b\nu_j \\ s &= \sqrt{\eta_a\mu_i\eta_b\nu_j}/2. \\ y &= (1-p_d)e^{-\mu'/4} \end{aligned}$$

There is also an improved calculation method. For a phase randomized WCS, the photon number distribution is [28]:

$$a_n^{\mu_i} = e^{-\mu_i}\frac{\mu_i^n}{n!}, b_m^{\nu_j} = e^{-\nu_j}\frac{\nu_j^m}{m!}, n, m = 0,1,2,\ldots.$$

The lower bound of counting rate of the single-photon pairs can be written from Eq.(3.16) to [27][28]:

$$s_{11}^{\omega} \geq \underline{s_{11}^{\omega}} = \frac{\hat{S}_+ - \hat{S}_-}{a_1^{\mu_1} b_1^{\nu_1} \tilde{a}_{12} \tilde{b}_{12}}. \tag{3.20}$$

where

$$\begin{aligned}
&\tilde{a}_{12} = a_1^{\mu_1} a_2^{\mu_2} - a_1^{\mu_2} a_2^{\mu_1}, \tilde{b}_{12} = b_1^{\nu_1} b_2^{\nu_2} - b_1^{\nu_2} b_2^{\nu_1}, \\
&\hat{S}_+^{\omega} = g_{11} S_{\mu_1\nu_1}^{\omega} + g_{02} S_{\mu_0\nu_2}^{\omega} + g_{20} S_{\mu_2\nu_0}^{\omega} + g_{00} S_{\mu_0\nu_0}^{\omega}, . \\
&\hat{S}_-^{\omega} = g_{12} S_{\mu_1\nu_2}^{\omega} + g_{21} S_{\mu_2\nu_1}^{\omega} + g_{01} S_{\mu_0\nu_1}^{\omega} + g_{10} S_{\mu_1\nu_0}^{\omega}
\end{aligned}$$

and

$$\begin{aligned}
&g_{11} = a_1^{\mu_1} a_2^{\mu_2} b_1^{\nu_1} b_2^{\nu_2} - a_1^{\mu_2} a_2^{\mu_1} b_1^{\nu_2} b_2^{\nu_1}, \\
&g_{12} = b_1^{\nu_1} b_2^{\nu_1} \tilde{a}_{12}, g_{21} = a_1^{\mu_1} a_2^{\mu_1} \tilde{b}_{12}, \\
&g_{02} = a_0^{\mu_1} g_{12}, g_{20} = b_0^{\nu_1} g_{21}, \\
&g_{00} = a_0^{\mu_1} b_0^{\nu_1} g_{11} - a_0^{\mu_1} b_0^{\nu_2} g_{12} - a_0^{\mu_2} b_0^{\nu_1} g_{21}, \\
&g_{01} = a_0^{\mu_1} g_{11} - a_0^{\mu_2} g_{21}, g_{10} = b_0^{\nu_1} g_{11} - b_0^{\nu_2} g_{12}.
\end{aligned}$$

Then, the upper bound of error rate is written from Eq.(3.17) to [28]

$$\begin{aligned}
e_{11}^{\omega} &\leq \overline{e_{11}^{\omega}} \\
&= \frac{\frac{m_{\mu_1\nu_1}^{\omega}}{N_{\mu_1\nu_1}^{\omega}} - a_0^{\mu_1}\frac{m_{\mu_0\nu_1}^{\omega}}{N_{\mu_0\nu_1}^{\omega}} - b_0^{\nu_1}\frac{m_{\mu_1\nu_0}^{\omega}}{N_{\mu_1\nu_0}^{\omega}} + a_0^{\mu_1} b_0^{\nu_1}\frac{m_{\mu_0\nu_0}^{\omega}}{N_{\mu_0\nu_0}^{\omega}}}{a_1^{\mu_1} b_1^{\nu_1} \underline{s_{11}^{\omega}}}.
\end{aligned} \tag{3.21}$$

3.3.2 Simulation of infinite key MDI-QKD

Substituting Eqs.(3.18) and (3.19) into Eqs.(3.16) and (3.17), we obtain the lower bound of the yield s_{11}^{ω} and the upper bound of the error rate e_{11}^{ω}. Then, with the parameters shown in Table.3.2 , we can estimate the final key rate of decoy state MDI-QKD.

In the following, we substitute the parameters into Eq.(3.8) to calculate the final key rates with several different combination of pulse intensities. First, we calculate the final key rate by changing the intensity of decoy state μ_1 and ν_1 with constant values of μ_2=ν_2=0.2 and e_d=0.01. As shown in Fig.3.5, the final key rate increased as the decoy intensity decreased. This is because we calculated asymptotic final key rate. If we consider the finite length effects, we will obtain the optimal intensity due to the statistical fluctuation.

Parameter	Value
f : error correction inefficiency	1.16
α : loss coefficient of fiber (dB/km)	0.2
p_d : dark count rate /pulse	3×10^{-6}
e_0 : error rate of background /pulse	0.5
η_d : detection efficiency	14.5%

Table.3.2. Parameters for simulating key rate of MDI-QKD

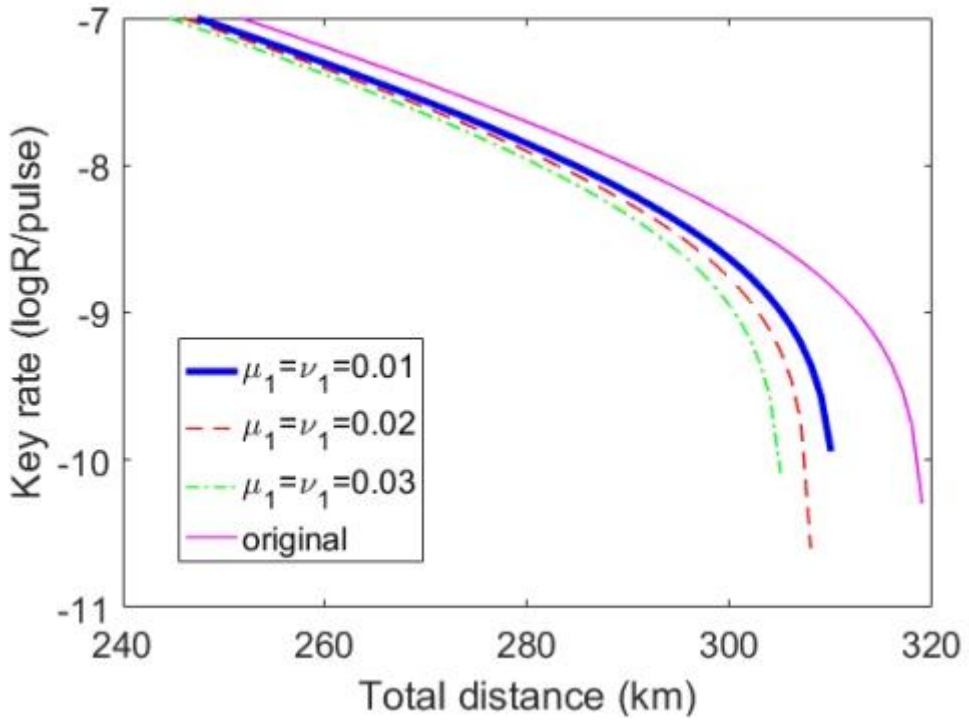


Figure 3.5. Key rate with different intensity of decoy state. The line of original means MDI-QKD with single photon.

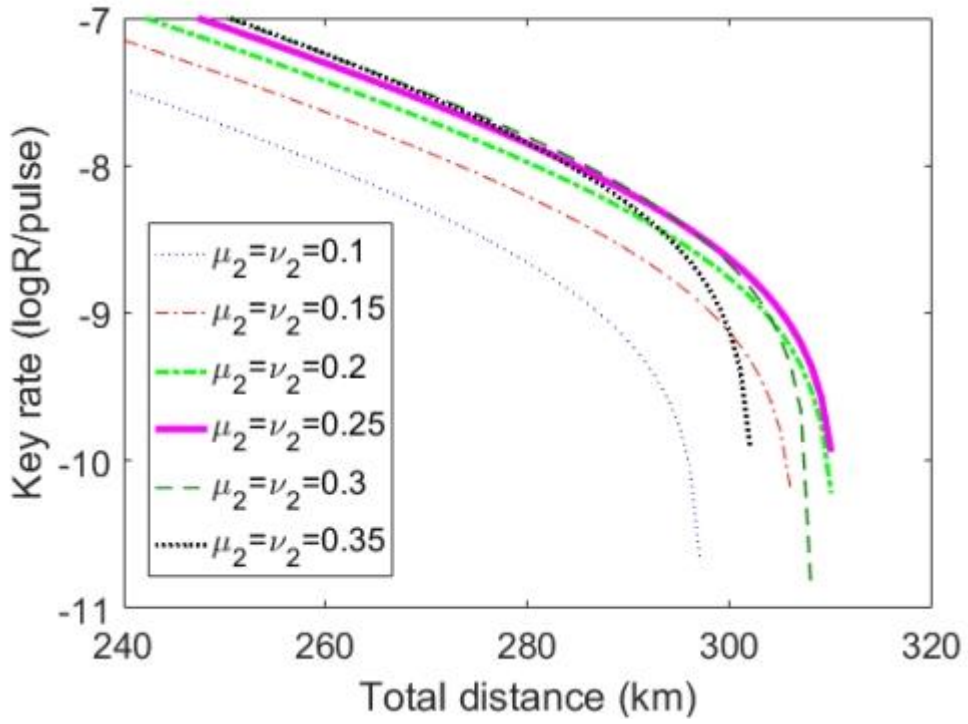


Figure 3.6 (a). Key rate with different intensities of signal state for e_d=0.01.

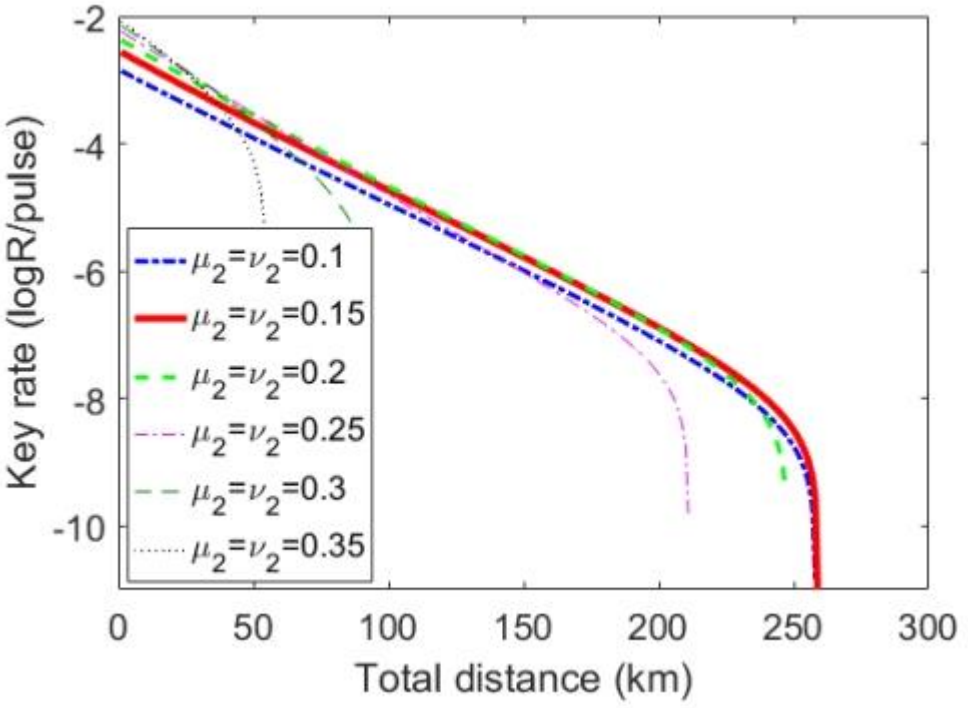


Figure 3.6 (b). Key rate with different intensities of signal state for e_d=0.05.

Then we changed the intensity of signal state μ_2 and v_2 with constant values of μ_1=v_1=0.01 and e_d from 0.01 to 0.05. As shown in Fig.3.6, the final key rate changed and the optimal intensity of signal state decreases from μ_2=v_2=0.25 to μ_2=v_2=0.15 as e_d increases from (a) 0.01 to (b) 0.05.

As a result, we believe that μ_1=v_1=0.01 and μ_2=v_2=0.25 are the best pulse intensities for the final key rate and transmission distance in the case of the standard transmission model. In addition, we will discuss the next chapter based on the optimal pulse intensities.

3.3.3 Finite key effects of MDI-QKD

In practical situations, the length of the raw key is finite, which induces a statistical fluctuation in parameter estimation. Here, we refer to [28] to calculate the effect of finite size. The expected lower and upper bounds of $\left\langle n_{\mu_i v_j}^{\omega} \right\rangle$ and $\left\langle m_{\mu_i v_j}^{\omega} \right\rangle$ are given by

$$\begin{aligned} \underline{E}\left(n_{\mu_i v_j}^{\omega}\right) \le \left\langle n_{\mu_i v_j}^{\omega} \right\rangle \le \overline{E}\left(n_{\mu_i v_j}^{\omega}\right) \\ \underline{E}\left(m_{\mu_i v_j}^{\omega}\right) \le \left\langle m_{\mu_i v_j}^{\omega} \right\rangle \le \overline{E}\left(m_{\mu_i v_j}^{\omega}\right) \end{aligned}. \tag{3.22}$$

where $\overline{E}(X)$ and $\underline{E}(X)$ can be defined as

$$\begin{aligned} \underline{E}(X,\xi) = \frac{X}{1+\delta_1(X,\xi)} \\ \overline{E}(X,\xi) = \frac{X}{1-\delta_2(X,\xi)} \end{aligned}. \tag{3.23}$$

where $\delta_1(X,\xi)$ and $\delta_2(X,\xi)$ are the positive solutions of

$$\begin{aligned} \left(\frac{e^{\delta_1}}{(1+\delta_1)^{1+\delta_1}}\right)^{\frac{X}{1+\delta_1}} = \xi, \\ \left(\frac{e^{-\delta_2}}{(1-\delta_2)^{1-\delta_2}}\right)^{\frac{X}{1-\delta_2}} = \xi, \end{aligned} \tag{3.24}$$

where ξ is the failure probability, which is set to 10^{-7}. Then the expected lower bound of $\left\langle \underline{s_{11}^{\omega}} \right\rangle$ and upper bound of $\left\langle \overline{e_{11}^{\omega}} \right\rangle$ can be calculated from the Chernoff bound in Equation (3.22). Then, the worst values of lower bound of s_{11}^{ω} and upper bound of e_{11}^{ω} become

$$s_{11}^{\omega} \ge \underline{\underline{s_{11}^{\omega}}} = \frac{\underline{O}\left(N_{\mu_2 v_2}^{\omega} a_1^{\mu_2} b_1^{\mu_2} \left\langle \underline{s_{11}^{\omega}} \right\rangle\right)}{N_{\mu_2 v_2}^{\omega} a_1^{\mu_2} b_1^{\mu_2}} \tag{3.25}$$

and

$$e_{11}^{\omega} \le \overline{\overline{e_{11}^{\omega}}} = \frac{\overline{O}\left(N_{\mu_2\nu_2}^{\omega} a_1^{\mu_2} b_1^{\mu_2} \underline{s_{11}^{\omega}} \left\langle \overline{e_{11}^{\omega}} \right\rangle\right)}{N_{\mu_2\nu_2}^{\omega} a_1^{\mu_2} b_1^{\mu_2} \underline{s_{11}^{\omega}}} \tag{3.26}$$

where $\overline{O}(X)$ and $\underline{O}(X)$ can be defined as

$$\begin{aligned} \overline{O}(X,\xi) &= \left[1+\delta_3(X,\xi)\right]X, \\ \underline{O}(X,\xi) &= \left[1-\delta_4(X,\xi)\right]X, \end{aligned} \tag{3.27}$$

where $\delta_3(X,\xi)$ and $\delta_4(X,\xi)$ are the positive solutions of

$$\begin{aligned} \left(\frac{e^{\delta_3}}{(1+\delta_3)^{1+\delta_3}}\right)^X &= \xi, \\ \left(\frac{e^{-\delta_4}}{(1-\delta_4)^{1-\delta_4}}\right)^X &= \xi. \end{aligned} \tag{3.28}$$

The final key rate with finite-sized effects will be [28], [29]

$$\begin{aligned} R \ge\ & p_{\mu_2} p_{\nu_2} p_{\mu_2}^{\mathrm{z}} p_{\nu_2}^{\mathrm{z}} \left\{ \mu_2\nu_2 e^{-\mu_2-\nu_2} s_{11}^{\mathrm{z}} \left[1-H\left(e_{11}^{\mathrm{x}}\right)\right] \right. \\ & \left. -S_{\mu_2\nu_2}^{\mathrm{z}} fH\left(E_{\mu_2\nu_2}^{\mathrm{z}}\right) \right\} - \frac{1}{N}\left(\log_2\frac{8}{\varepsilon_{\mathrm{cor}}} + 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} + 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\right) \end{aligned} \tag{3.29}$$

where $\varepsilon_{\mathrm{cor}}$ is the failure probability of error correction, ε' and $\hat{\varepsilon}$ are the coefficients while using the chain rules of smooth min- and max-entropy, $\varepsilon_{\mathrm{PA}}$ is the failure probability of privacy amplification [28].

