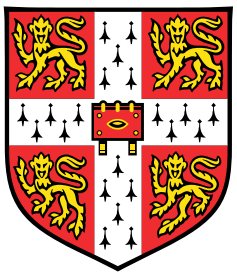
Design of New-generation Quantum Key Distribution Systems for Secure Communication



Anran Jin

Department of Engineering
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Jesus College September 2023

I would like to dedicate this thesis to my teachers and friends.

Declaration

This thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the preface and specified in the text. It is not substantially the same as any work that has already been submitted before for any degree or other qualification except as declared in the preface and specified in the text. It does not exceed the prescribed word limit for the Engineering Degree Committee.

Anran Jin
September 2023

Acknowledgements

I would like to express my sincere gratitude towards my supervisor Prof. Richard Penty, who has always been my firmest supporter throughout my PhD study. I feel deeply indebted of his enormous patience and tolerance, being features I would keep on to in my research career. I would also like to thank Prof. Ian White for guiding me into the field of quantum information. It is my great fortune to start my research life under such a kind gentleman.

I am genuinely grateful to Prof. Xiongfeng Ma and his amazing research group from Tsinghua University. I constantly recall the day when I contacted Prof. Ma for guidance on my research as a naive beginner, and when I found out that he was so approachable and knowledgeable. His insightful ideas, remarkable intuition and academic integrity will be kept as treasures of my life. I enjoyed the collaborations with his students Pei Zeng and Xingjian Zhang, from whom I learned very much both as researchers and friends.

I would like to thank my colleagues in the group for always being able to discuss and provide excellent ideas and feedbacks. They made me a warm home at Cambridge. I cherish the life at Jesus College with such many amazing staff and members. I specially thank Prof. Tim Wilkinson for his generosity and (arguably) good sense of humour which accompanied me ever since I entered Cambridge as an undergraduate.

Finally, I would like to acknowledge the enormous support from my friends, teachers and family during the pandemic time, which consumes half of my PhD stage. Those days were truly a torture for me, suffering from both physical and mental illness. As the world is gradually getting over those painful memories, I would like to say thank you to all of you who have fought.

This PhD project is supported by UK EPSRC Quantum Communications Hub and Cambridge Trust.

Abstract

Quantum information processing relies on the principles of quantum physics to gain unique advantages in various information processing tasks. Among them, the quantum key distribution (QKD) technique guarantees the information-theoretic security of the task of remote secure key distribution. Unlike its classical counterpart, the security of QKD does not rely on the lack of computational power of the current classical computers on one-way functions such as prime factorisation. QKD thus ensures the long-term security even at the presence of quantum computers. Moreover, QKD already enjoys mature deployments with national-wide QKD networks and satellite-assisted free-space QKD links.

The performances of QKD protocols are usually judged from both the theoretical and practical sides. On the theoretical side, a QKD protocol should be secure against any possible attacks from the adversaries, with reliable key rate lower bounds giving high distillable key rate and long allowable distance. On the practical side, a QKD protocol should preferably be deployable under the standard techniques from classical communication. It should also give good performances under non-ideal settings such as device imperfection and finite data size.

The current QKD protocols generally cannot triumph in both theories and practices. For instance, the Bennett-Brassard-1984 (BB84) protocol enjoys comprehensive security analysis valid under the most general attacks and finite data size, yet its single-photon detector is usually costly and requires low-temperature operation. On the other hand, the Grosshans-Grangier-2002 (GG02) protocol uses the standard coherent detection technique, yet its security is still to be completed under practical implementation. The situation is reasonable since realistic systems usually possess infinite uncharacterised dimensions, but theories are mainly effective in low dimensions.

This thesis focuses on the designs of new-generation QKD protocols that are both theoretically sound and practically favourable. Specifically, three potential candidates will be discussed:

- Twin-field QKD covering the longest distances but experimentally demanding
- Discrete-modulated continuous-variable QKD with high practicality but incomplete in security

- Time-bin-encoding continuous-variable QKD with complete security and high practicality

Their advantages and drawbacks will be contrasted from both the theoretical and practical perspectives. Adjustments to each protocol will be proposed to gain new features yielding better practical performances. New theoretical methods will be introduced to account for the complete security of practical QKD protocols. Simulation will be performed under realistic settings illustrating the performances of these new-generation protocols and their distinct enhancements to the performances of standard QKD. The related works in this thesis are believed to point out the directions in search of the next-generation QKD protocols with robust theories and practical high performances.

List of Publications

1. Jin, A., Zeng, P., Penty, R. V., and Ma, X. (2021). Reference-frame-independent design of phase-matching quantum key distribution. Physical Review Applied, 16(3).

2. Gong, Y., Jin, A., Li, H., Wonfor, A., and Penty, R. (2021). Security analysis of continuous-variable quantum key distribution using m-psk classical modulation schemes. In Quantum Information and Measurement, pages W3B–3. Optica Publishing Group.

3. Jin, A., Zhang, X., Jiang, L., Penty, R. V., and Zeng, P. (2023). Pilot-reference-free continuous-variable quantum key distribution with efficient decoy-state analysis. https://arxiv.org/abs/2309.03789. *In submission to Physical Review X Quantum.*

Table of contents

List of figures

List of tables

Chapter 1

Introduction and motivations

This chapter presents a brief overview of the main research object of this thesis, i.e., quantum key distribution (QKD). It will start by introducing the physical principles of QKD, before reviewing its developments up to now, both in theories and experiments. It then explains the motivation of this thesis, that is, to search for the new-generation QKD systems which are sound in both theories and practical performances.

1.1 Quantum key distribution

1.1.1 The quantum nature

Quantum mechanics is by far the most accurate depiction of the Nature in the non-relativistic scope. Quantum mechanics acknowledges the interaction between the measurement probes and the physical systems, which is commonly neglected in Newtonian mechanics (Landau and Lifshitz, 1981). Instead of representing physical quantities such as position and momentum as real numbers, quantum mechanics promotes these quantities to be operators on Hilbert spaces over the complex fields. Therefore in quantum mechanics, physical states are represented as vectors in Hilbert spaces, with the inner product understood as a "measurement". This formalism is to be explained in detail in Chapter. 2.

Representing physical states as vectors in Hilbert spaces, quantum mechanics predicts the existence of non-classical states which are forbidden in Newtonian mechanics. The existence of these non-classical states is identified as the "quantumness", paving the roads to new physical phenomena. Among them the most notorious is the Schrödinger's cat, illustrated in Fig. 1.1 (Yuan et al., 2015). A classical cat in a completely isolated box can be either in the state $|\text{Live}\rangle$ or $|\text{Dead}\rangle$, and a classical observer deterministically distinguishes the live and dead states. The anomaly comes when the two states are superposed, which is feasible

in a Hilbert state, obtaining the non-classical Schrödinger's cat state $(|\text{Live}\rangle + |\text{Dead}\rangle)/\sqrt{2}$. On the Schrödinger's cat state the classical observer, only capable of resolving live or dead, cannot yield deterministic results. This is essentially different from the classical probabilistic process as uncertainty is obtained from a *single* state instead an *ensemble* of states. What is more, after observing the Schrödinger's cat, i.e., opening the box, the state would collapse to the observed result, either the live or dead state, and further observations still yield deterministic results.

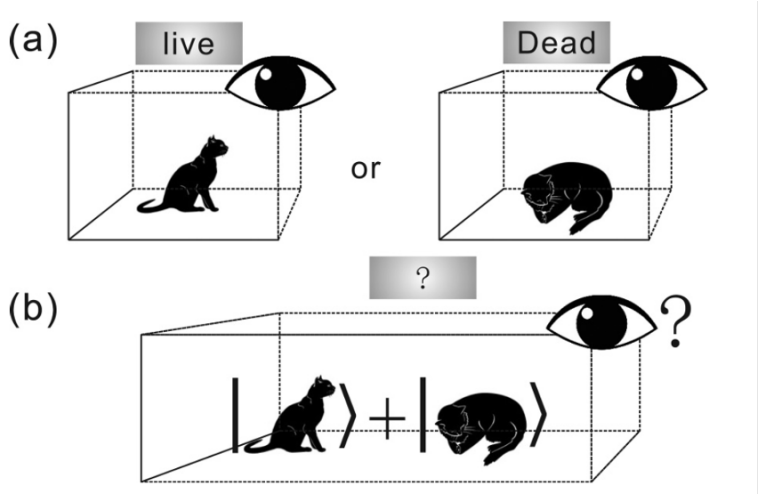


Fig. 1.1 Illustration of the Schrödinger's cat state. The classical observer would yield deterministic results for both the live and dead state, yet not for the Schrödinger's cat state, superposing coherently the live and dead state. Figure retrieved from (Yuan et al., 2015).

The properties of the Schrödinger's cat state can be re-examined from an information-theoretic perspective (Shannon, 1948). Denoting the live state as $|0\rangle$ and the dead state as $|1\rangle$, the Schrödinger's cat state would be represented as $(|0\rangle + |1\rangle)/\sqrt{2}$. The above arguments assert that the Schrödinger's cat state is uncertain in the $\{|0\rangle, |1\rangle\}$ basis, i.e., the Z basis, being eigenstates of the Pauli Z operator. On the contrary, in the $\{|+\rangle, |-\rangle\}$ basis, where $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$, the Schrödinger's cat state is deterministic being orthogonal to $|-\rangle$. This basis is termed the X basis as the eigenstates of the X operator. In fact, not only for the Schrödinger's cat state $|+\rangle$, but all the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are uncertain in either the X or Z basis, and deterministic in the other. This translates to the non-commutativity of the X and Z operators, i.e., $XZ \neq ZX$. This relation is non-classical as in Newtonian mechanics physical observables represented by real numbers are commutative.

1.1.2 QKD protocols

This non-commutativity of the X and Z bases gives rise to a wide possibility of non-classical physical processes, including the quantum key distribution (QKD). QKD is a quantum information processing technique that seeks to distribute identical, random and secrete key bits between two communication parties. The generated secure keys can support secure communications via the one-time pad method (Vernam, 1926).

Notice that the secure key distribution is not possible in classical communications since the distillable key rate is the difference between Alice and Bob's mutual information and Alice and Eve's mutual information (Shannon, 1949), where Alice and Bob are the communication parties and Eve is the eavesdropper. In this case, the ultimate attacking strategy is for Eve to intercept Alice's signals and copy them. Eve keeps the replica and sends the intact signals to Bob, and thus there would be no difference between Eve and Bob's knowledge of Alice's keys, therefore no secure key generated. Currently in the classical communications, security is based on the public-key cryptosystem such as the RSA algorithm (Rivest et al., 1978), which relies on the hard-to-compute one-way functions such as factoring and discrete logarithms. Whilst their classical computational complexity is still not known, the complexity equipped with quantum computational techniques, such as the Shor's algorithm (Shor, 1997), is known to be polynomial. With the rapid developments of quantum computing (Arute et al., 2019; Kim et al., 2023), the security of the current classical communications reveals serious caveats.

The solution to this security crisis lies in the power of quantumness, making use of the non-commutative X and Z bases. In the non-commutative quantum physics, a no-cloning theorem exists stating that one cannot reliably copy an unknown quantum state without disturbing it (Wootters and Zurek, 1982). In fact, if given an unknown state from either the X or Z basis, it would not be possible to yield deterministic results if the observation were made in a different basis, and the original state would be disturbed collapsing to the observation basis. This property of the quantum states enables us to create difference between Eve and Bob's knowledge on Alice's key bits, provided that Alice and Bob share the same basis whilst Eve chooses the other, thus generating genuinely secure key bits.

The idea above can be formulated further, arriving at the famous BB84 QKD protocol (Bennett and Brassard, 1984) utilising the non-commutativity of the X and Z bases. Protocol 1 below specifies the essential steps of the ideal BB84 protocol, assuming perfect single-photon sources and detectors are used. In practice, phase-randomised weak coherent sources are used in place of perfect single-photon sources (Gottesman et al., 2004). Fig. 1.2 below illustrates the setups of the polarisation-encoding BB84.

Protocol 1 ***Ideal BB84 protocol with single-photon sources and detectors***

1. ***State preparation****: For each round, Alice draws a random key bit. She chooses randomly the Z or X basis and prepares according to the random key bit and basis one of the four states* $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$*. She sends the state to Bob through an authenticated channel.*

2. ***Detection****: For each round, Bob draws a random basis Z or X, and measures the incoming signal under that basis. He records the basis choice and measurement result and acknowledges to Alice his reception. They repeat this quantum communication for sufficiently many rounds.*

3. ***Basis sifting****: After the quantum communications, Alice and Bob announce their basis choice of each round. They keep only the rounds with the same basis choices and discard the mismatched rounds.*

4. ***Information reconciliation****: For the rounds where they both selected Z basis, they sample a small portion and count the error rate. This is termed as the bit error rate. If the bit error rate is below a preset threshold, they perform information reconciliation to ensure they hold the same bit string. They otherwise abort the protocol.*

5. ***Privacy amplification****: For the rounds where they both selected X basis, they also sample and count the error rate. This is the phase error rate, related to privacy leakage. If the phase error rate is below a preset threshold, they perform hashing on the reconciled key bit strings according to the phase error rate. This is to ensure the key bits are secret. They otherwise abort the protocol.*

Up to now, BB84 is still one of the most practical QKD protocols due to its simplicity and high performances (Yuan et al., 2018; Grünenfelder et al., 2020; Li et al., 2023). The BB84-type protocols are usually termed the discrete-variable (DV) QKD protocols, due to the discrete spectra of the X and Z operators. In a standard DV QKD protocol, discrete key symbols are encoded and usually single-photon detectors are used for signal detection.

In quantum mechanics however, the X and Z operators are not the only two non-commutative observables. In fact, there exists a more well-known pair, the position operator $\hat{q}$ and the momentum operator $\hat{p}$, with the canonical quantization relation $[\hat{q}, \hat{p}] = i$ lying at the essence of quantum mechanics and quantum field theory. The spectra of the position and momentum operators are continuous, with each eigenstate concentrating at the corresponding position or momentum. A natural analogy with the BB84 protocol would be to basis-switch between $\hat{q}$ and $\hat{p}$ eigenstates. While this indeed yields a valid protocol (Gottesman and

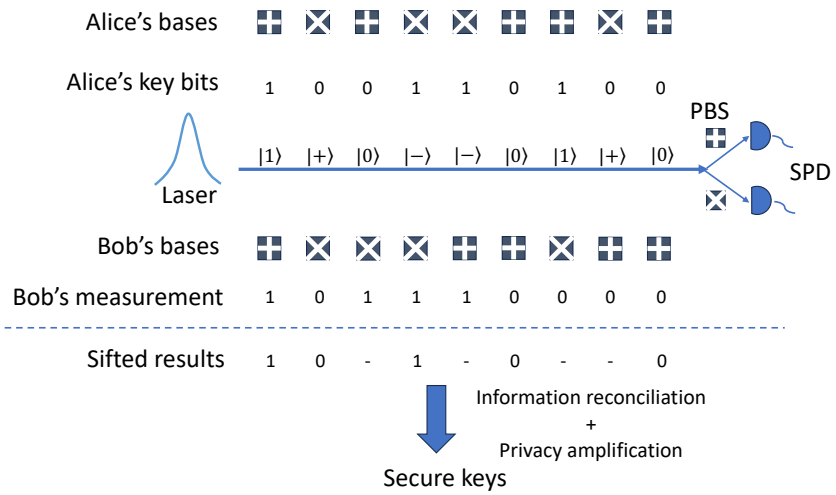


Fig. 1.2 Schematic diagram of the BB84 protocol encoding on photon polarisation. Alice chooses random bases either rectilinear (+) or diagonal (×), and encodes her key bits under the selected bases. Bob measures the received states based on random bases through a polarisation beam splitter (PBS) followed by two single-photon detectors (SPD). The final sifted keys are to be privacy-amplified to yield the secure keys.

Preskill, 2001), the position and momentum eigenstates, termed the squeezed states, are generally difficult to realise in practice.

A more practical choice would be the eigenstates of the annihilation operator $\hat{a} = (\hat{q} + i\hat{p})/\sqrt{2}$, i.e., the coherent states:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \alpha \in \mathbb{C}. \tag{1.1}$$

The coherent states are the standard carriers in classical optical communications, and the corresponding coherent detectors, homodyne and heterodyne detectors, are also prevailing in classical communications. Notice that the coherent states are non-orthogonal, forming an over-complete basis of the optical field. Therefore, even Bob cannot yield deterministic results from the measurements of coherent states, but Gaussian-distributed results with a minimal variance termed the shot noise. However, since Eve's extracting information would add to the shot noise of the coherent states, Alice and Bob can compare the variance between their key data and capture Eve's attack if the variance increase is too high. This leads to the GG02 protocol (Grosshans and Grangier, 2002) illustrated below, with homodyne detector and reverse reconciliation, i.e., Alice correcting to Bob's key string. The reverse reconciliation

would extend the key-transmittance performance over the 3 dB limit (Grosshans and Grangier, 2002; Grosshans et al., 2003).

Protocol 2 ***GG02 protocol with homodyne detector and reverse reconciliation***

1. ***State preparation****: For each round, Alice draws a random complex number α from the complex Gaussian distribution $\mathcal{N}_{\mathbb{C}}(0,V_0)$. She sends the coherent state $|\alpha\rangle$ to Bob through an authenticated channel. She also transmits a strong classical pulse serving as the phase reference of the signals, i.e., the local oscillator (LO).*

2. ***Detection****: For each round, Bob measures randomly the $\hat{q}$ or $\hat{p}$ quadrature using homodyne detector with the received LO, obtaining a real-valued key. He notifies Alice his choice of quadrature and Alice keeps the corresponding quadrature data. They repeat this quantum communication for sufficiently many rounds.*

3. ***Reverse information reconciliation****: They sample a small portion of rounds and compare their keys. They attempt to perform reverse reconciliation with Bob sending Alice the syndrome and Alice correcting her key string. In practice, this is usually done by discretising the continuous-valued keys and perform multi-dimensional reconciliation (Leverrier et al., 2008). If the error rate is too high they abort the protocol.*

4. ***Privacy amplification****: According to the key statistics, usually the variance, they calculate the distillable key rate and hash the reconcile key string to obtain the final secure keys.*

Notice that in the GG02 protocol, the keys and detection results are continuous-valued, in clear contrast with BB84. This kind of QKD protocols are termed the continuous-variable (CV) QKD, with usually coherent-state source and homodyne or heterodyne detector. The contrasts and relations between DV and CV QKD will be the main theme of this thesis.

1.1.3 Developments of DV and CV QKD

Commencing from the contrasting BB84 and GG02 protocols, DV and CV QKD have undergone two different roads of developments. Theoretically, DV QKD is generally more robust than CV QKD due to its simplicity. Lo and Chau (1999) proved the security of the entanglement-based DV QKD based on quantum error correction, which is reduced to the above prepare-and-measure BB84 protocol by Shor and Preskill (2000), employing the idea of the Calderbank-Shor-Steane (CSS) quantum error correcting code (Calderbank and Shor, 1996; Steane, 1996). The CSS code reduces to hashing when correcting phase errors, thus

removing the need for quantum computers. Koashi (2009) further removes the need for the specific CSS code by identifying the complementarity between the X and Z basis, providing a generic and simple framework of DV QKD security proofs. This line of logic will be exploited in Chapter. 3. The DV security proof is made further practical by introducing the decoy-state method (Hwang, 2003; Wang, 2005; Lo et al., 2005), tackling the source imperfection. Further works on the finite-size analysis (Scarani and Renner, 2008; Tomamichel et al., 2012), including the finite-size effect on the parameter estimation (Fung et al., 2010; Xu et al., 2014; Zhang et al., 2017), all render the DV security more comprehensive.

The security proof of CV QKD relies on the information-theoretic approach, where Devetak and Winter (2005) establish the general framework of distilling entanglements from bipartite quantum states under collective attacks, i.e., Eve's operation is independent and identically distributed (i.i.d.) of each round. Notice that the DV security is proved under the most general coherent attack regime, where Eve can keep in a quantum memory the states from each round and perform joint measurements in the end. The constraint of collective attack is partially removed using the quantum de Finetti theorem (Renner, 2007) and the uncertainty principle of the smooth entropy (Tomamichel and Renner, 2011), yet the dimension of the quantum system is assumed to be finite whilst a CV system has infinite dimension. For the specific Gaussian-modulated GG02 protocol, the CV security can be proved under coherent attack with finite data size (Leverrier, 2017) since the optimal attack from Eve is again Gaussian operations (Navascués et al., 2006; García-Patrón and Cerf, 2006). However in practice, continuous modulation is never possible and approximated by large discrete constellations. This imperfection invalidates the Gaussian-optimality proof, and the current proofs only accounts for the asymptotic regime under collective attack (Kaur et al., 2021). Another remarkable security loophole of CV QKD is the transmission of the local oscillator (LO), which can be manipulated by Eve to tamper the key rate (Ma et al., 2013, 2014). The CV security is thus less complete than the DV security from a practical perspective.

On the other hand, CV QKD has its own potential in practical implementation. Unlike the dedicated single-photon detectors used in DV QKD, the homodyne and heterodyne detectors in CV QKD are believed to be more cost-effective and can operate at room temperature. The spatio-temporal filtering of the local oscillators (LO) can exclude the scattering from other coexisting signals thus allowing dense wavelength-division multiplexing (DWDM) with intense classical channels (Qi et al., 2010; Kumar et al., 2015; Eriksson et al., 2019), and the high quantum efficiency gives CV QKD potential high key rates in the metropolitan distances (Wang et al., 2018a, 2020, 2022a). Although DV modulation is experimentally simpler than CV modulation, the discrete-modulated (DM) CV QKD (Zhao et al., 2009) has been proposed to simplify the Gaussian modulation with sound asymptotic collective security

proofs (Lin et al., 2019; Ghorai et al., 2019). On the key rate-distance side, CV QKD usually has higher key rate at shorter distances due to the higher efficiency of the coherent detectors, but DV QKD usually reaches longer distances since the coherent detector has an intrinsic shot-noise error whilst the single-photon detector is relatively accurate.

1.2 Motivation and outline

The last section clarified the trade-offs between DV and CV QKD. They are summarised in Table 1.1 below. Notice that these features are speaking for the standard BB84 and GG02 protocols, and during the last decade remarkably many new protocols have been proposed aiming at improving the theoretical and practical performances of QKD. This thesis is devoted to this aim, i.e., the searching of new-generation QKD protocols that are both sound in theories and robust in practical performances. This thesis will be focusing on the hybrid DV-CV features, attempting to combine the merits of both DV and CV QKD. Specifically, since in general the DV security techniques are more robust, whilst the CV implementation is more practical, it is tempting to give CV protocols DV-like security proofs in hope of extending the distance of CV QKD whilst keeping its high metropolitan key rate. In light of this goal, Three types of novel QKD protocols will be examined possessing both DV and CV features:

1. Twin-field (TF) QKD: coherent source with field interference and single-photon detectors

2. Discrete-modulated (DM) CV QKD: Discrete constellation with coherent detectors

3. Time-bin CV QKD: Two-mode time-bin encoding (discrete) with coherent detectors

This thesis is arranged as the following. Chapter 2 will be introducing briefly the mathematical backgrounds of quantum information, in order to regularise the conventions in this thesis. Chapter 3 will be reviewing the security proof of QKD, especially the complementarity approach by Koashi (2009), including the author's own work extending it from binary dimension to arbitrary prime-power dimensions (Jin et al., 2021).

In Chapter 4-6, the three types of state-of-the-art QKD protocols listed above will be studied. Chapter 4 examines the Twin-field (TF) QKD (Lucamarini et al., 2018) using coherent source with field interference and single-photon detectors. This type of QKD breaks the long-believed linear key rate-transmittance upper bound (Takeoka et al., 2014; Pirandola et al., 2017) by invoking the entanglement of vacuum and single photon, i.e., the entanglement with one particle instead of a pair of them. The TF QKD possesses by far the

	Pros	Cons
DV QKD	Long distance; Mature security analysis (source defection, coherent attack and finite size); Simple modulation	Dedicated single-photon detector; Low detector efficiency leading to low metropolitan key rate
CV QKD	Cost-effective; Room temperature operation; Filtering of LO enables dense wavelength-division multiplexing; High metropolitan-distance key rate.	Short distance; Incomplete and complicated security analysis; Complicated modulation

Table 1.1 Pros and cons of DV and CV QKD from both theoretical and experimental point of views. Generally DV QKD is more robust in theories, yet CV QKD is more practical to be implemented. A detailed discussion is placed in Sec. 1.1.3

.

best theoretical performance of QKD protocols, with key rate decaying only with the square root of the channel transmittance. Its experimental demonstrations (Minder et al., 2019; Fang et al., 2020; Pittaluga et al., 2021; Chen et al., 2021; Wang et al., 2022b; Chen et al., 2022; Liu et al., 2023) are also remarkable reaching over 511 km in field trials (Chen et al., 2021) and over 1000 km in laboratory (Liu et al., 2023). This thesis will mainly be looking at one of the variants of TF QKD, namely the phase-matching (PM) QKD (Ma et al., 2018; Zeng et al., 2020), which removes certain security assumptions in the original TF QKD analysis. In particular, the author introduces the reference-frame-independent (RFI) design of PM QKD with high-dimensional key encoding space (Jin et al., 2021). With the key phases spanning the unit circle, any fixed reference difference would be recorded as a fixed shift between Alice and Bob's raw keys, without tampering the key information. The RFI design removes the need for phase reference calibration, which is one of the key limitations in TF-type QKD implementations.

Chapter 5 looks at the discrete-modulated CV QKD with discrete constellations and coherent detectors. The DM CV QKD is promising for practical implementation due to its simplicity and the recent advance in its numerical key rate calculation (Coles et al., 2016; Winick et al., 2018). The author and his collaborators calculate the key rate of an arbitrary m-phase-shift-keying (m-PSK) DM CV QKD (Gong et al., 2021), and find that an 8-PSK protocol can reach further than 200 km with high key rate.

Chapter 6 introduces the time-bin-encoded CV QKD as in (Primaatmaja et al., 2022; Jin et al., 2023). The protocol encodes the key bit onto the relative intensities of two optical modes, and detects with phase-randomised homodyne detectors. The need for a common phase reference is thus removed, simplifying the experimental setup and closing the LO-

attack security loophole. Moreover, in (Jin et al., 2023), the author manages to prove the security of this CV-type protocol with the DV complementary method with a tagging-based key rate formula (Gottesman et al., 2004). This allows components with ill phase error rate to be discarded, improving the aggregate key rate. The author also provides an efficient decoy-state method for this CV protocol, which is another first-of-the-kind contribution. The thesis concludes in Chapter 7 with outlooks in further improving the performances and the practicality of QKD.

1.3 Novelty of this thesis

As is explained in the last section, the main text of this thesis is based on the three works of the author (Jin et al., 2021; Gong et al., 2021; Jin et al., 2023), with due collaborators (see the footnotes at the beginning of Section 4.4, 5.3, and 6.2). The novelty in these works are summarised as the following:

- Nontrivial extension of the phase-error-based QKD security proof with binary key space to arbitrary prime-power key space. See Section 3.1.
- Reference-frame-independent design of PM QKD, immune to any fixed misalignment, removing the needs for phase-reference calibration. See Section 4.4.
- Numerical calculation of the key rate of the m-PSK DM CV QKD, illustrating the promise of the 8-PSK protocol. See Section 5.3.
- Design of a novel time-bin-encoded CV QKD, removing the needs for phase reference thus simplifying the implementation and closing the LO security loopholes. See Section 6.2.
- Proving the security of the time-bin CV QKD using DV phase-error method. Applying the tagging technique from DV to a CV protocol. Providing an efficient decoy method for a CV protocol. See Section 6.2.

Chapter 2

Preliminaries and backgrounds

This chapter briefly reviews the mathematical formalism of quantum information. The discussion is divided into DV and CV systems, where DV quantum information stands upon the finite dimensional Hilbert space of a physical system such as polarisation and spin, and CV quantum information is upon the $\mathscr{L}^2(\mathbb{R}^3)$ state space of a harmonic oscillator. This chapter will review the representation of quantum states, observables, measurements and channels. Specifically, it will review the important CV Gaussian quantum information related to Gaussian states and Gaussian channels. It will review the quantum entropy as a counterpart of Shannon's classical entropy. See (Nielsen and Chuang, 2010; Wilde, 2011; Weedbrook et al., 2012) for more comprehensive reviews of quantum information theory.

2.1 DV quantum information theory

In quantum mechanics, states are represented by vectors in a Hilbert space $\mathscr{H}$ on the complex field $\mathbb{C}$ (Sakurai and Napolitano, 2020). A reasonable physical states are normalised with respect to the inner product, and the inner product between two different states depicts a projective measurement which will be explained later in this section. Notice the Dirac's bra-ket notation where $|\psi\rangle$ represents a state in $\mathscr{H}$ and $\langle\phi|$ represents a dual state. Their inner product is denoted by $\langle\phi|\psi\rangle$.

Just like the classical information theory building upon bits, the DV quantum information theory is upon "qubits" as states in a two-dimensional Hilbert space. Identifying the vectors inside with $\mathbb{C}^2$, the computational basis $\{|0\rangle, |1\rangle\}$ is defined as

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.1}$$

A qubit state $|\psi\rangle$ takes the form of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \in \mathbb{C}$. A physical state is required to be normalised, thus $|\alpha|^2 + |\beta|^2 = 1$. Furthermore, the "qudit" states can be defined being vectors within a d-dimensional Hilbert space. The corresponding computational basis $\{|i\rangle\}_{i=0}^{d-1}$ are accordingly the orthonormal coordinate vector basis. A qudit state takes the form

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle, \tag{2.2}$$

with normalisation condition $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$.