3.5 Summary

In this chapter, we first elaborate on the security issues present in practical QKD systems. To meet the security requirements of actual system detectors, researchers have proposed an MDI-QKD system model capable of resisting any detector attacks, emphasizing the advantages of MDI-QKD. Furthermore, several specific encoding schemes for MDI-QKD implementation are introduced. Building on the aforementioned work, we conduct an analysis of the key generation rates for three-intensity decoy-state MDI-QKD with polarization encoding under both infinite key length and finite key length scenarios.

References

[1] Makarov, Vadim, Andrey Anisimov, and Johannes Skaar. "Effects of detector efficiency

mismatch on security of quantum cryptosystems." Physical Review A 74.2 (2006): 022313.

[2] B. Qi, C.-H.F. Fung, H.-K. Lo, and X. Ma, Quantum Inf.Comput.,7,073(2007).

[3] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nature photonics, 4(10), 686-689. (2010).

[4] Bohm, David, and Yakir Aharonov. "Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky." Physical Review 108.4 (1957): 1070.

[5] Pearle, Philip M. "Hidden-variable example based upon data rejection." Physical Review D 2.8 (1970): 1418.

[6] Jennewein, Thomas, et al. "A fast and compact quantum random number generator." Review of Scientific Instruments 71.4 (2000): 1675-1680.

[7] Yuan, Z. L., James F. Dynes, and Andrew J. Shields. "Avoiding the blinding attack in QKD." Nature Photonics 4.12 (2010): 800-801.

[8] Acin, Antonio, Nicolas Gisin, and Lluis Masanes. "From Bell’s theorem to secure quantum key distribution." Physical review letters 97.12 (2006): 120405.

[9] Acín, Antonio, et al. "Device-independent security of quantum cryptography against collective attacks." Physical Review Letters 98.23 (2007): 230501.

[10] Pironio, Stefano, et al. "Device-independent quantum key distribution secure against collective attacks." New Journal of Physics 11.4 (2009): 045021.

[11] Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

[12] Braunstein, Samuel L., and Stefano Pirandola. "Side-channel-free quantum key distribution." Physical review letters 108.13 (2012): 130502.

[13] Tamaki, Kiyoshi, et al. "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw." Physical Review A 85.4 (2012): 042307.

[14] Ma, Xiongfeng, and Mohsen Razavi. "Alternative schemes for measurement-device-independent quantum key distribution." Physical Review A 86.6 (2012): 062319.

[15] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical review letters 85.2 (2000): 441.

[16] Koashi, Masato, and John Preskill. "Secure quantum key distribution with an uncharacterized source." Physical review letters 90.5 (2003): 057902.

[17] G. Brassard and L. Salvail, in Advances in Cryptology EUROCRYPT ’93, edited by G. Goos and J. Hartmanis(Springer-Verlag, Berlin, 1993).

[18] Shapiro, Jeffrey H., and Franco N. Wong. "On-demand single-photon generation using a modular array of parametric downconverters with electro-optic polarization controls." Optics letters. 32.18 (2007): 2698-2700.

[19] Ward, M. B., et al. "On-demand single-photon source for 1.3 μm telecom fiber." Applied Physics Letters 86.20 (2005).

[20] Tamaki, Kiyoshi, et al. "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw." Physical Review A 85.4 (2012): 042307.

[21] Yuan, Z. L., et al. "High speed single photon detection in the near infrared." Applied Physics Letters 91.4 (2007).

[22] Dixon, A. R., et al. "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes." Applied Physics Letters 94.23 (2009).

[23] Ma, Xiongfeng, Chi-Hang Fred Fung, and Mohsen Razavi. "Statistical fluctuation analysis for measurement-device-independent quantum key distribution." Physical Review A 86.5 (2012): 052305.

[24] Chan, Philip, et al. "Modeling a measurement-device-independent quantum key distribution system." Optics express 22.11 (2014): 12716-12736.

[25] Liu, Yang, et al. "Experimental measurement-device-independent quantum key distribution." Physical review letters 111.13 (2013): 130502.

[26] H.-K. Lo, X. Ma and K. Chen, “Decoy State Quantum Key Distribution”, Phys.Rev.Lett. 94, 230504 (2005).

[27] S. H. Sun, M. Gao, C. Y. Li and L. M. Liang, “Practical decoy-state measurement-device-independent quantum key distribution”, Phys.Rev.A. 87, 052329 (2013).

[28] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki and H.-K. Lo, “Finite-key analysis for measurement-device-independent quantum key distribution,” Nat Commun 5, 3732, 2014. DOI: 10.1038/ncomms4732

[29] X-L. Hu, C. Jiang, Z-W. Yu, and X-B. Wang, “Practical Long-Distance Measurement-Device-Independent Quantum Key Distribution by Four-Intensity Protocol,” Adv. Quantum Technol. 4, 2100069, 2021. DOI: 10.1002/qute.202100069.

Chapter 4

Effects of the two-photon temporal distinguishability

4.1 Introduction

According to Lo et al. [1], it is critical for the photons emitted by two independent lasers to be indistinguishable. Since MDI-QKD protocol is based on the photon bunching effect of two indistinguishable photons at a 50:50 beam splitter (BS), stable HOM interference [2], [3] should be observed. The validity of the HOM test was probed in principle. However, it is unclear how the imperfect HOM interference affects the security of a practical system. The relationship between the visibility of the HOM interference and the final key rate must be clarified, and methods that improve visibility must be established. Thus far, a few studies have explored this issue, with exceptions including the study by Curty et al. [4], which calculated only the effect of misalignment error in the limit of zero distance.

In practical MDI-QKD systems, there are two positions where temporal errors may occur, leading to distinguishability of the two photons. These are errors generated by two independent light sources and errors generated in long-distance quantum channels. Specifically, the errors from the light sources mainly include timing difference of the light pulses sent by Alice and Bob and time jitter of the lasers, while channel errors primarily consist of time drift generated when light pulses propagate in optical fibers, as illustrated in Figure 4.1.

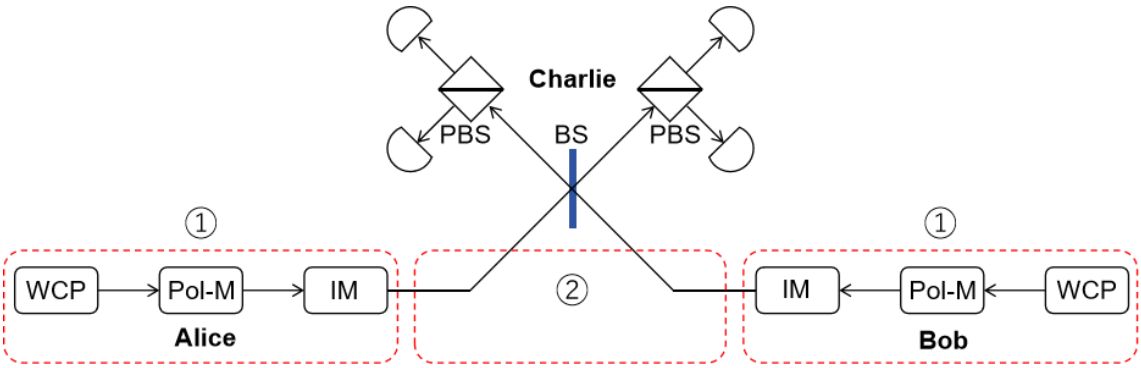


Figure 4.1. Temporal errors in MDI-QKD system.

The effects of imperfect visibility become serious for long distance transmission, because the fiber channel is exposed to perturbations in practical conditions. Precise control of the channel would be necessary to compensate the perturbation. However, the precise control may raise the cost for implementation. It is important to determine the target of the precision to maintain the final key rate in practice.

In this chapter, we explore the acceptable indistinguishability of the MDI-QKD. We calculated the key generation rate of a three-intensity decoy-state MDI-QKD protocol with a finite key length. Then, we calculated the effect of the visibility of the two-photon interference on the key generation rate. Finally, we calculated the acceptable time delay of the two Gaussian pulses at a 50:50 BS. Our numerical simulations show that high-visibility HOM-dip requires sophisticated time measurement devices.

4.2 Two photon interference in MDI-QKD

Interference is considered to be a key phenomenon in quantum physics [5] and it is widely applied in many quantum applications. In quantum cryptography, particularly in MDI-QKD protocol, HOM interference plays important role in Bell state measurement. The interference refers to the coherent construction or destruction of probability amplitudes. Therefore, the indistinguishability of photons directly affects the interference and thus the actual performance of the system.

In MDI-QKD system, the photons emitted independently by Alice and Bob need to remain indistinguishable at Charlie's measurement device to obtain clear. This is the biggest difference and difficulty with typical QKD scheme. HOM interference, which represents the actual performance of MDIQKD system [6]-[8]. It serves as a feedback signal for dynamic stabilization of the system [9]. Since practical MDI-QKD systems employ weak coherent states, it is necessary to study HOM interference of the weak coherent photons in a practical scenario, where the imperfections in real device affect the visibility of the HOM interference.

4.2.1 Hong-Ou-Mandel interference

HOM interference [2] shown in Fig.4.2 is the core of an implementation of the MDI-QKD protocol. When two identical photons enter simultaneously the two ports a and b of beam splitter (BS), the unitary property of BS cancels the two probability amplitudes that both photons transmit or reflect at the BS, as described below. As a result, the coincidence rate of ports c and d is 0, and the two photons will leave the same port. Here, the two photons are identical if they are indistinguishable in terms of frequency, polarization, spatial mode and other degrees of freedom.

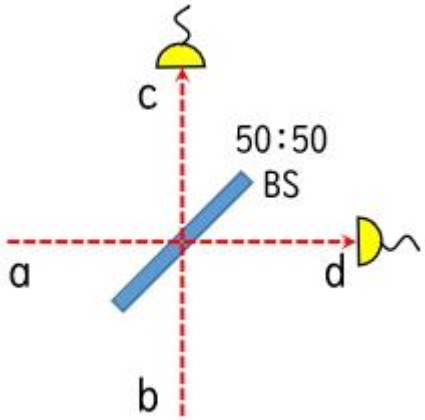


Figure 4.2. Hong-Ou-Mandel (HOM) interference

The effects of BS on the photons are represented by an annihilation operator (a, b, c, d), which satisfies the following relation:

$$\begin{cases} c = ta + rb \\ d = t'b + r'a \end{cases}, \tag{4.1}$$

where t, r, t' and r' are complex numbers. $R = |r|^2 \left(T = |t|^2\right)$ represents the reflectivity (transmittance) of BS and satisfies the relation of $|r|^2 + |t|^2 = 1$. According to the commutation relation of energy conservation and Boson's operator, we will obtain

$$\begin{cases} c = \sqrt{T}a + i\sqrt{R}b \\ d = i\sqrt{T}b + \sqrt{R}a \end{cases} \Leftrightarrow \begin{cases} a = \sqrt{T}c + i\sqrt{R}d \\ b = i\left(\sqrt{R}c - \sqrt{T}d\right) \end{cases}. \tag{4.2}$$

Then the incident photons of two ports of BS can be written as the direct product state of Fock state

$$\begin{aligned} |m,n\rangle_{a,b} &= |m\rangle_a |n\rangle_b = \frac{\left(a^+\right)^m}{\sqrt{m!}}|0\rangle_a \cdot \frac{\left(b^+\right)^n}{\sqrt{n!}}|0\rangle_b \\ &= \frac{i^n}{\sqrt{m!\cdot n!}}\left(\sqrt{T}c^+ + \sqrt{R}d^+\right)^m \left(\sqrt{R}c^+ - \sqrt{T}d^+\right)^n |0,0\rangle_{c,d} \end{aligned}, \tag{4.3}$$

where $R = T = 1/2$ for 50:50 BS. Then it will be

$$|m,n\rangle_{a,b} = \frac{i^n}{\sqrt{m!\cdot n!}}\left(\sqrt{\frac{1}{2}}\right)^{m+n} \left(c^+ + d^+\right)^m \left(c^+ - d^+\right)^n |0,0\rangle_{c,d}. \tag{4.4}$$

When m=n=1, we will obtain

$$|1,1\rangle_{a,b} = \frac{i}{2}\left(\left(c^{+}\right)^{2} - \left(d^{+}\right)^{2}\right)|0,0\rangle_{c,d}. \tag{4.5}$$

In this case, two input ports a and b have only a single photon incident. Photons emitted the same port. We call this Photon Bunching effect. The coincidence measurement between the port c and port d result in 0.

The two photons input into BS are in different states, according to Eq.(4.2), we can write the two-photon direct product state as follows after passing through BS:

$$\begin{aligned} a^{+}_{|0\rangle} b^{+}_{|1\rangle} |0,0\rangle_{a,b} &= \frac{1}{2}\left(c^{+}_{|0\rangle} + d^{+}_{|0\rangle}\right)\left(c^{+}_{|1\rangle} - d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} \\ &= \frac{1}{2}\left(c^{+}_{|0\rangle} c^{+}_{|1\rangle} - d^{+}_{|0\rangle} d^{+}_{|1\rangle}\right)|0,0\rangle_{c,d} - \frac{1}{2}\left(c^{+}_{|0\rangle} d^{+}_{|1\rangle} - c^{+}_{|1\rangle} d^{+}_{|0\rangle}\right)|0,0\rangle_{c,d} \end{aligned}. \tag{4.6}$$

If |0> and |1> are the eigenstates of measurement operator, we can accurately measure the Bell states $|\Psi^{-}\rangle$ (simultaneous detection of |0> at c and |1> at d, or |1> at c and |0> at d) and $|\Psi^{+}\rangle$ (|0> and |1> at c, or |0> and |1> at d). Thus, we can partially distinguish two of the four Bell states: $|\Psi^{+}\rangle$ and $|\Psi^{-}\rangle$.

According to the above analysis, MDI-QKD is actually a time reversed entanglement-based QKD protocol. If Charlie announces the successful measurement of $|\Psi^{-}\rangle$, it is equivalent to Alice and Bob post-selecting the entangled states $|\Psi^{-}\rangle$. Its security proof is equivalent to the time inversion entangled distribution protocol [10].

For practical use, WCP has advantages over the single photon state, but in polarization coding system [10] and phase coding system [11], WCP will increase the bit error rate of the X-basis significantly. This is because X-basis quantum state is not the eigenstate of the measurement operator, so it is possible to cause the wrong $|\Psi^{-}\rangle$ or $|\Psi^{+}\rangle$ response in the case of multi-photons. Since counting rate and bit error rate caused by single photon can be estimated by decoy state method, the existence of multi-photons will not change the estimation of counting rate and bit error rate of the system. However, multi-photons will have great impact on error correction process of the system, which is not conducive to the efficient operation of the system. Therefore, in practical MDI-QKD system, Z-basis, which is affected little by multi-photons, is used for coding. Since X-basis is affected significantly by multi-photons it is used to estimate phase error rate.