The composite system $\mathscr{H}_{AB}$ of two subsystems $\mathscr{H}_A$ and $\mathscr{H}_B$ is represented by the tensor product, i.e., $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$. The computational basis of $\mathscr{H}_{AB}$ is usually denoted as

$$|ij\rangle_{AB} := |i\rangle_A \otimes |j\rangle_B, \quad i = 0, \cdots, d_A - 1, j = 0, \cdots, d_B - 1, \tag{2.3}$$

where $\mathscr{H}_A$ and $\mathscr{H}_B$ take the computational bases $\{|i\rangle\}_{i=0}^{d_A-1}$ and $\{|i\rangle\}_{i=0}^{d_B-1}$ respectively.

The processes a quantum state can undergo can be categorised as evolution and measurements. Evolution identifies the quantum state changing coherently with time, with no information leakage to the environment. An evolution is represented by a unitary operator U on the Hilbert space, that is to say,

$$U^\dagger U = U U^\dagger = I, \tag{2.4}$$

where $(\cdot)^\dagger$ represents the operator adjoint and I is the identity operator. An evolution is usually termed a quantum gate in the quantum circuit, and is usually depicted as

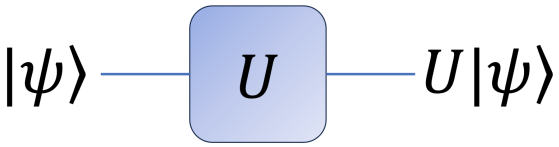


Fig. 2.1 The quantum circuit diagram representing the unitary evolution U on the state $|\psi\rangle$. The evolution is termed the U-gate.

Since unitary operators preserve the inner product, i.e., $\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1$, and hence the evolution maps a physical state to a physical state. It is sometimes useful to represent the unitary operators as unitary matrices in $\mathscr{U}(d;\mathbb{C})$ for qudit states. Some examples of unitary evolution are

- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, the quantum NOT gate flipping $|0\rangle$ and $|1\rangle$.

- $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1, \end{bmatrix}$, the quantum NOT gate flipping $|+\rangle$ and $|-\rangle$.
- $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, the Hadamard gate mapping the Z-basis $\{|0\rangle, |1\rangle\}$ to the X-basis $\{|+\rangle, |-\rangle\}$.
- The controlled unitary. For a unitary U on system B, a controlled U gate, or a $C-U$ gate, is the operator on the composite system between B and a control qubit system A. In specific, $C-U_{AB} = |0\rangle_A\langle 0| \otimes I_B + |1\rangle_A\langle 1| \otimes U_B$. This is equivalent to first measure the control qubit system A in the computational basis. If the result is 0 the gate does nothing to the system B, and if the result is 1 the unitary U is applied to B. The qubit system A can definitely be promoted to a qudit system given a set of unitaries $\{U_i\}_{i=0}^{d-1}$ with $U_0 = I$. The qudit-controlled unitary is defined as

$$C_d - U_{AB} = \sum_{i=0}^{d-1} |i\rangle_A\langle i| \otimes (U_i)_B. \tag{2.5}$$

  A control-U gate is depicted as

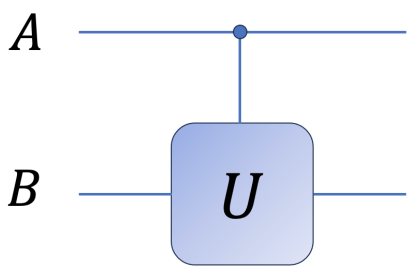


Fig. 2.2 The quantum circuit diagram representing the controlled unitary operation. System A is a qubit system. The gate measures system A in the computational basis and applies the unitary U to system B if the result is 1 and do nothing if the result is 0.

The second type of processes that a quantum state can undergo is the measurement, identifying the interaction between the quantum system and the classical measurement probe. A measurement is represented by an observable O, being an Hermitian operator on the Hilbert space, i.e., $O^\dagger = O$. This is equivalent to requiring the eigenvalues of O to be real numbers. The Hermitian observable O is the physical quantities in quantum mechanics, being operators rather than real numbers as in classical physics. An observable on a qudit system takes a

spectrum decomposition:

$$O = \sum_{i=0}^{d-1} \lambda_i |\psi_i\rangle\langle\psi_i|. \tag{2.6}$$

Since the eigenvalues λ_i are all real numbers, an observable O can be interpreted as a physical quantity that can take values in the λ_i's, and the actual value taken is to be determined by the measurement of the observable on the quantum state.

We define the projective measurement formalism. The measurement is a non-deterministic process. For a quantum state $|\psi\rangle$, the measurement of the observable O yields a probability distribution where the probability of getting λ_i as the outcome is

$$\Pr(i) = \langle\psi|\psi_i\rangle\langle\psi_i|\psi\rangle = |\langle\psi|\psi_i\rangle|^2. \tag{2.7}$$

When observing λ_i as the outcome, the quantum state $|\psi\rangle$ collapses to the i-th eigenspace as

$$|\psi_i'\rangle = \frac{\langle\psi_i|\psi\rangle}{|\langle\psi_i|\psi\rangle|}|\psi_i\rangle. \tag{2.8}$$

Sometimes when the measurement outcome λ_i's are not of interest, a measurement can be written according to its projector basis $\{|\psi_i\rangle\}_{i=0}^{d-1}$. A measurement is depicted as the following in a quantum circuit:

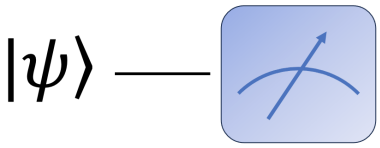


Fig. 2.3 The quantum circuit diagram representing a measurement. It is usually placed at the end of the circuit when quantum information is extracted to classical information.

The prevalent measurement observables in this thesis are represented by the Pauli matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.9}$$

In the bra-ket notation they take the forms of

$$X = |+\rangle\langle+| - |-\rangle\langle-|, \quad Y = |+i\rangle\langle+i| - |-i\rangle\langle-i|, \quad Z = |0\rangle\langle0| - |1\rangle\langle1|, \tag{2.10}$$

where $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$. These observables explain the so-called $Z(X)$-measurement, being measurements distinguishing between $|0\rangle$ and $|1\rangle$ ($|+\rangle$ and $|-\rangle$). The Y-measurement thus distinguishes between $|+i\rangle$ and $|-i\rangle$.

The above discussions reviewed the quantum information on closed quantum systems. Frequently, only one of the many subsystems of a closed composite system is in hold. For example, if the box containing the Schrödinger's cat is not perfectly isolated, information regarding the live-or-death of the cat will be leaked to the outside environment, rendering the Schrödinger's cat not in a closed superposition state, but entangled with the environment as a subsystem of the composite system between the cat and the environment. This is the process of decoherence, explaining why quantumness is hardly observed within daily scope. Since one subsystem does not provide the full information of the whole system, the open quantum state on the subsystem has uncertainty, and is represented as a density operator

$$\rho_A = \sum_i p_i |\psi_i\rangle_A \langle\psi_i|, \tag{2.11}$$

where $\{|\psi_i\rangle\}_i$ are the possible states that the subsystem can be in, but they are distributed according to the probability distribution $\{p_i\}_i$. From the form of Eq. (2.11), it is clear that the density operators are positive semi-definite and unit-traced.

The process of purification can be done to take a mixed ensemble ρ_A to an entangled pure state $|\Psi\rangle_{AE}$ with

$$|\Psi\rangle_{AE} = \sum_i \sqrt{p_i} |\psi_i\rangle_A \otimes |i\rangle_E, \tag{2.12}$$

where $\{|i\rangle_E\}$ is an orthonormal basis on the environment E. When reducing a composite system to its subsystem, the partial trace operation can be invoked to trace out the unwanted subsystems. The pratial trace operation is linear with $\mathrm{Tr}_B(|ij\rangle_{AB}\langle ij|) = |i\rangle_A\langle i|$ on the computational basis. It is clear that

$$\mathrm{Tr}_E(|\Psi\rangle_{AE}\langle\Psi|) = \rho_A. \tag{2.13}$$

To describe the evolution and measurements on the open quantum system, define the quantum channel formalism as a linear map between density operators. Denote the space of density operators on a Hilbert space $\mathscr{H}$ as $\mathscr{D}(\mathscr{H})$. A quantum channel from system A to B is a linear map $\mathscr{N}^{A\to B} : \mathscr{D}(\mathscr{H}_A) \to \mathscr{D}(\mathscr{H}_B)$ that satisfies:

1. Completely positive (CP): $I_R \otimes \mathscr{N}$ is a positive map for a reference system R of arbitrary size. I_R denotes the identity map on $\mathscr{D}(\mathscr{H}_R)$ and a positive map maps any positive semi-definite operators to positive semi-definite operators.

2. Trace preserving (TP): $\mathrm{Tr}\left\{\mathscr{N}^{A\to B}(\rho_A)\right\} = 1$ if $\mathrm{Tr}\{\rho_A\} = 1$, i.e., a quantum channel maps density operators to density operators.

A quantum channel takes the Kraus representation, where

$$\mathscr{N}^{A\to B}(\rho_A) = \sum_l K_l \rho_A K_l^\dagger, \tag{2.14}$$

where $\{K_l\}$ is a set of linear operators from $\mathscr{H}_A$ to $\mathscr{H}_B$, and

$$\sum_l K_l^\dagger K_l = I_A. \tag{2.15}$$

An important example is the quantum measurement channel, describing a general measurement on an open quantum system A. Given a group of linear operator $\{M_l\}$ from $\mathscr{H}_A$ to $\mathscr{H}_B$ satisfying

$$\sum_l M_l^\dagger M_l = I_A, \tag{2.16}$$

a quantum measurement $\mathscr{M}^{A\to C}$ has Kraus representation

$$\begin{aligned}\mathscr{M}^{A\to C}(\rho_A) &= \sum_l (M_l \otimes |l\rangle_C\langle l|)\rho_A (M_l \otimes |l\rangle_C\langle l|)^\dagger \\ &= \sum_l M_l \rho_A M_l^\dagger \otimes |l\rangle_C\langle l|,\end{aligned} \tag{2.17}$$

where the system C is a classical register storing the measurement result l, with $\{|l\rangle\}$ being orthonormal. Tracing out system C, it can be seen that the measurement channel takes ρ_A to $M_l\rho_A M_l^\dagger/\mathrm{Tr}\{M_l\rho_A M_l^\dagger\}$ with probability $\Pr(l) = \mathrm{Tr}\{\rho_A M_l^\dagger M_l\}$. When $M_l = |\psi_l\rangle\langle\psi_l|$ for an orthonormal basis $\{|\psi_l\rangle\}$, the above quantum measurement channel reduces to the projective measurement setup.

In many circumstances, the outcome states after the measurement are not of interest, but only the outcome probability. Defining

$$E_l = M_l^\dagger M_l, \tag{2.18}$$

the outcome probability is then $\Pr(l) = \mathrm{Tr}\{\rho_A E_l\}$. This is the positive operator-valued measurement (POVM) formalism, with E_l being positive semi-definite and $\sum_l E_l = I_A$.

2.2 CV quantum information theory

This section reviews the CV quantum information theory. See (Weedbrook et al., 2012; Sanchez, 2007) for more comprehensive reviews. Whilst the DV quantum information is based on the finite-dimensional Hilbert space, the CV quantum information is based on the infinite-dimensional Hilbert space with continuous eigenspectra. Specifically, a CV system is represented by the bosonic mode, being the quantised radiation mode of the electromagnetic field. The Hilbert space of a CV system is the eigenspace of the harmonic oscillator, with the corresponding creation and annihilation operators $a^\dagger$ and a, and the canonical quantisation identity:

$$[\hat{a}, \hat{a}^\dagger] = 1. \tag{2.19}$$

An orthonormal basis of the CV quantum system is the Fock basis $\{|n\rangle\}_{n=0}^{\infty}$, corresponding to the number of photons in the optical mode. The Fock states are the eigenstates of the photon number operator $\hat{a}^\dagger\hat{a}$, with relations:

$$\begin{aligned} &\hat{a}|0\rangle = 0 \quad \hat{a}|n\rangle = \sqrt{n}|n-1\rangle \ (n \geq 1) \\ &\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \end{aligned} \tag{2.20}$$

The eigenstates of the annihilation operator are the coherent states $|\alpha\rangle$ for $\alpha \in \mathbb{C}$, where

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{2.21}$$

The coherent state $|\alpha\rangle$ takes a Fock basis decomposition as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{2.22}$$

The position and momentum quadrature operators $\hat{q}$ and $\hat{p}$ are defined as:

$$\begin{aligned} \hat{q} &:= \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}) \\ \hat{p} &:= \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}), \end{aligned} \tag{2.23}$$

with canonical quantisation relation $[\hat{q}, \hat{p}] = i$. The position and momentum operators $\hat{q}$ and $\hat{p}$ have eigenstates $|q\rangle$ and $|p\rangle$ for $q, p \in \mathbb{R}$,

$$\hat{q}|q\rangle = q|q\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \tag{2.24}$$

with normalisation identities

$$\langle p'|p\rangle = \delta(p'-p), \quad \langle q'|q\rangle = \delta(q'-q), \quad \langle q|p\rangle = \frac{1}{\sqrt{2\pi}} e^{iqp}, \tag{2.25}$$

with $\delta(\cdot)$ being the Dirac delta function.

The operations on a CV quantum state still follow the DV formalism introduced in the last section, inheriting the ideas of density operators and quantum channels. However it is impossible to represent a CV density operator as a finite-dimensional matrix as in the DV theory. The CV density operator is usually represented by a characteristic complex-valued multivariate function, termed the Wigner function. For a CV state on N bosonic modes, group the quadrature operators together to form a $2N$-vector operator

$$\hat{r} = (\hat{r}_1, \cdots, \hat{r}_{2N})^T = (\hat{q}_1, \hat{p}_1, \cdots, \hat{q}_N, \hat{p}_N)^T. \tag{2.26}$$

The canonical commutation relations can be written compactly as

$$[\hat{r}_j, \hat{r}_k] = i\Omega_{jk}, \tag{2.27}$$

where the symplectic form Ω is the $2N \times 2N$ matrix

$$\Omega := \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2.28}$$

Define the Weyl operator as

$$D_\xi := \exp\left(-i\xi^T \Omega \hat{r}\right), \tag{2.29}$$

for $\xi \in \mathbb{R}^{2N}$. The characteristic function of a CV density operator ρ is

$$\chi_\rho(\xi) = \mathrm{Tr}\{\rho D_\xi\}. \tag{2.30}$$

This transform is one-to-one with the inverse transform

$$\rho = \frac{1}{(2\pi)^N} \int d^{2N}\xi \ \chi_\rho(-\xi) D_\xi. \tag{2.31}$$

The quasi-probability distribution Wigner function is defined as the symplectic Fourier transform of the characteristic function

$$W(\zeta) = \frac{1}{(2\pi)^{2N}} \int d^{2N}\xi \; e^{i\zeta^T \Omega \xi} \chi_\rho(\xi). \tag{2.32}$$

An important class of CV states is the Gaussian states, with Gaussian characteristic function and Wigner function. For a general CV state, define the displacement vector $d \in \mathbb{R}^{2N}$

$$d := \mathrm{Tr}\{\rho \hat{r}\}, \tag{2.33}$$

and the covariance matrix γ

$$\gamma_{jk} := \mathrm{Tr}\left\{\rho\{(\hat{r}_j - d_j), (\hat{r}_k - d_k)\}\right\}, \tag{2.34}$$

where the inner $\{\}$ denotes the anti-commutator. A Gaussian state has characteristic function

$$\chi_\rho(\xi) = \exp\left(-\frac{1}{4}\xi^T \Gamma \xi + iD^T \xi\right), \tag{2.35}$$

where $D = \Omega d$ and $\Gamma = \Omega\gamma\Omega$. The Wigner function of the Gaussian state is

$$W(r) = \frac{1}{\pi^N \sqrt{\det\gamma}} \exp\left(-(r-d)^T \gamma^{-1} (r-d)\right). \tag{2.36}$$

A physical Gaussian state necessarily and sufficiently satisfies canonical commutation relation $\gamma + i\Omega \geq 0$. For general states this condition is necessary but not sufficient. The sub-states of a multi-mode Gaussian state are still Gaussian. Their displacement vectors and covariance matrices can be obtained as the entries corresponding to the due subsystems.

A Gaussian channel is a quantum channel that brings Gaussian states to Gaussian states. The action of a Gaussian channel over a Gaussian state is represented by

$$d_{out} = T d_{in} + l, \quad \gamma_{out} = T\gamma_{in}T^T + V, \tag{2.37}$$

with $l \in \mathbb{R}^{2N}$ and T, V being $2N \times 2N$ real matrices and $V = V^T$. A Gaussian channel is completely positive in the sense that

$$V + i\Omega - iT\Omega T^T \geq 0. \tag{2.38}$$

Below are some useful examples of Gaussian states and Gaussian channels:

1. **Coherent states:** A coherent state $|\alpha\rangle$ is a Gaussian state with displacement vector $d = [\sqrt{2}\mathrm{Re}(\alpha), \sqrt{2}\mathrm{Im}(\alpha)]^T$ and covariance matrix $\gamma = I$, where Re and Im represent the real and imaginary part of a complex number respectively.

2. **Thermal state:** The thermal state has null mean and covariance matrix $\gamma = (2\bar{n}+1)I$, where $\bar{n}$ is its mean photon number. The thermal state has a Fock basis decomposition

$$\rho_{TH} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n|. \tag{2.39}$$

3. **Phase rotation:** A phase rotation on Gaussian states can be represented as a two-dimensional rotation matrix with $d_{out} = R(\theta)d_{in}$ and

$$R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}. \tag{2.40}$$

4. **Beam splitter:** A beam splitter of transmittance T interferes two incoming modes and splits them in a T-by-$(1-T)$ portion. It is represented by

$$\begin{bmatrix} d_1 \\ d_2 \end{bmatrix}_{out} = \begin{bmatrix} \sqrt{T}I & \sqrt{1-T}I \\ -\sqrt{1-T}I & \sqrt{T}I \end{bmatrix} \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}_{in} \tag{2.41}$$

5. **One-mode squeezing and squeezed states:** A one-mode squeezing operation distributes unevenly the uncertainty on the q and p quadratures. It is represented by $d_{out} = S(r)d_{in}$ where

$$S(r) = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix}. \tag{2.42}$$

   Applying the squeezing operation to the coherent states gives the squeezed state with covariance matrix

$$\gamma_s = \begin{bmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{bmatrix}. \tag{2.43}$$

   When $r \to \pm\infty$, the q and p-quadrature eigenstates are obtained respectively.

6. **Two-mode squeezing and EPR state:** The two-mode squeezing generates pairs of photons in two modes. It is represented by $d_{out} = S_2(r)d_{in}$ where

$$S_2(r) = \begin{bmatrix} \cosh rI & \sinh rZ \\ -\sinh rZ & \cosh rI \end{bmatrix}, \tag{2.44}$$

where Z is the Pauli Z matrix. Applying the two-mode squeezing to the two-mode vacuum, the Einstein-Podolski-Rosen (EPR) state is obtained with null mean and covariance

$$\gamma_{EPR} = \begin{bmatrix} \nu I & \sqrt{\nu^2-1}Z \\ \sqrt{\nu^2-1}Z & \nu I \end{bmatrix}, \tag{2.45}$$

with $\nu = \cosh 2r$. The EPR state has a Fock basis representation of

$$|r\rangle_{EPR} = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(-\tanh r)^n |n\rangle_A |n\rangle_B. \tag{2.46}$$

It can be seen that the EPR state on each mode alone reduces to a thermal state with mean photon number $\bar{n} = \sinh^2 r$.

7. **Thermal noise channel:** The thermal noise channel is the fibre-channel model adopted in the simulation of QKD performances. For a channel with transmittance η, it is characterised by

$$d_{out} = \sqrt{\eta} d_{in}, \quad \gamma_{out} = \eta\gamma_{in} + \eta\chi I, \tag{2.47}$$

where χ is the added noise referring to the input

$$\chi = \frac{1-\eta}{\eta} + \varepsilon, \tag{2.48}$$

where ε is termed the excess noise from the input, and $\eta\varepsilon$ is the excess noise from the output. The thermal noise channel is equivalent to combining a thermal state with variance $\eta\chi/(1-\eta)$ with the signal through a beam splitter of transmittance η.

8. **Homodyne and heterodyne detection:** A homodyne detection measures the combination of q and p quadrature

$$\hat{Q}_\varphi = \cos\varphi\hat{q} + \sin\varphi\hat{p} \tag{2.49}$$

for an LO of φ angle with the measured signal. The outcome probability is the marginal probability of the Wigner function with

$$\Pr(q) = \int W(q,p)dp, \quad \Pr(p) = \int W(q,p)dq. \tag{2.50}$$

For a one-mode system A and an N-mode system B with covariance matrix

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & C \\ C^T & \gamma_B \end{bmatrix}, \tag{2.51}$$

measuring mode A with homodyne detector system B in an N-mode Gaussian state with variance

$$\gamma_B^{out} = \gamma_B - C(\Pi A \Pi)^{-1} C^T, \tag{2.52}$$

where $\Pi = \mathrm{diag}(1,0)$. The inverse is the pseudo-inverse.

A heterodyne detection measures according to the over-complete basis $\{\pi^{-1/2}|\alpha\rangle\langle\alpha|\}$. It is equivalent to combining the incoming mode with vacuum with a 1/2-beam splitter and measuring the two output modes with q and p-quadrature homodyne detectors respectively. A partial measurement leaves the output mode in a Gaussian state with covariance matrix

$$\gamma_B^{out} = \gamma_B - C(A+I)^{-1} C^T. \tag{2.53}$$

In practice, a homodyne detector is modelled by combining the incoming mode with certain thermal noise called the electronic noise, due to the detector imperfection. A homodyne detector with efficieny η_d and electronic noise ν_{el} (from detector output) gives the following output mode, before which being measured by a perfect homodyne detector:

$$\gamma_{out} = \eta_d \gamma_{in} + \eta_d \chi_d I, \tag{2.54}$$

and the added noise reads

$$\chi_d = \frac{1-\eta_d}{\eta_d} + \frac{\nu_{el}}{\eta_d}. \tag{2.55}$$

2.3 Quantum entropy and entanglement

The uncertainty within a quantum state is central to the discussion throughout, and the quantum entropy is a quantification of this uncertainty. For a quantum state with density operator ρ, the von-Neumann entropy is defined as

$$S(\rho) := -\mathrm{Tr}\{\rho \log(\rho)\}, \tag{2.56}$$

where the logarithm is taken with base 2 if without specification. The von-Neumann entropy is non-negative, and immediately a pure state has zero entropy. If the density operator takes a spectral decomposition as in Eq. (2.11), the von-Neumann entropy reduces to the classical Shannon entropy $H(\cdot)$ (Shannon, 1948):

$$S(\rho) = -\sum_i p_i \log(p_i) = H(p_i). \tag{2.57}$$

For a Gaussian state with covariance matrix γ, its entropy can be expressed by the symplectic eigenvalues ν_i of γ, i.e., the eigenvalues of $|i\Omega\gamma|$. The entropy can be expressed as (Holevo et al., 1999)

$$S(\rho) = \sum_{i=1}^{N} g(\nu_i), \tag{2.58}$$

where

$$g(x) = \frac{x+1}{2}\log\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log\left(\frac{x-1}{2}\right). \tag{2.59}$$

The corresponding quantities in the classical entropy are transferred naturally to the quantum entropy, where the conditional entropy reads

$$S(A|B) := S(\rho_{AB}) - S(\rho_A), \tag{2.60}$$

the mutual information reads

$$I(A:B) := S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \tag{2.61}$$

and the relative entropy reads

$$D(\rho||\sigma) := \mathrm{Tr}(\rho\log(\rho)) - \mathrm{Tr}(\rho\log(\sigma)). \tag{2.62}$$

It is worth noticing that in classical information theory the conditional entropy is non-negative, whilst in quantum information it is not. For example, consider the entangled state $(|00\rangle + |11\rangle)/\sqrt{2}$. According to Eq. (2.57), the von Neumann entropy of a quantum state is the Shannon entropy of its eigenvalues. Since $(|00\rangle + |11\rangle)/\sqrt{2}$ is a pure state, it has zero entropy as a whole. However, on each subsystem, it is the mixed state $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$, with entropy $-1/2\log_2(1/2) - 1/2\log_2(1/2) = 1$ bit. The conditional entropy of $(|00\rangle + |11\rangle)/\sqrt{2}$ is thus -1 bit. This translates to the fact that by acquiring information on system A, immediately the uncertainty on system B is settled. This demonstrates the entanglement between the two systems, and an entangled state can in turn be defined as the state where the conditional entropy of some subsystems given the other is negative.

Chapter 3

Security analysis of QKD

This chapter reviews the security analysis methods of both DV and CV QKD. The DV security analysis follows the phase-error-correction approach (Lo and Chau, 1999; Shor and Preskill, 2000; Koashi, 2009).It reviews the DV security in detail under the complementarity formalism by Koashi (2009). The author's proof of d-dimensional QKD security is introduced extending the binary QKD security (Jin et al., 2021). In light of this, the latent Hilbert space is assumed to be d-dimensional with $d = p^r$ for some prime number p and positive integer r. These are the dimensions where field structure exists, and so do the due addition and multiplication operations with inverse (see Appendix A.1 for the mathematical backgrounds). A finite field with d elements is denoted as GF(d), in short of the Galois Field. This chapter discuss the quantum information on GF(d) extending the usual GF(2), or binary, quantum information.

This chapter also briefly review the CV security under collective attack based on the Devetak-Winter formula (Devetak and Winter, 2005), and how the security can be extended to coherent attack, especially the Gaussian optimality in the GG02 protocol (García-Patrón and Cerf, 2006; Navascués et al., 2006).

3.1 DV security based on phase error correction

3.1.1 Security definition

The rigorous definition of the security of QKD was based on the composable security defined in (Ben-Or et al., 2005; Renner and König, 2005). In a general prepare-and-measure QKD protocol, Alice prepares quantum states based on her keys and sends to Bob for him to measure to obtain his keys. It is usually convenient to analyse the entanglement-based protocol (Lo and Chau, 1999), where Alice prepare bipartite states on system AB, keeping

the system A herself and sends system B to Bob. They measure the states at their possession to obtain the final keys. In fact, in the entanglement-based protocol, Alice and Bob measure their states respectively after the quantum communication. Alice can equivalently move the final measurements on her system ahead to the beginning since she does not operate on her system (Shor and Preskill, 2000). The entanglement-based protocol thus reduces to the prepare-and-measure protocol.

Denote the classical key strings Alice and Bob hold as k_A and k_B respectively. Note that these are strings in GF(d), and “digits" is used in replace of “bits". They record the final key string k_{fin} in the key-generating system K, which is usually taken as Alice's system in practice. The eavesdropper Eve may have information on their keys by holding a quantum state $\rho_E(k_A,k_B,k_{fin})$. Hence after the protocol, the final joint state shared by Alice, Bob and Eve is

$$\rho_{ABKE}^{fin} = \sum_{\kappa_A,\kappa_B,\kappa_{fin}} \Pr_{A,B,K}(\kappa_A,\kappa_B,\kappa_{fin}) |\kappa_A\rangle_A\langle\kappa_A| \otimes |\kappa_B\rangle_B\langle\kappa_B| \otimes \left|\kappa_{fin}\right\rangle_K\left\langle\kappa_{fin}\right| \otimes \rho_E(\kappa_A,\kappa_B,\kappa_{fin}), \tag{3.1}$$

where k_A, k_B and k_{fin} are length-$(N-m)$ digit strings. The $(N-m)$ denotes that N-digit raw keys are generated and m digits are lost in the post-processing.

The ideal state requires the key strings shared by Alice and Bob to be identical, termed correctness, and viewing by Eve their keys should be uniformly distributed, termed secrecy. The ideal state is thus

$$\rho_{ABKE}^{ideal} = (d^{N-m})^{-1} \sum_{\kappa} |\kappa\rangle_A\langle\kappa| \otimes |\kappa\rangle_B\langle\kappa| \otimes |\kappa\rangle_K\langle\kappa| \otimes \rho_E, \tag{3.2}$$

where Alice and Bob share the correct reconciled length-$(N-m)$ key string κ, which is completely random and decoupled from Eve's system.

In this way, a QKD protocol is defined to be ε-secure, if the final distilled state ρ_{ABKE}^{fin} is close to the ideal state ρ_{ABKE}^{ideal} for a properly chosen ρ_E

$$\min_{\rho_E} \frac{1}{2} ||\rho_{ABKE}^{fin} - \rho_{ABKE}^{ideal}||_1 \leq \varepsilon, \tag{3.3}$$

where $||A||_1 := Tr\{\sqrt{A^\dagger A}\}$ is the trace norm.

3.1.2 QKD security based on complementarity

Based on the above security definition, the security proof of QKD based on complementarity can be introduced, where the binary case is proved by Koashi (2009) and the general GF(d) case is proved by the author (Jin et al., 2021).