4.2.2 Error rate of two photon interference

Then we focus on the error rate e_d, which is directly related to the visibility of the two-photon interference, and it can be written as:

$$e_d = e_d^0 + \frac{1-V}{2} \tag{4.7}$$

where e_d^0 is the correction parameter and is assumed to be 0. The quantum bit error rate (QBER) in X basis can be related to the visibility with Eqs. (3.18) and (4.7).

The error rate is related to the HOM interference visibility as follows. We can model the photon-pair state as a mixture of perfectly indistinguishable photons and the completely independent photons with the fraction of $1-\varepsilon$ and ε, respectively. The two-photon interference in the BSM on the indistinguishable photons provides only two possible outcomes with probability of 1/2, whereas it provides all four outcomes with the probability of 1/4 for the independent photons. For example, if both Alice and Bob send x_0, the BSM fails with BS+PBS implementation for the indistinguishable photons, however, the outcomes Ψ^+ or Ψ^- may appear for the independent photons with each probability of 1/4. Therefore, the error rate in the BSM on the mixture will read $\varepsilon/2$. Since the visibility of the HOM interference of the mixture is reduced to $V = 1-\varepsilon$, we obtain the error rate given in Eq. (4.7). If Alice and Bob send the other photon-pair states, the same error rate is obtained. If there is no eavesdropper on the channel, the phase error rate e_{11}^x coincides with the background error rate e_d. Figure 4.3 shows the relationship between the visibility and phase error rate.

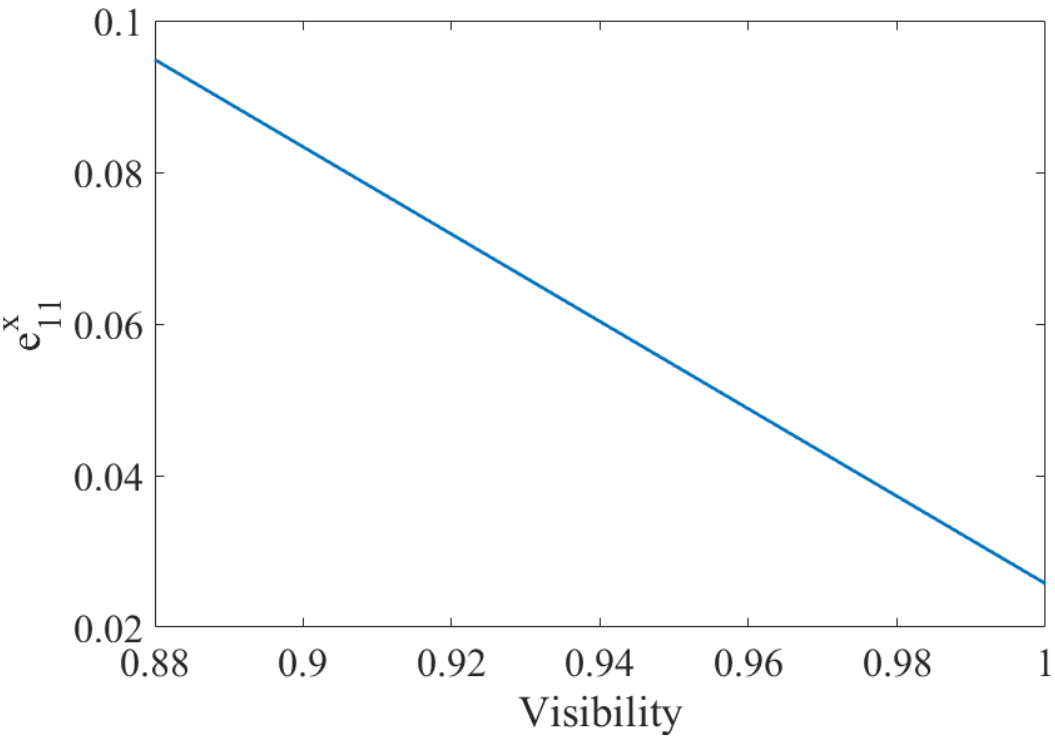
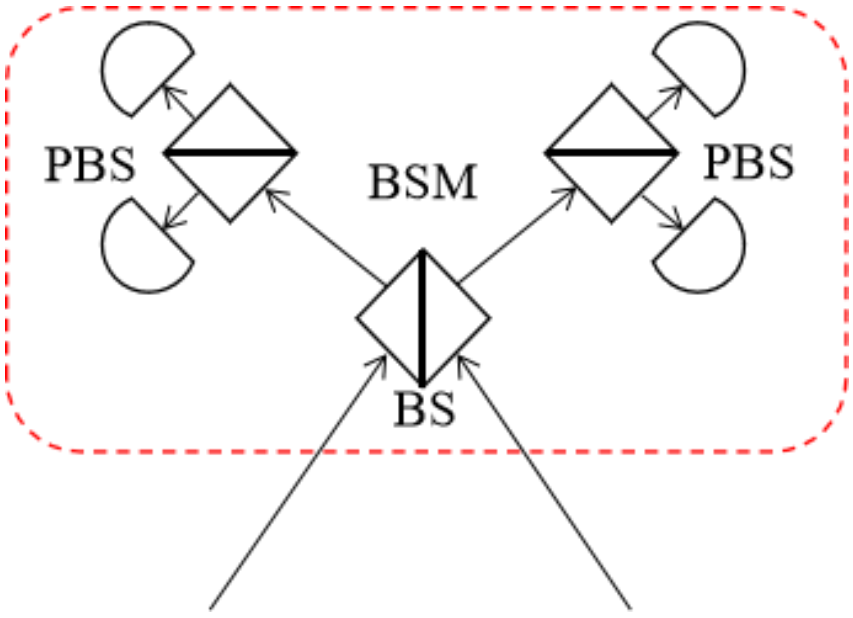


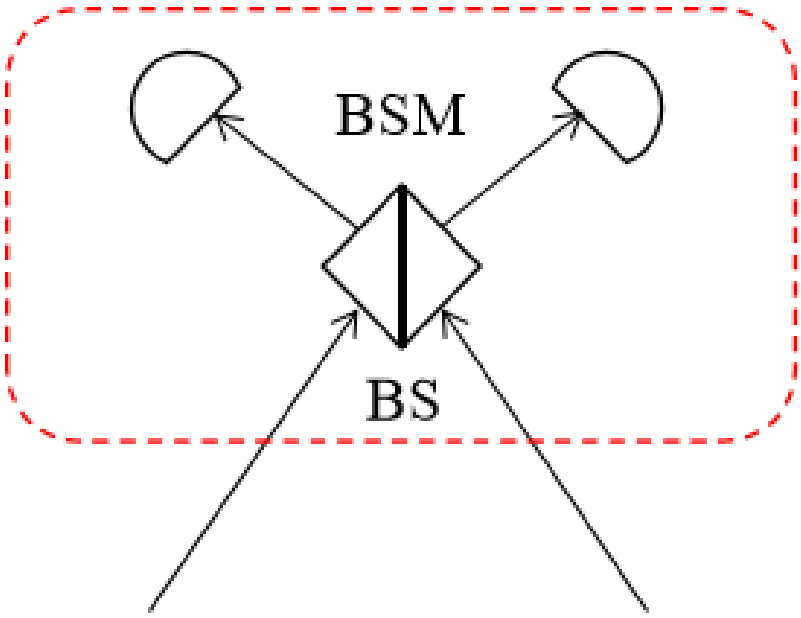
Figure 4.3. The relationship between error rate of single photon pairs e_{11}^x and visibility.

4.2.3 Effect of different Bell state measurements

Notice that according to different BSM implementation methods adopted by different protocols, the error rates for X- and Z-basis are also different. When polarization-encoding protocol is adopted, BSM with a BS followed by polarization beam splitters (PBS) is considered successful when photons are detected at different ports of the PBS. The success probability of BSM is 1/2. Suppose photons are distinguishable. In Z-basis, BSM succeeds when Alice and Bob send different polarization. Although Ψ^+ may be mistaken for Ψ^-, bits are flipped for both Ψ^+ and Ψ^- outcomes, so there is no bit error. In x-basis, even if Alice and Bob send same polarization, photons may be detected at different ports of the PBS to cause error with the probability of 1/2. On the other hand, the BSM with only a BS is successful, when it detects Ψ^-, that is, the photons are detected on the different ports of the BS. It happens with the probability of 1/2 regardless of the polarization. Therefore, the error rate is 1/2 for both bases. If it is a complete BSM, the probability of success is unity, but both x- and z-basis will have errors with the probability of 1/2. As a result, the BS+PBS method seems to be practical in terms of the asymmetry of error rate. In this case, e_d should have no effect on z-basis in the error rate calculation in Equation (3.18).



(a) BSM with BS+PBS



(b) BSM with BS only

Figure 4.4. Two different forms of BSM.

4.3 Effect of the two-photon distinguishability

4.3.1 Effect of the visibility

The visibility of the two-photon interference V can be directly estimated from the coincidence probability in the HOM interference experiment by:

$$V = \frac{p_{\max} - p_{\min}}{p_{\max}} \tag{4.8}$$

where $p_{\max}$ and $p_{\min}$ are the maximum and minimum coincidence probabilities, respectively. In the HOM experiment, we measure the coincidence probability, defined as the probability of detecting photons at each output port of the beam splitter in a time window smaller than the pulse duration. The coincidence probability takes the minimum $p_{\min}$ when photons arrive at the beam splitter simultaneously, but almost constant value $p_{\max}$ when the time delay between the photons is larger than the pulse duration.

Considering the different success rates of different BSM methods, we need to multiply the key rate R by a coefficient, which is 1 for complete BSM, 1/2 for BS+PBS and 1/4 for BS-only. We verify the difference between the effects of indistinguishability of these methods as shown in Fig.4.5, Fig.4.6 and Fig.4.7. The key rate of complete BSM is highest when $V = 1$, but when V is near 0.9, the key rate becomes lower than the BS+PBS method. We can also clearly see that the BS+BPS method has much higher tolerance for indistinguishability.

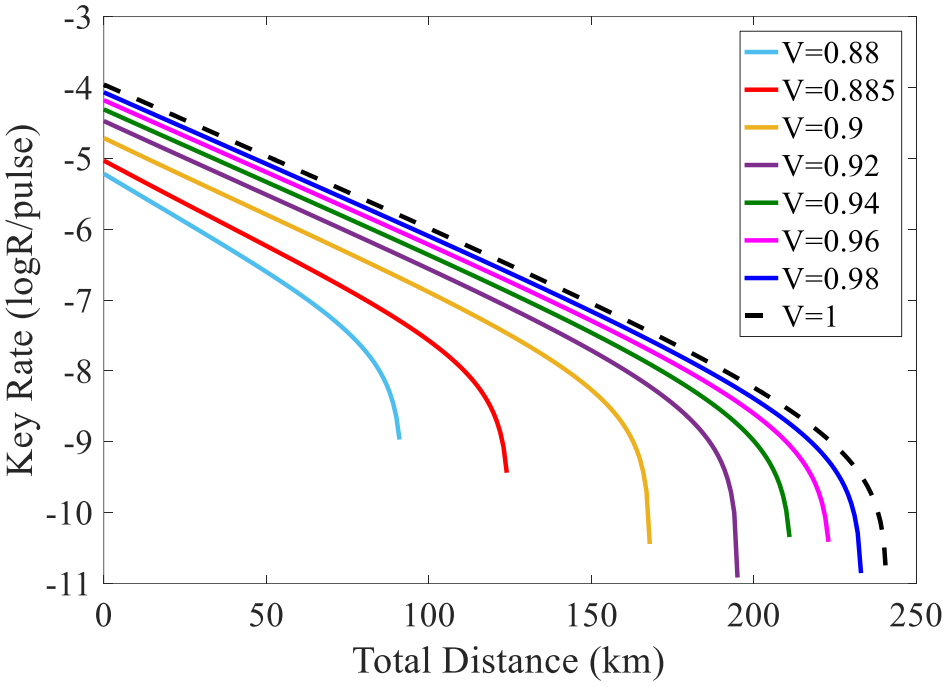


Figure 4.5. Key rate with different visibilities of infinite sized MDI-QKD protocol with a complete BSM.

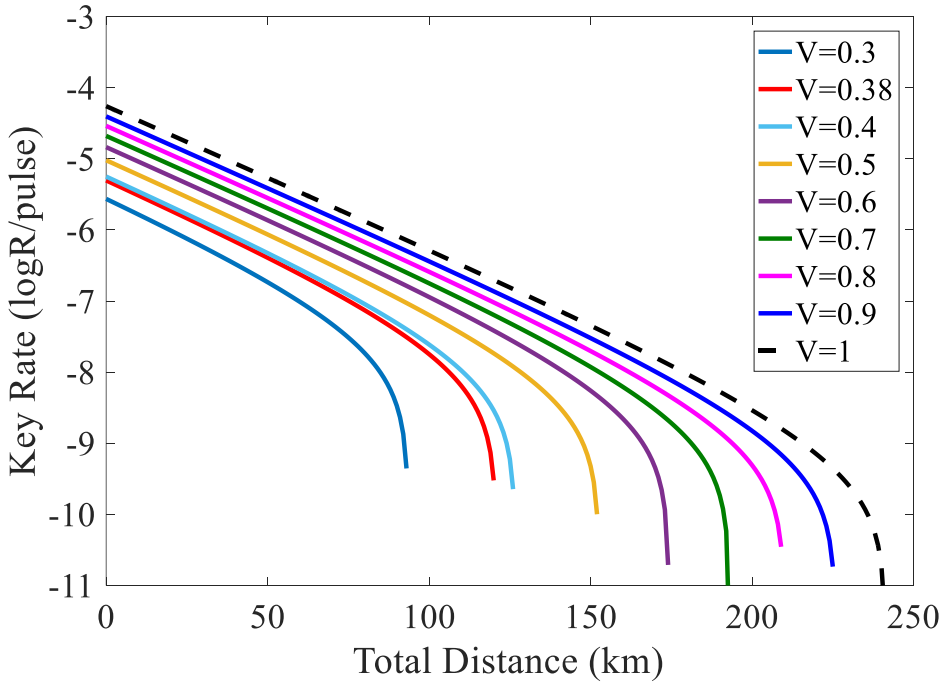


Figure 4.6. Key rate with different visibilities of infinite sized MDI-QKD protocol with a BS+PBS BSM.

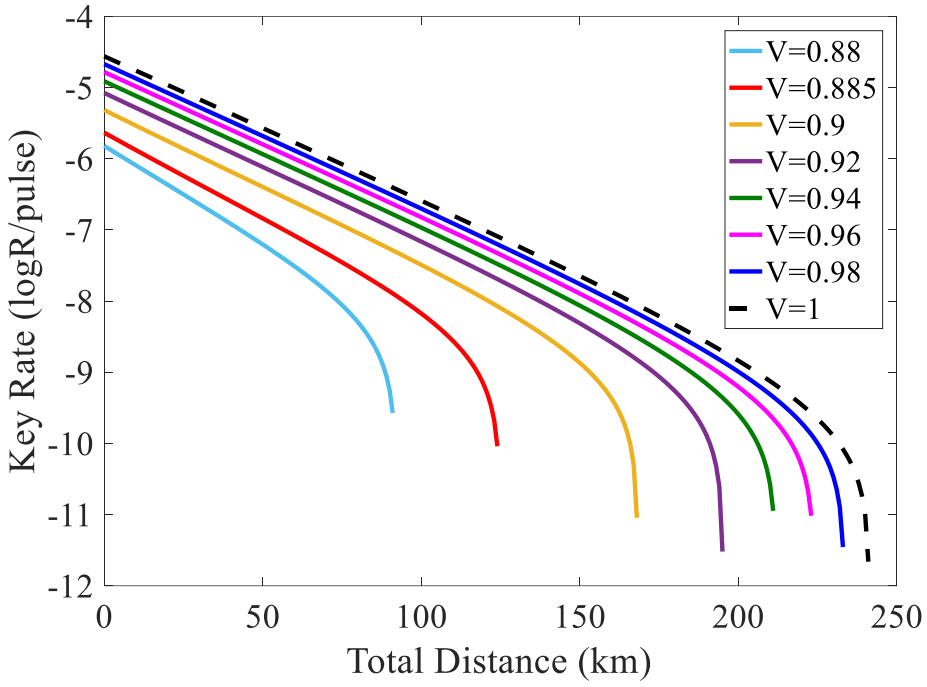


Figure 4.7. Key rate with different visibilities of infinite sized MDI-QKD protocol with a BS-only BSM.