The core of Koashi (2009)'s qubit-based security proof is to reduce the two-body private and random key distribution to a single-body private and random number generation, i.e. to reduce entanglement distillation to coherence distillation (Ma et al., 2019). The security of the actual protocol can thus be proved if the single body squashing protocol is secure. Consider the entanglement-based general actual protocol below:

Protocol 3 General actual QKD protocol in GF(d)

1. ***State distribution*** *Alice and Bob share a bipartite state ρ_{AB} in the space $(\mathscr{H}_A \otimes \mathscr{H}_B)^{\otimes N}$ after N runs of quantum communications.*

2. ***Measurement*** *Alice and Bob measure their systems $\mathscr{H}_A^{\otimes N}$ and $\mathscr{H}_B^{\otimes N}$ respectively. They obtain two N-digit unreconciled key strings.*

3. ***Error correction*** *They reconcile the key strings through an encrypted classical channel consuming l_{ec} digits of secret key. They agree on an N-digit raw key string κ_{rec} except for a small failure probability ε_{cor}.*

4. ***Privacy amplification*** *Alice randomly chooses $(N-m)$ N-digit strings $\{V_k\}_{k=1,\cdots,N-m}$, which are linearly independent, and announces them to Bob. The final key length is $(N-m)$, where the k-th key digit is $\kappa_{rec} \cdot V_k$, where the dot product is to be understood with addition and multiplication in the finite field $GF(d)$. Denote the final key as κ_{fin}.*

After the protocol, the overall state shared by Alice and Bob and Eve is given by Eq. (3.1), and the corresponding ideal state is given by Eq. (3.2). In the error correction step of the actual protocol, it is claimed that Alice and Bob can correct their strings to κ_{rec} except for a small failure probability ε_{cor}. The protocol is termed ε_{cor}-correct where

$$\Pr_{A,B,K}(\kappa_A \text{ or } \kappa_B \neq \kappa_{rec}) \leq \varepsilon_{cor} \tag{3.4}$$

This property simply states Alice and Bob would very likely be sharing the same correct key strings. Hence intuitively, Alice and Bob and the reconciled key generation system K can be thought as a single party, i.e. they are squashed into one system.

More precisely, if Alice and Bob can apply a squashing operation Λ on $(\mathscr{H}_A \otimes \mathscr{H}_B)^{\otimes N}$ to convert it to a key space $\mathscr{K}^{\otimes N}$ and an ancillary space $\mathscr{H}_R$, and the key measurement statistics

on $\mathscr{K}^{\otimes N}$ is the same as κ_{rec} in the actual protocol, the following squashing protocol can be derived:

Protocol 4 **Squashing protocol from two-party to single-party**

1. ***State distribution*** *Alice and Bob share a bipartite state ρ_{AB} in the space $(\mathscr{H}_A \otimes \mathscr{H}_B)^{\otimes N}$ after N runs of quantum communications.*
2. ***Squashing*** *They apply Λ on ρ_{AB} and convert it to a key space $\mathscr{K}^{\otimes N}$ and an ancillary space $\mathscr{H}_R$, i.e. $\Lambda(\rho_{AB}) \in \mathscr{K}^{\otimes N} \otimes \mathscr{H}_R$.*
3. ***Measurement*** *They measure $\mathscr{H}_R$ by $\mathscr{M}_R$ to obtain result γ. They then measure $\mathscr{K}^{\otimes N}$ to obtain κ_{rec}, with the same measurement statistics as that in the actual protocol.*
4. ***Privacy amplification*** *They randomly choose $(N-m)$ N-digit strings $\{V_k\}_{k=1,\cdots,N-m}$, which are linearly independent. The final key length is $(N-m)$, where the k-th key digit is $\kappa_{rec} \cdot V_k$. Denote the final key as κ_{fin}.*

Since the key space $\mathscr{K}^{\otimes N}$ measurement statistics is the same as that of the actual protocol, the final state after the squashing protocol is therefore

$$\rho_{KE}^{fin} = \sum_{\kappa_{fin}} \Pr_K(\kappa_{fin}) \big| \kappa_{fin} \big\rangle_K \big\langle \kappa_{fin} \big| \otimes \rho_E(\kappa_{fin}), \tag{3.5}$$

where the probability distribution $\Pr_K(\kappa_{fin})$ is the marginal distribution of $\Pr_{A,B,K}(\kappa_A, \kappa_B, \kappa_{fin})$ in the actual final state (3.1), and

$$\rho_E(\kappa_{fin}) = \frac{1}{\Pr_K(\kappa_{fin})} \sum_{\kappa_A, \kappa_B} \Pr_{A,B,K}(\kappa_A, \kappa_B, \kappa_{fin}) \rho_E(\kappa_A, \kappa_B, \kappa_{fin}). \tag{3.6}$$

The ideal squashed state is

$$\rho_{KE}^{ideal} = (d^{N-m})^{-1} \sum_{\kappa} |\kappa\rangle_K \langle\kappa| \otimes \rho_E, \tag{3.7}$$

Likewise, the squashing protocol is termed ε_{sec}-secret if the squashed state ρ_{KE} is close to ideality, i.e.

$$\min_{\rho_E} \frac{1}{2} || \rho_{KE}^{fin} - \rho_{KE}^{ideal} ||_1 \leq \varepsilon_{sec} \tag{3.8}$$

Koashi (2009) proved that as long as the squashing protocol is ε_{sec}-secret with an ε_{cor}-correct error correction, the actual protocol is $(\varepsilon_{sec} + \varepsilon_{cor})$-secure. Although in the original proof the quantum system is of dimension 2, but it can be trivially generalised to arbitrary dimension.

3.1.3 The phase-error-correction protocol

It now remains to show that the single-body squashing protocol 4 is secret. This is done by invoking phase-error correction, which bears intuitions from the uncertainty principle of two complementary operators: if the X-basis measurement of $\mathscr{K}^{\otimes N}$ is completely certain, the Z-basis measurement of it, which is by convention the key generation measurement, is completely random (Tomamichel and Renner, 2011). The Z and X operators are only defined in dimension 2, and for dimension d with computational basis $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$, the d-dimensional Z and X operators are defined as:

$$\begin{aligned} Z &= \sum_{l=0}^{d-1} \gamma_p^l |l\rangle\langle l|, \\ X &= \sum_{l=0}^{d-1} |l+1\rangle\langle l|, \text{ addition with respect to GF}(d). \end{aligned} \tag{3.9}$$

The d-dimensional X basis, as eigenstates of the X operator, is defined as

$$\begin{aligned} \left|\tilde{l}\right\rangle &:= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \gamma_p^{-lj} |j\rangle, \\ |j\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \gamma_p^{lj} \left|\tilde{l}\right\rangle, \end{aligned} \tag{3.10}$$

with $X\left|\tilde{l}\right\rangle = \gamma_p^l \left|\tilde{l}\right\rangle$. This is the basis complementary to the computational Z basis. They are reviewed in detail in Appendix. A.2.

Assume Z-basis measurement on $\mathscr{K}^{\otimes N}$ is used for key generation in the squashing protocol. If, before the key generation measurement on $\mathscr{K}^{\otimes N}$, Alice and Bob are able to determine the X-basis measurement result of $\mathscr{K}^{\otimes N}$ to be $\mathbf{x}^*$ except for a small failure probability ε_T', they would have

$$\left\langle \tilde{\mathbf{x}}^* \middle| \rho_K \middle| \tilde{\mathbf{x}}^* \right\rangle = F(\rho_K, \left|\tilde{\mathbf{x}}^*\right\rangle\left\langle\tilde{\mathbf{x}}^*\right|) \geq 1 - \varepsilon_T', \tag{3.11}$$

i.e. the state on $\mathscr{K}^{\otimes N}$ is close to the X eigenstate $\left|\tilde{\mathbf{x}}^*\right\rangle$ in terms of fidelity $F(\rho,\sigma) := \mathrm{Tr}\left\{\sqrt{\rho^{\frac{1}{2}}\sigma^{\frac{1}{2}}}\right\}$. It can then be shown that (Fung et al., 2010) there exists σ_E on Eve's system such that

$$F(\rho_{KE}, \left|\tilde{\mathbf{x}}^*\right\rangle\left\langle\tilde{\mathbf{x}}^*\right| \otimes \sigma_E) \geq 1 - \varepsilon_T' \tag{3.12}$$

Hence, the overall state before the key generation measurement is approximately a separate state if it can be assured that the state on $\mathscr{K}^{\otimes N}$ is close to a X eigenstate, i.e. its X-basis

measurement result can be determined. Note that the state $\left|\tilde{\mathbf{x}}^*\right\rangle\left\langle\tilde{\mathbf{x}}^*\right| \otimes \sigma_E$ yields ρ_{KE}^{ideal} after Z-basis measurements and privacy amplification, and fidelity never decreases after quantum operations (Wilde, 2011). Hence, the squashing protocol is secure (and so is the actual protocol) as long as the X-basis measurement result of the key generation system $\mathscr{K}^{\otimes N}$ can be determined.

In order to gain information on the X-basis measurement result of $\mathscr{K}^{\otimes N}$, the ancillary system $\mathscr{H}_R$ left after the squashing operation Λ can be invoked. Measuring $\mathscr{H}_R$ by $\mathscr{M}_R$ gives a result γ, which provides information of the X-basis measurement result of $\mathscr{K}^{\otimes N}$. To be more specific, given each measurement result γ on $\mathscr{H}_R$, suppose the candidates of $\mathscr{K}^{\otimes N}$ X-basis measurement result are summarized in the set T_γ. Suppose the cardinality of the candidate sets, except for a small probability ε_T, can be bounded by:

$$|T_\gamma| \leq d^{Ns}. \tag{3.13}$$

In this case, suppose $m = N(s+\zeta)$ random X-parity checks are made, i.e. phase-error correction (see Appendix A.3), the X-basis measurement result of $\mathscr{K}^{\otimes N}$ can be derived with an exponentially small failure probability $\varepsilon_T' \equiv \varepsilon_T + d^{-N\zeta}$ (Bennett et al., 1996). Hence, the $\sqrt{\varepsilon_T'}$-secrecy of the following single-body phase-error correction protocol can be claimed:

Protocol 5 **Phase-error correction protocol with random parity checks**

1. ***State distribution*** *Alice and Bob share a bipartite state ρ_{AB} in the space $(\mathscr{H}_A \otimes \mathscr{H}_B)^{\otimes N}$ after N runs of quantum communications.*

2. ***Squashing*** *They apply Λ on ρ_{AB} and convert it to a key space $\mathscr{K}^{\otimes N}$ and an ancillary space $\mathscr{H}_R$, i.e. $\Lambda(\rho_{AB}) \in \mathscr{K}^{\otimes N} \otimes \mathscr{H}_R$. The Z-basis measurement statistics on $\mathscr{K}^{\otimes N}$ is the same as κ_{rec} in the actual protocol.*

3. ***Ancillary measurement*** *They measure $\mathscr{H}_R$ by $\mathscr{M}_R$ to obtain result γ. The candidate-set cardinality $|T_\gamma| \leq d^{Ns}$ except for a small probability ε_T.*

4. ***phase-error correction*** *For $m = N(s+\zeta)$, they randomly choose m N-digit strings $\{W_j\}_{j=1,\cdots,m}$ and perform X-parity measurements $\{\mathscr{M}_X(W_j)\}$ on $\mathscr{K}^{\otimes N}$ to determine its X-basis measurement result.*

5. ***Key generation*** *They choose an arbitrary linearly independent set $\{V_k\}_{k=1,\cdots,N-m}$ satisfying $V_k \cdot W_j = 0$ for any (j,k). They perform Z-parity check measurements $\{\mathscr{M}_Z(V_k)\}$ to obtain the $(N-m)$-digit final key κ_{fin}.*

It only remains to show the equivalence of the phase-error correction protocol and the squashing protocol. Observe that this can be done if it is feasible to, just like that in Ref. (Koashi, 2009), swap the key generation step with the phase-error correction step and omit the latter as well. Then the Z-parity check measurements can be viewed as random hashing, and the measurement $\mathscr{M}_R$ on the ancilla $\mathscr{H}_R$ is not required. In the two-dimensional proof, X and Z operators are also observables, and thus the parity check measurements can be expressed as tensor products of X and Z's, which are observables. In this case, the commuting argument is guaranteed by the commutation of X-parity check observables and Z-parity check observables since $V_k \cdot W_j = 0$. However, in high dimensions, the parity check measurements with multiple outcomes cannot be easily expressed as Pauli operators, so here the parity check measurements are described with measurement Kraus operators (see Appendix A.3 for the definitions). In the section below, it is shown that this commuting argument is still valid: as long as W_j is orthogonal with V_k, the statistics of the Z-parity measurement $\{\mathscr{M}_Z(V_k)\}$ would not change even if it is performed in prior an X-parity measurement $\{\mathscr{M}_X(W_j)\}$ (Eq. (3.16)). In this way, the security of the actual protocol is proved:

Theorem 1 *If the actual protocol can be converted into a squashing protocol with squashing operation Λ and ancillary measurement $\mathscr{M}_R$ such that:*

1. *The Z-basis measurement statistics on $\mathscr{K}^{\otimes N}$ is the same as κ_{rec} in the actual protocol.*
2. *Given each measurement outcome γ on $\mathscr{H}_R$, the size of X-basis measurement outcome on $\mathscr{K}^{\otimes N}$ is bounded by $|T_\gamma| \leq d^{Ns}$, except for a small probability ε_T,*

then the squashing protocol is $\sqrt{\varepsilon_T'}$-secret, and the actual protocol is $(\sqrt{\varepsilon_T'} + \varepsilon_{cor})$-secure, where $\varepsilon_T' = \varepsilon_T + d^{-N\zeta}$ and $m = N(s+\zeta)$.

It is useful to derive the key-rate formula based on the phase error of high-dimensional QKD. Our goal is to determine the X-basis measurement outcome X^* on $\mathscr{K}^{\otimes N}$, and infer X^* based on the ancillary measurement result γ. Based on each γ, suppose an estimation of X^* is made as X_γ. Denote the phase error number vector of a given γ as $\vec{N}_{ph} := \vec{wt}(X_\gamma - X^*)$, where the subtraction is defined for GF(d) strings, and the vector weight function for GF(d) is defined as:

$$\vec{wt}(\mathbf{a}) = \begin{bmatrix} \text{No. of 0 in } \mathbf{a} \\ \text{No. of 1 in } \mathbf{a} \\ \cdots \\ \text{No. of } d\text{-1 in } \mathbf{a} \end{bmatrix} \tag{3.14}$$

Hence, the phase error number vector $\vec{N}_{ph}$ counts the numbers of different types of phase error of our estimation X_γ. Denote the average phase error number vector for all γ as $\vec{N}_{ph}$, and the

phase-error rate vector as $\vec{E}_{ph} := \vec{N}_{ph}/N$, i.e. it counts the phase-error rate of different types of phase error. Based on Shannon's typical sequences arguments, taking the reconciliation cost as l_{ec} bits, the key generation length of a d-dimensional QKD is

$$\begin{aligned} R &= N - m - l_{ec}/\log_2 d \text{ (dits)} \\ &\geq N(1 - H_d(\vec{E}_{ph})) - l_{ec}/\log_2 d \text{ (dits)} \\ &= N(\log_2 d - H_2(\vec{E}_{ph})) - l_{ec} \text{ (bits)}, \end{aligned} \tag{3.15}$$

where H_2 and H_d are the $\log_2$ and $\log_d$ based Shannon-entropy functions respectively. Note that a similar formula is derived by Sheridan and Scarani (2010) using the Devetak-winter formula under collective attack, but our proof covers coherent attack naturally.

3.1.4 The commuting argument in high dimension

It now remains to show that the Z and X parity check measurements can be swapped if they are orthogonal. Denote γ_p as the complex number satisfying $\gamma_p^p = 1$. In the arguments below, the addition, multiplication and dot product are to be understood within GF(d).

Given two N-digit GF(d) strings $\mathbf{a}$ and $\mathbf{b}$ such that $\mathbf{a} \cdot \mathbf{b} = 0$, it requires to be shown that

$$\mathscr{M}_Z^{\mathbf{a}} \circ \mathscr{M}_X^{\mathbf{b}} = \mathscr{M}_Z^{\mathbf{a}} \text{ in terms of measurement statistics.} \tag{3.16}$$

If $\mathbf{a} = 0$, the argument follows trivially as the measurement result is always zero. For non-zero $\mathbf{a}$ and an arbitrary state ρ, the probability that it falls into the l-th eigenspace of $\mathscr{M}_Z(\mathbf{a})$ is:

$$\sum_{\mathbf{z}\cdot\mathbf{a}=l} \langle \mathbf{z}|\rho|\mathbf{z}\rangle \tag{3.17}$$

On the other hand, the state after $\mathscr{M}_X(\mathbf{b})$ is:

$$\sum_{j=0}^{d-1} \sum_{\mathbf{x_j},\mathbf{x'_j}\cdot\mathbf{b}=j} \left|\tilde{\mathbf{x}}_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}_\mathbf{j}\right|\rho\left|\tilde{\mathbf{x}}'_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}'_\mathbf{j}\right| \tag{3.18}$$

The probability that its $\mathscr{M}_Z(\mathbf{a})$ result falls into the l-th eigenspace is thus:

$$\sum_{\mathbf{z}\cdot\mathbf{a}=l} \langle \mathbf{z}| \left(\sum_{j=0}^{d-1} \sum_{\mathbf{x_j},\mathbf{x'_j}\cdot\mathbf{b}=j} \left|\tilde{\mathbf{x}}_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}_\mathbf{j}\right|\rho\left|\tilde{\mathbf{x}}'_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}'_\mathbf{j}\right| \right) |\mathbf{z}\rangle \tag{3.19}$$

Our task is to show that Eq. (3.17) = Eq. (3.19).

First examine three lemmas. In the argument below, the scaling constants are ignored to simplify the notations.

Lemma 1

$$\sum_{\mathbf{z}} \gamma_p^{\mathbf{z}\cdot\mathbf{x}} = \begin{cases} 1 & \mathbf{x} = \mathbf{0} \\ 0 & \mathbf{x} \neq \mathbf{0} \end{cases} \tag{3.20}$$

where $\mathbf{z}$ *traverses all GF(d) strings with some fixed length.*

Lemma 2 *If* $\mathbf{x}$ *is 0 at one of the non-zero positions of* $\mathbf{a}$*, then for any GF(d) member l:*

$$\sum_{\mathbf{z}\cdot\mathbf{a}=l} \gamma_p^{\mathbf{z}\cdot\mathbf{x}} = \begin{cases} 1 & \mathbf{x} = \mathbf{0} \\ 0 & \mathbf{x} \neq \mathbf{0} \end{cases} \tag{3.21}$$

Proof: Since $\mathbf{x}$ is 0 at one of the non-zero positions of $\mathbf{a}$, that digit is essentially redundant in the summation. Denote the $(N-1)$-digit sub-string of $\mathbf{z}$ with that digit removed as $\mathbf{z}'$. Since $\mathbf{z}$ traverses all N-digit strings that satisfy $\mathbf{z}\cdot\mathbf{a} = l$, $\mathbf{z}'$ actually takes values of all $(N-1)$-digit strings. To see this, observe that for any $(N-1)$-digit string $\mathbf{z}'$, there is one and only one N-digit string $\mathbf{z}$ that satisfies $\mathbf{z}\cdot\mathbf{a} = l$ corresponds to it. This is guaranteed in a field structure. Hence, the summation is transformed to the case of Lemma 1.

Lemma 3

$$\sum_{\mathbf{z}\cdot\mathbf{a}=l} \gamma_p^{\mathbf{z}\cdot\mathbf{x}} = \begin{cases} \gamma_p^{x_0 l} & \mathbf{x} = x_0\mathbf{a}, \quad x_0 = 0, 1, \cdots, d-1 \\ 0 & \textit{otherwise} \end{cases} \tag{3.22}$$

Proof: Assume $\mathbf{a}$ is non-zero at digit n. As in a field structure, there always exists $x_0 \in \{0, 1, \cdots, d-1\}$ such that $\mathbf{x}_n = x_0\mathbf{a}_n$. The following decomposition can be made:

$$\sum_{\mathbf{z}\cdot\mathbf{a}=l} \gamma_p^{\mathbf{z}\cdot\mathbf{x}} = \sum_{\mathbf{z}\cdot\mathbf{a}=l} \gamma_p^{x_0(\mathbf{z}\cdot\mathbf{a})} \gamma_p^{\mathbf{z}\cdot(\mathbf{x}-x_0\mathbf{a})} = \gamma_p^{x_0 l} \sum_{\mathbf{z}\cdot\mathbf{a}=l} \gamma_p^{\mathbf{z}\cdot(\mathbf{x}-x_0\mathbf{a})} \tag{3.23}$$

Note that $(\mathbf{x} - x_0\mathbf{a})$ is guaranteed to be zero at digit n, where $\mathbf{a}$ is non-zero. Lemma 2 can then be applied to arrive at the desired result.

The main claim that (3.17) = (3.19) is now to be proved:

$$
\begin{aligned}
&\sum_{\mathbf{z}\cdot\mathbf{a}=l}\langle\mathbf{z}|\left(\sum_{j=0}^{d-1}\sum_{\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j}\left|\tilde{\mathbf{x}}_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}_\mathbf{j}\right|\rho\left|\tilde{\mathbf{x}}'_\mathbf{j}\right\rangle\left\langle\tilde{\mathbf{x}}'_\mathbf{j}\right|\right)|\mathbf{z}\rangle\\
&=\sum_{\mathbf{z}\cdot\mathbf{a}=l}\sum_{j=0}^{d-1}\sum_{\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j}\left\langle\tilde{\mathbf{x}}_\mathbf{j}\right|\rho\left|\tilde{\mathbf{x}}'_\mathbf{j}\right\rangle\gamma_p^{-\mathbf{z}\cdot\mathbf{x_j}+\mathbf{z}\cdot\mathbf{x}'_\mathbf{j}}\\
&=\sum_{\mathbf{z}\cdot\mathbf{a}=l}\sum_{j=0}^{d-1}\sum_{\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j}\sum_{\mathbf{k},\mathbf{k}'}\langle\mathbf{k}|\rho|\mathbf{k}'\rangle\gamma_p^{-\mathbf{z}\cdot\mathbf{x_j}+\mathbf{z}\cdot\mathbf{x}'_\mathbf{j}-\mathbf{x}'_\mathbf{j}\cdot\mathbf{k}'+\mathbf{x_j}\cdot\mathbf{k}}\\
&=\sum_{\mathbf{k},\mathbf{k}'}\sum_{j=0}^{d-1}\sum_{\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j}\langle\mathbf{k}|\rho|\mathbf{k}'\rangle\gamma_p^{-\mathbf{x}'_\mathbf{j}\cdot\mathbf{k}'+\mathbf{x_j}\cdot\mathbf{k}}\sum_{\mathbf{z}\cdot\mathbf{a}=l}\gamma_p^{\mathbf{z}\cdot(\mathbf{x}'_\mathbf{j}-\mathbf{x_j})}\\
&=\sum_{\mathbf{k},\mathbf{k}'}\sum_{j=0}^{d-1}\sum_{x_0=0}^{d-1}\sum_{\substack{\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j\\ \mathbf{x}'_\mathbf{j}-\mathbf{x_j}=x_0\mathbf{a}}}\langle\mathbf{k}|\rho|\mathbf{k}'\rangle\gamma_p^{x_0 l}\gamma_p^{\mathbf{x_j}\cdot(\mathbf{k}-\mathbf{k}')}\gamma_p^{-x_0\mathbf{k}'\cdot\mathbf{a}}\\
&=\sum_{\mathbf{k},\mathbf{k}'}\sum_{x_0=0}^{d-1}\sum_{\mathbf{x_j}}\langle\mathbf{k}|\rho|\mathbf{k}'\rangle\gamma_p^{x_0(l-\mathbf{k}'\cdot\mathbf{a})}\gamma_p^{\mathbf{x_j}\cdot(\mathbf{k}-\mathbf{k}')}\\
&=\sum_{\mathbf{k}'\cdot\mathbf{a}=l}\langle\mathbf{k}|\rho|\mathbf{k}'\rangle\delta_{\mathbf{k}=\mathbf{k}'}\\
&=\sum_{\mathbf{k}\cdot\mathbf{a}=l}\langle\mathbf{k}|\rho|\mathbf{k}\rangle,
\end{aligned}
\tag{3.24}
$$

which is exactly the $\mathscr{M}_Z^{\mathbf{a}}$ statistics without $\mathscr{M}_X^{\mathbf{b}}$ in (3.17). Lemma 1 and Lemma 3 are applied in the 6-th and 4-th equalities. Notice that in the summation it requires $\mathbf{x_j},\mathbf{x}'_\mathbf{j}\cdot\mathbf{b}=j$ for any GF(d) member j, which is equivalent to $(\mathbf{x}'_\mathbf{j}-\mathbf{x_j})\cdot\mathbf{b}=0$. Hence, $\mathbf{x}'_\mathbf{j}-\mathbf{x_j}=x_0\mathbf{a}$ is within the summation range since it is required that $\mathbf{a}\cdot\mathbf{b}=0$. Therefore, the swapping argument that performing X parity checks and then Z hashed key generation is equivalent to the latter on its own can be extended to higher-dimensional cases.

3.2 CV security based on entanglement distillation

This section reviews briefly the security proofs of CV QKD. As is mentioned in Chapter 1, the CV security is not as robust as that of DV QKD. Essentially, the ambient Hilbert space of CV quantum information is infinite-dimensional. This renders operations on a CV mode hard to characterise. In fact, the complete security, i.e., the security under coherent attack, is only proved for the GG02 protocol using Gaussian modulation.

The usual approach to the security of a CV protocol is the Devetak-Winter formula (Devetak and Winter, 2005), based on entanglement distillation in the collective asymptotic regime. If Alice and Bob and Eve share the classical-quantum-quantum tripartite state

$$\rho_{ABE} = \sum_x \Pr(x)|x\rangle_A\langle x| \otimes \rho_x^{BE} \tag{3.25}$$

after the quantum communication, the distillable secure key rate $r(\rho_{ABE})$ is lower-bounded by

$$r(\rho_{ABE}) \geq S(X|E) - S(X|B), \tag{3.26}$$

where $S(\cdot|\cdot)$ is the conditional von Neumann entropy. Since Eve's system is not accessible, Alice and Bob have to assume the worst case scenario where Eve launches the optimal attack to yield the lowest possible key rate. The key rate with knowledge only on system A and B is then

$$r(\rho_{AB}) \geq \inf_{\rho_{ABE}} S(X|E) - S(X|B), \tag{3.27}$$

and the infimum is taken on all the tripartite states with $\mathrm{Tr}_E\{\rho_{ABE}\} = \rho_{AB}$.

The usual method to extend the Devetak-Winter formula Eq. (3.25) to coherent attack and asymptotic regime resorts to the smoothed min/max entropy quantities (Renner, 2008). In fact, for a QKD protocol taking N rounds of successful communication, Alice and Bob can be though as sharing a joint state on $\mathscr{H}^{\otimes 2N}$, and attempting to distill secure keys in one shot. The smoothed min/max entropy $H_{\min}^{\varepsilon}$ and $H_{\max}^{\varepsilon}$, extending the usual von Neumann entropy, are specifically designed for this one-shot scenario (Konig et al., 2009).

A technique termed the quantum de Finetti theorem is invoked to reduce the coherent attack to collective attack (Renner, 2007). In fact, the quantum de Finetti theorem acknowledges the permutation symmetry of QKD protocols, in the sense that random permutations between rounds do not affect the key rate. It is shown that the permutation-invariant states are close to mixtures of product states, in the sense that the uniform mixture of product states gives the identity operator on the permutation-invariant state space. The key rate can thus be related to the key rate on single systems, i.e., the collective scenario. The Devetak-Winter key rate in the coherent regime can be written as (Tomamichel and Renner, 2011)

$$r \approx H_{\min}^{\varepsilon}(\mathbf{X}|E) - H_{\max}^{\varepsilon}(\mathbf{X}|B), \tag{3.28}$$

where the approximation comes from certain small security parameters.

To apply the general Devetak-Winter formula Eq. (3.28) to CV QKD protocols, certain caveats need to be resolved. First, the security parameters in Eq. (3.28) usually increase with the Hilbert space dimension, and thus the key rate formula is not accurate for CV systems

with infinite dimensions. This is usually tackled by imposing an energy test on the received modes, aborting the protocol if the measured energy is above a preset threshold, and showing the closeness of the energy-truncated protocol and the original protocol (Leverrier, 2017).

Second, the optimal attack by Eve resulting in the lowest key rate is hard to characterise, and for now it is only tackled for protocols using Gaussian modulation such as GG02. However, in realistic, a continuous modulation is never possible, and approximated by large-number discrete constellations. The security of practical Gaussian protocols are thus not completed. It is still fascinating to look at the security of ideal Gaussian protocols, based on Gaussian optimality. In fact, it is shown that for a continuous real function f with strong superadditivity and invariance under local unitary, i.e., $f(U^{\otimes N}\rho U^{\dagger\otimes N}) = f(\rho)$, the Gaussian states give its lower bound:

$$f(\rho) \geq f(\rho_G), \tag{3.29}$$

where ρ_G is the Gaussian state with the same first and second moments as ρ. The possible attacks by Eve are thus characterised by symplectic transformations of the first and second moments, and the key rate lower bound can be computed easily (Laudenbach et al., 2018). The local-unitary invariance can be understood as the $U(N)$ symmetry of a CV system, in addition to the permutation symmetry of general QKD protocols (Leverrier, 2017).

For most CV protocols, the security is only computed in the collective case with the Devetak-Winter formula Eq. (3.25). To characterise Eve's attack, numerical optimisation can applied minimising the key rate with constraints as the experimental statistics (Winick et al., 2018; Bunandar et al., 2020). This formalism will be exploited in Chapter 5.

3.3 Imperfect sources: photon-number tagging and decoy method

[1] Phase-randomised weak coherent sources, instead of perfect single-photon sources, are used in practice for the BB84 protocol. The perfect single-photon source is basis-independent in the sense that the mixture of Z basis is the same as the mixture of X basis, i.e.,

$$\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|). \tag{3.30}$$

The basis independence guarantees that Eve cannot determine certainly the bases used in any rounds, ensuring the X-basis bit error rate is a fair reflection of the Z-basis phase error rate.

[1] The discussion carried in this section is on the conventional GF(2) quantum information, but can be extended to GF(d) trivially.

This is however not the case for the two-photon components, since

$$\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \neq \frac{1}{2}(|{+}{+}\rangle\langle {+}{+}| + |{-}{-}\rangle\langle {-}{-}|). \tag{3.31}$$

This basis dependence gives Eve some chances to determine the basis choices without disturbing the signals. In the two-photon rounds, it is thus not reliable to use the X-basis bit error rate as the Z-basis phase error rate.