4.3.2 Results and discussion

Due to the lack of an evaluation criterion, we tentatively decided on the definition of acceptable visibility range. First, we defined the maximum communication distance where the key rate falls into zero in our simulation. Then, we define the acceptable visibility which provide the maximum communication distance more than the half of that calculated for the ideal situation (V = 1). The minimum visibility is 0.38 for successful infinite-sized key generation.

For the convenience of calculation, we set Alice and Bob to have the same light source intensity and probability. Here we have chosen 0.4 and 0.05 for the signal and decoy intensity. The optimization of each distance point requires a large amount of additional calculation, so we refer to the probabilities of sources chosen by Alice and Bob in [12] to carry out the simulation calculation. We set the probability of signal and decoy source to 0.6 and 0.3 and the probability of signal and decoy source in z basis to 0.98 and 0.27. Here we use the same three intensities for each basis and the same parameter values. Although an increase in N moves the key rate closer to that of the infinite case, the total data length is limited to ensure key sharing in a realistic time frame. The effect of the total data length on communication speed should be considered in practice. In the next, we select $N = 10^{14}$ for a clock rate of 2.5 GHz and communication duration of 4×10^{5} s to obtain a high key rate and practical communication period for calculation.

In the following, we also calculate the finite-sized final key rates with different visibilities to examine the effect of the distinguishability of the two photons. Here, we set $N = 10^{14}$ and changed V from 0.3 to 1. The curves in Fig.4.6 show that the acceptable condition of visibility $V = 0.42$ is more stringent for finite-size key generation than the $V = 0.38$ of the infinite-size, as shown in Fig.4.8.

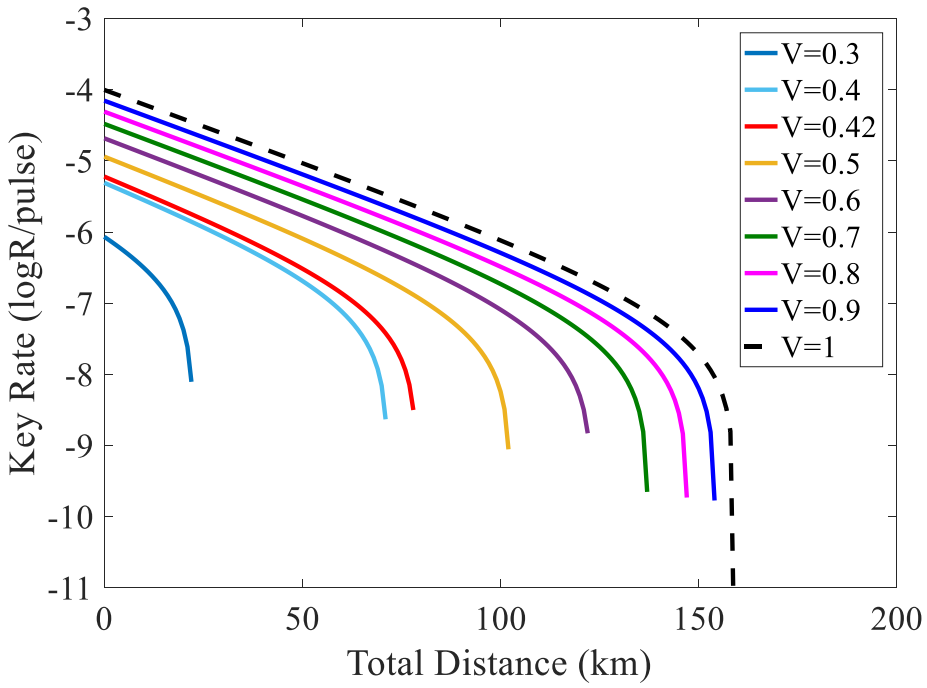


Figure 4.8. Key rate with different visibilities of finite-sized MDI-QKD protocol with a BS+PBS BSM. The total number of pulses send by Alice and Bob is $N=10^{14}$.

4.4 Acceptable time delay of two photon pulses

4.4.1 Gaussian photon pulses

With the acceptable visibility we can also calculate the acceptable time delay between the two photons from Alice and Bob. We considered two Gaussian photon pulses, which are typically assumed [3]:

$$\varphi_i(\omega) = \frac{1}{\pi^{1/4}\sqrt{\sigma_i}} e^{-\frac{(\omega-\bar{\omega}_i)^2}{2\sigma_i^2}}, (i = a, b), \tag{4.9}$$

where $\bar{\omega}_i$ is the central frequency of pulse i, and σ_i is its spectral width. If Alice's and Bob's Gaussians are identical, the coincidence probability of the HOM dip can be simply written as [13]:

$$p = 1 - \frac{1}{2} e^{-\sigma_i^2 \tau^2}, \tag{4.10}$$

which refers to the visibility V. The time delay of Alice's and Bob's photon pulses is τ. If the time duration of the photon pulse is assumed to be τ_L, the product of the time and bandwidth $\Delta\nu_L$ when both are at full width at half maximum (FWHM) is [14]

$$\tau_L \Delta\nu_L = \frac{2\ln 2}{\pi}\left[1+\left(\frac{\beta}{\gamma}\right)^2\right]^{1/2} \geq C_B, \tag{4.11}$$

where β is the phase modulation parameter, and γ describes the Gaussian pulse envelope relation to the temporal half-width of the radiant power of the pulse by

$$\tau_L = \left(\frac{2\ln 2}{\gamma}\right)^{1/2}. \tag{4.12}$$

The spectral FWHM is given by the spectral width as

$$\Delta\omega^2 = \left(2\pi\Delta\nu_L\right)^2 = \left(2\sqrt{2\ln 2}\sigma\right)^2. \tag{4.13}$$

So, equation (4.9) provides the condition of $\Delta\nu_L$ for Gaussian pulses as

$$\exp\left(-\frac{\left(2\pi\Delta\nu_L\right)^2}{8\sigma_i{}^2}\right) = \frac{1}{2}. \tag{4.14}$$

In the special case of a transform-limited pulse $\beta = 0$ (without phase modulation), the product C_B results becomes 0.441[14]. By substituting (4.11) and (4.14) into (4.10), we can calculate the coincidence probability, p as follow

$$p = 1 - \frac{1}{2} e^{-\frac{(2\ln 2)\tau^2}{\tau_L^2}}. \tag{4.15}$$

The $\beta = 0$ is the simplest case but can be achievable with proper dispersion compensation in the experiment. If $\beta \neq 0$, the phase modulation results in the temporal frequency shift or chirping, which would increase the distinguishability.

4.4.2 Time delay of two photons

In the following, we fix the time duration to 100 and 200 ps. Because of the different key rates obtained by different decoy state calculation methods, we choose the result of the most efficient infinite-sized protocol. The HOM dips are shown in Fig.4.9. They show that the acceptable time delay is 45.5 ps for 100-ps width and 89.0 ps for 200-ps width.

It should be noted that the calculation results we obtained are based on the three-intensity model. However, the four-intensity model [15], [16] with better performance have been proposed and implemented. It was suggested in four-intensity model will improve the performance for smaller number of pulses. Since the small data size is very important for practical QKD application, we should explore the improvement of the estimation with decoy method in the future. Fortunately, our conclusions are based on HOM interference, so this method is applicable to any quantum communication model (including MDI-QKD, mode-pairing QKD [17], etc.) that depends on two-photon interference.

Time control is important because the fluctuation in the fiber length in the field has a greater effect as the distance increases. If the pulse duration increases, the time-control requirement is relaxed. However, this implies low clock frequency. A shorter time duration requires strict control of the laser spectrum, and a longer time duration reduces the pulse generation rate and, thus, the key generation rate. In addition, if the window of the photon detector is widened, the dark counts and, thus, the error rate increase.

The time delay of the two pulses is detected using Charlie's time-digital converter (TDC). The measured time delay data are processed by a computer and used to control the delay line (DL) on one side to reduce the time delay of the two photon pulses to increase visibility.

Commercially available TDC devices, such as Maxim Integrated's MAX35101 and Sciosense's TDC-GPX2, provide a time resolution of 10-20 ps. Although an accuracy of 45.5 ps can be realized with these devices, stricter control would be required to reduce the errors due to the distinguishability. We still need to explore electrical methods with more sophisticated TDC devices or optical methods to detect differences in arrival time.

Note that this value is for the present criteria. A different criterion will change the requirement. It is necessary to calculate it according to the system specifications.

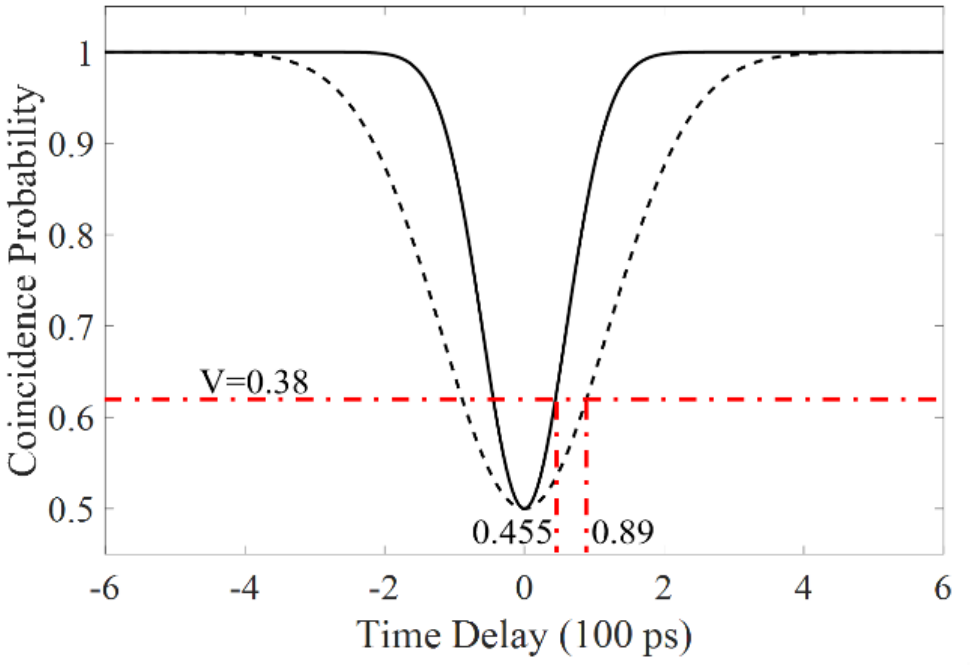


Figure 4.9. HOM-dip of 100 ps (black solid line) and 200 ps (black dotted line) time duration. The red dotted line of V=0.38 represents the position with the minimum coincidence probability of 0.62.

4.5 Summary

In this chapter, we first introduced Hong-Ou-Mandel (HOM) interference and the errors in two-photon interference within MDI-QKD. For the implementation of this protocol, the photons generated by the two independent laser sources must be indistinguishable. We calculated the final key rate of the infinite-sized and finite-sized MDI-QKD to determine the effects of two-photon distinguishability on the visibility of their interference. From this analysis, we derived reasonable ranges for visibility under conditions of both infinite and finite key lengths. Our simulation results show that the acceptable condition of visibility V = 0.42 is more stringent for finite-size key generation than the V = 0.38 of the infinite-size. We also compared the impacts of different Bell State Measurements (BSMs) across various protocols, concluding that the Beam Splitter + Polarizing Beam Splitter (BS+PBS) type BSM exhibits superior performance.

Subsequently, we calculated the coincidence probability for Gaussian photon pulse interference in the HOM setup. Based on the visibility values previously determined, we identified the acceptable range of delays for two-photon pulses within the BSM of MDI-QKD. We conclude that the acceptable time delay is 45.5 ps for 100-ps width and 89.0 ps for 200-ps width. We also estimated an acceptable time delay between two photons from two independent pulse lasers.

This study provides quantitative conditions for timing-control accuracy, which will play an important role in improving the performance of practical MDI-QKD systems. Because synchronization is crucial to achieving high visibility of two-photon interference, we still need to improve the method to measure and control the relative time difference between photons from remote sources.

References

[1] H.-K. Lo, M. Curty, and B. Qi, “Measurement-Device-Independent Quantum Key Distribution,” Phys. Rev. Lett. 108, 130503, 2012.

[2] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki and H.-K. Lo, “Finite-key analysis for measurement-device-independent quantum key distribution,” Nat Commun 5, 3732, 2014. DOI: 10.1038/ncomms4732

[3] C. K. Hong, Z. Y. Ou and L. Mandel, “Measurement of subpicosecond time intervals between two photons by interference,” Phys. Rev. Lett. 59, 2044, 1987.

[4] A. M. Brańczyk, “Hong-Ou-Mandel Interference,” 2017. arXiv: 1711. 00080v1.

[5] R. P. Feynman, R. B. Leighton and M. Sands, “The Feynman Lectures on Physics”, American Journal of Physics, 33, 750 (1965).

[6] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão and J. P. von der Weid, “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits”, Phys.Rev.A 88, 052303 (2013).

[7] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty and A. J. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers”, Nature Photonics, 2016, 10: 312‑315.

[8] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen and J.-W. Pan, “Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network”, Phys.Rev.X 6, 011024 (2016).

[9] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, “Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks”, Phys.Rev.Lett. 111, 130501 (2013).

[10] H.-K. Lo, M. Curty and B. Qi, “Measurement-Device-Independent Quantum Key Distribution”, Phys.Rev.Lett. 108, 130503 (2012).

[11] X. Ma and M. Razavi, “Alternative schemes for measurement-device-independent quantum key distribution”, Phys.Rev.A. 86, 062319 (2012).

[12] Z-W. Yu, Y-H. Zhou, and X-B. Wang, “Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method” Phys.

Rev. A. 91, 032318, 2015.

[13] H. Kim, O. Kwon and H. S. Moon, “Time-resolved two-photon interference of weak coherent pulses,” Appl. Phys. Lett. 118, 244001, 2021.

[14] J. Herrmann and B. Wilhelmi, “Principle of ultrashort optical pulse generation: Mode synchronization technology,” in Lasers for Ultrashort Light Pulses, Tokyo, Japan: Kyoritsu-pub. 1991, pp. 75-80.

[15] Y. Zhou, Z. Yu and X. Wang, “Making the decoy-state measurement-device-independent quantum key distribution practically useful,” Phys. Rev. A. 93, 042324, 2016.

[16] X-L. Hu, C. Jiang, Z-W. Yu, and X-B. Wang, “Practical Long-Distance Measurement-Device-Independent Quantum Key Distribution by Four-Intensity Protocol,” Adv. Quantum Technol. 4, 2100069, 2021. DOI: 10.1002/qute.202100069.

[17] P. Zeng , H. Zhou, W. Wu and X. Ma, “Mode-pairing quantum key distribution,” Nat Commun 13, 3903, 2022.

Chapter 5

Synchronization scheme of MDI-QKD

5.1 Introduction

The MDI-QKD (Measurement-Device-Independent Quantum Key Distribution) protocol mandates that the two photons arriving at the measurement device must be indistinguishable. In the previous chapters, we calculated the theoretical range of acceptable time delay errors for two-photon pulses. To achieve this, precise time control is imperative to eliminate any distinguishability caused by variations in the arrival times of the photons. In conventional methodologies [1]-[3], the temporal difference between the photon arrivals is ascertained at a specific measuring instrument, referred to as Charlie. Subsequently, a control signal is transmitted to the users, Alice and Bob, to adjust their photon emission timings. However, these methods incorporate a long feedback loop and may result in unstable control dynamics, especially during long-distance transmissions where signal degradation can occur.