In general, an imperfect source can emit basis-dependent and independent components. For the phase-randomised weak coherent source for BB84 with intensity μ, it is diagonalised in the Fock basis as

$$\frac{1}{2\pi}\int_0^{2\pi} \left|\sqrt{\mu}e^{i\theta}\right\rangle\left\langle\sqrt{\mu}e^{i\theta}\right| = \sum_{n=0}^{\infty} \Pr_\mu(n)|n\rangle\langle n|, \tag{3.32}$$

where $\Pr_\mu(n) = e^{-\mu}\mu^n/n!$ is the Poisson distribution. It would be ideal if Alice can measure each round with a photon-number resolving detector to determine the photon number of the current round. Bob can then be notified whether to distill keys from this round or not based on this photon-number tag. Although the photon-number resolving measurement is not practical, it can be shown that if Alice and Bob can determine the ratio $(1-\Delta)$ of the detected rounds from the basis-independent source, secure keys can still be distilled from the overall key strings without knowing the specific tagging. This method is termed the GLLP formalism named after the initials of the inventors (Gottesman et al., 2004). In fact, if Alice were virtually given the tagging information of each round, she could sort the sifted key string k_A into two sub-strings k_{good} and k_{bad} coming from basis-independent and dependent sources respectively. The length of the good and bad strings are respectively $(1-\Delta)N$ and ΔN, where N is the total rounds of sifted keys.

The phase error rate e_p of the basis-independent good rounds can be estimated via the complementary bit error rate, whilst that of the basis-dependent bad rounds cannot, and can be as high as 1/2. k_{good} can be compensated to a length-N string k'_{good} by setting the bad positions as zero, and k_{bad} to a length-N k'_{bad} by filling the good positions with zero. Abuse slightly the notation by denoting the position-wise addition between strings as "$+$" also, the identity holds:

$$k'_{good} + k'_{bad} = k_A. \tag{3.33}$$

Denote the $(1-\Delta)(1-H(e_p))N \times (1-\Delta)N$ linear hashing matrix distilling secure keys from k_{good} as T. Tk_{good} is thus a length-$(1-\Delta)(1-H(e_p))N$ secure key string. If random columns are inserted to T referring to the bad positions to make it a $(1-\Delta)(1-H(e_p))N \times N$

matrix T', $T'k'_{good}$ is still a secure key string. Applying T' to k_A:

$$T'k_A = T'(k'_{good} + k'_{bad}) = T'k'_{good} + T'k'_{bad}. \tag{3.34}$$

Since $T'k'_{good}$ is secure, $T'k_A$ is also secure regardless of Eve's knowledge on $T'k'_{bad}$. In practice, Alice can select a random universal hashing matrix to do privacy amplification on k_A and its sub-matrix will automatically be a smaller universal hashing matrix on k_{good}. Therefore the secure key rate with $(1-\Delta)$-ratio of good tags is

$$r \geq -H(e_b) + (1-\Delta)[1-H(e_p)]. \tag{3.35}$$

In general, if Alice and Bob can group their sifted key bits, and for each group g they can derive the corresponding phase error rate e_p^g of these rounds of keys, then with the same argument as before, they can distill a key rate (Ma, 2008)

$$r \geq -H(e_b) + \sum_g q_g[1-H(e_p^g)], \tag{3.36}$$

where q_g is the ratio of the sifted key bits with tag g. It is usually called the gain of component-g.

Based on Eq. (3.36), the BB84 key rate with coherent source is given by

$$r \geq -Q_\mu H(E_\mu) + Q_1[1-H(e_1)], \tag{3.37}$$

where Q_μ and E_μ are the ratio of successful detection and the bit error rate of the detected rounds, under source intensity μ. Q_1 is the gain of single-photon components, i.e., the probability of sending single photon and being detected, and e_1 is the phase error rate of these rounds.

It is in fact not easy to estimate Q_1 and e_1 in practice, since it is hard to tell whether a given detection comes from single photon or two photons. Reliable bounds on these parameters can however be derived based on the decoy state method (Hwang, 2003; Lo et al., 2005; Wang, 2005). Denote the conditional probability of successful detection given n photons being sent as Y_n, termed the n-photon yield, the gain Q_μ and error rate E_μ can be expanded as

$$Q_\mu = \sum_{n=0}^{\infty} \Pr_\mu(n) Y_n, \tag{3.38}$$

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} \Pr_\mu(n) e_n Y_n. \tag{3.39}$$

A crucial observation is that by varying the source intensity, the distribution of different photon components would change, yet the yield of any n-photon component remains invariant since Eve cannot tell which source intensity the photon comes from (Lo et al., 2005), or in other words

$$\begin{aligned} Y_n(\mu) &= Y_n(\nu) \\ e_n(\mu) &= e_n(\nu). \end{aligned} \tag{3.40}$$

Thus by varying the source intensity in a set of $\{\mu, \nu_1, \cdots, \nu_k\}$, the linear equation system is given as:

$$\begin{aligned} Q_\mu &= \sum_{n=0}^{\infty} \Pr_\mu(n) Y_n \\ E_\mu Q_\mu &= \sum_{n=0}^{\infty} \Pr_\mu(n) e_n Y_n \\ Q_{\nu_1} &= \sum_{n=0}^{\infty} \Pr_{\nu_1}(n) Y_n \\ E_{\nu_1} Q_{\nu_1} &= \sum_{n=0}^{\infty} \Pr_{\nu_1}(n) e_n Y_n \\ &\cdots \\ Q_{\nu_k} &= \sum_{n=0}^{\infty} \Pr_{\nu_k}(n) Y_n \\ E_{\nu_k} Q_{\nu_k} &= \sum_{n=0}^{\infty} \Pr_{\nu_k}(n) e_n Y_n. \end{aligned} \tag{3.41}$$

The rounds with μ intensity are called the signals for key generation, and the other rounds are called the decoy rounds. Typically in the BB84 protocol, the parameters Q_1 and e_1 can be reliably estimated with a vacuum and weak-intensity decoy (Ma et al., 2005).

Notice that the photon-number tagging and decoy method are long-believed to be confined to DV scheme. It will be shown in Chapter 6 the author's work on extending these methods to CV QKD (Jin et al., 2023).

Chapter 4

Twin-field QKD

This chapter discusses the Twin-field (TF) QKD, which is the most loss-tolerant QKD type reaching the farthest distance in optical fibres (Liu et al., 2023). It will review the developments of the TF QKD as well as the intuition behind its remarkable loss tolerance. It will mainly be looking at the setup of a particular variant of the TF QKD, namely the phase-matching (PM) QKD (Ma et al., 2018). It will review the recent experimental advances in demonstrating the TF-type QKD, and identify the reference misalignment as the major practical limiting factor of its performance. This brings about the author's work on the reference-frame-independent design of PM QKD using the high-dimensional encoding introduced in Section 3.1.2. In Section 4.4, the high-dimensional PM QKD will be presented immune to any fixed reference misalignment with simple experimental setup, and robust to random fluctuation.

4.1 Breaking the linear key rate-transmittance bound

For long it is believed that the key rate R of any QKD protocols should at most scale linearly with the channel transmittance η, that is, $R \leq O(\eta)$. This is reasonable since in the prepare-and-measure setup each key bit is generated for each round of successful detection, whose probability is $O(\eta)$. In fact, Takeoka et al. (2014) have rigorously shown that the repeaterless point-to-point QKD has a key rate upper bound of $\log_2(1+\eta/1-\eta)$, and Pirandola et al. (2017) further tightened the upper bound to $-\log_2(1-\eta)$, all scaling linearly with the channel transmittance η when η is small. Since the channel transmittance decays exponentially with the fibre distance, this linear key rate-transmittance upper bound severely limits the coverage of QKD, being around 140 km limit for BB84 (Ma et al., 2005).

The measurement-device-independent (MDI) QKD (Lo et al., 2012) is a novel type of QKD which departs from the point-to-point scheme. Instead of Alice transmitting to Bob,

the two communication parties transmit to a untrusted third party together in the MDI QKD, where the third party interferes the signals from each side and announces the results. Based on the announced results, Alice and Bob can adjust their keys to hold reliable raw key strings. They can then estimate the bit and phase error rate and run information reconciliation and privacy amplification as in the standard point-to-point QKD.

Unfortunately, the key rate of the original polarization-encoding MDI QKD (Lo et al., 2012) still scales linearly with the channel transmittance. To be specific, in the polarization-encoding MDI QKD, a successful detection requires the reception of both photons from Alice and Bob. Suppose the third party is placed at the middle between Alice and Bob, where the two fibres connecting from Alice and Bob each has transmittance $\sqrt{\eta}$. The probability of receiving both photons is still η, and hence the key rate still scales linearly with the transmittance.

Examining from the entanglement-based perspective, it is not hard to see that the polarization-encoding MDI QKD generates the Bell state $(|01\rangle + |10\rangle)/\sqrt{2}$, which possesses two photons since $|0\rangle$ and $|1\rangle$ are both single-photon polarization state. However, if the entangled state $(|01\rangle + |10\rangle)/\sqrt{2}$ is between Fock states, i.e., the vacuum $|0\rangle$ and the single-photon state $|1\rangle$, it would only take one photon to generate entanglement. Thus, the net detection rate would scale in the square root manner $O(\sqrt{\eta})$ as a successful detection requires the reception of only one photon from either side. This is one of the key intuition behind TF QKD, able to break the linear key rate-transmittance bound. In fact, it is shown that the key rate of TF QKD along distance L can be reduced to the key rate of BB84 QKD along distance $L/2$, with restrictions on Eve's attack (Lucamarini et al., 2018). The restriction is removed with enhanced security analysis by Tamaki et al. (2018) and Curty et al. (2019). This thesis will mainly be discussing one of the variants of TF QKD, namely the phase-matching (PM) QKD (Ma et al., 2018), with security proof based on encoding-symmetry (Zeng et al., 2020; Jin et al., 2021).

4.2 Setups of PM QKD

This section discusses the basic setups of the PM QKD, as a variant of the TF QKD. It is essentially the non-basis-switching version of TF QKD. The security proof and the parameter estimation approaches are placed in Section 4.4. In the d-dimensional PM QKD as in protocol 6 below, the two communication parties Alice and Bob encode their key digits $\kappa_a, \kappa_b \in \{0, 1, \cdots, d-1\}$ onto the phase of coherent states, and send the encoded states to a untrusted third party Eve who is supposed to perform the Mach-Zehnder interferometry, that is, to mix the two modes through a balanced beam splitter and measure the output modes

with two single-photon detectors (SPD). Ideally, if the two incoming coherent states are of the same intensity and same phase, only the left one of the two SPDs will click (the *L*-click event); if the two incoming coherent states are of the same intensity and opposite phase, only the right one of the two SPDs will click (the *R*-click event). Hence, if they group the rounds with single *L* clicks and *R* clicks respectively, they would obtain a pair of correlated phase strings. They can then distill secure keys, respectively from the *L*-click group and the *R*-click group, and the total secure key length is the sum of that from the two groups. Fig. 4.1 illustrates the schematic setup of the d-dimensional PM QKD.

Protocol 6 ***PM QKD protocol with* d*-dimensional encoding space***

1. ***Encoding****: Alice randomly generates a key "dit" κ_a from $\{0,1,\cdots,d-1\}$ and prepares the coherent state $\left|\sqrt{\mu/2}\,\exp(i\frac{2\pi}{d}\kappa_a)\right\rangle_A$. Similarly, Bob randomly picks κ_b and prepares $\left|\sqrt{\mu/2}\,\exp(i\frac{2\pi}{d}\kappa_b)\right\rangle_B$.*

2. ***Measurement****: Alice and Bob send the two optical modes AB to an untrusted party, Eve, who is supposed to perform interference measurement and announce the detection results: no click, double click, L click or R click.*

3. ***Sifting****: After many rounds of quantum communications, Alice and Bob keep only the rounds with L or R click. They end up with two correlated d-dimensional strings.*

4. ***Parameter estimation****: From the raw data they retained, Alice and Bob estimate the security parameters and derive the secure key rate.*

5. ***Key generation****: Based on the parameter estimation results, Alice and Bob reconcile their raw strings by consuming certain secure keys. They then perform privacy amplification to extract the secure final keys from the reconciled keys.*

4.3 Review on experimental demonstrations

This section reviews the experimental demonstrations of the TF-type QKD before entering to its security analysis. TF QKD is considered a breakthrough not only because of its remarkable key rate performances, but also its feasibility of field demonstrations. In fact, ever since its first demonstration over 90 dB variable optical attenuator (Minder et al., 2019), the TF-type QKD has been successfully demonstrated over 511 km in field trials (Chen et al., 2021) and 1000 km in laboratory (Liu et al., 2023).

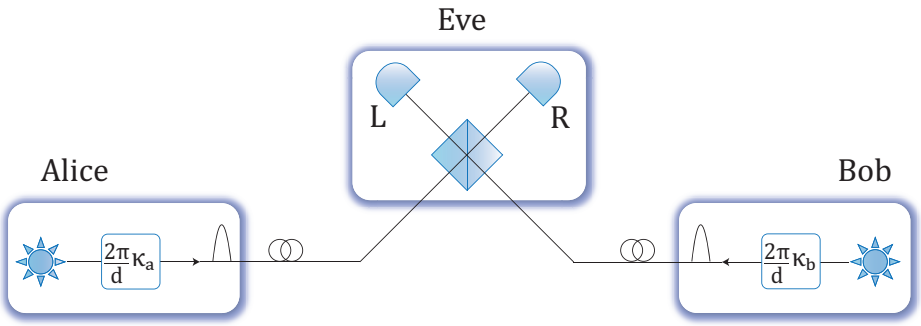


Fig. 4.1 Schematic diagram of the PM QKD protocol with d-dimensional encoding (Ma et al., 2018). Alice prepares the coherent state $\left|\sqrt{\mu/2}\ \exp(i\frac{2\pi}{d}\kappa_a)\right\rangle_A$, where $\kappa_a \in \{0,1,\cdots,d-1\}$. Similarly Bob prepares $\left|\sqrt{\mu/2}\ \exp(i\frac{2\pi}{d}\kappa_b)\right\rangle_B$. They send the two coherent states to interfere at an untrusted measurement site. Ideally, if the phase difference $\frac{2\pi}{d}|\kappa_a-\kappa_b|=0$, the detector gives a single L click. If $\frac{2\pi}{d}|\kappa_a-\kappa_b|=\pi$, the detector gives a single R click.

The experimental implementations of the TF-type QKD is still challenging due to the long-distance single-mode interference required. This challenge is unprecedented in the usual polarisation-encoding QKD where the information is encoded onto the qubit subspace from the relative polarization between two modes. The two adjacent optical modes would serve as the reference for each other. However, in the phase-encoding TF QKD, to grant high interference visibility, the two incident light fields from Alice and Bob must have correlated phases at very long distances (Lucamarini et al., 2018). This imposes stringent requirements on the stability of the system since any drifts in the local phases would impair the key generation rate.

It is thus crucial to stabilise carefully the corresponding phase drift and identify the phase references. In practical TF QKD experiments, the system is usually pre-run for several rounds in order to adjust the phase reference misalignment (Minder et al., 2019). Besides, the phase-locking technique with optical phase locking loop (OPLL) (Santarelli et al., 1994; Ferrero and Camatel, 2008) can be employed to stabilise the phase drift with feedback control. In Section 4.4 below, the reference-frame-independence design of the TF-variant PM QKD will be introduced to completely remove the necessity of phase reference setup.

4.4 Reference-frame-independent design of PM QKD

From the last section it can be seen that the practicality of the TF QKD is significantly limited by the phase-reference misalignment. Whilst the phase-locking technique stabilises

the phase drifts within the channels, the intrinsic misalignment between Alice and Bob's phase references is another mismatch to be tackled. Phase post-compensation is a feasible approach (Ma et al., 2018; Zeng et al., 2020; Ma and Razavi, 2012), where extra phase randomization is introduced and the experimental data with aligned phase slices are post-selected afterwards. Since the intrinsic phase mismatch is relatively fixed, the data with aligned phase slices will be suitable for key generation. However, in this section, it will be shown that the approaches to setup a aligned phase reference, no matter in prior or posterior, can be completely removed given the reference-frame-independence design (Laing et al., 2010; Lee et al., 2020). This brings about the author's work (Jin et al., 2021) on the reference-frame-independent design of PM QKD[1], which shows that any fixed or slowly fluctuating phase misalignment, completely controlled by the adversary in the worst case, can be coped by high-dimensional encoding without any experimental complication.

If looking at the essence of the phase post-compensation technique, the discrete randomization in fact expands the key space from dimension two to high dimension. After the detection stage, the key space is reduced back to two-dimensional through post-selection of the matching phases. The variation in the key-space dimension complicates the protocol. Naturally, the post-selection stage can be removed by implementing high-dimensional key space from the beginning. The potential of high-dimensional protocols against channel errors is already demonstrated for prepare-and-measure protocols, where, in contrast with the conventional two-dimensional BB84 protocol which tolerates an error rate of 11% , the four-dimensional BB84 protocol can tolerate up to 35.6% (Chau, 2005), and the 16-dimensional BB84 protocol can tolerate 45.4% (Chau, 2005). These results shine light on introducing high-dimensional PM QKD to combat errors introduced by misalignment.

The focus is thus on the d-dimensional PM QKD protocol 6 which encodes key information onto d uniformly separated phase slices and matches phases via interference detection at an untrusted measurement site. By extending the encoding symmetry approach (Zeng et al., 2020) to dimension d, making use of the d-dimensional complementarity analysis in Section 3.1.2, the security analysis of the d-dimensional PM QKD is presented and its reference-frame independence when d is large can be demonstrated: it is completely immune to any degree of fixed-phase misalignment and robust to small phase fluctuation, where these disturbances are assumed to be controlled by the adversary. In fact, with encoded phases spanning the unit circle, the error statistics at arbitrary fixed phase reference difference can be recovered and treated separately, from which the misalignment angle can be identified. As the high-dimensional PM QKD employs the same setup as the two-dimensional PM QKD

[1]This section is based on the author's work (Jin et al., 2021) with contributions from other collaborators. The author finished the security proofs and performed the simulations on the protocol performances. P. Zeng and X. Ma assisted with the security proof and results presentation. R.V. Penty supervised the project.

whilst removing the necessity of phase post-compensation, it is in fact a pragmatic approach to mitigate the effect of reference mismatch.

First look at the security of QKD protocols with the symmetric-encoding property. As its name implies, the encoding possesses certain discrete symmetries in the sense that the encoded states are indistinguishable when Alice and Bob applied the same encoding operations. In other words, Eve is only able to distinguish the relative encoding between Alice and Bob, yet by knowing the relative encoding Alice and Bob each can determine the key encoded by the other. This gives Alice and Bob advantages over Eve, enabling them to distill secure keys with no phase error (Zeng et al., 2020). It is then shown that the PM QKD (in fact all TF-type protocols) falls into the category of symmetric-encoding QKD, and the parameter estimation can be tackled by introducing discrete phase randomisation. It will be demonstrated with simulation that a 17-dimensional protocol is completely immune to any degree of fixed misalignment and robust to slow phase fluctuations.

Notice that throughout the analysis d is taken to be a prime number, with reasons to be clarified in Section 4.4.5.

4.4.1 Symmetric encoding protocol in high dimension

First consider the symmetric encoding property of the d-dimensional PM QKD (Zeng et al., 2020), with a schematic diagram in Fig. 4.2. In a d-dimensional symmetric encoding QKD, Alice and Bob start with a bipartite state ρ_{AB}. They independently generate a random key "dit" κ_a and κ_b from $\{0,1,\cdots,d-1\}$ and apply $U(\kappa_{a(b)}) := U^{\kappa_{a(b)}}$ to their subsystem A and B respectively, where $U^d = I$. Notice that in PM QKD (also all the TF-type QKD), the encoding operator U is the rotation operator

$$U = e^{i\frac{2\pi}{d}a^\dagger a}, \tag{4.1}$$

that rotates a coherent state by an angle of $2\pi/d$. The modulated state $\rho'_{AB}(\kappa_a,\kappa_b)$ can be written as

$$\rho'_{AB}(\kappa_a,\kappa_b) = [U_A(\kappa_a)\otimes U_B(\kappa_b)]\rho_{AB}[U_A(\kappa_a)\otimes U_B(\kappa_b)]^\dagger, \tag{4.2}$$

which is then sent to the third party Eve who is supposed to make announcements regarding their key difference $(\kappa_a - \kappa_b) \bmod d$ based on her measurement results. Based on the announcements from Eve, Alice and Bob can modify their key dits to generate a pair of correlated key strings, with information reconciliation and privacy amplification to generate the final secure key.

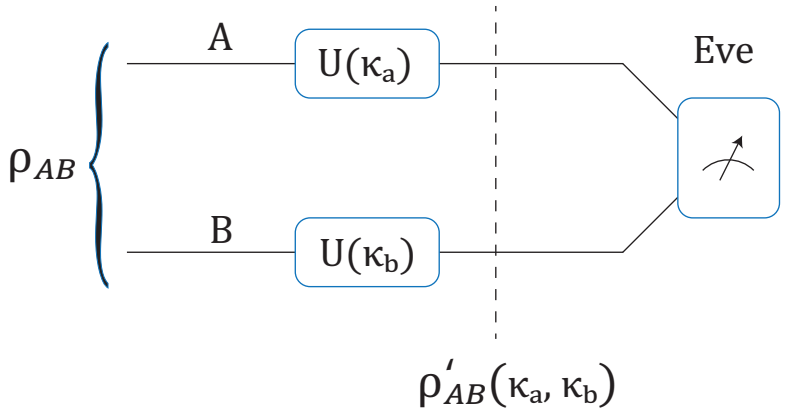


Fig. 4.2 Schematic diagram of the d-dimensional symmetric encoding QKD, where κ_a, κ_b take values in $\{0,1,\cdots,d-1\}$. Alice and Bob share the bipartite state ρ_{AB} and each applies a unitary operation $U(\kappa) := U^{\kappa}$ according to their key values κ_a and κ_b. The untrusted party Eve is supposed to make announcements regarding the key difference $(\kappa_a - \kappa_b) \bmod d$ based on the measurements at her own control.

The setup extends the binary symmetric encoding protocol in (Zeng et al., 2020).

A pure state $|\psi\rangle_{AB}$ on AB is called an l-symmetric state, for l in $\{0,1,\cdots,d-1\}$, if it is the l-th eigenstate of $U_A \otimes U_B$:

$$(U_A \otimes U_B)|\psi\rangle_{AB} = \gamma_d^l |\psi\rangle_{AB}, \tag{4.3}$$

where $\gamma_d = e^{i2\pi/d}$. For a mixture of l-symmetric states, $\rho_{AB} = \sum_j p_j \left|\psi_l^{(j)}\right\rangle\left\langle\psi_l^{(j)}\right|$, the relation holds:

$$\rho'_{AB}(\kappa_a,\kappa_b) = [I_A \otimes U_B(\kappa_b - \kappa_a)]\rho_{AB}, \tag{4.4}$$

where the subtraction is under modulus d. Hence, the encoded mixture l-symmetric states are indistinguishable as long as the two key dits κ_a and κ_b differ by the same number. As a result, the raw key dit κ_a is "hidden" in the encoded state $\rho'_{AB}(\kappa_a,\kappa_b)$ as long as the pre-shared state ρ_{AB} is a mixture of pure symmetric states.

To give a more rigorous argument, the entanglement-based symmetric encoding protocol can be resorted, as shown in Fig. 4.3 below. In the entanglement-based protocol, Alice and Bob each holds an ancillary system A' and B' in the state $|+\rangle_d = \sum_{j=0}^{d-1}|j\rangle$. This serves as the control dit of the encoding operator U, i.e. transferring the classical random encoding to a quantum control operation. Its equivalence with the prepare-and-measure symmetric encoding protocol follows if the final measurement is moved prior to the control operation.

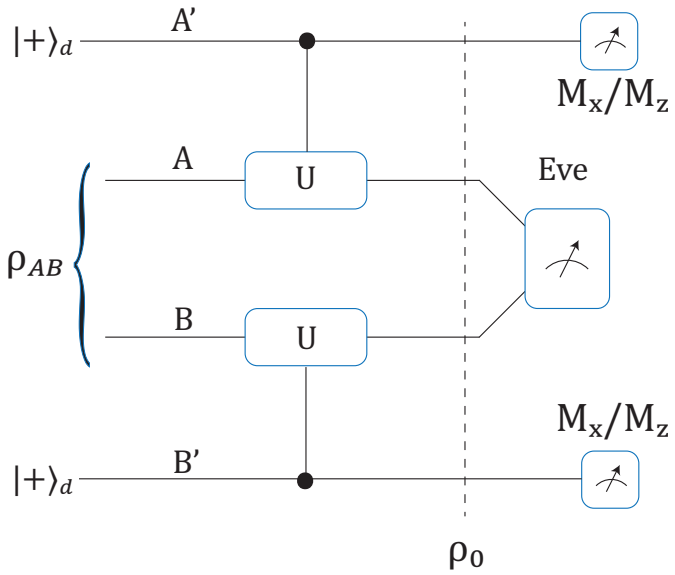


Fig. 4.3 Schematic diagram of the entanglement-based d-dimensional PM QKD, where ρ_{AB} is a bipartite state on two optical modes, and the encoding operation U rotates the coherent state by $2\pi/d$. The optical mode is phase rotated by $2\pi k/d$ if the k-th control dit is triggered. The encoded state ρ_0 is sent to the untrusted Eve for measurement, who is supposed to announce the key difference $(\kappa_a - \kappa_b)$ mod d, where κ_a and κ_b refer to the control dits triggered in $A'B'$. Alice and Bob distill secure keys from the qudit systems A' and B'. The setup extends the binary entanglement-based symmetric encoding protocol in (Zeng et al., 2020).

Alice and Bob send the shared state ρ_{AB} through the controlled encoding operation, where

$$C_{A'A}(U) = \sum_{j=0}^{d-1} |j\rangle_{A'}\langle j| \otimes U_A^j, \tag{4.5}$$

and similarly for $C_{B'B}(U)$. The unitary encoding operation is d-rotation symmetric, i.e., $U^d = I$. They then send the systems A and B further to Eve for detection. At the end of the quantum communications, they share N pairs of qudit systems for key generation.

Following the security proof of d-dimensional QKD given in Section 3.1.2, taking A' as the key generation system and B' as the ancillary system, the X-measurement results of A' is to be determined with the knowledge of that of B'. This can be done as long as the originally separate $|+\rangle_{A'}$ and $|+\rangle_{B'}$ are now entangled after the symmetric encoding operations. In other words, the shared state ρ_{AB} needs to give the same encoded state after different encoding operations, i.e. ρ_{AB} being the eigenstate of $U_A \otimes U_B$.

Since $(U \otimes U)^d = I$, the eigenvalues of $(U \otimes U)$ are $\{\gamma_d^j := \exp(i\frac{2\pi}{d}l)\}_{l=0}^{d-1}$. The eigenspace of γ_d^l is denoted by $\mathscr{H}^{(l)}$. Denote a generic state $|\psi\rangle \in \mathscr{H}^{(l)}$ as $|\psi_l\rangle$, hence

$$(U \otimes U)|\psi_l\rangle = \gamma_d^l |\psi_l\rangle. \tag{4.6}$$

Protocol 7 **High-dimensional symmetric-encoding protocol**

1. ***State preparation****: Alice and Bob share a state ρ_{AB} at the beginning of each run. They initialize their qudits A' and B' in $|+\rangle_d$. They apply the control gate $C_{A'A}(U)$ and $C_{B'B}(U)$ respectively.*

2. ***Measurement****: Alice and Bob send ρ_{AB} to an untrusted party, Eve, who is supposed to perform joint measurement and announce the detection results.*

3. ***Sifting****: Given a specific announcement of Eve, Alice and Bob keep or discard the qudits of systems A' and B'. Alice and Bob perform the above steps for many rounds and end up with a joint $2N$-qudits state $\rho_{A'B'} \in (\mathscr{H}_A' \otimes \mathscr{H}_B')^{\otimes N}$.*

4. ***Key generation****: Alice and Bob perform local Z-measurements on $\rho_{A'B'}$ to obtain two correlated raw key strings κ_A and κ_B. They reconcile the key string to κ_{rec} by an encrypted classical channel, consuming l_{ec}-bit keys.*

First consider the case when a l-symmetric state $|\psi_l\rangle_{AB}$ is the input state of the entanglement-based protocol. The initial state is

$$\begin{aligned} |{+}{+}\rangle_{A',B'}|\psi_l\rangle_{A,B} &= \frac{1}{d}\sum_{j,k=0}^{d-1}|jk\rangle_{A',B'}|\psi_l\rangle_{A,B} \\ &= \frac{1}{\sqrt{d}}\sum_{u=0}^{d-1}\left|\Phi_{u,0}\right\rangle_{A',B'}|\psi_l\rangle_{A,B}, \end{aligned} \tag{4.7}$$

where the $\left|\Phi_{u,0}\right\rangle$ denotes the generalised Bell state in dimension d. Its definition and the identities used in the derivation below are shown in Appendix A.2.

After the encoding unitary operation, $C_{A'A}(U)$ and $C_{B'B}(U)$, the state becomes

$$|\Psi\rangle_{A',B',A,B} = \frac{1}{\sqrt{d}}\sum_{u=0}^{d-1}\left|\Phi_{u,l}\right\rangle_{A',B'}\left|\psi_l^u\right\rangle_{A,B}, \tag{4.8}$$

here $\left|\psi_l^u\right\rangle := (I\otimes U^u)|\psi_l\rangle$. To derive Eq. (4.8), the following property has been applied:

$$[C_{A'A}(U)\otimes C_{B'B}(U)]|\Phi_{u,v}\rangle_{A',B'}|\psi_l\rangle_{A,B} = \left|\Phi_{u,v+l}\right\rangle_{A',B'}\left|\psi_l^u\right\rangle_{A,B}. \tag{4.9}$$

In this case, the space of A' and B' are spanned by $\{\Phi_{u,l}\}_{u=0}^{d-1}$. Note that

$$\mathrm{Tr}\left[\Phi_{u,l}\left|\tilde{j},\tilde{k}\right\rangle_{A1,B1}\left\langle\tilde{j},\tilde{k}\right|\right] = \frac{1}{d}\delta_{j,l-k}, \tag{4.10}$$

which is irrelevant of u. Therefore, if Alice and Bob perform X-measurement on A' obtaining result l_a, the X-measurement result l_b is directly related as $l_a = l - l_b \bmod d$. This implies that the protocol is completely secure as long as Alice and Bob share l-symmetric states for a fixed l. Hence, the security of the high-dimensional symmetric encoding QKD is derived for symmetric states.

However, in the general setup, the shared state ρ_{AB} is usually not a mixture of pure symmetric states, but a mixture of different symmetric states, that is,

$$\rho_{AB} = \sum_{l=0}^{d-1}\sum_j p_l^{(j)}\left|\psi_l^{(j)}\right\rangle\left\langle\psi_l^{(j)}\right|, \tag{4.11}$$

where $\left|\psi_l^{(j)}\right\rangle$ are the l-symmetric states and $\sum_{l=0}^{d-1}\sum_j p_l^{(j)} = 1$. This mixture source is equivalent to Alice and Bob preparing l-symmetric states for probability of $\sum_j p_l^{(j)}$ for each run. However, the parity information, i.e. which symmetric state is sent each round, is not known to Alice and Bob (and known by Eve in the worst case scenario). Hence, they cannot

deal with each symmetric state separately, and thus there is no longer perfect privacy. The phase-error rate vector is defined as

$$\vec{E}_{ph} = \left[\frac{N_0}{N}, \frac{N_1}{N}, \cdots, \frac{N_{d-1}}{N}\right], \tag{4.12}$$

where N_l is the number of detections caused by l-symmetric states. According to the key-rate formula Eq. (3.15) of d-dimensional QKD, the asymptotic key rate of the d-dimensional symmetric encoding protocol is

$$r = \log_2 d - H_2(\vec{E}_{bit}) - H_2(\vec{E}_{ph}) \text{ bits}. \tag{4.13}$$

4.4.2 High-dimensional PM QKD with continuous randomization

The high-dimensional entanglement-based PM QKD falls into the category of symmetric encoding protocol discussed above. The encoding operation U is given by

$$U = e^{i\frac{2\pi}{d}a^\dagger a}, \tag{4.14}$$

where a is the annihilation operator. It is clear that U is d-rotational symmetric, i.e. $U^d = I$. It can be seen that, when applied on the Fock state $|n\rangle$, this operation adds an additional phase $\exp(2\pi in/d)$.

The key rate of the d-dimensional PM QKD is thus given by Eq. (4.13), yet it cannot be used directly in practice as the phase-error vector $\vec{E}_{ph}$ based on the hypothetical qudit systems is not experimentally accessible. This boils down to the estimation of the phase-error vector, i.e., the yields of different photon-number components. A continuous phase randomisation can thus be applied to the encoded coherent states to generate mixture of Fock states. This results in the following d-dimensional entanglement-based PM QKD protocol with continuous randomization:

Protocol 8 ***High-dimensional entanglement-based PM QKD with continuous randomization***

1. ***State preparation****: Alice and Bob prepare the coherent state* $\left|\sqrt{\mu/2}\, e^{i\phi_a}\right\rangle_A \otimes \left|\sqrt{\mu/2}\, e^{i\phi_b}\right\rangle_B$ *on two optical modes A and B, where* ϕ_a *and* ϕ_b *are selected randomly from* $[0, 2\pi)$*, and* μ *taken from multiple values as in decoy methods. They initialize their qudits* A' *and* B' *in* $|+\rangle_d := \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle$*. They apply the control gate* $C_{A'A}(U)$ *and* $C_{B'B}(U)$ *respectively, where* U *rotates a coherent state by* $2\pi/d$*.*

2. ***Measurement**: Alice and Bob send the two optical modes AB to an untrusted party, Eve, who is supposed to perform joint measurement and announce the detection results: no-click, double-click, L-click or R-click.*

3. ***Sifting**: After many rounds of quantum communications, Alice and Bob keep only the rounds with L or R click. They announce the random phases ϕ_a and ϕ_b publicly and keep only the rounds where $|\phi_a - \phi_b| \in \{k\frac{2\pi}{d}\}_{k=0}^{d-1}$. They end up with a joint $2N$-qudits state $\rho_{A'B'} \in (\mathscr{H}_A' \otimes \mathscr{H}_B')^{\otimes N}$.*

4. ***Parameter estimation**: Alice and Bob estimate the phase-error vector $\vec{E}_{ph}$ with decoy states.*

5. ***Key generation**: Alice and Bob perform local Z-measurements on $\rho_{A'B'}$ to obtain two correlated raw key strings κ_A and κ_B. They reconcile the key string to κ_{rec} by an encrypted classical channel, consuming l_{ec}-bit keys. They perform privacy amplification according to the phase-error vector to generate the final keys.*

Notice that after Eve's announcement of the detection results, Alice and Bob announce the random phases and post-select the phase-matched rounds where $|\phi_a - \phi_b| \in \{k\frac{2\pi}{d}\}_{k=0}^{d-1}$. This is valid since Alice and Bob are essentially tagging the rounds based on their random phase difference, which is compatible with the random phase announcement. (Ma and Razavi, 2012; Ma et al., 2018; Maeda et al., 2019).

For states with $\phi_a - \phi_b = \delta$, the continuous randomization in fact generates the input state:

$$\begin{aligned}&\frac{1}{2\pi}\int_0^{2\pi} d\phi \left|\sqrt{\mu/2}\, e^{i\phi}\right\rangle_A \left\langle\sqrt{\mu/2}\, e^{i\phi}\right| \otimes \left|\sqrt{\mu/2}\, e^{i(\phi+\delta)}\right\rangle_B \left\langle\sqrt{\mu/2}\, e^{i(\phi+\delta)}\right| \\ &= \sum_{k=0}^{\infty} P_\mu(k) \left|\bar{k}^\delta\right\rangle_{AB} \left\langle\bar{k}^\delta\right|,\end{aligned} \tag{4.15}$$

where $P_\mu(k) = \exp(-\mu)\mu^k/k!$ is the Poisson distribution. The k-photon state $\left|\bar{k}^\delta\right\rangle_{AB}$ is

$$\left|\bar{k}^\delta\right\rangle_{AB} = \frac{(a^\dagger + e^{i\delta} b^\dagger)^k}{\sqrt{2^k k!}} |00\rangle_{AB}, \tag{4.16}$$

which is a k-symmetric state. The phase-error rate vector can thus be defined with entries:

$$\vec{E}_{ph}(k) = \sum_{n=0}^{\infty} q_{nd+k}, \quad k \in \{0, \cdots, d-1\}, \tag{4.17}$$

where q_k is the fraction of detection events caused by $\left|\bar{k}^{\delta}\right\rangle_{AB}$.

Since Fock states are invariant with intensity μ, their yields do not vary with μ, and the decoy methods can be applied given the overall gain Q_μ (Lo et al., 2005; Wang, 2005):

$$Q_\mu = \sum_{k=0}^{\infty} P_\mu(k) Y_k, \tag{4.18}$$

and the fraction of detection is given by

$$q_k^\mu = P_\mu(k) \frac{Y_k}{Q_\mu}. \tag{4.19}$$

Although it requires infinite decoy levels to estimate each q_l exactly, since the optimal coherent light intensity is far below 1, three or more-photon components are negligible in the source, and hence in the detected signals. Therefore, three decoy levels are enough to estimate the phase-error vector $\vec{q}_\mu$ (see also the finite-size analysis in (Zeng et al., 2020)) and the detection fraction $\vec{q}_\mu$ is to be estimated with decoy states based on Eq. (4.18) and (4.19).

4.4.3 High-dimensional PM QKD with discrete randomization

It is a common practice to approximate the ideal continuous randomization with discrete randomization (Lo et al., 2005; Cao et al., 2015; Ma et al., 2018). In the state preparation stage of the d-dimensional entanglement-based PM QKD, instead of continuously randomizing the phase of the coherent states, Alice and Bob apply a D-slice discrete phase randomization for a large D, and post-select the phase-matched rounds similarly.

For the rounds where Alice and Bob share a phase reference difference of δ, they generate the input state as a mixture of "pseudo"-Fock states:

$$\begin{aligned} &\frac{1}{D}\sum_{j=0}^{D-1} \left|\sqrt{\mu/2}\, e^{i\frac{2\pi j}{D}}\right\rangle_A \left\langle\sqrt{\mu/2}\, e^{i\frac{2\pi j}{D}}\right| \otimes \left|\sqrt{\mu/2}\, e^{i(\frac{2\pi j}{D}+\delta)}\right\rangle_B \left\langle\sqrt{\mu/2}\, e^{i(\frac{2\pi j}{D}+\delta)}\right| \\ &= \sum_{k=0}^{\infty} P_D^\mu(k) \left|\bar{\lambda}_k^{\delta}\right\rangle_{AB} \left\langle\bar{\lambda}_k^{\delta}\right|, \end{aligned} \tag{4.20}$$

where

$$\begin{aligned} \left|\bar{\lambda}_k^{\delta}\right\rangle &= \frac{e^{-\mu/2}}{\sqrt{P_\mu(k)}} \sum_{n=0}^{\infty} \frac{(\sqrt{\mu})^{nD+k}}{\sqrt{(nD+k)!}} \left|\overline{nD+k}^{\delta}\right\rangle \\ P_D^\mu(k) &= \sum_{n=0}^{\infty} \frac{\mu^{nd+k} e^{-\mu}}{(nd+k)!}, \end{aligned} \tag{4.21}$$

with k-photon state $\left|\bar{k}^{\delta}\right\rangle$ defined in Eq. (4.16).

The k-pseudo Fock state $\left|\bar{\lambda}_k^{\delta}\right\rangle$ is also a k-symmetric state of $U \otimes U$, so the security analysis still applies. It is however less favoured than Fock states since for moderate D it varies with intensity μ, thus enabling Eve to discriminate signal states with decoy states, cracking the decoy method (Lo et al., 2005). It is therefore required that D is large so that the yield of $\left|\bar{\lambda}_k^{\delta}\right\rangle$ approximates the yield of $\left|\bar{k}^{\delta}\right\rangle$, which is invariant with the intensity. Denote the yield and the detection fraction of the non-ideal k-th symmetric state as Y_{λ_k} and q_{λ_k}. In (Zeng et al., 2020), a bound between the deviation of Y_{λ_1} and q_{λ_1} from Y_1 and q_1 is given, and can be straightforwardly extended to general k-photon states:

$$\begin{aligned} |Y_k - Y_{\lambda_k}^{\mu}| &\leq \sqrt{\frac{\mu^D k!}{(D+k)!}} \\ |q_k^{\mu} - q_{\lambda_k}^{\mu}| &\leq \frac{\mu^{D/2+k} e^{-\mu}}{Q_{\mu}\sqrt{(D+k)!/k!}}, \end{aligned} \tag{4.22}$$

A straightforward calculation reveals that Eq. (4.22) gives a tighter bound for multi-photon fractions than single-photon fraction. Hence it is sufficient to check the accuracy of single-photon fraction estimation. Denote the transmittance from Alice or Bob to Eve as η. In the first-order limit where the gain $Q_{\mu} \approx \eta\mu$ and yield $Y_l \approx l\eta$, Table 4.1 below illustrates the estimation inaccuracy of single photon components in terms of $|q_1^{\mu} - q_{\lambda_1}^{\mu}|/q_1^{\mu}$ at transmittance $\eta = 10^{-6}$ for 8 to 16 phase slices. The light intensity μ is taken as 0.1, which is a moderate value around the optimal values given in the simulations in Section 4.4.4. The 10^{-6} transmittance is chosen since PM QKD can reach at most around 500 km for a -0.2 dB/km attenuating fiber and 20% detectors. The minimum transmittance from Alice to Eve is therefore:

$$\eta = 10^{-0.2\times 250/10} \times 0.2 = 2 \times 10^{-6} \tag{4.23}$$

From Table 4.1, it can be seen that more than a 10-phase randomization is sufficient for an estimation of single-photon fraction with less than 10^{-3} inaccuracy. The 16-phase randomization in the original two-dimensional PM QKD is thus conservative.

Table 4.1 Estimation inaccuracy of single-photon fraction in PM QKD with discrete randomization at $\eta = 10^{-6}$

	$D = 8$	$D = 10$	$D = 12$	$D = 14$	$D = 16$
$\Delta q_1/q_1$	0.17	1.6×10^{-3}	1.3×10^{-5}	8.7×10^{-8}	5.3×10^{-10}

The final version of the d-dimensional PM QKD protocol with discrete randomisation for parameter estimation is given as the following, with d being a prime number:

Protocol 9 ***High-dimensional PM QKD protocol with parameter estimation***

1. ***Encoding****: Alice randomly generates a key "dit" κ_a from $\{0,1,\cdots,d-1\}$ and a random intensity μ_a as in the decoy method. She prepares the coherent state $\left|\sqrt{\mu_a/2}\, e^{i\frac{2\pi}{d}\kappa_a}\right\rangle_A$. Similarly, Bob randomly picks κ_b and μ_b, and prepares $\left|\sqrt{\mu_b/2}\, e^{i\frac{2\pi}{d}\kappa_b}\right\rangle_B$.*

2. ***Discrete phase randomization****: Alice and Bob independently phase randomize their coherent states for a large enough phase slice number D. That is, they randomly pick ϕ_a and ϕ_b from $\{j\frac{2\pi}{D}\}_{j=0}^{D-1}$ and prepare $\left|\sqrt{\mu_a/2}\, e^{i(\phi_a+\frac{2\pi}{d}\kappa_a)}\right\rangle_A$ and $\left|\sqrt{\mu_b/2}\, e^{i(\phi_b+\frac{2\pi}{d}\kappa_b)}\right\rangle_B$ respectively.*

3. ***Measurement****: Alice and Bob send the two optical modes AB to an untrusted party, Eve, who is supposed to perform interference measurement and announce the detection results: no click, double click, L click or R click.*

4. ***Sifting****: After many rounds of quantum communications, Alice and Bob keep only the rounds with L or R click. They announce the random intensities and phases μ_a, ϕ_a and μ_b, ϕ_b publicly. They keep only the rounds with $\mu_a = \mu_b$. For each intensity group, they group the rounds based on their absolute phase difference $|\phi_a - \phi_b| \in \{k\frac{2\pi}{d}\}_{k=0}^{d-1}$ and perform separate post-processing.*

5. ***Parameter estimation****: From each group of the raw data they retained, Alice and Bob retrieve the gain Q_μ and the bit-error rate vector $\vec{E}_{bit}^{\mu}$. They estimate the phase-error rate vector $\vec{q}_\mu$ based on Eq.* (4.18) *and* (4.19)*.*

6. ***Key generation****: Based on the parameter estimation results, Alice and Bob reconcile their raw strings by consuming certain secure keys. They then perform privacy amplification to extract the secure final keys from the reconciled keys.*

The final key-rate formula can be expressed as:

$$r = \frac{d}{D} Q_\mu [\log_2 d - H_2(\vec{E}_{bit}^{\mu}) - H_2(\vec{q}_\mu)], \tag{4.24}$$

where all the parameters can be retrieved from experiments. Notice the d/D factor signifies the loss due to phase-randomisation post-selection. When $d = 2$, this essentially introduces a significant sifting factor $2/D$. For high-dimensional PM QKD that $d \geq 10$, however, simply putting $D = d$ can render the post-selection to be omitted since ϕ_a and ϕ_b are themselves code phases. This manifests the simplicity in implementing high-dimensional PM QKD.

4.4.4 Reference-frame independence of high-dimensional PM QKD

This section demonstrates, with simulation, that without phase post-compensation, the high-dimensional PM QKD sufficiently achieves reference-frame independence (Laing et al., 2010). Two practical scenarios are considered: fixed-phase misalignment and small phase fluctuation. The fixed-phase misalignment corresponds to the intrinsic reference system mismatch and the phase fluctuation is a random phase drift added by the fiber that is independent of the encoding, both assumed to be controlled by the adversary. By virtue of the encoding symmetry, the phase-error rate is decoupled with channel noise (Zeng et al., 2020), that is, the bit-error patterns. Hence, phase misalignment affects only the bit-error rate, whilst the phase-error rate depends merely on light intensity. It is shown that fixed phase misalignment does not increase the bit-error rate of the high-dimensional PM QKD. Although phase fluctuation does add to its bit-error rate, the decrease in key rate is smaller than that of two-dimensional PM QKD due to the concavity of Shannon-entropy function.

To justify our arguments, the asymptotic performance of 17-dimensional PM QKD against two-dimensional without phase post-compensation is simulated. The simulation model is similar to that illustrated in Appendix B of (Ma et al., 2018), with parameters given in Table 4.2. A detailed description is placed in Appendix B.1. The key-rate formula generally follows Eq. (4.24).

The high-dimensional PM QKD will first be demonstrated to achieve almost completely immunity to fixed-phase misalignment, in clear contrast with the two-dimensional PM QKD, which is sensitive to phase-reference mismatch. In the two-dimensional PM QKD, the worst case scenario is that Alice and Bob hold phase references that differ by $\delta = \pi/2$. The protocol would not correlate Alice and Bob's keys. Suppose Alice sends phase A_0, it can be seen that no matter Bob sends B_0 or B_1, the interference result would highly likely be double clicks, and any single click does not provide too much information that helps Alice to distinguish Bob's key bit. However, in a d-dimensional PM QKD, suppose the phase references are differed by $\delta + 2k\pi/d$ with $\delta \in [0, 2k\pi/d)$ and k being integer. Note the $2k\pi/d$ term results only in a deterministic shift between key phases, and therefore can be tackled by classical post-processing. Hence, the effective misalignment only ranges in $[0, 2k\pi/d)$, which gets smaller as d increases, as shown in Fig. 4.4 below. What is more, for the 17-dimensional PM QKD, it is plotted in Fig. 4.5 that the key rate at 100 km against misalignment ranging from 0 to $2\pi/17$. It can be seen that the lowest key rate is reached when the misalignment is $\pi/34$, which is one fourth between two key phases. This is reasonable since when the misalignment is half between two key phases at $\pi/17$, the A_0 phase would be determinedly matched to B_8 as they differ by π, causing R click. Hence, $\pi/34$ is the worst-case misalignment right between the two deterministic misalignment 0 and $\pi/17$. It can be seen from Fig. 4.5 that

the effect of the fixed misalignment to the key rate of the 17-dimensional PM QKD is of 0.1% scale, and hence negligible in practice.

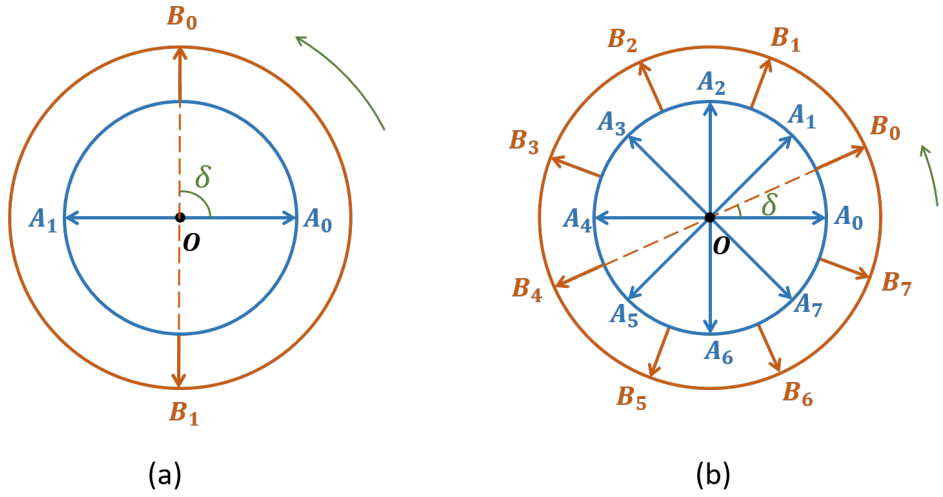


Fig. 4.4 Encoding circles of low- and high-dimensional PM QKD against worst-case misalignment. In the low-dimensional case, both encoding phases are far away from the deviated phase locations, thus giving much uncertainty. Yet in the high-dimensional case, the deviated phases are closer to key phases, enabling the error correction to coordinate the phase shift.

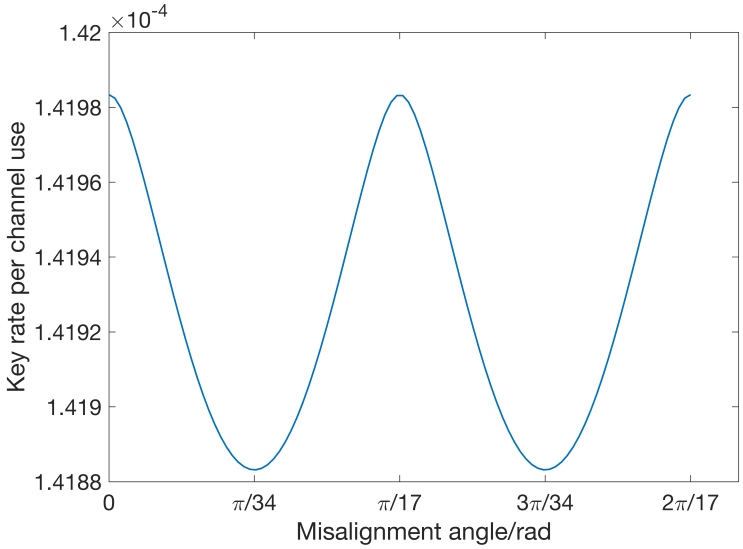


Fig. 4.5 Key rate of the 17-dimensional PM QKD at 100 km against fixed misalignment. The $\pi/17$ misalignment correlates the opposite key phases by R clicks, and hence giving almost no effect on the key rate. The worst-case misalignment is reached at $\pi/34$, whose relative effect is negligible.

To justify the above argument, the asymptotic performance of the two-dimensional PM QKD against the 17-dimensional PM QKD is simulated under various fixed misalignment compared with the linear repeaterless bounds (Pirandola et al., 2017; Takeoka et al., 2014). The linear bound used here is the PLOB bound (Pirandola et al., 2017), which corresponds to the secret key capacity of the lossy channel. As shown in Fig. 4.6 below, without phase post-compensation, the key rate of two-dimensional PM QKD decreases continuously as the fixed misalignment increases. When the misalignment reaches $\pi/4$, the key rate of binary PM QKD generally discounts by a factor of 10, and when it further increases to $\pi/3$, the two-dimensional PM QKD cannot break the linear bound anymore. In clear contrast, the 17-dimensional PM QKD is almost completely immune to any phase misalignment. As can be seen in the figure, the 17-dimensional PM QKD performs almost identically under $\pi/34$ misalignment (the worst case) and no misalignment. Its key rate is similar to that of the perfectly aligned two-dimensional PM QKD, despite a slight decrease in the maximal reachable distance (mainly due to the dark count increasing the bit-error loss of the 17-dimensional PM QKD.) On the other hand, the two-dimensional PM QKD clearly cannot generate any keys under $\pi/2$ misalignment.

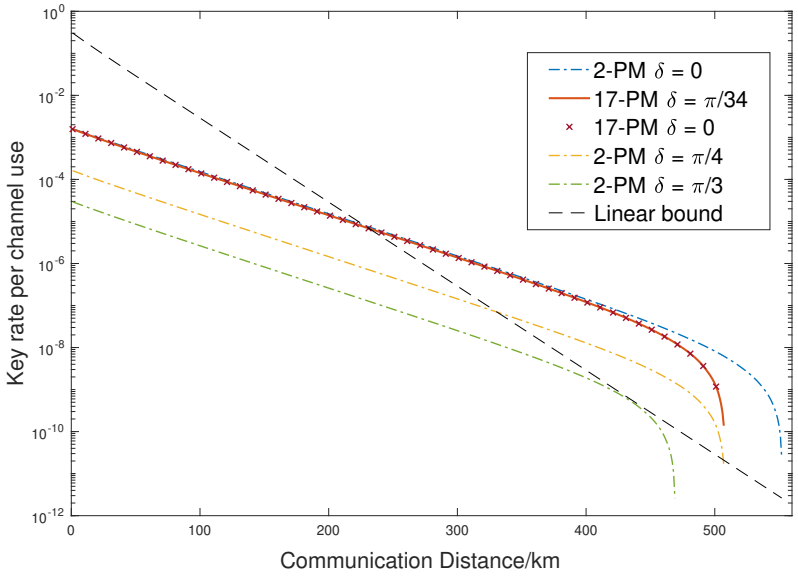


Fig. 4.6 Rate-distance performance of two- and 17-dimensional PM QKD against various fixed-phase misalignment, in comparison with the linear key-rate bounds (Pirandola et al., 2017; Takeoka et al., 2014). The linear bound used in the plot is the PLOB bound (Pirandola et al., 2017). The key-rate performance of the 17-PM under the worst-case $\pi/34$ misalignment is similar to that of the 2-PM with no misalignment. The key rate of 2-PM decreases gradually and cannot generate keys at the worst-case $\pi/2$ misalignment.

Table 4.2 Summary of parameters used in the simulation of high-dimensional PM QKD

Parameters	**Values**
fiber attenuation α	0.2 dB/km
Dark count rate p_d	1×10^{-8}
Error correction efficiency γ	0.95
Detector efficiency η_d	20%
No. of phase slices D	16

The effect of a slow phase fluctuation is now considered. When phase fluctuation is applied, the original code phases can no longer be recovered exactly since the fluctuation is random within a range of angles. In reality the phase fluctuation may come from the sources and the fiber, whilst the latter is length dependent. To illustrate our ideas, a simplified model is adopted that during each round a random noisy phase (independent of encoding) uniformly distributed in $[-\phi_{lim}, \phi_{lim}]$ is added to the encoded coherent state, for Alice and Bob respectively. The focus is on the term $\log_2(d) - H(\vec{E}_{bit})$, which denotes the mutual information between Alice and Bob, and the term $H(\vec{q_\mu})$, which denotes the cost due to phase-error rate, i.e., the leak of raw key information. Fixing the communication distance at 300 km, it is compared in Fig. 4.7a the change in mutual information $\log_2(d) - H(\vec{E}_{bit})$ and privacy leakage $H(\vec{q_\mu})$ for two- and 17-dimensional PM QKD against the phase fluctuation range ϕ_{lim}. The light intensity μ is fixed at 0.2 and 0.03, respectively, for the two- and 17-dimensional, which is around the optimal value under no fluctuation shown in Fig. 4.7c. It can be seen that the privacy leakage term $H(\vec{q_\mu})$ remains unchanged for both the two-dimensional and 17-dimensional regardless of the fluctuation range. This demonstrates the property of the encoding symmetry analysis that it decouples channel disturbance from privacy leakage (Zeng et al., 2020), and hence the fluctuation from the channel does not affect privacy.

Notice that the two-dimensional has greater privacy leakage than the 17-dimensional. This is reasonable since in the two-dimensional key space the adversary is essentially guessing between two symbols, which is significantly easier than the 17-dimensional case where she guesses between 17 symbols. In contrast, the mutual information term $\log_2(d) - H(\vec{E}_{bit})$ drops for both cases, as the fluctuation clearly results in higher bit error. It can be seen that the mutual information of the two-dimensional is higher than that of the 17-dimensional, which implies that the two-dimensional has fewer bit errors. This can be understood as the single-photon interference detector outputs binary results (left or right click), and thus it is ideal for binary key space and yields very low bit-error rate for the two-dimensional protocol when no fluctuation is applied (the mutual information is close to 1 bit as shown in the figure). It however does not provide full information for the 17-dimensional protocol

unless the input coherent states are in the same or opposite phases. It thus generates lower mutual information for the 17-dimensional than the two-dimensional, although their overall key rates are similar since the 17-dimensional has lower privacy leakage. Moreover, the mutual information of the two-dimensional PM QKD decreases more rapidly than that of the 17-dimensional. This is reasonable since the bit-error rate of the two-dimensional is very low under no fluctuation. Yet when fluctuation adds to its bit-error rate, the change rate in the term $H(\vec{E}_{bit})$ is significantly higher since the derivative of the Shannon-entropy function $H(p)$ is infinity when p tends to 0. Hence, it is seen in Fig. 4.7a that the mutual information of two-dimensional PM QKD drops more rapidly than that of the 17-dimensional under phase fluctuation.

In order to cope with the drop in mutual information, the privacy leakage term has to be lowered, which can be achieved through suppressing the intensity μ of the source. Fig. 4.7b illustrates the effects of light intensity μ on the mutual information and privacy leakage. The channel distance is fixed at 300 km, and a phase fluctuation of range $\phi_{lim} = \pi/3$ is applied. As expected from the encoding symmetry analysis, the mutual information term generally does not relate with the light intensity. As the light intensity drops, the single-photon fraction from the light source increases, and so does the single-photon fraction in the detection. This further lowers the uncertainty in the detection fraction of each photon number state $\vec{q}_\mu$, i.e. it lowers the privacy leakage $H(\vec{q_\mu})$, as shown in Fig. 4.7b. In order to compensate the faster drop in mutual information of two-dimensional PM QKD, its source intensity has to decrease further than that of the 17-dimensional, as shown in Fig. 4.7c.