In this chapter, we introduce an innovative method in which the difference in photon arrival times is detected and managed directly at Charlie. To facilitate this, the reference signal for time adjustment is generated by an optical frequency comb (OFC), which is meticulously synchronized with the quantum signal. This synchronization ensures that the quantum signal photons are aligned with the reference signal pulses, thereby enhancing the temporal alignment of the photons.

We conducted a proof-of-principle experiment to validate the effectiveness of this new approach. The results of this experiment confirmed that the time synchronization precision required for the successful execution of the MDI-QKD protocol could indeed be achieved. This proposed methodology not only confirms the practical feasibility of improved time control but also significantly simplifies the implementation process of MDI-QKD, making it more robust and efficient for practical quantum cryptographic applications.

5.2 Existing schemes

5.2.1 Experimental setup

Tang et al. [1] and Valivarthi et al. [2] demonstrated disturbance compensation schemes; however, these schemes rely on long-distance feedback channels, which may introduce unnecessary errors. Even when the signal source is compensated and corrected, errors generated in long-distance fiber channels may still be overlooked. Fan-Yuan et al. [3] also implemented a multi-user MDI-QKD network using passive techniques of reference-frame-independent (RFI) protocol and polarization-compensation-free (PCF) method.

In reference [1], by creating a system operating at a 75 MHz clock rate that is fully automatic and highly stable, and by using superconducting nanowire single-photon detectors with detection efficiencies exceeding 40%, we have extended the secure transmission distance of MDIQKD (Measurement-Device-Independent Quantum Key Distribution) up to 200 km and achieved a secure key generation rate that is three orders of magnitude higher.

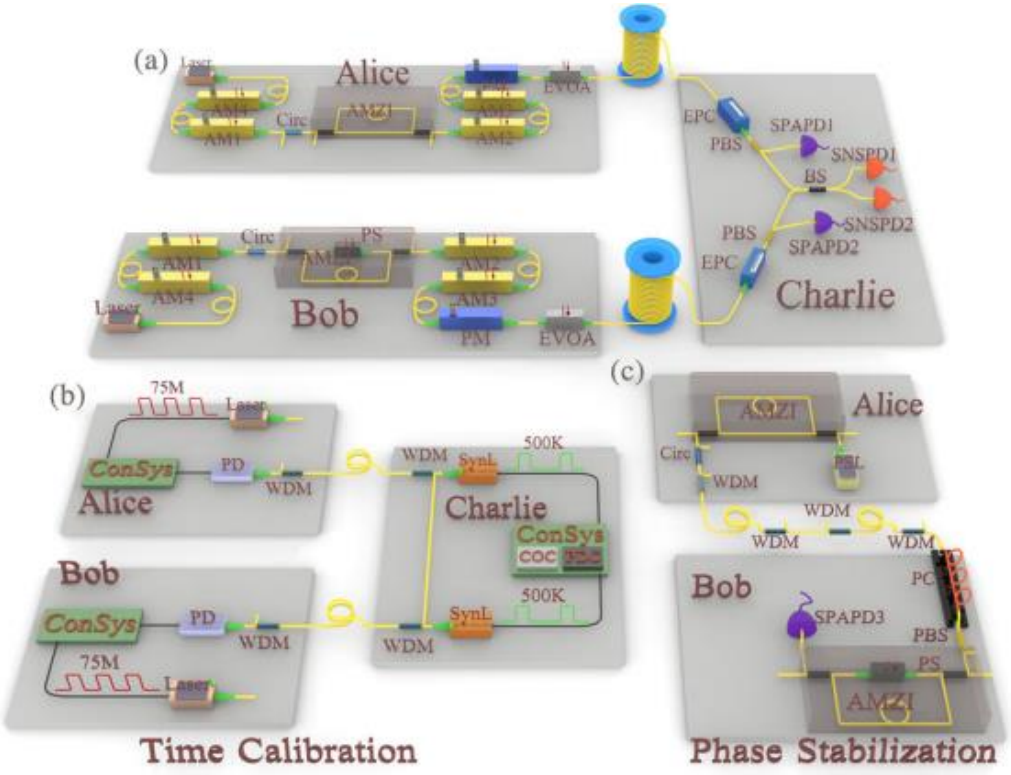


Figure 5.1. The time calibration scheme for MDI-QKD described in [1]. Two SynLs (1570 nm) are adopted, with the 500 kHz shared time reference generated from a crystal oscillator circuit (COC) and with the time delayed by a programmable delay chip (PDC). Alice (Bob) receives the SynL pulses with a PD and then regenerates a system clock of 75 MHz. WDM: wavelength division multiplexer, ConSys: control system.

As illustrated in Figure 5.1, for the timing mechanism, two trains of synchronization laser (SynL, 1570 nm) pulses are transmitted from Charlie to Alice and Bob through two separate fiber links,

utilizing shared time references produced by a crystal oscillator circuit located at Charlie's facility. Alice (and Bob) employs a photoelectric detector (PD) to capture the SynL pulses. The signals from the PD are then used to reconstruct a 75 MHz system clock, ensuring synchronization across the entire system. Subsequently, we accurately align the two trains of signal laser pulses using a feedback control mechanism. Alice and Bob send their signal laser pulses to Charlie in an alternating fashion. Charlie, equipped with a superconducting nanowire single-photon detector (SNSPD), measures the arrival times of these pulses. Based on the differential arrival times, Charlie modifies the time delay between the two SynL pulse trains using a programmable delay chip. The timing resolution achieved is 10 ps, and the overall timing calibration precision is maintained below 20 ps, both significantly finer than the 2.5 ns pulse width of the signal laser.

However, the scheme proposed in [1] necessitates the optimization of high-speed laser modulation techniques, which is crucial for further enhancing the system clock rate. For instance, employing state-of-the-art components to achieve GHz-level clock rates [4] and reducing overall timing jitter. There is still significant room for improvement in the efficiency of superconducting nanowire single-photon detectors (SNSPDs) [5]. Ideally, increasing the clock rate and detector efficiency can further enhance the transmission distance and secure key rate.

Additionally, in the experiment described in [1], two separate fibers were used to transmit signal laser pulses and synchronization laser pulses, respectively. To enhance the appeal of MDIQKD in practical applications, utilizing a single fiber to simultaneously transmit both types of laser pulses [6]-[8] and minimizing noise originating from Raman spontaneous scattering [9], [10] would be ideal.

For Charlie to successfully perform a Bell State Measurement (BSM), the photons emitted by Alice and Bob must be indistinguishable in all degrees of freedom, including spatial, spectral, polarization, and temporal degrees. Spatial overlap is easily ensured by using single-mode fibers. Spectral overlap is achieved by carefully tuning and stabilizing the wavelengths of the Distributed Feedback (DFB) lasers. However, since photons typically travel long distances (tens of kilometers) through independent fibers, they are subject to varying environmental conditions, leading to fluctuations in polarization states and arrival times at Charlie's location. Therefore, the scheme employs feedback mechanisms to actively compensate for these variations. To achieve efficient key generation, it is imperative that the feedback systems do not interfere with the actual key distribution process (ensuring maximum operational time for key distribution), and that all expensive components of the control module are integrated into Charlie.

To compensate for the varying transmission times of the photon pulses sent from Alice and Bob to Charlie, [2] observes the degree of Hong-Ou-Mandel (HOM) interference at Charlie [11]. For this purpose, the signals from two SNSPDs are sent to an HOM unit, which monitors the coincidence detection rate corresponding to both photons arriving in the same mode. Due to photon

bunching, the coincidence count rate reaches a minimum when photons from Alice and Bob simultaneously arrive at the PMBS, providing an accurate feedback signal to maintain timing synchronization. At this point, Alice's qubit generation time is adjusted with an accuracy of 27.8 ps to sustain the coincidence count rate at its minimum. Consequently, timing synchronization is achieved through a self-contained feedback mechanism, obviating the need for additional SNSPDs or high-bandwidth PDs [12].

In the MDI-QKD system in [2], as shown in Figure. 5.2, a time-tagging module is utilized to record the preparation information of Alice and Bob's qubits. Alice and Bob record the emission time with an accuracy of 50 ns, as well as the basis (X or Z), bit value (0 or 1), and the chosen mean photon number (vacuum, decoy, signal). Additionally, the successful BSM time at Charlie and the projected state are recorded. Understanding the exact propagation time from Alice and Bob to Charlie allows for backtracking and determining which two qubits interacted at Charlie.

Charlie sends a common clock signal to synchronize the qubit preparation devices of Alice and Bob. During the time-tagging process, Alice and Bob send their prepared qubit information (excluding time) to memory buffers, specifically first-in-first-out (FIFO) buffers in their FPGAs, while the corresponding qubits are sent to Charlie. The memory buffer time is set to be equal to the time required for the qubits to reach Charlie plus the time required for the BSM signal to reach Alice (or Bob) from Charlie. Subsequently, a simple logic operation allows only the successful BSM-generated qubits to be singled out and only these qubits are further processed.

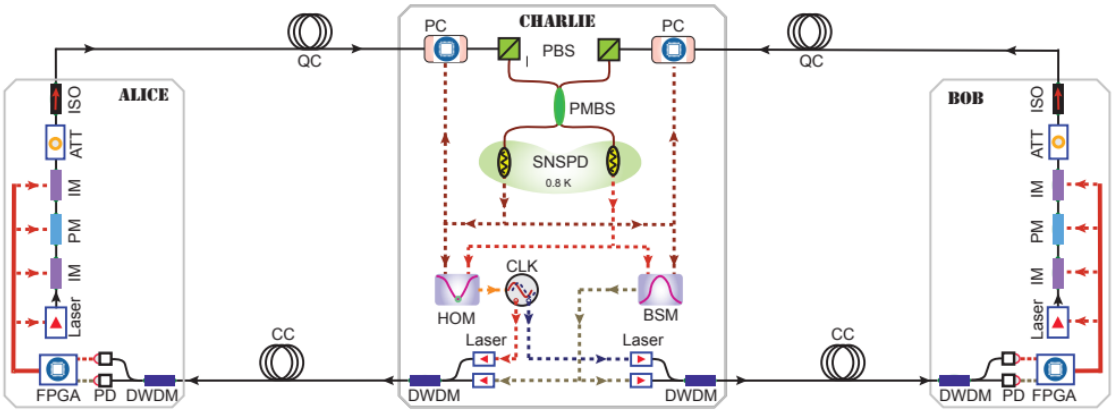


Figure 5.2. The experimental step of MDI-QKD described in [2]. PC: polarization controller, PBS: polarization beam splitter, PMBS: polarization maintaining beam splitter, SNSPD: superconducting nanowire single photon detector, HOM: Hong-Ou-Mandel measurement, CLK: clock, BSM: Bell state measurement, DWDM: dense wavelength division multiplexers, PD: photon detector, FPGA: field-programmable gate array, IM: intensity modulator, PM: phase modulator, ATT: attenuator, ISO: isolator, QC: quantum channel, CC: classical channel. Note that the CLK and BSM signals are distributed to Alice and Bob electronically in the experiment.

In [2], two spooled fibers of 40 kilometers in length were employed. The average photon number per qubit was 0.03. The measured visibility was determined to be 46.4±0.5%, slightly lower than the maximum possible value of 50% for pulses with a Poisson photon-number distribution. In the experiment, after accumulating approximately 30 million bytes of tagged data, Alice and Bob compared their data files. Based on the comparison, gains and quantum bit error rates (QBER) were calculated to determine the secure key rate [13]. Ultimately, over an 80-kilometer spooled fiber, the secret key rate exceeded 0.1 kbps. By increasing the clock rate from 20 MHz to 2 GHz (limited by the 200 ps clock jitter of the SNSPD [14], [15]), this rate could be increased to approximately 10 kbps. If standard fiber (0.2 dB/km) were replaced with ultra-low-loss fiber (0.16 dB/km), the distance could be further extended [16], [17].

5.2.2 Disadvantages of existing schemes

The experimental schemes employed in the previous studies [1], [2] can be simplified to the measurement-feedback-modulation system depicted in Figure 5.3 to compensate for the arrival time difference.

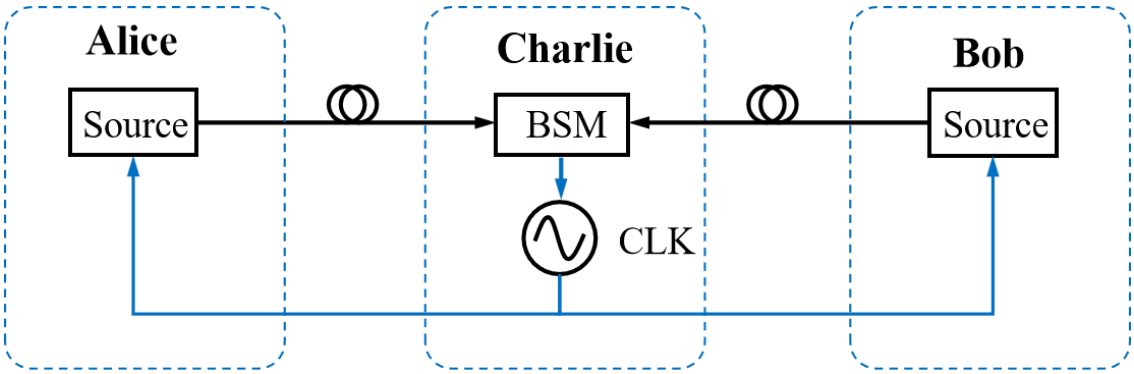


Figure 5.3. Basic composition of the timing control in [1], [2]. Charlie conducts BSM on the received signals and subsequently transmits synchronized clock signals to Alice and Bob for calibration based on the measurement results. CLK: clock, BSM: Bell state measurement.

Their synchronization mechanism relies on Charlie to transmit synchronous clock signals to Alice and Bob through the feedback channel, enabling the compensation for arrival time differences. However, the stability of the feedback control can be compromised by the inherent loop delay in transmitting control signals between Charlie, Alice, and Bob. To mitigate this issue, it's crucial that the changes in the transmission lines occur at a slower rate compared to the transmission time itself. Any disturbances in the transmission process can disrupt the synchronization process, potentially leading to inaccuracies. Additionally, even after achieving

synchronization, the signals transmitted by Alice and Bob may encounter new disturbances as they traverse long-distance fiber channels, further complicating the process of maintaining synchronization.

5.3 Proposed scheme

5.3.1 Improved time synchronization scheme

We propose an improved method to decrease the impact of temporal distinguishability, without depending on the long-distance feedback to eliminate the effects of time delay and channel noise. Our proposal is based on the observation that Charlie's actions will not impact the security of the MDI-QKD protocol. Charlie's actions include assisting Alice and Bob in synchronizing the pulse arrival times. Figure 5.4 illustrates the proposed configuration of the MDI-QKD system.

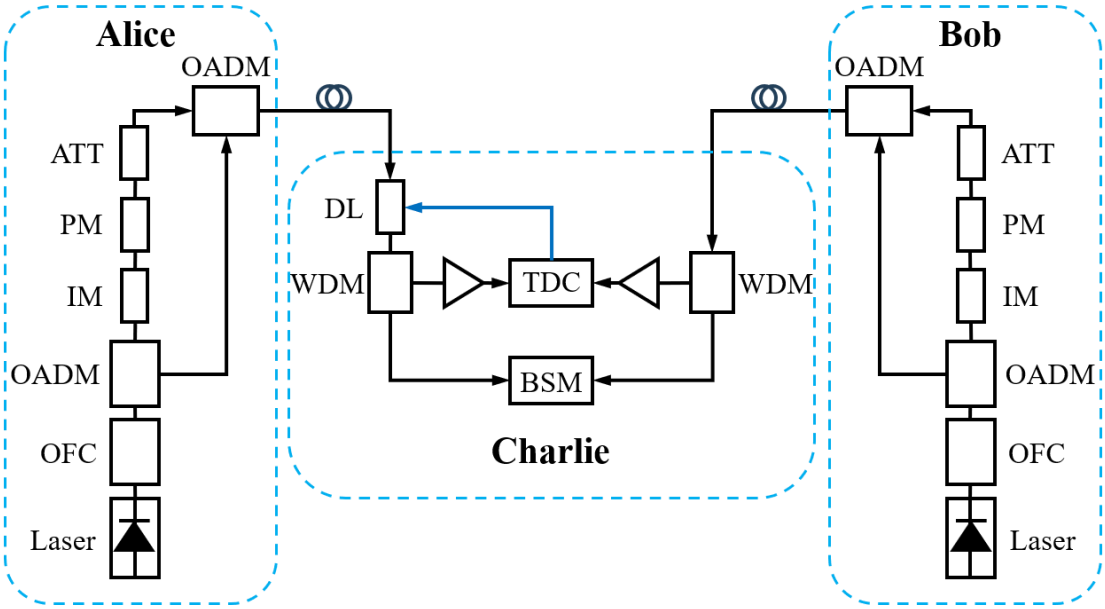


Figure 5.4. Schematic layout of the proposed MDI-QKD system. OFC, optical frequency comb modulator; OADM, optical add–drop multiplexer; IM, intensity modulator; PM, phase modulator; ATT, attenuator; DL, delay line; WDM, wave division multiplexing; TDC, time-digital converter; BSM, Bell state measurement.

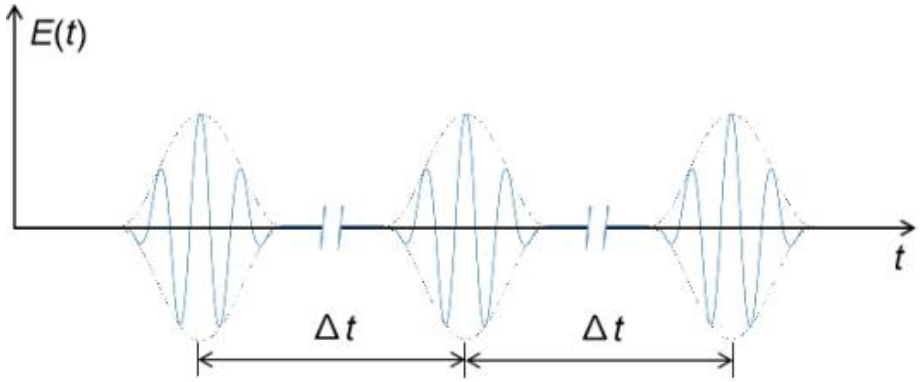
As in typical setups involving Alice and Bob, independent laser sources generate weakly coherent pulses (WCPs). To meet the requirements for both the signal pulses for BSM and the reference pulses for delay detection, we propose utilizing an optical frequency comb (OFC) [35]. The OFC produces evenly spaced signals in the wavelength domain that are synchronized in both time and phase. Using an optical add–drop multiplexer (OADM), Alice and Bob select a wavelength as the signal and send it back to the comb after modulation and attenuation. Another

unmodulated wavelength is utilized for the reference. Charlie separates the reference pulses and signal pulses with a wave division demultiplexer. He measures the time difference between Alice's reference pulses and Bob's reference pulses using a time-digital converter (TDC). The difference supplies a feedback signal to the delay line (DL). Since the signal pulses and reference pulses undergo the same delay caused by the DL placed before the wave division multiplexer (WDM) and are initially synchronized, the synchronization of the reference pulses implies the synchronization of the signal pulses. The delay that occurs after the signal passes through the long-distance channel is effectively eliminated. Finally, Charlie performs BSM on the synchronized signals.

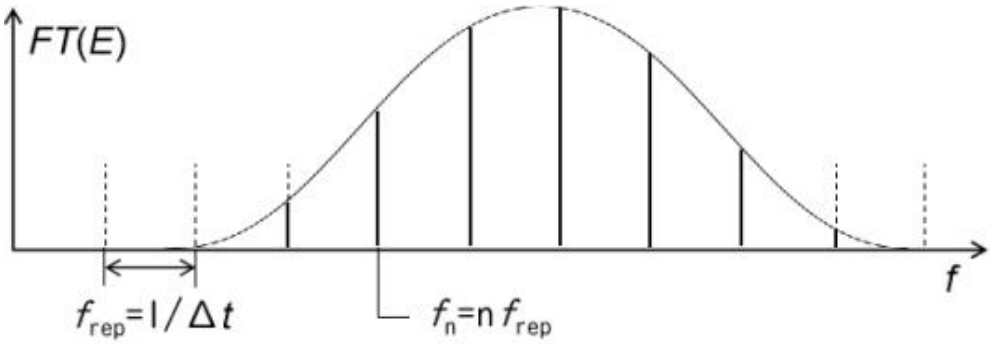
5.3.2 Optical frequency comb

In order to modulate the attenuated weak coherent pulse train into a periodic strong pulse train, we consider using optical frequency comb (OFC).

Generally, there are three methods of long-distance frequency transmission through optical fiber [18]. The first method is to transmit a continuous laser signal modulated by amplitude. This method is very straightforward, but because modulation introduces noises and requires high frequency electronics technology to support [19]. The second method is to transmit a stable continuous optical frequency signal of extremely narrow linewidth directly [20]. The advantage is that the optical signal will not be affected by dispersion. However, the system of grafting microwave signal and optical frequency signal requires a number of stable optical frequency comb systems with wide bandwidth, which is usually very complex. The last one is the optical frequency comb generated by the transfer mode-locked laser [21], [22]. The frequency interval of the comb teeth is the repetition frequency of the mode-locked pulse train, generally in the MHz-GHz range. We can lock with the microwave frequency standard by controlling the cavity length of the laser. In this way, the transmitted optical band signals are also loaded with RF information. At the same time, mode-locked pulses are generally generated based on the intrinsic electronic nonlinear optical response of the material. Generally, the rising edge of the pulse is in the femtosecond order and has the advantages of high detection SNR and low duty cycle.



(a) Time domain



(b) Frequency domain

Figure.5.5. Time domain and Frequency domain of OFC.

OFC is generated by a mode-locked laser. It is a laser source with ultra-short pulses. If the laser pulse repetition frequency and carrier envelope frequency shift are precisely controlled, according to Fourier transform, a series of comb spectral lines with uniform distribution, fixed position and extremely wide spectral range are obtained in frequency domain. It can be used as a reference to measure the unknown frequency or stabilize the laser to a specific frequency. While in time domain, it is shown as a pulse train with stable repetition frequency, as shown in Fig.5.5.

OFC can be generated based on different external modulators, such as phase modulator (PM) [23]-[27], intensity modulator (IM) [28]-[30], electrical absorption modulator (EAM) [31], polarization modulator [32], etc. The method of PM for continuous laser is simple and flexible. However, a lot of PMs are generally used in the scheme, so the cost is relatively high. OFC generated by IM has tunable bandwidth and spacing of comb lines, with considerable number of comb lines and better flatness. In the scheme of generating OFC by EAM, the time window of EAM in amplitude selector circuit is much shorter. Using EAM as the limiter gate can make the output spectral lines have better flatness, but the bandwidth and spacing of the spectral lines are not tunable, and the number of comb lines is small. In addition, OFC can also be generated by optical nonlinear effect [33]. However, it is difficult to control the optical nonlinear effect process, and the center wavelength and spacing of the comb line are not tunable.

The scheme to generate OFC based on external modulator is simple, easy to implement and stable. The output spectrum is relatively flat, and the number of comb lines is considerable, but it requires RF signal as the driving signal to provide voltage with a specific frequency to the modulator. We chose a wide and flat tunable OFC scheme based on the dual-drive Mach-Zendell modulator (MZM) [34], which is simple, flexible and easy to operate.

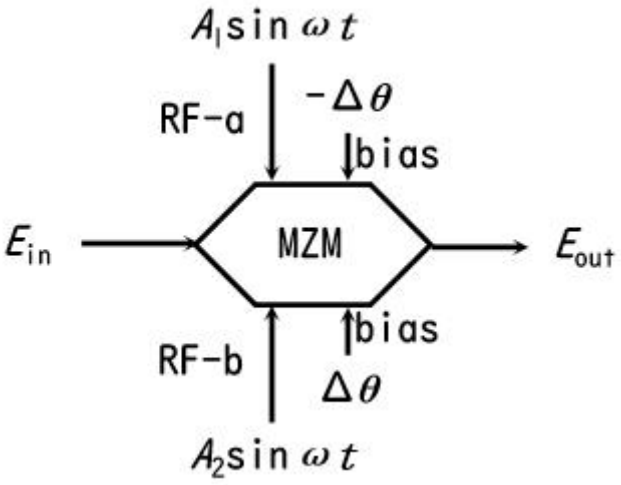


Figure.5.6. Concept of optical frequency comb generation using a dual-drive MZM.

The principle of OFC using a MZM is shown in Fig.5.6. In the OFC generator, an input continuous-wave (CW) light wave is modulated with a large amplitude RF signal using a dual-drive MZM. Higher-order sideband frequency components are generated. And these components can be used as a frequency comb because the signal has a spectrum with a constant frequency spacing [34]. The intensity of each component is highly dependent on the harmonic order. The spectral unflattens can be canceled if the dual arms of the MZM are driven by in-phase sinusoidal signals, RF-a and RF-b in Fig.5.9, with a specific amplitude difference.

Suppose that the optical phase shift induced by signals RF-a and RF-b, respectively. The optical field at the output of the MZM is given by [69]:

$$E_{\text{out}} = \frac{1}{2} E_{\text{in}} \sum_{k=-\infty}^{k=+\infty} \left[I_k\left(A_1\right) e^{j(k\omega t+\theta_1)} + I_k\left(A_2\right) e^{j(k\omega t+\theta_2)} \right] \tag{5.1}$$

where $I_k(A)$ denotes the kth-order Bessel function.

Power conversion efficiency from the input CW light to each harmonic mode can be asymptotically approximated as:

$$\begin{aligned} \eta_k = \frac{P_k}{P_{in}} \approx \frac{1}{2\pi \bar{A}} \Big\{ & 1 + \cos\left(2\Delta\theta\right)\cos\left(2\Delta A\right) \\ & + \left[\cos\left(2\Delta\theta\right) + \cos\left(2\Delta A\right)\right] \cos\left[2\bar{A} - \frac{(2k+1)\pi}{2} \right] \Big\} \end{aligned} \tag{5.2}$$

where $\bar{A} = (A_1 + A_2)/2$, $\Delta A = (A_1 - A_2)/2$, and $\Delta\theta = (\theta_1 - \theta_2)/2$. Here, $2\Delta A$ means a peak-to-peak phase difference induced in each arm; $2\Delta\theta$ means a DC bias difference between the arms. This expression describes the generated comb well as long as $\bar{A}$ is large enough. To make the comb flat in the optical frequency domain, the intensity of each mode should be independent of k.

From Eq.(5.2), the driving condition becomes

$$\Delta A \pm \Delta\theta = \frac{\pi}{2} \tag{5.3}$$

under which frequency components of the generated OFC should have the same intensity.

Under this condition, the intrinsic conversion efficiency is theoretically derived from Eqs.(5.2) and (5.3), resulting in

$$\eta_k = \frac{1-\cos 4\Delta\theta}{4\pi\bar{A}}. \tag{5.4}$$

So, the optimal driving condition for flatly generating an OFC with the maximum conversion efficiency is given by

$$\eta_{k\max} = \frac{1}{2\pi\bar{A}} \text{ when } \Delta A = \Delta\theta = \frac{\pi}{4}. \tag{5.5}$$

This is the optimal driving condition for flatly generating an OFC with the maximum conversion efficiency.

The bandwidth of the generated frequency comb should be limited, otherwise, total energy is diverged. Thus, we assume that optical energy is equally distributed to each frequency mode around the center wavelength and the optical level out of the band is zero. This assumption is reasonable because the approximation for Eq.(5.2) is valid for small *k*, and η_k rapidly approaches zero for large *k*. Since the total energy, $\bar{P}_{out}$, can be calculated in the time domain, the bandwidth of the frequency comb becomes:

$$\begin{aligned}\Delta\omega &= \frac{\overline{P_{\text{out}}}\omega}{\eta_k P_{\text{in}}} = 2\pi\bar{A}\omega\frac{1-\cos\left(2\Delta A\right)I_0\left(2\Delta A\right)}{1-\cos\left(4\Delta A\right)} \\ &\approx \pi\bar{A}\omega\end{aligned} \tag{5.6}$$

which is almost independent of ΔA (or $\Delta\theta$).

5.3.3 Experimental setup

The experiments were carried out to verify the feasibility of the proposal with the setup shown in Fig. 5.7. We have shown that the signal synchronizes with the reference separated by WDM, and we have measured the time error of this synchronization. The generation of the signal and reference for Alice and Bob employed a single OFC.

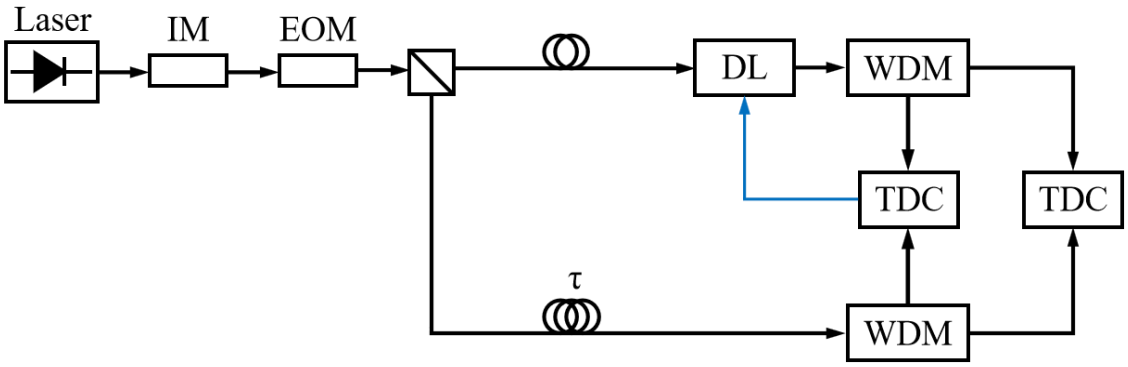


Figure 5.7. Experimental setup used to verify the synchronization of optical frequency comb signals. EOM: electro-optic modulator is used for optical frequency comb modulation. An adjustable time delay τ is added to one side output of the beam splitter. Time delay detected by TDC is compensated by DL modulation on the other side (or the same side).

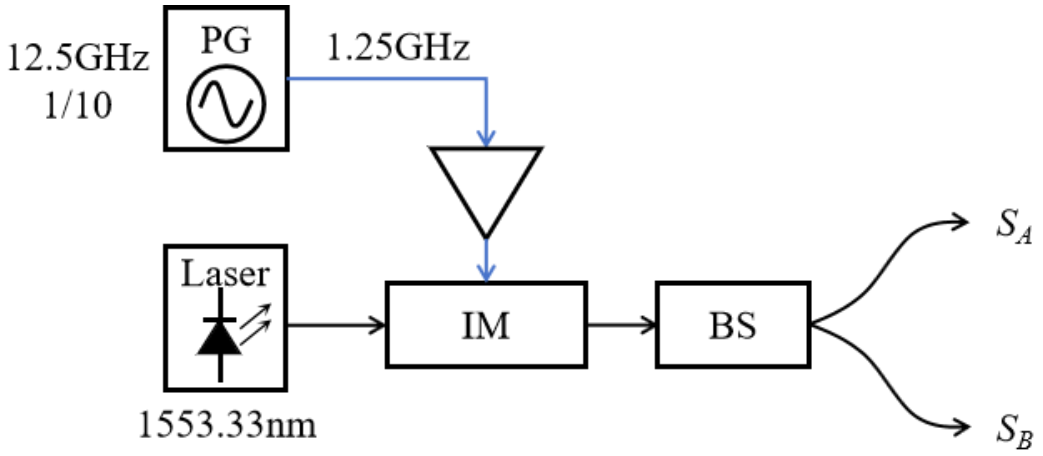


Figure 5.8. Experimental setup of generation of pulses.