The drop in the intensities results in a further drop in the overall gain $Q_\mu \approx \eta\mu$. Hence, as shown in Fig. 4.7d, under a small phase fluctuation of range $\phi_{lim} = \pi/3$, the 17-dimensional PM QKD yields higher secure key rates than the two-dimensional. Moreover, when fixed misalignment is introduced, the key rate of two-dimensional PM QKD decreases further, whilst that of the 17-dimensional remains. It can thus be concluded that the high-dimensional PM QKD is more robust to small phase fluctuation than the two-dimensional PM QKD.

4.4.5 Concluding remarks

The high-dimensional PM QKD protocol is presented, its security proved and its robustness against phase misalignment demonstrated. Under a reasonable fiber-optic simulation setup, it is demonstrated that when the protocol dimension is high enough, the key-rate performance is almost completely immune to fixed phase-reference-mismatch and robust to small phase fluctuation, i.e. it is reference-frame-independent. In general, our work points out the feasibility of increasing protocol dimension in order to combat misalignment. Our security

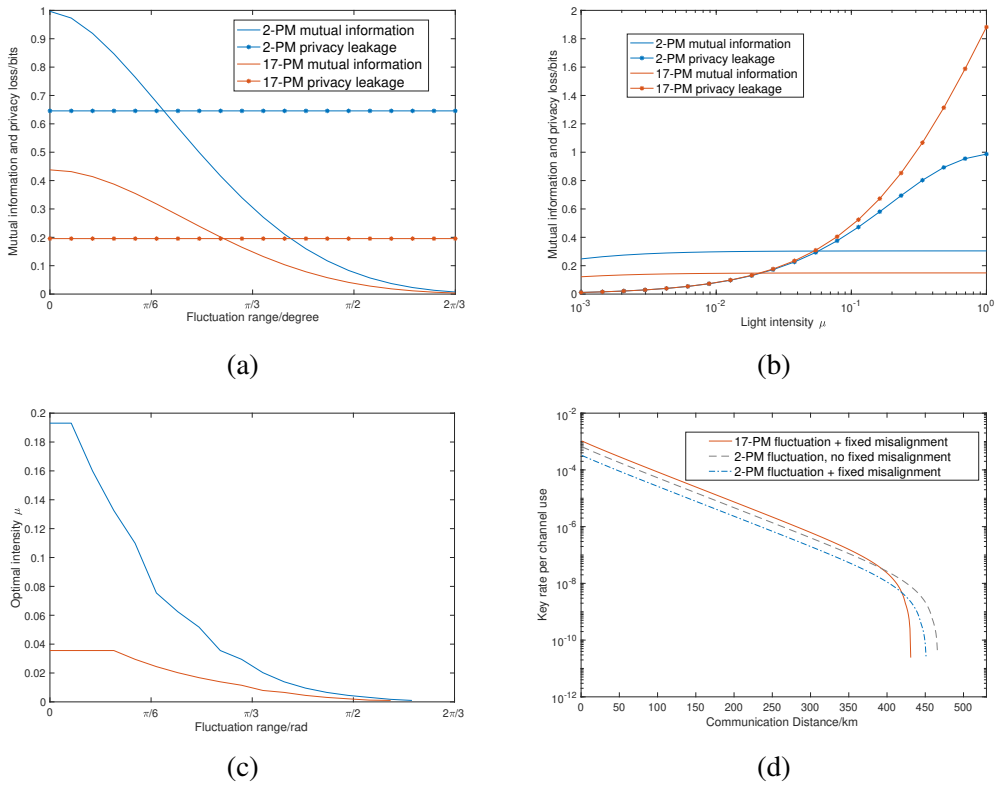


Fig. 4.7 High-dimensional PM QKD under phase fluctuation. **(a)** Mutual information and privacy leakage against phase fluctuation range ϕ_{lim} for 2- and 17-PM, light intensity 0.2 and 0.03 respectively, communication distance 300 km. The fluctuation does not affect the privacy as a result of encoding symmetry. The mutual information of the 2-PM decreases faster than that of the 17-PM. **(b)** Mutual information and privacy leakage against light intensity μ for 2- and 17-PM, fluctuation range $\pi/3$, communication distance 300 km. The light intensity does not affect the mutual information. **(c)** Optimal light intensity μ against phase fluctuation range ϕ_{lim} for 2- and 17-PM, communication distance 300 km. The 2-PM light intensity decreases rapidly as the fluctuation increases in order to compensate its faster drop in mutual information. **(d)** Simulated key-rate performance: 17-PM under both $\pi/6$ fixed misalignment and $\pi/3$ range fluctuation (red line), 2-PM under the same scenario (blue dotted line), 2-PM under fluctuation only, no fixed misalignment (gray dotted line). The 17-PM is superior than the 2-PM under small phase fluctuation.

argument provides the theoretical cornerstone for the analysis of high-dimensional QKD protocols.

The focus has been on the prime-dimensional PM QKD, although the general security proof in Section 3.1.2 covers all the systems of prime power dimensions. This is due to the incompatibility of the rotating encoding and the additive group of prime power finite fields. For instance, the encoding operations of a four-dimensional PM QKD form the order-4 cyclic group $\{I,U,U^2,U^3\} \equiv Z_4$, where U is the $\pi/2-$rotation operator. In contrast, the additive group of GF(4) is the Klein-4 group $\{a,b|a^2 = b^2 = 1\}$. This incompatibility invalidates the Fock-state form of the symmetric states. One possible solution is to alter the encoding operations. For instance for four dimensions, the encoding operations can be changed to $\{I,U,V,UV\}$, where U is the $\pi-$rotation operator, and V satisfies:

$$V|x+ip\rangle = |p+ix\rangle \tag{4.25}$$

Clearly, this encoding operation set is also valid. Since $U^2 = V^2 = I$, the encoding operation group is isomorphic to the Klein-4 group, and hence compatible with the addition in GF(4). However, the caveat is that the operation V is arguably not physical not being unitary or anti-unitary. The ambiguous prime power case is thus not included in the security proof.

Chapter 5

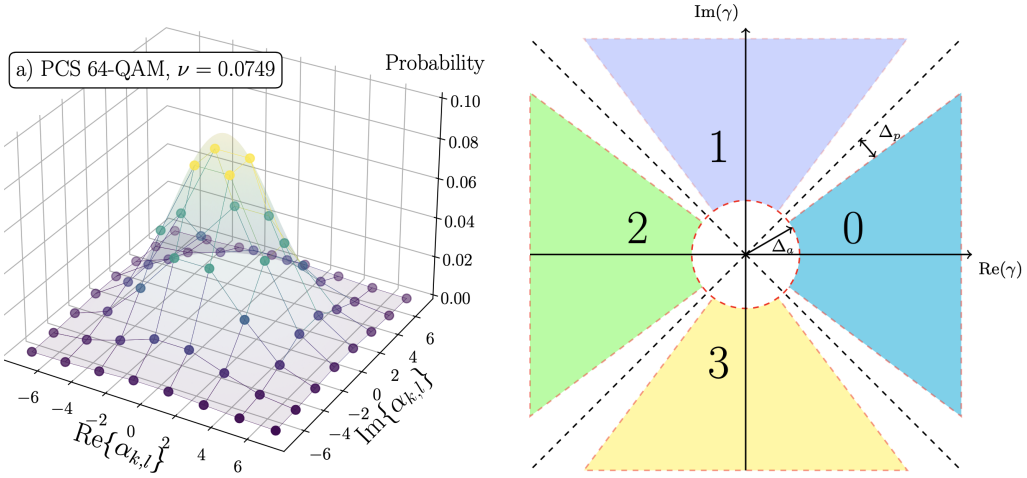
Discrete-modulated CV QKD

This chapter introduces the discrete-modulated (DM) CV QKD in this chapter. The DM CV QKD uses finitely many key constellations, in contrast to the infeasible infinite constellations in the Gaussian-modulated protocols. The setups of various DM CV QKD protocols will be examined, and the corresponding experimental demonstrations will be briefly reviewed. In Section 5.2, the numerical key rate calculation method (Winick et al., 2018) for general finite-dimensional QKD will be reviewed, and in Section 5.3 this numerical method will be applied to the key rate calculation of the m-phase-shift-keying (m-PSK) CV QKD, with photon-number cutoffs, to obtain a reliable and tight collective key rate lower bound (Gong et al., 2021).

5.1 Setups of DM CV QKD

The DM CV QKD was proposed as an alternative to the Gaussian-modulated CV QKD to simplify the encoding and post-processing schemes (Leverrier and Grangier, 2009, 2011). The DM CV QKD shares great similarity to the classical communication with discrete constellations such as the quadrature amplitude modulation (QAM) and the phase shift keying (PSK). In fact, a DM CV QKD protocol also depends on a constellation and a key mapping function. The constellation requires Alice selecting with different probabilities from a finite set of coherent states $\{|\alpha_i\rangle\}_{i=0}^{m-1}$. These coherent states distribute on the quadrature plane following either the QAM constellation, with a discretised Gaussian shape (Roumestan et al., 2021, 2022; Pan et al., 2022), or the PSK constellation, distributing uniformly on a circle (Hirano et al., 2017; Wang et al., 2023). Fig. 5.1a and Fig. 5.1b illustrate the constellations of a 64-QAM and 4-PSK respectively, retrieved from (Roumestan et al., 2022) and (Lin et al., 2019).

Bob receives the coherent states transmitted by Alice with a heterodyne detector normally, obtaining a complex number α for each round. Bob has to convert the continuous results to the given discrete key states, with a pre-determined key mapping function f, with $f(\alpha)$ taking values from $\{\alpha_0, \cdots, \alpha_{m-1}, \phi\}$, where ϕ denotes a discarded round. Fig. 5.1b from (Lin et al., 2019) illustrates the key mapping of the 4-PSK protocol. The coloured regions with key labelling represent the key mapping rules: the results close to the origin and the boundaries of adjacent regions are discarded to reduce the error rate. The general DM CV QKD protocol 10 is shown below.



(a) (b)

Fig. 5.1 Constellations of DM CV QKD.**(a)** 64-QAM following a Gaussian shape and discretised Gaussian distribution. (Roumestan et al., 2022) **(b)** 4-PSK constellation with four states $|\alpha\rangle$,$|-\alpha\rangle$,$|i\alpha\rangle$,$|-i\alpha\rangle$ (Lin et al., 2019). The coloured regions with key labelling represent the key mapping rules: the results close to the origin and the boundaries of adjacent regions are discarded to reduce the error rate.

Protocol 10 ***Discrete-modulated CV QKD protocol***

1. ***State preparation****: For each round, Alice draws a random complex number α_i from a finite constellation $\{\alpha_0, \cdots, \alpha_{m-1}\}$ with certain probability for each symbol. She transmits the coherent state $|\alpha_i\rangle$ to Bob through a quantum channel. She also transmits the LO to fix the phase reference.*

2. ***Detection****: For each round, Bob receives the signal with a heterodyne detector with the received LO, obtaining a complex number α. He passes this complex number to the pre-determined key mapping function f outputting one of the key states $\{\alpha_0, \cdots, \alpha_{m-1}\}$,*

or the round being discarded. They repeat this quantum communication for sufficiently many rounds.

3. ***Reverse information reconciliation**: They sample a small portion of rounds and compare their keys. They attempt to perform reverse reconciliation with Bob sending Alice the syndrome and Alice correcting her key string. If the error rate is too high they abort the protocol.*

4. ***Privacy amplification**: According to the key statistics, usually the variance, they calculate the distillable key rate and hash the reconcile key string to obtain the final secure keys.*

On the experimental side, the 64 and 256-QAM DM CV QKD exhibit high key rates for metropolitan distances. In fact, Roumestan et al. (2021) demonstrated around 92 Mbps at 9.5 km and 24 Mbps at 25 km, using 256-QAM, and Pan et al. (2022) demonstrated 292.185 Mbps, 156.246 Mbps, 50.491 Mbps and 7.495 Mbps at 5.059 km, 10.314 km, 24.490 km, and 50.592 km using 64-QAM. The DM CV QKD is thus a suitable choice for the high-rate metropolitan QKD networks.

5.2 Key rate calculation based on numerical optimisation

This section introduces the numerical key rate calculation of the collective DM CV QKD. The security of DM CV QKD is still far from completeness. In fact, the current security analyses (Leverrier and Grangier, 2009; Lin et al., 2019; Ghorai et al., 2019) generally follows the entanglement-distillation approach based on the Devetak-Winter formula (Devetak and Winter, 2005), explained in Section 3.2. These analyses are valid only under asymptotic collective attacks, and are only extended to finite size under more restrictive attacks (Papanastasiou and Pirandola, 2021).

It is even a difficult task to calculate the collective key rate of the DM CV QKD under a finite-energy assumption. In fact, as in Eq. (3.27), a Devetak-Winter-formula-based key rate requires the optimisation traversing all possible attacks by Eve. Early key rate calculation restricts to Gaussian attacks (Hirano et al., 2017; Leverrier and Grangier, 2009) since by the Gaussian optimality the Gaussian state ρ_{AB}^{G}, with the same first and second moment as the actual state ρ_{AB} shared by Alice and Bob, gives a lower key rate than ρ_{AB}. This lower bound on the key rate is however loose when the modulation is non-Gaussian (Leverrier and Grangier, 2011). It is thus tempting to numerically find the optimal attacks by Eve that result in the worst key rates given by the experimental statistics.

The numerical key rate calculation scheme on arbitrary QKD protocols by Winick et al. (2018) will be introduced. The numerical approach is reliable in the sense that it converts the minimisation problem in the Devetak-Winter formula Eq. (3.27) to its dual maximisation problem. Specifically, the minimisation traversing Eve's attacks cannot always reach the true global minimum, and the resulted key rate is thus not under the worst possible case, and the key string distilled regarding this key rate is thus not entirely secure. Winick et al. (2018) applies a standard gradient-descent method from convex optimisation to approach the reliable lower bound successively following the gradient, arriving at a true lower bound of the distillable key rate. The focus is on the setup of the optimisation problem here. Consider the following general procedure of a QKD protocol in the entanglement-based setup:

1. **State measurements**: Alice and Bob share the bipartite state ρ_{AB} after the quantum communication. They measure their halves of the state with POVMs $P^A = \{P_j^A\}$ and $P^B = \{P_j^B\}$, retrieving statistics:

$$\mathrm{Tr}\left\{(P_j^A \otimes P_j^B)\rho_{AB}\right\} = p_{jk}. \tag{5.1}$$

   Eq. (5.1) together with the locality constraints that

$$\mathrm{Tr}_B\{\rho_{AB}\} = \rho_A \tag{5.2}$$

   give the constraints of the optimisation.

2. **Announcements**: Alice and Bob make announcements $\tilde{A}$ and $\tilde{B}$ to the public channel (leaking information to Eve) and record the measurement results in their own registers $\bar{A}$ and $\bar{B}$. This boils down to the announcement channels represented by the Kraus operator

$$K_a^A = \sum_{\alpha_a} \sqrt{P^A_{(a,\alpha_a)}} \otimes |a\rangle_{\tilde{A}} \otimes |\alpha_a\rangle_{\bar{A}}, \tag{5.3}$$

   where the POVM is relabelled according to the announcements $P^A = \{P_j^A\} = \{P^A_{(a,\alpha_a)}\}$. The announcement channel on Bob's side is similar with POVM $P^B = \{P_j^B\} = \{P^B_{(b,\beta_b)}\}$. The state after the announcements becomes

$$\begin{aligned}\rho^{(2)}_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}} &= \mathscr{A}(\rho_{AB}) \\ &= \sum_{a,b}(K_a^A \otimes K_b^B)\rho_{AB}(K_a^A \otimes K_b^B)^\dagger.\end{aligned} \tag{5.4}$$

3. **Post-selection**: Alice and Bob keep the useful rounds only based on the announcements. Let $\mathbf{A}$ be the set of announcements (a,b) being kept, the post-selection is represented

by a projector:

$$\Pi = \sum_{(a,b)\in\mathbf{A}} |a\rangle_{\tilde{A}}\langle a| \otimes |b\rangle_{\tilde{B}}\langle b|. \tag{5.5}$$

The state after the projector is

$$\rho^{(3)}_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \frac{\Pi\rho^{(2)}_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}}\Pi}{p_{pass}}, \tag{5.6}$$

where $p_{pass} = \mathrm{Tr}\{\rho^{(2)}_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}}\Pi\}$ is the probability that the state passes the post-selection.

4. **Key mapping**: The final key is generated by a key-mapping function f on the outcome of Alice's measurements (a, α_a) and Bob's announcement b. The key-mapping isometry V stores the raw key information in system R in a coherent fashion in the sense that

$$V = \sum_{a,\alpha_a,b} |f(a,\alpha_a,b)\rangle_R \otimes |a\rangle_{\tilde{A}}\langle a| \otimes |\alpha_a\rangle_{\bar{A}}\langle\alpha_a| \otimes |b\rangle_{\tilde{B}}\langle b|. \tag{5.7}$$

The isometry act as

$$\rho^{(4)}_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} = V\rho^{(3)}_{A\tilde{A}\bar{A}B\tilde{B}\bar{B}}V^\dagger. \tag{5.8}$$

5. **Decoherence**: The coherence in the state is realised by a pinching channel $\mathscr{Z}$, resulting in the classical key system Z^R:

$$\mathscr{Z}(\sigma) = \sum_j (|j\rangle_R\langle j| \otimes \mathbb{I})\sigma(|j\rangle_R\langle j| \otimes \mathbb{I}), \tag{5.9}$$

and the final state is

$$\rho^{(5)}_{Z^R A\tilde{A}\bar{A}B\tilde{B}\bar{B}} = \mathscr{Z}(\rho^{(4)}_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}}). \tag{5.10}$$

The key rate is thus based on the final state $\rho^{(5)}$ as

$$r = p_{pass}\left[S(Z^R|E\tilde{A}\tilde{B}) - \mathrm{leak}^{\mathrm{EC}}_{\mathrm{obs}}\right], \tag{5.11}$$

where $\mathrm{leak}^{\mathrm{EC}}_{\mathrm{obs}}$ is the cost of error correction observed from experiments. By Coles (2012), the privacy loss term $S(Z^R|E\tilde{A}\tilde{B})$ can decouple from Eve's system E by the relative entropy in the sense that

$$\begin{aligned} S(Z^R|E\tilde{A}\tilde{B}) &= D(\rho^{(4)}_{RA\tilde{A}\bar{A}B\tilde{B}\bar{B}} || \rho^{(5)}_{Z^R A\tilde{A}\bar{A}B\tilde{B}\bar{B}}) \\ &= D\left(\mathscr{G}(\rho_{AB}) || \mathscr{Z}(\mathscr{G}(\rho_{AB}))\right), \end{aligned} \tag{5.12}$$

where the quantum channel $\mathscr{G}$ is the composite action

$$\mathscr{G}(\sigma) = V\Pi\mathscr{A}(\sigma)\Pi V^{\dagger}. \tag{5.13}$$

This relation is reasonable since $\rho^{(5)}$ is the decoherence of the key system of $\rho^{(4)}$, and if the two states are close it is more likely for Eve to be entangled with the key system. The following convex minimisation problem is then formulated:

$$\begin{aligned} &\min D\left(\mathscr{G}(\rho_{AB})||\mathscr{Z}(\mathscr{G}(\rho_{AB}))\right) \\ &\text{s.t. } \mathrm{Tr}\left\{(P_j^A \otimes P_j^B)\rho_{AB}\right\} = p_{jk} \\ &\quad \mathrm{Tr}_B\{\rho_{AB}\} = \rho_A. \end{aligned} \tag{5.14}$$

5.3 Key rate of PSK protocols

The key rate of a PSK DM CV QKD protocol will be analysed based the work (Gong et al., 2021) that the author participated in[1]. This m-PSK protocol is a direct generalisation of the 4-PSK protocol from (Lin et al., 2019) using homodyne detection. The m-PSK protocol is described below:

Protocol 11 ***PSK DM CV QKD protocol using homodyne detection***

1. ***State preparation****: For each round, Alice decides whether it is signal or not based on the distribution $\{p_A, 1-p_A\}$. In a signal round, Alice draws a random key bit 0 or 1 and transmits $|\alpha\rangle$ or $|-\alpha\rangle$ accordingly to Bob through an authenticated channel, where α is a preset positive number. For a non-signal round, Alice randomly transmits one state from $\{|\alpha\exp(j2\pi i/m)\rangle\}_{j=0,j\neq\pm1}^{m-1}$. She also transmits the LO to fix the phase reference.*

2. ***Detection****: For each round, from a probability distribution $\{p_B, 1-p_B\}$, Bob decides to measure the $\hat{q}$ or $\hat{p}$ quadrature of the received state with a homodyne detector with the received LO. He obtains a real-numbered outcome y. They repeat this quantum communication for sufficiently many rounds.*

3. ***Sifting and key mapping****: Through an authenticated classical channel, Alice announces whether each round is a signal or not, and Bob announces whether he measured $\hat{q}$ or p quadrature of that round. They keep the signal rounds with q quadrature*

[1]This section is based on the work (Gong et al., 2021) that the author participated in. Y. Gong and the author finished the security analysis, and Y. Gong programmed the simulations for key rate calculation. H. Li and A. Wonfor polished the analysis on the experimental side. R.V. Penty supervised the project.

being measured for key generation, and leave other rounds for parameter estimation only. For the key-generating rounds, Bob maps the measurement outcome y to a key bit 0 or 1 based on the preset key mapping function.

4. ***Reverse information reconciliation**: They sample a small portion of rounds and compare their keys. They attempt to perform reverse reconciliation with Bob sending Alice the syndrome and Alice correcting her key string. If the error rate is too high they abort the protocol.*

5. ***Privacy amplification**: According to the statistics from both the signal and non-signal rounds, they calculate the distillable key rate and hash the reconcile key string to obtain the final secure keys.*

As the protocol only generates keys from distinguishing $|\alpha\rangle$ and $|-\alpha\rangle$, the key mapping function is similar to the BPSK protocol where for the measurement outcome y, the key mapping function f reads (See Fig. 5.2a for the illustration of constellations and key mappings):

$$f(y) = \begin{cases} 0 & y \geq \Delta_c, \\ 1 & y \leq -\Delta_c, \\ \text{discard} & -\Delta_c < y < \Delta_c. \end{cases} \tag{5.15}$$

The key-rate calculation follows the numerical method Eq. (5.14). For an m-PSK protocol, Alice's system A is m-dimensional with $|0\rangle$ and $|1\rangle$ representing the key states. The entanglement-based source state is given by

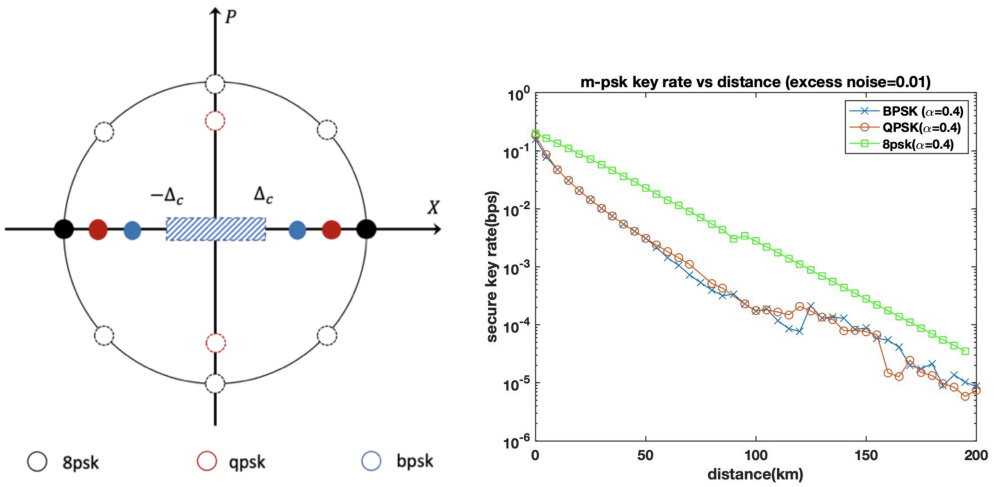
$$|\Psi\rangle_{AA'} = \sum_{j=0}^{m-1} \sqrt{p_j}|j\rangle_A \big|\alpha_j\big\rangle_{A'}, \tag{5.16}$$

where $\{\big|\alpha_j\big\rangle\} = \{|\alpha \exp(j2\pi i/m)\rangle\}_{j=0}^{m-1}$. Alice sends the subsystem A' through the channel mapping it to the unknown system B, and Bob performs measurements on it. The post-processing map $\mathscr{G}$ is the same as that in a BPSK protocol, which can be written compactly as $\mathscr{G}(\sigma) = K\sigma K^\dagger$, where (Lin et al., 2019)

$$K = \sum_{z=0}^{1} |z\rangle_R \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_A \otimes (\sqrt{I_z})_B. \tag{5.17}$$

The I_0 and I_1 are the interval operators representing the post-selection, defined as

$$I_0 = \int_{\Delta_c}^{\infty} dq|q\rangle\langle q|, \quad I_1 = \int_{-\infty}^{-\Delta_c} dq|q\rangle\langle q|. \tag{5.18}$$



(a) (b)

Fig. 5.2 **(a)** Constellation diagram of BPSK, QPSK and 8PSK CVQKD, where the black, red and blue circles represent the 8PSK, QPSK and BPSK respectively. The dashed area is the post-selection area for no key generation. **(b)** The secure key rate for BPSK, QPSK and 8PSK CVQKD using homodyne detection. This figure is generated by Y. Gong in (Gong et al., 2021).

The decoherence operator $\mathscr{Z}$ is to decouple the key system R by projections $|0\rangle_R\langle 0|\otimes\mathbb{I}_{AB}$ and $|1\rangle_R\langle 1|\otimes\mathbb{I}_{AB}$. The optimisation problem can be written based on Eq. (5.14) as

$$\begin{aligned}
&\min D(\mathscr{G}(\rho_{AB})||\mathscr{Z}(\mathscr{G}(\rho_{AB})))\\
&\text{s.t. } \mathrm{Tr}\{(|j\rangle_A\langle j|\otimes\hat{q}_B)\rho_{AB}\} = p_j\langle\hat{q}_B\rangle_j\\
&\quad \mathrm{Tr}\{(|j\rangle_A\langle j|\otimes\hat{p}_B)\rho_{AB}\} = p_j\langle\hat{p}_B\rangle_j\\
&\quad \mathrm{Tr}\{(|j\rangle_A\langle j|\otimes\hat{n}_B)\rho_{AB}\} = p_j\langle\hat{n}_B\rangle_j\\
&\quad \mathrm{Tr}\{(|j\rangle_A\langle j|\otimes\hat{d}_B)\rho_{AB}\} = p_j\langle\hat{d}_B\rangle_j\\
&\quad \mathrm{Tr}_B\{\rho_{AB}\} = \rho_A\\
&\quad \mathrm{Tr}\{\rho_{AB}\} = 1\\
&\quad \rho_{AB}\geq 0.
\end{aligned} \tag{5.19}$$

Notice that the statistics of the second moments of the quadrature measurements are also collected based on $\hat{n} = (\hat{q}^2+\hat{p}^2-1)/2$ and $\hat{d} = \hat{q}^2-\hat{p}^2$.

Based on the optimisation formalism above, the collective key rate of the m-PSK protocol can be calculated with the simulated statistics listed in Appendix B.2. The key rates of various PSK protocols are shown in Fig. 5.2b. This figure is generated by the author's collaborator Y. Gong of the work (Gong et al., 2021). The secure key rates at different distances are shown

for the BPSK, QPSK and 8-PSK schemes with the same parameters, i.e. fixed state $\alpha = 0.4$ and excess noise $\xi = 0.01$, with the same post-selection threshold and fixed calculation precision. As can be seen, all three protocols are proved secure over a 200-km channel (40 dB). The 8-PSK protocol has the highest secure key rate while QPSK and BPSK have a similar secure key rate. This is because for 8-PSK, 6 additional states are employed for channel parameter estimation and generate a much tighter lower bound over the feasible set. It is noteworthy that, even for the BPSK protocol, both $\langle \hat{q} \rangle$ and $\langle \hat{p} \rangle$ quadratures are measured and used for parameter estimation, causing the protocol to have a similar feasible region as QPSK and resulting in similar key rates.

5.4 Concluding remarks

To summarise, this chapter introduces the DM CV QKD scheme, which is believed to be practical in both the encoding and detection. The reliable numerical key rate calculation method by Lin et al. (2019) is reviewed, applied to the collective key rate calculation of the m-PSK protocols. An 8-PSK protocol is demonstrated clearly to generate high key rate and reach over 200 km. The DM CV QKD protocol can thus be identified as a suitable candidate for the implementation of long-distance quantum networks. It worth acknowledgement that there is an analytical key rate calculation method for DM CV QKD of arbitrary modulations by solving the key rate optimisation (Denys et al., 2021). Although it does not give a tight bound on the secure key rate, this method is useful when analysing the protocols with large constellations such as 256-QAM (Roumestan et al., 2022).

The main obstacle in the implementations of DM CV QKD is its lack of full security analysis. As was pointed out in Sec. 5.2, the security of DM CV QKD cannot invoke the Gaussian optimality as the Gaussian CV QKD, and hence the current security is restricted to collective attacks. On the other hand, the DV QKD enjoys a complete security analysis naturally valid under coherent attacks and handling the finite-size effect. Techniques such as decoy states (Lo et al., 2005; Wang, 2005) and GLLP formalism (Gottesman et al., 2004) all contribute to the parameter estimations. It is thus tempting to transplant these DV security methods to CV protocols, that is, protocols with coherent detection. A remarkable work is by Matsuura et al. (2021) tackling the security of the BPSK CV QKD based on phase error correction. In the next chapter, the author's work (Jin et al., 2023) will be introduced that presents a DV-like security analysis of a time-bin CV QKD protocol with simple parameter estimation based on DV techniques such as decoy states and photon-number tagging.