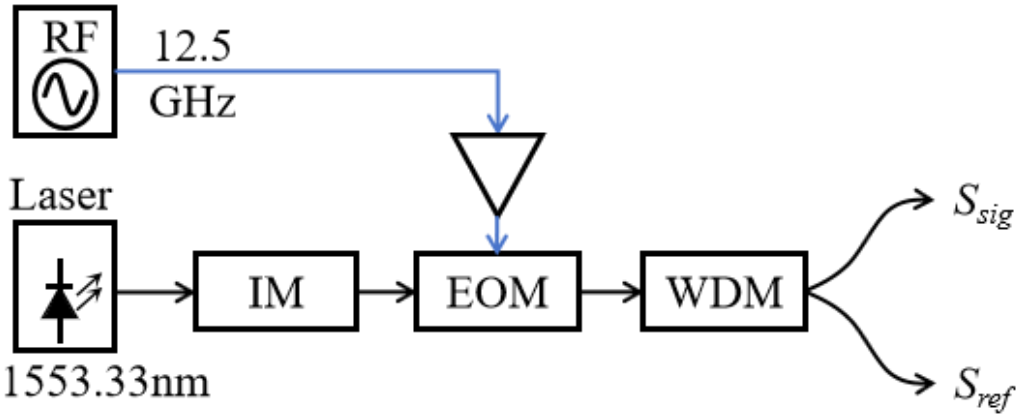


Figure 5.9. Experimental setup of generation of OFC.

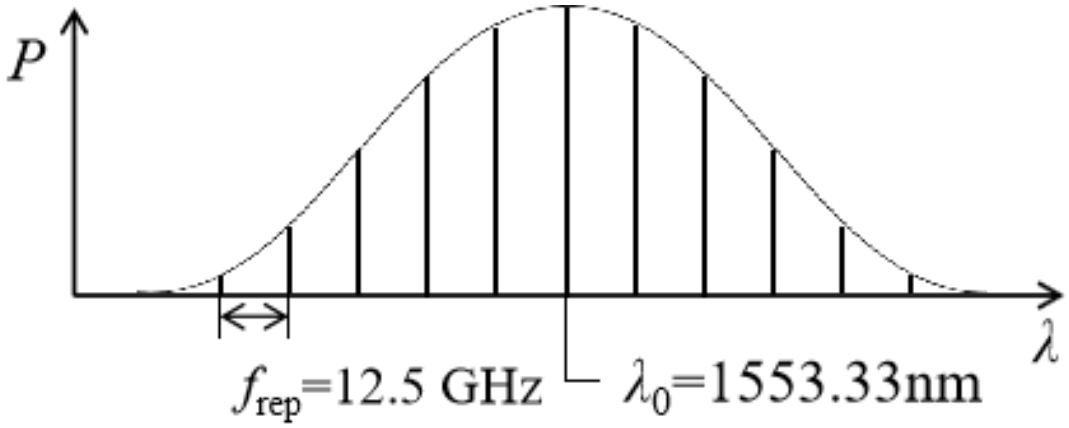


Figure 5.10. The spectral results of the OFC experiment.

We use an intensity modulator (IM) to modulate a continuous wave laser at 1553.33nm. The pulse generator divides a 12.5GHz electrical pulse signal by 1/10, producing pulses with a minimum width of 80ps at 1.25GHz. The modulated laser pulses are then evenly split into two sequences of light pulses using a 50:50 BS, as depicted in Figure 5.8. For OFC generation, we employ a phase modulator (PM) using an electro-optic modulator (EOM) as shown in Figure 5.9. It is modulated with a 12.5GHz RF signal to generate frequency lines spaced at intervals of 12.5GHz, as illustrated in Figure 5.10.

The current experiment used one laser and divided the optical pulse into two to mimic the two independent lasers. Since we observed an HOM interference between the adjacent laser pulses at 2.5 GHz, the timing jitter between the independent lasers may not affect the HOM interference significantly. A laser with a modulated pulse frequency of 1.25 GHz and a pulse duration of 150 ps operated at a wavelength of 1553.33 nm. The separation between the signal pulse and the reference pulse after the OFC was 25 GHz. The pulses were detected by high-speed pin photodiodes. We used Multiharp 150 as a TDC to measure the time difference of the reference pulses. The measured time delay was used for the feedback signal to modulate the DL. We used General Photonics' MDL-001, which has a modulation range of 0–560 ps at the modulation rate of up to 256 ps/s. To investigate signal synchronization, we utilized the same TDC to measure the time difference between signal pulses. This was instead of observing the HOM dip for communication pulse pairs. Both methods are in principle equivalent for evaluating the distinguishability of two photons. The cumulative time of the TDC was 10 s, so the delay was controlled every 10 s.

5.3.4 Results and discussion

Figure 5.11 illustrates the relationship between the time differences of reference and signal pulses, where a 100 ps delay is approximately 20 mm of the typical optical fiber channel length. The measurement–feedback–modulation process operates effectively, as observed in the figure. The

time delays of the two sets of pulses separated by WDM exhibit proportionality.

As the Multiharp 150 provides a time resolution of 5 ps, measurement errors occur in multiples of 5 ps. The error measurement between the reference and signal pulses falls within the range of ±15 ps. This includes the error measurement in the reference pulses and the signal pulses after time difference compensation. Since the pulse duration was 150 ps, the acceptable time difference between the signal pulses is calculated to be −66.8 ps to 66.8 ps to obtain the two-photon interference visibility of 0.38 required for key generation as shown in Figure 5.12. It is evident that the error measured by our experimental setup falls within this acceptable range. The wavelength dispersion will differ the arrival time of the reference pulse from the signal pulse. The typical value for the single-mode fiber is +17 ps/nm/km. The frequency difference of 25 GHz at 1550 nm refers to the wavelength difference of 0.2 nm, resulting in the time difference of 340 ps after

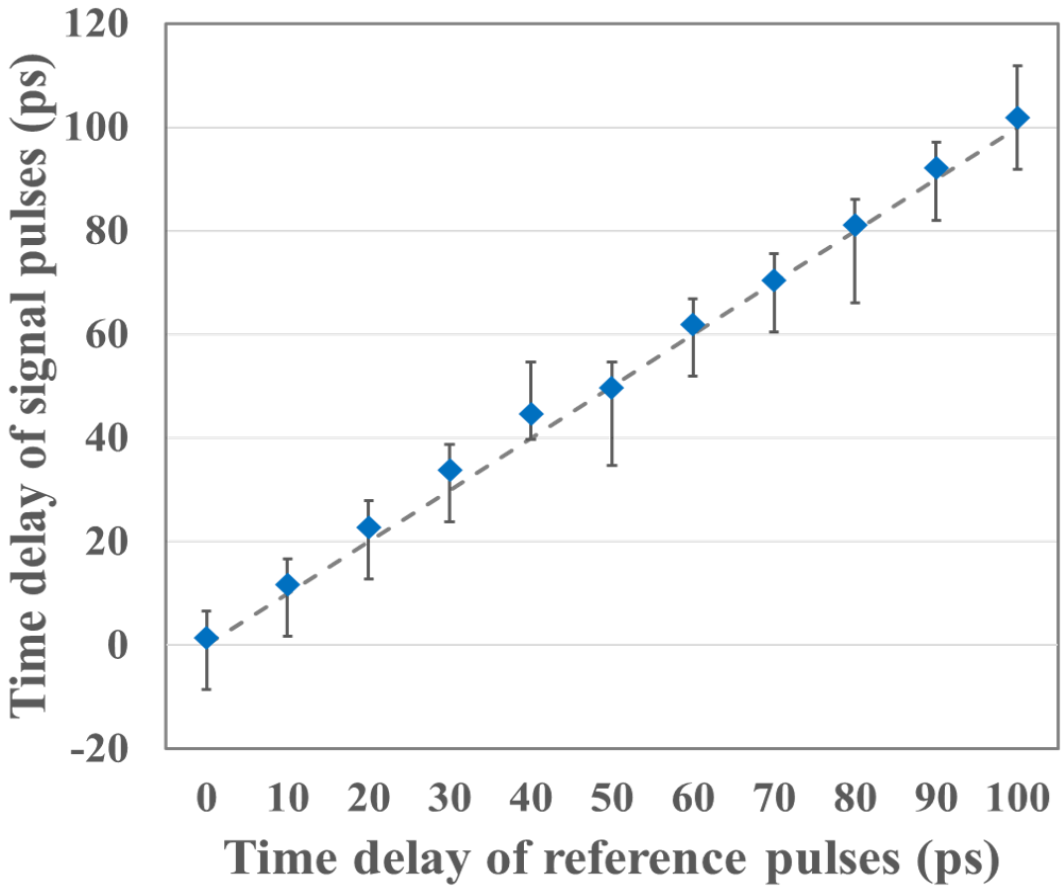


Figure 5.11. Time delay detection results of frequency optical comb signals separated by WDM. The abscissa is time delay measurement value of synchronization signal. The ordinate is time delay measurement value of detection signal. The dashed line represents the ideal value, and the blue diamonds are the average of the actual values.

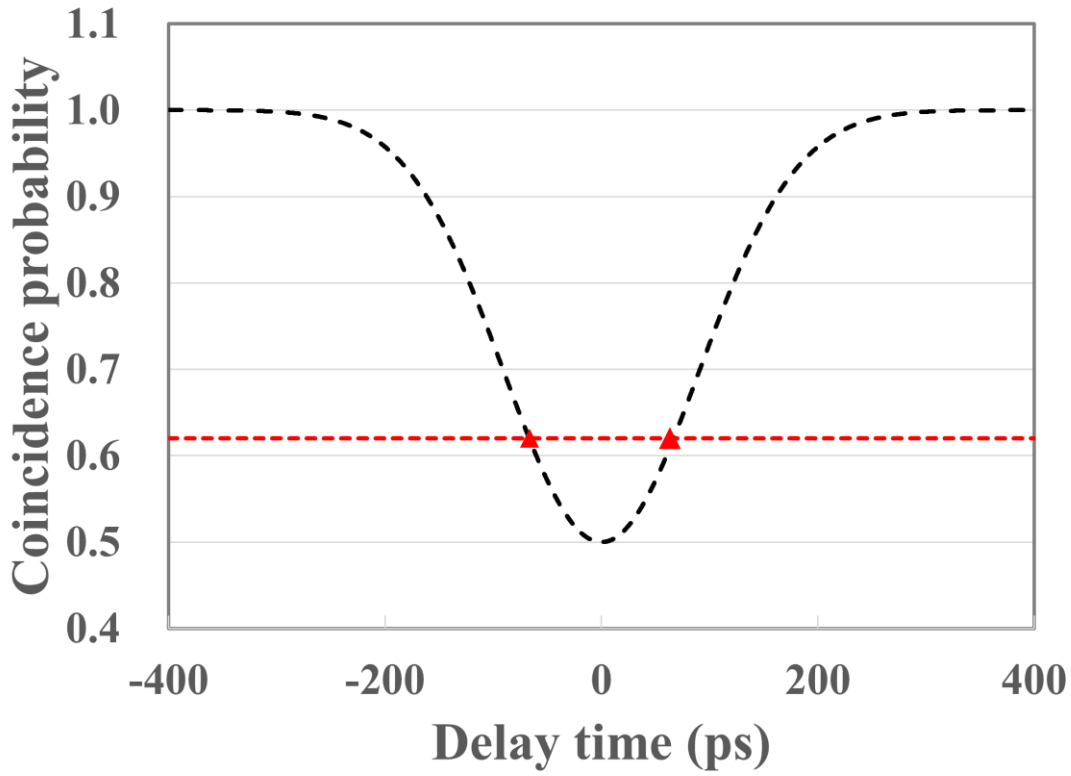


Figure 5.12. HOM-dip of 150 ps time duration Gaussian pulses.

The wavelength dispersion will differ the arrival time of the reference pulse from the signal pulse. The typical value for the single-mode fiber is +17 ps/nm/km. The frequency difference of 25 GHz at 1550 nm refers to the wavelength difference of 0.2 nm, resulting in the time difference of 340 ps after 100 km transmission. However, the difference is the same for Alice–Charlie and Bob–Charlie as long as the transmission distances are the same. Since the TDC detects the time difference of the pulse arrival times from Alice and Bob, the time difference between the reference and signal pulses does not affect the accuracy of the time difference measurement. In practical systems, dispersion compensation should be applied to reduce the pulse width deviation due to the laser chirping.

The intensity of the reference pulse was set to the smallest value for the current photodetector. It can be further reduced by using a more sensitive detector. The extinction ratio of the DWDM demultiplexer was about 25 dB. In a practical system, the scattering noise should be further reduced by 23 dB. It is possible by increasing the frequency difference and adding a narrow bandwidth filter. The TDM technique, which is used in CV-QKD systems, will be useful to reduce the noise. The TDM technique will also reduce the noise due to the nonlinear scattering. Note that the arrival time of the reference pulse may be different from that of the signal pulse if the difference is fixed.

Since all the components of the time synchronization system are integrated within Charlie's lab, time difference measurement, feedback, and time delay modulation are centralized in one location.

This consolidation effectively minimizes errors introduced into the time synchronization system. Our proposal requires no additional clock source in Charlie's system and avoids errors arising from the long-distance feedback. Although it is necessary to precisely match the clock frequencies at Alice and Bob, the phase of the clocks does not need to be synchronized in our proposal. Separation between reference and signal pulses can be improved by shifting timing. Polarization division will yield additional improvements. By utilizing a phase detector and a phase modulator in place of the TDC and DL, our proposal can compensate for phase fluctuations.

The system provides precise control of the pulse arrival time to obtain HOM interference with high visibility. However, the channel length will be changed more than the pulse period, say 400 ps, due to slow temperature variations. A temperature variation of 1℃ results in more than 1 m in a hundred kilometers, which corresponds to 5 ns of the time delay. A large delay will alter the pulse to interfere at the beam splitter and increase the error rate to 50%. Therefore, frame synchronization is necessary. The system should monitor the bit error rate and perform the frame synchronization when the bit error rate exceeds a threshold. The frame synchronization requires that the pulse periods of Alice and Bob are precisely locked. In this sense, synchronization of clock frequency is necessary. On the other hand, our DL range of 560 ps is sufficient to cover the drift within the pulse period of 400 ps for a 2.5 GHz clock system. To compensate for the fast jitter, it will be necessary to improve the feedback loop. This may be possible by adding an electrically driven phase modulator to our control system.

Our experimental setup is able to greatly reduce the requirement for synchronization in MDI-QKD systems. Our scheme can be combined with the existing methods [1]-[3].

5.4 Summary

In this chapter, we introduce an enhanced time synchronization scheme for the MDI-QKD protocol to mitigate distinguishability issues in the two-photon interference caused by the time fluctuations in long-distance transmissions. We propose to perform all steps of the synchronous measurement feedback modulation in Charlie's lab, eliminating the need for long-distance feedback and extra clock sources. By minimizing the temporal distinguishability in the two-photon interference, with DL providing the delay compensation, the signals of Alice and Bob are synchronized for the BSM. To implement this scheme, we propose to use an optical frequency comb to generate the reference and signal pulses to be synchronized with each other. We conducted an experiment to validate the feasibility of the proposal. The results prove successful synchronization between the reference and signal pulses. The obtained timing error of ±15 ps meets the calculated acceptable range for pulses with a 150 ps pulse width. Our proposal is expected to make a significant contribution to the practical application of the MDI-QKD protocol. Interestingly, TF-QKD employing frequency

optical combs to establish mutual coherence has also been proposed [36]. This shows that this technique can be widely used in future QKD networks.

References

[1] Tang, Yan-Lin, et al. "Measurement-device-independent quantum key distribution over 200 km." Physical review letters 113.19 (2014): 190501.