Chapter 6

Time-bin-encoding CV QKD

This chapter introduces the time-bin-encoding CV QKD protocol. As elaborated previously, CV QKD has great practicality due to the coherent detectors used, yet unlike DV QKD it lacks a robust security analysis. It is thus desirable to combine the merits of CV and DV QKD to yield some new-generation QKD protocols with good practical performances and reliable security.

The first review is on the recent progresses on protocols combining the CV and DV features in Section 6.1. The works by Matsuura et al. (2021, 2023) will be discussed, establishing the phase-error scheme for the binary-modulated CV QKD using the squashing model (Gottesman et al., 2004; Beaudry et al., 2008). The works by Qi (2021) and Primaatmaja et al. (2022) will also be mentioned, both analysing the CV protocols from the photon-number basis.

Section 6.2 introduces the time-bin-encoding CV QKD protocol and analyse its security based on the phase-error approach. The DV-like analysis secures the protocol under the most general coherent attacks, and covers the finite-size effects. The parameter estimation is made simple using DV methods such as photon-number tagging and decoy states. The need for LO transmission is removed due to the encoding on relative intensities.

6.1 Review on hybrid CV-DV QKD

This section reviews the recent works on QKD protocols combining the CV and DV features. Notably, Matsuura et al. (2021) proposed a phase-error-based security analysis for the BPSK CV QKD distinguishing $|\alpha\rangle$ and $|-\alpha\rangle$. The DV-like security analysis covers the most general coherent attacks intrinsically, and possesses a robust finite-size method inherited from the DV analysis.

The core ingredient of their security analysis is a trace-non-increasing quantum operation that converts a CV optical mode to a DV qubit, which is called the "squashing" channel analogous to the detector squashing models (Gottesman et al., 2004; Beaudry et al., 2008). The squashing channel gives an equivalent protocol producing the same key statistics as the homodyne detection. Passing the received optical modes through the squashing channel, Alice and Bob together hold a bipartite DV-DV system, on which the phase-error rate can be defined. This is illustrated in Fig. 6.1 below, retrieved from (Matsuura et al., 2021).

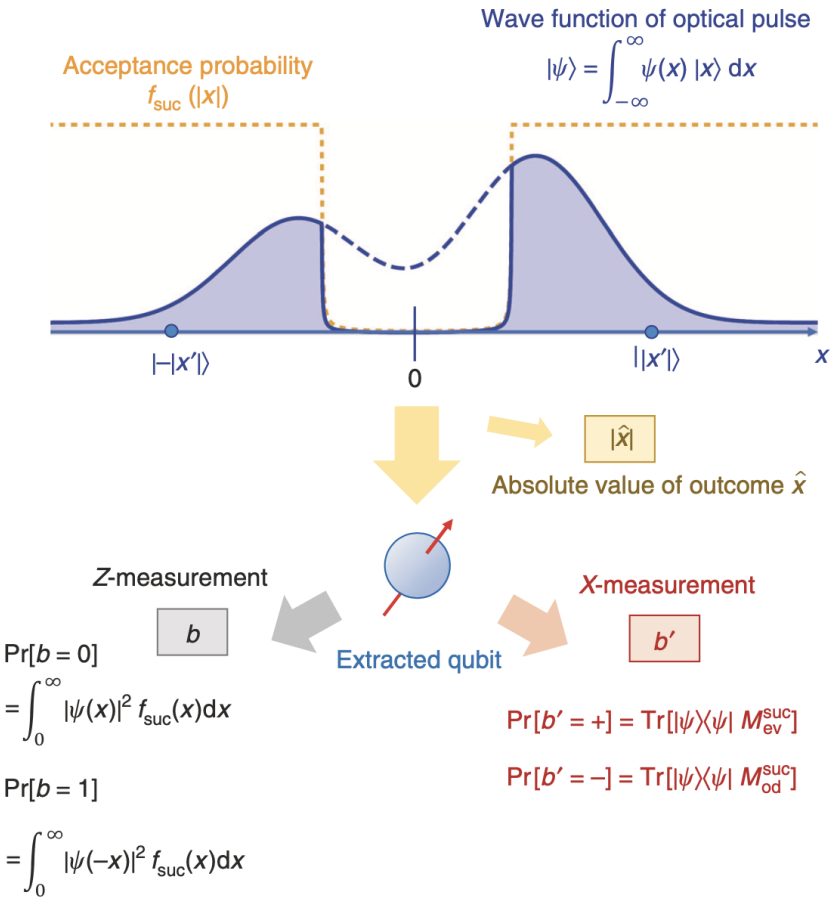


Fig. 6.1 Bob performs on the optical pulse the homodyne detection obtaining result $\hat{x}$. Then, Bob extracts a qubit through the squashing channel. A Z-basis measurement on this qubit gives the same sifted key bit as in the actual protocol. On the other hand, the X-basis measurement on this qubit reveals the parity of photon number of the received optical pulse.

According to (Matsuura et al., 2021), the phase-error rate of the squashing protocol is equivalent to the rate of parity flips of the optical modes in the actual protocol. Whilst the parity flip is difficult to estimate with linear optics, a fidelity bound is invoked to give a bound on the phase error. By tailoring the phase-error operator according to the pure-

loss channel, the asymptotic key rate of the protocol can scale linearly with the channel transmittance (Matsuura et al., 2023).

As a variant of the single-photon-detector BB84, Qi (2021) proposed to replace the SPDs with conjugate homodyne detectors (Qi et al., 2020). On the Z-basis, the conjugate homodyne detector functions as a threshold detector distinguishing vacuum and non-vacuum, although the results would be erroneous due to the intrinsic shot noise. On the X-basis, the conjugate homodyne detector can be applied repeatedly to extrapolate the statistics of photon numbers. Based on the GLLP argument, the secure keys can be extracted separately for each photon-number component. The interested single-photon error rate can be bounded by the gain of the vacuum, obtainable by the photon-number tomography using the conjugate homodyne (Qi et al., 2020). The resulted key rate is high in the metropolitan distances and can reach over 100 km.

The time-bin CV QKD protocol by Primaatmaja et al. (2022) will also be mentioned, which encodes the key bit onto the relative intensities of the two optical modes. The transmission of LO is thus removed due to the relative encoding. Although the security analysis is still within the CV scope with Devetak-Winter formula and numerical optimisation, the key rate is extracted based on photon-number components due to the block-diagonal structure of the source and the receiver. Section 6.2 will introduce the DV security analysis of this time-bin CV QKD with photon-number tagging and decoy method (Jin et al., 2023).

6.2 Time-bin-encoding CV QKD with DV security analysis

[1]This section introduces the time-bin-encoding CV QKD with a DV security analysis (Jin et al., 2023) in this section. This work is a successful attempt at the general security of a coherent-detected QKD protocol based on optical modes. The need for global references is also removed due to the encoding on the relative intensities. The parameter estimation is made simple by the phase randomisation on both the source and the receiver. Therefore the photon number for each round can be tagged, and the associated privacy can be effectively estimated using a carefully designed coherent-detection method, and independently extract encryption keys from each component. Simulations manifest that the protocol using multi-photon components increase the key rate by two orders of magnitude compared to the one using only single-photon component. Meanwhile, the protocol with four-intensity decoy analysis

[1]This section is based on the author's work (Jin et al., 2023) with due collaborators. A. Jin conveived the idea, finished the ideal-case security analysis and designed the decoy method. X. Zhang finished the security analysis under coherent attack and finite size and designed the homodyne tomography method. P. Zeng advised on the security analysis and the parameter estimation methods. L. Jiang and R.V. Penty supervised the project.

is sufficient to yield tight parameter estimation with a short-distance key-rate performance comparable to the best BB84 results.

The protocol description of the time-bin-encoding CV QKD will be placed in Sec. 6.2.1. Its security analysis based on phase-error correction (Lo and Chau, 1999; Shor and Preskill, 2000; Koashi, 2009) will be presented in Sec. 6.2.2, identifying an equivalent protocol squashing the optical modes into qubits with identical key mapping statistics as in (Matsuura et al., 2021). The block-diagonal structures of both the source and the receiver are exploited as in (Primaatmaja et al., 2022), thus invoking the photon-number tagging technique (Gottesman et al., 2004; Ma, 2008) standard in DV QKD in this CV protocol. The parameters in the key-rate formula will be calculated with quantities on optical modes, and the estimation of these quantities are to be explained in Sec. 6.2.3 with homodyne tomography (D'Ariano et al., 2007) and decoy method (Lo et al., 2005; Wang, 2005). Finally the performances of the time-bin CV QKD will be simulated under realistic fiber-channel setups in Sec. 6.2.4.

6.2.1 Protocol description

The proposed time-bin-encoding CV QKD protocol 12 is presented and its schematic diagram depicted in Fig. 6.2. The two communication parties, Alice and Bob, employ the time-bin degree of freedom to encode keys. They use Z-basis for key generation and X-basis for parameter estimation. At the moment, the details of the X-basis parameter settings are not presented and the choices of the random phase factors, $\varphi_a^1, \varphi_a^2, \varphi_b^1$ and φ_b^2, and the light intensity, $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$, will be specified in Sec. 6.2.3.

Protocol 12 ***Phase-randomized time-bin-encoding CV QKD***

1. ***Encoding:***

   - Z-basis*:*
     (a) *Alice randomly selects a key bit* $k_a \in \{0,1\}$*, a phase factor* $\varphi_a \in [0, 2\pi)$*, and a light intensity* $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) *Alice prepares a coherent state of* $|0\rangle_{A1}\left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle_{A2}$ *for* $k_a = 0$ *or* $\left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle_{A1}|0\rangle_{A2}$ *for* $k_a = 1$.
   - X-basis*:*
     (a) *Alice randomly selects two phase factors* φ_a^1 *and* φ_a^2 *and a light intensity* $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) *Alice prepares a coherent state of* $\left|\sqrt{\mu_a/2}e^{i\varphi_a^1}\right\rangle\left|\sqrt{\mu_a/2}e^{i\varphi_a^2}\right\rangle$.

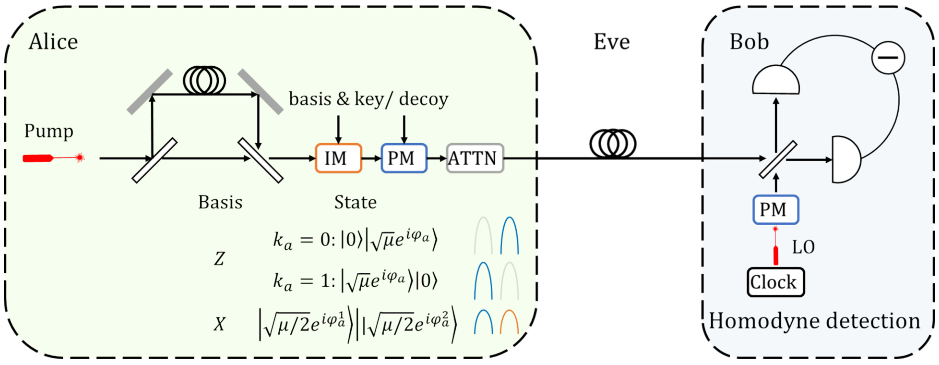


Fig. 6.2 Schematic diagram of the time-bin CV QKD. The setups of Alice and Bob are shaded in green and blue, respectively. Alice obtains a time-bin encoding on two modes via time delay. She prepares two-mode phase-randomized states according to the basis choice and raw key value in the key generation rounds. The state modulation consists of intensity modulation (IM), phase modulation (PM), and necessary attenuation (ATTN). Upon receiving the state, Bob measures each mode with homodyne detectors. He uses a synchronized clock to distinguish adjacent modes and applies phase modulation (PM) to the local oscillator (LO).

2. ***Transmission:*** *Alice sends the state through a quantum channel to Bob.*

3. ***Detection****:*

   - *Z*-basis*:*

     (a) Bob randomly selects a phase factor $\varphi_b \in [0, 2\pi)$.

     (b) Bob uses homodyne detectors both with LO phases φ_b *to measure the modes and obtain quadratures* q_1 *for the first bin and* q_2 *for the second bin.*

     (c) Bob decodes the key bit as 0 *if* $(|q_1| < \tau) \wedge (|q_2| > \tau)$, 1 *if* $(|q_1| > \tau) \wedge (|q_2| < \tau)$, *and* $\emptyset$ *otherwise.*

   - *X*-basis*:*

     (a) Bob randomly selects two phases φ_b^1 *and* φ_b^2.

     (b) Bob uses homodyne detectors with LO phases φ_b^1 *and* φ_b^2 *to measure the modes and obtain quadratures* q_1 *and* q_2.

4. ***Sifting****: Alice and Bob perform basis sifting, where they obtain raw keys in the rounds where they both chose Z-basis with light intensity* $\mu_a = \mu$ *and* $k_b \neq \emptyset$.

5. ***Parameter estimation and key generation****: Alice and Bob estimate the bit and phase-error rate. Based on the parameter estimation, Alice and Bob perform information reconciliation and privacy amplification to obtain the final keys.*

The idea behind the protocol design will be briefly explained. The source states of our scheme resemble the ones in the time-bin-encoding BB84 protocol with coherent states (Bennett and Brassard, 1984), where the light intensities of the consecutive pulses naturally encode the key-bit information. As the key information is encoded in the relative intensity between the two modes, Alice does not need to send a pilot phase reference as in common CV QKD.

In our scheme, Bob decodes the Z-basis key bit information by measuring the light intensity of the pulses using the homodyne detectors. For instance, when Bob observes q_1 to be close to 0 and q_2 to be far away from 0, he may naturally guess that the original state sent by Alice corresponds to $k_a = 0$. However, unlike the key decoding with photon-number detectors, the result of measuring a coherent state's quadrature is subjected to a Gaussian distribution rather than a fixed value. The inherent shot noise of the homodyne detection introduces an intrinsic error in distinguishing a vacuum state from a pulse with a non-zero intensity (Weedbrook et al., 2012). To suppress the bit error, a threshold value, τ, is introduced in key decoding. The pulse intensity will be considered non-zero only when the quadrature value is larger than τ. The choice of τ should be optimized with respect to the channel transmittance and pulse intensity.

The X-basis is designed to estimate the information leakage of different photon-number components of the Z-basis. Thanks to the phase randomization of both the sources and the detectors, the Z-basis states are block-diagonal on the total photon-number basis on the two optical modes after emitted from the source and before being measured by the homodyne detectors. As will be clarified in Sec. 6.2.2, total photon-number measurements can be equivalently introduced at these two locations. As a result, Eve's eavesdropping strategy is effectively "twirled" to a photonic channel that only acts on the states incoherently with respect to the total photon numbers. One can thus virtually tag the emitted and received pulses according to the photon-number space, allowing the GLLP framework (Gottesman et al., 2004) for analyzing the key privacy contained in each photon-number subspace. In particular, dealing with photon-number spaces effectively brings our security analysis to the DV regime. In Sec. 6.2.2, observables shall be constructed to estimate the m-photon component phase-error rates $e^X_{m,m}$ for privacy estimation. Intuitively, the phase-error rates $e^X_{m,m}$ provide upper bounds on the key information leakage to the eavesdropper, Eve.

To estimate the m-photon component phase-error rates, $e^X_{m,m}$, ideally, it needs a source emitting the photon-number cat states, $(|0\rangle|m\rangle \pm |m\rangle|0\rangle)/\sqrt{2}$, and photon-number-resolving measurements. While this is not directly implementable, unbiased estimators of $e^X_{m,m}$ can be established using only coherent states and homodyne measurements to establish , as shown in Table 6.1. On the source side, a generalized decoy-state method is employed to estimate

the behaviors of photon-number-cat state $(|0\rangle|m\rangle \pm |m\rangle|0\rangle)/\sqrt{2}$ using coherent states with various intensities (Lo et al., 2005; Wang, 2005), which shall be discussed in Sec. 6.2.3. On the detection side, the homodyne tomography technique is employed and the photon-number observables are estimated via quadrature measurement results (Vogel and Risken, 1989; Smithey et al., 1993; D'Ariano et al., 1994, 1995; Leonhardt and Paul, 1995; D'Ariano, 1995).

Table 6.1 State preparation and detection settings in the ideal implementation and the realistic implementation. For brevity,the subscripts of modes are omitted and the detection is expressed with the measurement operators. In the key generation rounds, Bob applies phase-randomized homodyne detection for key-decoding, ideally being the photon-number-resolving detection. The expression of measurement operator $\hat{\Pi}(q_1, q_2)$ is given in Eq. (6.9), where q_1 and q_2 represent the quadratures of the two modes. The operator is block-diagonal on the total photon-number basis. For parameter estimation, ideally, Alice sends photon-number-cat states, and Bob performs a corresponding projective measurement. In the realistic setting, Alice can only prepare phase-randomized weak coherent states, and Bob can only perform phase-randomized homodyne measurements. The homodyne measurement operator, $\hat{Q}_{\varphi_1} \otimes \hat{Q}_{\varphi_2}$, is given in Eq. (6.6). Afterward, Bob estimates the photon-number-cat state measurement expectations via homodyne tomography methods, as shown in Eq. (6.35).

basis	source	
	ideal	real
Z	$\|0\rangle_{A_1}\|m\rangle_{A_2}$ $\|m\rangle_{A_1}\|0\rangle_{A_2}$	$\|0\rangle_{A_1}\left\|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_2}$ $\left\|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_1}\|0\rangle_{A_2}$
X	$\frac{1}{\sqrt{2}}(\|0\rangle_{A_1}\|m\rangle_{A_2} \pm \|m\rangle_{A_1}\|0\rangle_{A_2})$	$\left\|\sqrt{\frac{\mu}{2}}e^{i\varphi_a^1}\right\rangle_{A_1}\left\|\sqrt{\frac{\mu}{2}}e^{i\varphi_a^2}\right\rangle_{A_2}$
basis	detection	
	ideal	real
Z	$\|0m\rangle\langle 0m\|$ $\|m0\rangle\langle m0\|$	$\hat{\Pi}(q_1, q_2)$, Eq. (6.9)
X	$\frac{1}{2}(\|0m\rangle \pm \|m0\rangle)(\langle 0m\| \pm \langle m0\|)$	$\hat{Q}_{\varphi_1} \otimes \hat{Q}_{\varphi_2}$, Eq. (6.6), estimation via Eq. (6.35)

6.2.2 Security analysis

The security of the phase-randomized time-bin-encoding CV QKD protocol will be analysed along the complementarity approach (Shor and Preskill, 2000; Gottesman et al., 2004; Koashi, 2009). As outlined in Fig. 6.3, a series of equivalent protocols of the realistic implementation shall be established that do not change the statistics of any observer, with which the phase-

error observable can be defined and the key privacy can be estimated. The raw key generation can be effectively regarded as qubit measurements on a pair of entangled qubits, which allows borrowing the mature complementarity-based security analysis in the DV regime. In brief, on the source side, the preparation of key states is transformed to an entanglement-based protocol (Lo and Chau, 1999; Shor and Preskill, 2000), where a qubit measurement controls the key-encoding process, as shown in Fig. 6.3(b). On the detection side, it will be proved that the homodyne measurement can be squashed into an effective qubit measurement, as shown in Fig. 6.3(c). Moreover, it shall be rigorously proved that phase randomization twirls the photonic modes into diagonal states on the Fock basis and explain how to apply the tagging idea of the GLLP framework (Gottesman et al., 2004; Ma, 2008). It shall also be shown how to estimate the phase-error rates for different photon-number components from Fock-basis observables. Later in Sec. 6.2.3, it will be shown that the estimation can be realized in the realistic implementation with coherent states and homodyne detection.

To focus on the essence of security analysis, this section presents the results in a single-round analysis , where one can interpret it as the quantum Shannon limit under collective attacks. Nevertheless, the complementarity-based security analysis is inherently adapted to the most general case, namely the coherent attack, where the statistics over the rounds may not be independent and identically distributed (i.i.d.) (Xu et al., 2020). For parameter estimation with non-i.i.d. finite statistics, statistical techniques like martingale theory can help. This discussion can be found in the appendix of (Jin et al., 2023).

A. Entanglement-based squashing protocol

Here, the equivalence of the time-bin CV QKD protocol to a qubit-based entanglement distribution protocol is shown, where the protocols generate the same transmitted quantum states and measurement statistics. The latter protocol enables us to simplify the security analysis and estimate the information leakage from phase-error rates.

First examine the key-generation rounds in the protocol where both users choose the Z-basis, of which the whole procedure is depicted in Fig. 6.3(a). In the realistic implementation, Alice prepares phase-randomized coherent states,

$$\int_0^{2\pi} \frac{d\varphi_a}{2\pi} \left|\Psi(k_a)_{\varphi_a}\right\rangle_{A_1A_2} \left\langle\Psi(k_a)_{\varphi_a}\right|, \tag{6.1}$$

where

$$\left|\Psi(k_a)_{\varphi_a}\right\rangle_{A_1A_2} = \begin{cases} |0\rangle_{A_1} \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_2}, & \text{if } k_a = 0, \\ \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_1} |0\rangle_{A_2}, & \text{if } k_a = 1. \end{cases} \tag{6.2}$$

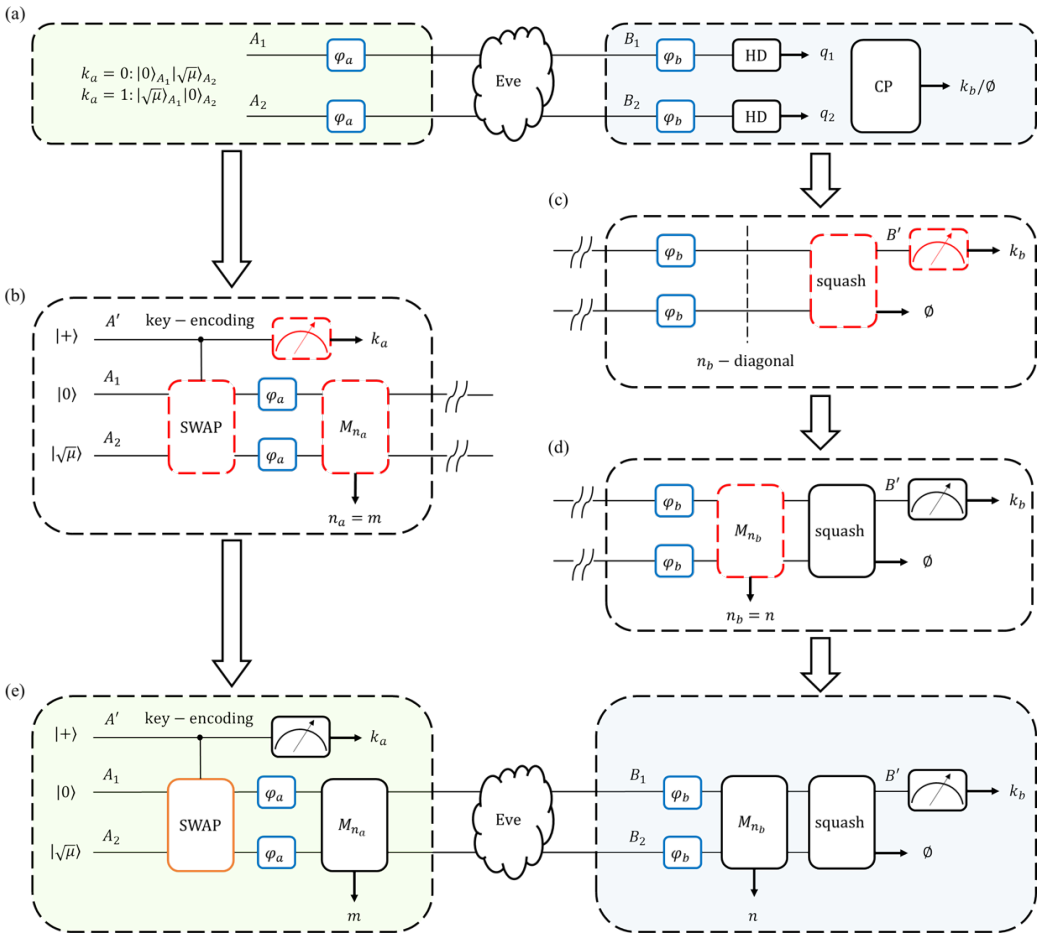


Fig. 6.3 Equivalent quantum circuits in key generation rounds. Reductions in each step are plotted with red dashed boxes. (a) The realistic implementation. The operations on Alice's and Bob's sides are shaded in green and blue, respectively. Alice prepares weak coherent states on two modes, which depend on the basis choice and the raw key value. On Bob's side, Bob measures the two modes with homodyne detectors (HD) and obtains quadratures q_1 and q_2. Afterward, Bob performs classical post-processing (CP) on the data and obtains a raw key k_b probabilistically, where the key decoding may fail due to the key mapping threshold, denoted as $\emptyset$. The blue rounded boxes represent phase randomization processes in state preparation or for the LOs in homodyne detection. (b) Equivalent entanglement-based state preparation. Key encoding can be interpreted as a qubit control operation on two modes where the control qubit measurement gives Alice's raw key k_a. The joint state on the two modes is diagonal on the Fock basis after phase randomization. One can insert a photon-number measurement, $\hat{M}_{n_a}$, and read out the total photon number, m, without changing the state. (c) Equivalent key-decoding measurement. The joint state of the two modes becomes diagonal on the Fock basis due to detector phase randomization. In key decoding, the modes are first squashed into a qubit probabilistically, where the failure gives the abort signal $\emptyset$. Upon successful squashing into a qubit, the computational-basis measurement gives the raw key bit. (d) Due to detector phase randomization, one can insert a photon-number measurement, $\hat{M}_{n_b}$, and read out the total photon number, n, without changing the state. (e) Equivalent circuit for security analysis. After the above reductions, the key generation measurements can be equivalently defined on a pair of (sub-normalized) qubit states.

Denote the optical modes sent to Bob as A_1 and A_2, which are CV systems. Treat the phase of optical modes, φ_a, as fully randomized over $[0, 2\pi)$. Finite phase randomization, $\varphi_a \in \{2j\pi/D\}_{j\in[D]}$, suffices for a practical implementation, where its difference from the full phase randomization is negligible when D is sufficiently large (Cao et al., 2015). This is also the case in later discussions on the detector phase randomization. Alice's key-state preparation can be effectively seen as an entanglement-based protocol (Lo and Chau, 1999; Shor and Preskill, 2000). Given the phase value, φ_a, Alice first prepares the following entangled state,

$$\left|\Psi_{\varphi_a}\right\rangle_{A'A_1A_2} = \frac{1}{\sqrt{2}}\left(|0\rangle_{A'}\left|\Psi(k_a=0)_{\varphi_a}\right\rangle_{A_1A_2} + |1\rangle_{A'}\left|\Psi(k_a=1)_{\varphi_a}\right\rangle_{A_1A_2}\right), \tag{6.3}$$

where system A' is a qubit system that superposes the two possible key states. The entangled state can be prepared by the quantum circuit in Fig. 6.3(b). Up to phase randomization, systems A' and A_1A_2 are initialized in $|+\rangle$ and $|0\rangle\left|\sqrt{\mu}\right\rangle$, and a control-swap operation is then applied from the qubit system to the optical modes. Alice obtains raw key bit k_a by measuring system A' on the computational basis, and the optical modes are prepared into the corresponding key state, $\left|\Psi(k_a)_{\varphi_a}\right\rangle$. The complementary observable of Alice's key-generation measurement can thus be defined over qubit system A', which measures the complementary basis of $\{|+\rangle, |-\rangle\} := \{(|0\rangle \pm |1\rangle)/\sqrt{2}\}$.

At the detection side in Fig. 6.3(a), Bob receives two optical modes B_1 and B_2, takes homodyne measurements, and maps the quadratures to a raw key or an abort signal. This process can be described by a trace-non-preserving completely positive map,

$$\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2}) = \int_0^{2\pi}\frac{d\varphi_b}{2\pi}\int_{\mathbf{R_0}} dq_1 dq_2 \hat{K}^{(q_1,q_2,\varphi_b)}\hat{\rho}_{B_1B_2}\hat{K}^{(q_1,q_2,\varphi_b)\dagger}, \tag{6.4}$$

where

$$\hat{K}^{(q_1,q_2,\varphi_b)} := |0\rangle_{B'}\langle q_1(\varphi_b), q_2(\varphi_b)|_{B_1,B_2} + |1\rangle_{B'}\langle q_2(\varphi_b), q_1(\varphi_b)|_{B_1,B_2}, \tag{6.5}$$

$|q(\varphi)\rangle$ is the rotated position eigenstate of quadrature observable

$$\hat{Q}_\varphi = \hat{a}e^{-i\varphi} + \hat{a}^\dagger e^{i\varphi}, \tag{6.6}$$

with $\hat{a}$ and $\hat{a}^\dagger$ denoting the annihilation and creation operators, respectively, and $\mathbf{R_0} \in \mathbb{R}^2$ records the region that decodes the real-valued tuple, (q_1, q_2), as $k_b = 0$. Note that in our protocol, $\mathbf{R_0} = \{|q_1| < \tau\} \times \{|q_2| > \tau\}$, and the region decodes the quadratures to $k_b = 1$ under the mapping $(q_1, q_2) \mapsto (q_2, q_1)$, which is denoted as $\mathbf{R_1} = \{|q_1| > \tau\} \times \{|q_2| < \tau\}$. The LOs of homodyne measurements are synchronically randomized, as denoted by φ_b in

Eq. (6.4). As the key-decoding region does not cover the entire parameter space, $\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}$ is hence not trace-preserving, where $\text{Tr}[\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2})]$ gives the probability of obtaining raw key bit $k_b \in \{0,1\}$. Bob's raw key can be equivalently seen as obtained by measuring the squashed sub-normalized qubit on the computational basis, and the probabilities are given by

$$\begin{aligned}
\Pr(k_b=0) &= \langle 0|\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2})|0\rangle = \int_0^{2\pi}\frac{d\varphi_b}{2\pi}\int_{\mathbf{R_0}} dq_1dq_2\langle q_1(\varphi_b),q_2(\varphi_b)|\hat{\rho}_{B_1B_2}|q_1(\varphi_b),q_2(\varphi_b)\rangle,\\
\Pr(k_b=1) &= \langle 1|\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}(\hat{\rho}_{B_1B_2})|1\rangle = \int_0^{2\pi}\frac{d\varphi_b}{2\pi}\int_{\mathbf{R_1}} dq_1dq_2\langle q_1(\varphi_b),q_2(\varphi_b)|\hat{\rho}_{B_1B_2}|q_1(\varphi_b),q_2(\varphi_b)\rangle.
\end{aligned} \tag{6.7}$$

Similar to the treatment to A', the complementary observable of Bob's key generation measurement on qubit system B' can be defined.