[2] Valivarthi, Raju, et al. "A cost-effective measurement-device-independent quantum key distribution system for quantum networks." Quantum Science and Technology 2.4 (2017): 04LT01.

[3] Fan-Yuan, Guan-Jie, et al. "Robust and adaptable quantum key distribution network without trusted nodes." Optica 9.7 (2022): 812-823.

[4] Takesue, Hiroki, et al. "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors." Nature photonics 1.6 (2007): 343-348.

[5] Marsili, Francesco, et al. "Detecting single infrared photons with 93% system efficiency." Nature Photonics 7.3 (2013): 210-214.

[6] Chapuran, T. E., et al. "Optical networking for quantum key distribution and quantum communications." New Journal of Physics 11.10 (2009): 105001.

[7] Choi, Iris, Robert J. Young, and Paul D. Townsend. "Quantum key distribution on a 10Gb/s WDM-PON." Optics express 18.9 (2010): 9600-9612.

[8] Patel, K. A., et al. "Coexistence of high-bit-rate quantum key distribution and data on optical fiber." Physical Review X 2.4 (2012): 041010.

[9] Subacius, Darius, Anton Zavriyev, and Alexei Trifonov. "Backscattering limitation for fiber-optic quantum key distribution systems." Applied Physics Letters 86.1 (2005): 011103.

[10] da Silva, Thiago Ferreira, et al. "Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems." Journal of lightwave technology 32.13 (2014): 2332-2339.

[11] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak and W. Tittel “Quantum teleportation across a metropolitan fibre network,” Nat. Phot. 10, 676–680(2016).

[12] Q. Sun, Y. Mao, S. Chen, W. Zhang, Y. Jiang, Y. Zhang, W. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T. Chen, L. You, X. Chen, Z. Wang, J. Fan, Q. Zhang and J.-W. Pan. “Quantum teleportation with independent sources and prior entanglement distribution over a network.” Nat. Phot. 10, 671–675 (2016).

[13] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok and W. Tittel, “Modeling a measurement-device-independent quantum key distribution system,” Opt. Express 22(11), 12716 – 12736 (2014).

[14] R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam and W. Tittel, “Efficient Bell-state analyzer for time-bin qubits,” Opt. Express 2014, 22, 24497

[15] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits and S. W. Nam, “Detecting single infrared photons with 93% system efficiency,” Nat. Phot. 7, 210–214 (2013).

[16] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang and J.-W. Pan, “Measurement device independent quantum key distribution over 404 km optical fibre,” arXiv:1606.06821 (2016).

[17] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew and H. Zbinden, “Provably secure and practical quantum key distribution over 307?km of optical fibre,” Nat. Phot. 9, 163–168 (2015).

[18] S. M. Foreman, K. W. Holman, D. D. Hudson, D. J. Jones and J. Ye, “Remote transfer of ultrastable frequency references via fiber networks”, Review of Scientific Instruments, 78: 021101 (2007).

[19] M. Fujieda, M. Kumagai, T. Gotoh and M. Hosokawa, “Ultrastable Frequency Dissemination via Optical Fiber at NICT”, IEEE Transactions on Instrumentation and Measurement, 2009, 58(4): 1223-1228.

[20] K. Predehl1, G. Grosche, S. M. F. Raupach, S. Droste, O. Terra, J. Alnis, Th. Legero, T. W. Hänsch, Th. Udem, R. Holzwarth and H. Schnatz, “A 920-Kilometer Optical Fiber Link for Frequency Metrology at the 19th Decimal Place”, Science, 2012, 336(6080): 441-444.

[21] G. Marra, H. S. Margolis and D. J. Richardson, “Dissemination of an optical frequency comb over fiber with 3×10^{-18} fractional accuracy”, Opt. Express, 2012, 20(2): 1775-1782.

[22] K. Jung, J. Shin, J. Kang, S. Hunziker, C.-K. Min and J. Kim, “Frequency comb-based microwave transfer over fiber with 7×10^{-19} instability using fiber-loop optical-microwave phase detectors”, Opt. Lett. 2014, 39(6): 1577-1580.

[23] J. Zhang, J. Yu, N. Chi, Z. Dong, X. Li, Y. Shao, J. Yu and L. Tao, “Flattened comb generation using only phase modulators driven by fundamental frequency sinusoidal sources with small frequency offset”, Optics Letters, 2013, 38(4): 552-554.

[24] Y. Y. (K.) Ho and L. Qian, “Dynamic arbitrary waveform shaping in a continuous fiber”, Optics Letters, 2008, 33(11): 1279-1281.

[25] Z. Jiang, C.-B. Huang, D. E. Leaird and A. M. Weiner, “Optical arbitrary waveform processing of more than 100 spectral comb lines”, Nature Photonics, 2007, 1: 463‑467.

[26] D. J. Geisler, N. K. Fontaine, T. He, R. P. Scott, L. Paraschis, J. P. Heritage and S. J. B. Yoo, “Modulation-format agile, reconfigurable Tb/s transmitter based on optical arbitrary waveform generation”, Optics Express, 2009, 17(18): 15911-15925.

[27] R. P. Scott, N. K. Fontaine, J. P. Heritage and S. J. B. Yoo, “Dynamic optical arbitrary waveform generation and measurement”, Optics Express, 2010, 18(18): 18655-18670.

[28] L. Shang, A. Wen, G. Lin and Y. Gao, “A flat and broadband optical frequency comb with tunable bandwidth and frequency spacing”, Optics Communications, 2014, 331: 262-266.

[29] S. Preussler, N. Wenzel and T. Schneider, “Flat, rectangular frequency comb generation with tunable bandwidth and frequency spacing”, Optics Letters, 2014, 39(6): 1637-1640.

[30] X. Zhou, X. Zheng, H. Wen, H. Zhang and B. Zhou, “Generation of broadband optical frequency comb with rectangular envelope using cascaded intensity and dual-parallel modulators”, Optics Communications, 2014, 313: 356-359.

[31] F. Zhang, J. Wu, Y. Li and J. Lin, “Flat optical frequency comb generation and its application for optical waveform generation”, Optics Communications, 2013, 290: 37-42.

[32] C. Chen, F. Zhang and S. Pan, “Generation of Seven-Line Optical Frequency Comb Based on a Single Polarization Modulator”, IEEE Photonics Technology Letters, 2013, 25(22): 2164-2166.

[33] S. G. Zhang, S. Q. Li, W. Zhang, P. Wang, D. H. Li, Z. Y. Wei, N. C. Shen , Y. X. Nie , Y. P. Gao and H. N. Han, “Precise control of femtosecond Ti:sapphire laser frequency comb”, Acta Physica Sinica, 2007, 56(5): 2760-2764.

[34] T. Sakamoto, T. Kawanishi and M. Izutsu, “Asymptotic formalism for ultraflat optical frequency comb generation using Mach-Zehnder modulator”, Opt. Lett., 2007, 32: 1515–1517.

[35] Tan, Yu-Jie, et al. "Modified time-delay interferometry with an optical frequency comb." Physical Review D 106.4 (2022): 044010.

[36] Zhou, Lai, et al. "Twin-field quantum key distribution without optical frequency dissemination." nature communications 14.1 (2023): 928.

Chapter 6

Conclusion

To address potential security vulnerabilities in practical quantum key distribution (QKD) systems, measurement-device-independent quantum key distribution (MDI-QKD) has been proposed. MDI-QKD protects legitimate users from attacks on measurement devices. The decoy method allows for unconditionally secure quantum key generation using lasers. For MDI-QKD, it is crucial that the photons emitted by two independent lasers are indistinguishable. As the MDI-QKD protocol relies on the photon bunching effect of two indistinguishable photons at a 50:50 beam splitter (BS), stable Hong-Ou-Mandel (HOM) interference should be observed. The validity of HOM testing has been explored in principle. However, in real-world environments, fiber channels are susceptible to interference, and non-ideal visibility effects become particularly pronounced in long-distance transmission. Therefore, it is necessary to elucidate the relationship between HOM interference visibility and the final key rate, and to establish methods for improving visibility.
In this thesis, we introduced the MDI-QKD and analyzed the effect of two-photon temporal distinguishability on the key generation rate of MDI-QKD. Based on this, we proposed a scheme of MDI-QKD with time synchronization to reduce the two-photon temporal distinguishability.

In chapter 2, we introduce the components of QKD systems and common QKD protocols, with a focus on the BB84 protocol. It then emphasizes the photon number splitting (PNS) attack. In response to this attack, QKD protocols, combined with the decoy state method, can achieve secure and efficient key transmission. This lays the groundwork for the subsequent chapters' discussion on practical system implementations.

In chapter 3, we elaborate on the security issues present in practical QKD systems. To meet the security requirements of actual system detectors, researchers have proposed an MDI-QKD system model capable of resisting any detector attacks, emphasizing the advantages of MDI-QKD. Furthermore, several specific encoding schemes for MDI-QKD implementation are introduced. Building on the aforementioned work, we conduct an analysis of the key generation rates for three-intensity decoy-state MDI-QKD with polarization encoding under both infinite key length and finite key length scenarios.

In chapter 4, we first introduced Hong-Ou-Mandel (HOM) interference and the errors in two-photon interference within MDI-QKD. For the implementation of this protocol, the photons generated by the two independent laser sources must be indistinguishable. We calculated the final

key rate of the infinite-sized and finite-sized MDI-QKD to determine the effects of two-photon distinguishability on the visibility of their interference. From this analysis, we derived reasonable ranges for visibility under conditions of both infinite and finite key lengths. Our simulation results show that the acceptable condition of visibility $V = 0.42$ is more stringent for finite-size key generation than the $V = 0.38$ of the infinite-size. We also compared the impacts of different Bell State Measurements (BSMs) across various protocols, concluding that the Beam Splitter + Polarizing Beam Splitter (BS+PBS) type BSM exhibits superior performance. Subsequently, we calculated the coincidence probability for Gaussian photon pulse interference in the HOM setup. Based on the visibility values previously determined, we identified the acceptable range of delays for two-photon pulses within the BSM of MDI-QKD. We conclude that the acceptable time delay is 45.5 ps for 100-ps width and 89.0 ps for 200-ps width. We also estimated an acceptable time delay between two photons from two independent pulse lasers.

In chapter 5, we introduce an enhanced time synchronization scheme for the MDI-QKD protocol to mitigate distinguishability issues in the two-photon interference caused by the time fluctuations in long-distance transmissions. We propose to perform all steps of the synchronous measurement feedback modulation in Charlie's lab, eliminating the need for long-distance feedback and extra clock sources. By minimizing the temporal distinguishability in the two-photon interference, with DL providing the delay compensation, the signals of Alice and Bob are synchronized for the BSM. To implement this scheme, we propose to use an optical frequency comb to generate the reference and signal pulses to be synchronized with each other. We conducted an experiment to validate the feasibility of the proposal. The results prove successful synchronization between the reference and signal pulses. The obtained timing error of ±15 ps meets the calculated acceptable range for pulses with a 150 ps pulse width.

In this study, we provide quantitative criteria for the visibility of two-photon interference and the accuracy of time-delay control, which will play a crucial role in enhancing the performance of practical MDI-QKD systems. Since synchronization is pivotal for achieving high visibility of two-photon interference, we propose an improved method for measuring and controlling the relative time difference between photons emitted from remote sources, aiming to achieve precision in quantitative criteria. Our proposed approach cleverly circumvents the timing distinguishability errors caused by time shifts in long-distance fiber channels. Combining existing mature technologies, it is anticipated to make significant contributions to the practical implementation of QKD protocols. Recently, twin-field quantum key distribution (TF-QKD) employing frequency optical combs to establish mutual coherence has also been proposed, indicating the potential wide application of this technique in future quantum key distribution networks.

Acknowledgements

The experience of pursuing my doctoral degree at Hokkaido University over the past few years has been incredibly memorable and life-changing for me, and it wouldn't have been possible without the support and guidance of many peoples.

First and foremost, I would like to express my deep and sincere gratitude to my supervisor, Prof. Akihisa Tomita, for providing me with the opportunity to conduct research and for offering invaluable guidance throughout the entire research process. He led me into the practical work of quantum communication and taught me the methodology to conduct research. During the most challenging experiments, he personally provided me with guidance and troubleshooting. Additionally, he offered a wealth of valuable suggestions for academic conference presentations and journal submissions. It can be said that without his guidance, the completion of this research would have been impossible. His vision, sincerity, and professional spirit have deeply inspired me. He is the researcher I admire most in the industry and the life mentor I respect the most. Not only has he shown full care in my academic pursuits, but he has also provided tremendous support in my life as an international student. It has been my honor and privilege to spend these years of study under his guidance.

I sincerely express my gratitude to Prof. Atsushi Okamoto for his generous provision of professional guidance and research assistance. His profound suggestions and comments have greatly enhanced the quality and presentation of my research. I genuinely thank Associate Prof. Kazuhisa Ogawa for his guidance and advice during my master's and first year of doctoral studies. His assistance in my field has broadened my research perspectives. I also extend my gratitude to all professors and staff of the Faculty of Information Science and Technology at Hokkaido University for their support and kindness.

I am grateful to all my research colleagues and friends who have consistently encouraged me and provided assistance in many aspects. A special thanks to my senior colleague Dr. Weiyang Zhang for providing invaluable insights into my research work and international student life. Special thanks to Dr. Zeyu Shen, Dr. Shuanglu Zhang, Ms. Jingyan Yang, Ms. Xinruinan Zhang, and Mr. Jianglian Wang. I appreciate their friendship, which has made me feel warmth during my study abroad journey.

I gratefully acknowledge the funding received from the D-Drive research assistance of Hokkaido University which helped me reduce my tuition burden.

I am particularly grateful for the unconditional love and support from my parents, who have supported me financially and emotionally throughout my life. During the pandemic years, I was unable to return to my home country to visit my relatives, leaving regrets, but I have always

cherished all the people who care for me. I want to say that it is their support that has shaped my colorful journey as an international student.

I would like to express my gratitude to everyone who supported me during my time in Japan. Regardless of how far apart we may eventually be, you have all been shining stars in my life, guiding me on my path forward.

May 13, 2024

Graduate School of Information Science and Technology

Hokkaido University

Haobo Ge

Research Achievements

1 Original articles

1.1 Scholarly journal articles

[1] Haobo Ge, Akihisa Tomita, Atsushi Okamoto, and Kazuhisa Ogawa, “Analysis of the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution,”IEEE Trans. on Quantum Eng. 4, pp.1–8 (2023). (IF=2.3)

[2] Haobo Ge, Akihisa Tomita, Atsushi Okamoto, and Kazuhisa Ogawa, “Reduction of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution,” Optics Letters, 49, pp.822-825 (2024). (IF=3.6)

1.2 International conference proceedings

[1] Haobo Ge, Akihisa Tomita, Atsushi Okamoto, and Kazuhisa Ogawa, “Analysis of the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution,” 23rd Asian Quantum Information Science Conference (AQIS2023), Seoul, Korea, August, B40(46), pp.163-165 (2023).

2 Presentation

[1] 葛　皓波, 富田章久, 小川和久, 岡本　淳,“デコイ法を用いた測定装置に依存しない量子鍵配送に対する二光子判別可能性の影響”, 第 41 回量子情報技術研究会 (QIT41), 東京, 2019 年 11 月.

[2] Haobo Ge, Akihisa Tomita, Kazuhisa Ogawa, and Atsuhi Okamoto, “Analysis of the effects of the two-photon distinguishability on decoy state measurement-device-independent quantum key distribution”, EU-USA-Japan International Symposium on Quantum Technology(ISQT2019), Kyoto, November 2019.

[3] 葛　皓波, 富田章久, 小川和久, 岡本　淳,“測定装置に依存しない量子鍵配送に対する二光子時間的判別可能性の影響 ”, 第 45 回量子情報技術研究会 (QIT45), オンライン, 2021 年 11 月.

[4] Haobo Ge, Akihisa Tomita, Atsushi Okamoto, and Kazuhisa Ogawa, “A scheme of reducing the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution,” Quantum Innovation 2023, Tokyo, Japan, PO-CC-04, November 2023.