B. Photon-number tagging of the source and receiver

It have been shown that raw keys can be equivalently seen as generated from qubit measurements on A' and B'. Should Alice and Bob instead measure the qubit system on the complementary bases, the probability they obtain different results, or the phase-error rate, e^X, could be used to upper-bound the average privacy amplification cost per round as $h(e^X)$, where $h(p) = -p\log p-(1-p)\log(1-p)$ is the binary entropy function. Nevertheless, the actual privacy leakage may be less than the direct calculation. Note that the above privacy leakage estimation is averaged over the overall quantum state transmitted from Alice to Bob. The contribution to the privacy leakage of different components in quantum signals can differ. For instance, Eve can apply the photon-number-splitting (PNS) attack in the rounds in which Alice transmits two photons and Bob receives only a single photon (Brassard et al., 2000; Lütkenhaus, 2000); hence no privacy should be expected, rendering the phase-error probability to be $1/2$ in these rounds. If Alice and Bob can distinguish such rounds from the others, they can simply discard them in privacy amplification. The GLLP framework makes the above statement rigorous (Gottesman et al., 2004; Ma, 2008). Suppose Alice and Bob can categorize the transmitted quantum signals into different groups, or tags, and evaluate phase-error probabilities separately. The privacy amplification cost can be evaluated by $\sum_i Q_i h(e_i^X)$, where Q_i is the probability that a signal in the i'th group is transmitted and detected, namely the gain, and e_i^X is the phase-error probability of the group. Due to the concavity of the entropy function, this estimation is no larger than $h(\sum_i Q_i e_i^X)$.

In DV QKD, the tagging idea has been well practiced. In the coherent-state-based BB84 protocol, phase randomization on the source side diagonalizes the quantum signals on the Fock basis (Lo et al., 2005; Wang, 2005), and an ideal single-photon detector naturally

distinguishes the single photon components from other detected Fock components, allowing Alice and Bob to tag the quantum states with respect to the photon number (Ma et al., 2005). Similarly, it can now be proved that the photon-number tag can also be applied to the phase-randomized CV QKD protocol 12. On the source side, the phase randomization diagonalizes the state on the joint Fock basis,

$$\begin{aligned}\hat{\rho}^Z &= \int_0^{2\pi} \frac{d\varphi_a}{2\pi} \quad \frac{1}{2}|0\rangle_{A_1}\langle 0| \otimes \left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_2}\left\langle\sqrt{\mu}e^{i\varphi_a}\right| + \frac{1}{2}\left|\sqrt{\mu}e^{i\varphi_a}\right\rangle_{A_1}\left\langle\sqrt{\mu}e^{i\varphi_a}\right| \otimes |0\rangle_{A_2}\langle 0| \\ &= \sum_{m=0}^{\infty} \Pr(m)\frac{1}{2}\left(|0m\rangle_{A_1A_2}\langle 0m| + |m0\rangle_{A_1A_2}\langle m0|\right),\end{aligned} \tag{6.8}$$

where $\Pr(m) = e^{-\mu}\mu^m/m!$ is the Poisson distribution. Consequently, one can virtually insert a photon-number measurement after phase randomization to measure the total photon number on the two modes without changing the state, as shown in Fig. 6.3(b). On the detection side, when Bob takes the Z-basis measurement, the phase-randomized homodyne detector POVM elements can be expanded on the Fock basis (Primaatmaja et al., 2022),

$$\begin{aligned}\hat{\Pi}(q_1,q_2) &= \int_0^{2\pi} \frac{d\varphi_b}{2\pi} |q_1(\varphi_b)\rangle_{B_1}\langle q_1(\varphi_b)| \otimes |q_2(\varphi_b)\rangle_{B_2}\langle q_2(\varphi_b)| \\ &= \sum_{n=0}^{\infty}\sum_{k_0=0}^{n}\sum_{l_0=0}^{n} \psi_{k_0}(q_1)\psi_{l_0}(q_1)\psi_{n-k_0}(q_2)\psi_{n-l_0}(q_2)|k_0,n-k_0\rangle_{B_1B_2}\langle l_0,n-l_0|,\end{aligned} \tag{6.9}$$

where

$$\psi_n(q_j) = \frac{1}{\sqrt{2^n n!\sqrt{2\pi}}} H_n(q_j/\sqrt{2})e^{-q_j^2/4} \tag{6.10}$$

is the coordinate representation of Fock state $|n\rangle$, with H_n being the n-th Hermite polynomial. Therefore, one can virtually insert another photon-number measurement after phase randomization before the squashing channel Eq. (6.4) on the detection side to measure the total photon number of the received state, as shown in Fig. 6.3(d).

Based on the above results, a virtual quantum circuit of the protocol can be depicted when both Alice and Bob chooses the Z-basis in Fig. 6.3(e). Denote the photon-number measurement results on the source side and the detection side as m and n, respectively. Alice and Bob can thus distill secrete keys separately based on the photon-number tag of (m,n). A lower bound on the key rate can then be given by (Gottesman et al., 2004; Ma, 2008)

$$r \geq \sum_{m=0}^{\infty} Q_{m,m}[1 - h(e^X_{m,m})] - fQ^Z h(e^Z), \tag{6.11}$$

where $Q_{m,m}$ and $e^X_{m,m}$ denote the gain and the phase-error rate in the rounds where m photons are sent and m photons are received, Q^Z is the Z-basis gain, e^Z is the bit-error rate, and f is the efficiency of information reconciliation. Note not to confuse the gains with quadrature observables. All the gains and error rates in the key-rate formula are restricted to the rounds with light intensity $\mu_a = \mu$. The rounds where the total photon number decreases after state transmission are discarded, as the photons that are lost may come from Eve's interception, with which Eve can apply a PNS attack. The corresponding phase-error probability is $1/2$; hence these rounds do not contribute to key generation. In addition, as the transmission channel is naturally lossy in a usual setting, the terms where the total photon number increases are not considered.

Note that the key-rate formula in Eq. (6.11) assumes forward reconciliation, where Bob reconciles his raw keys to Alice's, k_a, and then the users perform privacy amplification. The rounds where Alice sends a non-vacuum state while Bob receives a vacuum state are hence insecure, since the information carriers are lost through the channel. Instead, if reverse reconciliation is used, where Alice reconciles her raw keys to Bob's, the rounds where Bob receives a vacuum state become secure. One can interpret Bob's raw keys in these rounds as generated from local random numbers, and no information is known *a priori* in transmission. This is a common practice in usual CV QKD and in accordance with the observation by Qi (2021). Theorem 2 gives the key-rate lower bound with reverse reconciliation as the main key-rate formula to be used:

Theorem 2 *For the time-bin CV QKD protocol 12, in the asymptotic limit with reverse reconciliation, the distillable secure key rate r is lower bounded by* r_{rev}*:*

$$r \geq r_{\mathrm{rev}} = Q_{*,0} + \sum_{m=1}^{\infty} Q_{m,m}[1 - h(e^X_{m,m})] - f Q^Z h(e^Z), \tag{6.12}$$

where $Q_{m,m}$ *and* $e^X_{m,m}$ *denote the gain and the phase-error rate in the rounds where m photons are sent and m photons are received,* Q^Z *is the Z-basis gain,* e^Z *is the bit-error rate, and* f *is the efficiency of information reconciliation.* $Q_{*,0}$ *represents the gain of the rounds where Bob receives a vacuum state for whatever state sent by Alice.*

C. Phase-error probability calculation

The key-rate formula in Eq. (6.12) is now evaluated with Fock-basis observables (Matsuura et al., 2021). The bit-error rate e^Z can be directly measured, as the Z-measurement statistics in the entanglement-based squashing model are the same as the realistic statistics. To evaluate the gains and phase-error probabilities, the state before the phase-error measurement under

each photon-number tag is firstly determined. Define $\hat{P}_m$ as the projector onto the m-photon state on modes A_1 and A_2. When sending m photons, the source in Fig. 6.3(b) collapses to

$$\hat{P}_m^{A_1A_2}\hat{\rho}_{A'A_1A_2}\hat{P}_m^{A_1A_2} = \Pr(m)|\Psi_m\rangle_{A'A_1A_2}\langle\Psi_m|, \tag{6.13}$$

where

$$\begin{aligned} |\Psi_m\rangle_{A'A_1A_2} &= \frac{1}{\sqrt{2}}(|0\rangle_{A'}|0m\rangle_{A_1A_2} + |1\rangle_{A'}|m0\rangle_{A_1A_2}), \\ \Pr(m) &= \frac{e^{-\mu}\mu^m}{m!}. \end{aligned} \tag{6.14}$$

Upon transmitting the m-photon state, $|\Psi_m\rangle_{A'A_1A_2}$, the n-photon state is selected on the detection side after the squashing channel,

$$\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}\left\{\hat{P}_n^{B_1B_2}\mathscr{N}_E^{A_1A_2\to B_1B_2}\left[\Pr(m)|\Psi_m\rangle_{A'A_1A_2}\langle\Psi_m|\right]\hat{P}_n^{B_1B_2}\right\} = Q_{m,n}\hat{\rho}_{A'B'}^{(m,n)}, \tag{6.15}$$

where $\mathscr{N}_E^{A_1A_2\to B_1B_2}$ represents Eve's channel, and $Q_{m,n}$ denotes the probability of sending an m-photon state and accepting an n-photon state, namely the gain for the states tagged by the photon-number tuple, (m,n). Note the probability that Bob aborts the signal is reflected in $Q_{m,n}$. The normalized state, $\hat{\rho}_{A'B'}^{(m,n)}$, is a bipartite qubit, with which the phase-error probability can be evaluated:

$$e_{m,n}^X = \text{Tr}\left[\hat{\rho}_{A'B'}^{(m,n)}\left(|+-\rangle_{A'B'}\langle+-| + |-+\rangle_{A'B'}\langle-+|\right)\right]. \tag{6.16}$$

With respect to the complementary-basis measurement result on the qubit A', $+$ or $-$, the state on modes A_1 and A_2 collapses to

$$|\Psi_m^{\pm}\rangle_{A_1A_2} = \frac{1}{\sqrt{2}}(|0m\rangle \pm |m0\rangle)_{A_1A_2} \tag{6.17}$$

with equal probabilities. For the state on Bob's systems B_1 and B_2 under tag (m,n), $\hat{\rho}_{B_1B_2}^{(m,n)}$, the statistics of the complementary measurement are given by

$${}_{B'}\langle\pm|\mathscr{F}_{\text{rand}}^{B_1B_2\to B'}[\hat{\rho}_{B_1B_2}^{(m,n)}]|\pm\rangle_{B'} = \text{Tr}\left[\hat{\rho}_{B_1B_2}^{(m,n)}\hat{M}_{\pm}\right] = \text{Tr}\left[\hat{\rho}_{B_1B_2}^{(m,n)}\hat{P}_n\hat{M}_{\pm}\hat{P}_n\right], \tag{6.18}$$

where

$$\hat{M}_{\pm} = \frac{1}{2}\int_{\mathbf{R_0}} dq_1 dq_2 \int_0^{2\pi} \frac{d\varphi_b}{2\pi} \left[|q_1(\varphi_b), q_2(\varphi_b)\rangle \pm |q_2(\varphi_b), q_1(\varphi_b)\rangle\right]\left[\langle q_1(\varphi_b), q_2(\varphi_b)| \pm \langle q_2(\varphi_b), q_1(\varphi_b)|\right]. \tag{6.19}$$

In the last equation in Eq. (6.18), the fact is utilised that $\hat{\rho}_{B_1B_2}^{(m,n)}$ acts on the n-photon space of system B_1B_2. Combining the above results, the phase-error rate for each tag can be expressed with observables on optical modes:

Proposition 1 *The phase-error rate $e_{m,n}^X$ of the rounds where m photons are sent and n photons are accepted can be calculated by:*

$$\frac{Q_{m,n}e_{m,n}^X}{\Pr(m)} = \frac{1}{2} Tr\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(|\Psi_m^+\rangle_{A_1A_2}\langle\Psi_m^+|)\hat{P}_n\hat{M}_-\hat{P}_n + \mathscr{N}_E^{A_1A_2\to B_1B_2}(|\Psi_m^-\rangle_{A_1A_2}\langle\Psi_m^-|)\hat{P}_n\hat{M}_+\hat{P}_n\right], \tag{6.20}$$

where $Q_{m,n}$ denotes the probability of sending an m-photon state and accepting an n-photon state, and $\Pr(m)$ is the probability of the source emitting m photons. $\mathscr{N}_E$ denotes Eve's channel on the two optical modes and $\hat{P}_n$ denotes the projector onto the n-photon subspace. $|\Psi_m^{\pm}\rangle$ and $\hat{M}_{\pm}$ defined in Eq. (6.17) *and* (6.19) *respectively.*

The identity $\hat{P}_n\hat{M}_{+(-)}\hat{P}_n$ can be written on the Fock basis using Eq. (6.9), expressing the phase-error rate as quantities on optical modes. Here, the final results for a protocol that utilizes up to the two-photon components are listed:

- For the single-photon component,

$$\begin{aligned}\frac{Q_{1,1}e_{1,1}^X}{\Pr(1)} = \frac{c_1}{2}\Bigg\{&\mathrm{Tr}\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(\left|\Psi_1^+\right\rangle_{A_1A_2}\left\langle\Psi_1^+\right|)\frac{1}{2}(|01\rangle - |10\rangle)_{B_1B_2}(\langle 01| - \langle 10|)\right]\\ &+\mathrm{Tr}\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(\left|\Psi_1^-\right\rangle_{A_1A_2}\left\langle\Psi_1^-\right|)\frac{1}{2}(|01\rangle + |10\rangle)_{B_1B_2}(\langle 01| + \langle 10|)\right]\Bigg\},\end{aligned} \tag{6.21}$$

  where

$$c_1 = \int_{\mathbf{R_0}} dq_1 dq_2 [\psi_0^2(q_1)\psi_1^2(q_2) + \psi_0^2(q_2)\psi_1^2(q_1)], \tag{6.22}$$

  and gain $Q_{1,1}$ is given by

$$\frac{Q_{1,1}}{\Pr(1)} = c_1 \mathrm{Tr}\left\{\mathscr{N}_E\left[\mathrm{Tr}_{A'}(|\Psi_1\rangle_{A'A_1A_2}\langle\Psi_1|)\right](|01\rangle_{B_1B_2}\langle 01| + |10\rangle_{B_1B_2}\langle 10|)\right\}. \tag{6.23}$$

Up to the less-than-unity factor c_1 that arises from the data post-selection in key mapping, the formulae are the same as the complementary-basis result in the coherent-state-based BB84 protocol (Marand and Townsend, 1995).

- For the two-photon subspace, Eq. (6.9) and Eq. (6.20) give:

$$\begin{aligned}\frac{Q_{2,2}e^X_{2,2}}{\Pr(2)} =& \frac{1}{2}c_2^- \mathrm{Tr}\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(\left|\Psi_2^+\right\rangle_{A_1A_2}\left\langle\Psi_2^+\right|)\frac{1}{2}(|02\rangle_{B_1B_2}-|20\rangle_{B_1B_2})(\langle 02|_{B_1B_2}-\langle 20|_{B_1B_2})\right]\\ &+\frac{1}{2}c_2^+ \mathrm{Tr}\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(\left|\Psi_2^-\right\rangle_{A_1A_2}\left\langle\Psi_2^-\right|)\frac{1}{2}(|02\rangle_{B_1B_2}+|20\rangle_{B_1B_2})(\langle 02|_{B_1B_2}+\langle 20|_{B_1B_2})\right]\\ &+c_2^{11}\mathrm{Tr}\left[\mathscr{N}_E^{A_1A_2\to B_1B_2}(\left|\Psi_2^-\right\rangle_{A_1A_2}\left\langle\Psi_2^-\right|)|11\rangle_{B_1B_2}\langle 11|\right],\end{aligned} \tag{6.24}$$

where

$$\begin{aligned}c_2^+ &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2)+\psi_2(q_1)\psi_0(q_2)]^2,\\ c_2^- &= \int_{\mathbf{R_0}} dq_1dq_2[\psi_0(q_1)\psi_2(q_2)-\psi_2(q_1)\psi_0(q_2)]^2,\\ c_2^{11} &= \int_{\mathbf{R_0}} dq_1dq_2[2\psi_1^2(q_1)\psi_1^2(q_2)],\end{aligned} \tag{6.25}$$

and the two-photon gain is given by

$$\begin{aligned}\frac{Q_{2,2}}{\Pr(2)} =& c_2^+\mathrm{Tr}\left\{\mathscr{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\frac{1}{2}(|02\rangle_{B_1B_2}+|20\rangle_{B_1B_2})(\langle 02|_{B_1B_2}+\langle 20|_{B_1B_2})\right\}\\ &+c_2^-\mathrm{Tr}\left\{\mathscr{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]\frac{1}{2}(|02\rangle_{B_1B_2}-|20\rangle_{B_1B_2})(\langle 02|_{B_1B_2}-\langle 20|_{B_1B_2})\right\}\\ &+c_2^{11}\mathrm{Tr}\left\{\mathscr{N}_E^{A_1A_2\to B_1B_2}[\mathrm{Tr}_{A'}(|\Psi_2\rangle_{A'A_1A_2}\langle\Psi_2|)]|11\rangle_{B_1B_2}\langle 11|\right\}.\end{aligned} \tag{6.26}$$

- The probability of accepting a vacuum state when employing reverse reconciliation is given by

$$Q_{*,0} = \mathrm{Tr}\left[\hat{P}_0^{B_1B_2}\mathscr{N}_E^{A_1A_2\to B_1B_2}\left(\hat{\rho}^Z\right)\hat{P}_0^{B_1B_2}\right]\int_{\mathbf{R_0}} 2\psi_0^2(q_1)\psi_1^2(q_2)dq_1dq_2, \tag{6.27}$$

where $\hat{\rho}^Z$ is the Z-basis state sent by the source given in Eq. (6.8); hence $Q_{*,0}$ is given by the product of the probability of receiving a vacuum-state in the Z-basis rounds and

a post-selection-related integration factor. Note that the former value is independent of the post-selection.

6.2.3 Parameter estimation and practical protocol

This section shows how to estimate the parameters derived in Section 6.2.2 with a practical setup. In the actual protocol, photon-number-resolving detectors are not in possession, with which one can directly measure the above parameters. In addition, the phase-error probabilities and gains are defined by particular Fock-basis states, yet the actual photon source emits coherent states. Nevertheless, unbiased estimators can be constructed with the available states and detection settings to evaluate these values. On the detection side, the homodyne tomography technique can be applied to evaluate the photon-number observables (Vogel and Risken, 1989; Smithey et al., 1993; D'Ariano et al., 1994, 1995; Leonhardt and Paul, 1995; D'Ariano, 1995). The homodyne tomography allows unbiased estimation of the expected value of a variety of observables, including the photon-number observables, of measuring an unknown quantum state. On the source side, the decoy-state method (Lo et al., 2005; Wang, 2005) can be extended to evaluate the statistics defined by the non-classical Fock states with the use of the coherent states at hand. A practical version of the protocol will be given at the end of this section.

A. Effective photon-number resolving via homodyne tomography

The first issue to be tackled is the estimation of photon-number statistics. Due to the lack of photon-number-resolving detectors, these operators are not directly measurable. Nevertheless, unbiased estimation (Vogel and Risken, 1989; Smithey et al., 1993; D'Ariano et al., 1994, 1995; Leonhardt and Paul, 1995; D'Ariano, 1995) can be obtained using homodyne tomography . For a systematic review, see the tutorial textbook by D'Ariano et al. (2007).

Start with a single-mode system. Consider the displacement operators given by

$$\begin{aligned}\hat{D}(\alpha) &= \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}) \\ &= \exp\left[(-ik)\frac{\hat{a}^\dagger e^{i\varphi} + \hat{a}e^{-i\varphi}}{2}\right] \\ &:= \exp(-ik\hat{Q}_\varphi),\end{aligned} \tag{6.28}$$

where $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators of the mode, respectively, α is a complex scalar, and α^* denotes the complex conjugate of α. In the second equation, polar variables are used to represent α, $\alpha = (-i/2)ke^{i\varphi}$. $\hat{Q}_\varphi$ is called the quadrature operator.

Measuring $\hat{Q}_\varphi$ corresponds to the homodyne measurement, where the phase of the LO is φ. By definition, $\hat{D}(\alpha)$ is a Hermitian operator. The set of all displacement operators forms an orthogonal and complete function basis on a mode; hence any linear operator on a mode, $\hat{O}$, can be expanded with displacement operators,

$$\hat{O} = \int_0^\pi \frac{d\varphi}{\pi} \int_{-\infty}^{\infty} \frac{dk|k|}{4} \mathrm{Tr}(\hat{O} e^{ik\hat{Q}_\varphi}) e^{-ik\hat{Q}_\varphi}. \tag{6.29}$$

When measuring $\hat{O}$ on a state, $\hat{\tilde{\rho}}$, the expected value is given by

$$\begin{aligned} \langle \hat{O} \rangle =& \mathrm{Tr}(\hat{O}\hat{\tilde{\rho}}) \\ =& \int_0^\pi \frac{d\varphi}{\pi} \int_{-\infty}^{\infty} \frac{dk|k|}{4} \mathrm{Tr}(\hat{O} e^{ik\hat{Q}_\varphi}) \mathrm{Tr}(\hat{O} e^{-ik\hat{Q}_\varphi}) \\ :=& \int_0^\pi \frac{d\varphi}{\pi} \int_{-\infty}^{\infty} dq \mathrm{Tr}[\hat{O} K(\hat{Q}_\varphi - q)] p(q|\varphi) \\ :=& \int_0^\pi \frac{d\varphi}{\pi} \int_{-\infty}^{\infty} dq \mathscr{R}[\hat{O}](q,\varphi) p(q|\varphi), \end{aligned} \tag{6.30}$$

where the value of the term

$$K(q) := \int_{-\infty}^{\infty} \frac{dk}{4} |k| e^{ikq} \tag{6.31}$$

should be determined by the Cauchy principal value, $p(q|\varphi)$ is the conditional probability of obtaining quadrature q when the phase of the homodyne measurement is φ, and $\mathscr{R}[\hat{O}](q,\varphi)$ is the kernel function of $\hat{O}$ with respect to the homodyne measurement. Eq. (6.30) gives a sampling procedure to estimate $\langle \hat{O} \rangle$ for a general unknown system using homodyne measurements (D'Ariano et al., 1994, 1995; D'Ariano, 1995). Namely,

1. Repeat the following process for N times:
   (a) Choose the LO phase of the homodyne measurement, $\varphi_i \in [0, \pi]$, uniformly at random.
   (b) Measure the system and record the result, q_i.
2. Calculate the average value of the kernel function with respect to the observed statistics, $\sum_{i=1}^N \mathscr{R}[\hat{O}](q_i, \varphi_i)/N$.

When the kernel function is bounded, the law of large numbers guarantees the convergence,

$$\langle \hat{O} \rangle = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \mathscr{R}[\hat{O}](q_i, \varphi_i). \tag{6.32}$$

In our protocol, the photon-number operators of interest are $|n\rangle\langle n+d|$, where $|n\rangle$ is the eigenstate of the n-photon eigenstate. For a single mode, the estimator of this operator is given by

$$\mathscr{R}_\eta[|n\rangle\langle n+d|](q,\varphi) = e^{id(\varphi+\frac{\pi}{2})}\sqrt{\frac{n!}{(n+d)!}}\int_{-\infty}^{\infty} dk|k|\exp\left(\frac{1-2\eta}{2\eta}k^2 - ikq\right)k^d L_n^d(k^2), \tag{6.33}$$

where η is the detector efficiency, and L_n^d is the generalized Laguerre polynomial (D'Ariano et al., 1994, 1995; Leonhardt et al., 1995). The kernel function is bounded when $\eta > 1/2$, allowing for a converging tomography result by increasing samples (D'Ariano et al., 1995; D'Ariano, 1995). This is a rather mild requirement for the current technologies (Hansen et al., 2001; Grandi et al., 2017).

Homodyne tomography can be generalized to estimate the statistics of a multiple-mode observable. In our case, one needs to estimate separable observables on two modes, $\hat{O}_1 \otimes \hat{O}_2$, where the modes are specified with subscripts. One can apply independent homodyne measurements to each mode for the estimation. Notably, as $\hat{D}(\alpha_1)\otimes\hat{D}(\alpha_2)$ forms a complete basis on the joint system, then

$$\hat{O}_1\otimes\hat{O}_2 = \int_0^\pi \frac{d\varphi_1}{\pi}\int_{-\infty}^{\infty}\frac{dk_1|k_1|}{4}\mathrm{Tr}(\hat{O}_1 e^{ik_1\hat{Q}_{\varphi_1}})\int_0^\pi\frac{d\varphi_2}{\pi}\int_{-\infty}^{\infty}\frac{dk_2|k_2|}{4}\mathrm{Tr}(\hat{O}_2 e^{ik_2\hat{Q}_{\varphi_2}})(e^{-ik_1\hat{Q}_{\varphi_1}}\otimes e^{-ik_2\hat{Q}_{\varphi_2}}). \tag{6.34}$$

Consequently,

$$\begin{aligned}\langle\hat{O}_1\otimes\hat{O}_2\rangle &= \mathrm{Tr}[(\hat{O}_1\otimes\hat{O}_2)\hat{\hat{\rho}}] \\ &= \int_0^\pi\frac{d\varphi_1}{\pi}\int_{-\infty}^{\infty}dq_1\int_0^\pi\frac{d\varphi_2}{\pi}\int_{-\infty}^{\infty}dq_2\mathscr{R}[\hat{O}_1](q_1,\varphi_1)\mathscr{R}[\hat{O}_2](q_2,\varphi_2)p(q_1,q_2|\varphi_1,\varphi_2).\end{aligned} \tag{6.35}$$

As a remark, note that the quantum state of the two modes, $\hat{\hat{\rho}}$, can generally be entangled. In the experiment, the users simply need two independently phase-randomized homodyne detectors and record the joint conditional probability distribution of quadratures (q_1,q_2) given the LO phases (φ_1,φ_2).

B. Generalised decoy-state method

To effectively realize the non-classical states on the source side, the standard decoy-state method (Lo et al., 2005; Wang, 2005) can be extended taking advantages of the two-mode coherent states with simultaneous phase randomization on the two modes. Denote the state

with phase difference φ as

$$\hat{\rho}_{\mu}^{\varphi}=\int_{0}^{2\pi}\frac{d\theta}{2\pi}\left|\sqrt{\tfrac{\mu}{2}}e^{i\theta}\right\rangle\left\langle\sqrt{\tfrac{\mu}{2}}e^{i\theta}\right|\otimes\left|\sqrt{\tfrac{\mu}{2}}e^{i(\theta+\varphi)}\right\rangle\left\langle\sqrt{\tfrac{\mu}{2}}e^{i(\theta+\varphi)}\right|, \tag{6.36}$$

where the light intensity is specified with the subscript, μ. With proper linear combination of these states, the photon-number-cat states of interest can be effectively constructed. It is well-known that $(|01\rangle\pm|10\rangle)/\sqrt{2}$ is the single-photon component of $\hat{\rho}_{\mu}^{0(\pi)}$,

$$\Pr_{\mu}(1)\left|\Psi_{1}^{+(-)}\right\rangle\left\langle\Psi_{1}^{+(-)}\right|=\hat{P}_{1}\hat{\rho}_{\mu}^{0(\pi)}\hat{P}_{1}, \tag{6.37}$$

where $\Pr_{\mu}$ represents the Poisson distribution determined by light intensity μ, as given in Eq. (6.14). Thus, the estimation problem is transformed into the estimation of the single-photon yields of $\hat{\rho}_{\mu}^{0}$ and $\hat{\rho}_{\mu}^{\pi}$. For the multi-photon components $(|0m\rangle\pm|m0\rangle)/\sqrt{2}$, a direct calculation shows

$$\Pr_{\mu}(m)|\Psi_{m}^{+}\rangle\langle\Psi_{m}^{+}|=\hat{P}_{m}\left(\hat{\rho}_{\mu}^{Z}+\frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_{\mu}^{\frac{2\pi k}{m}}-\frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_{\mu}^{\frac{2\pi k}{m}+\delta}\right)\hat{P}_{m}, \tag{6.38}$$

$$\Pr_{\mu}(m)|\Psi_{m}^{-}\rangle\langle\Psi_{m}^{-}|=\hat{P}_{m}\left(\hat{\rho}_{\mu}^{Z}-\frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_{\mu}^{\frac{2\pi k}{m}}+\frac{2^{m-2}}{m}\sum_{k=0}^{m-1}\hat{\rho}_{\mu}^{\frac{2\pi k}{m}+\delta}\right)\hat{P}_{m}, \tag{6.39}$$

where $\delta=\pi$ for odd m and $\pi/2$ for even m, and $\hat{\rho}_{\mu}^{Z}$ is the state emitted from the source in a key generation round. Consequently, the terms that define $e_{m,m}^{X}$ and $Q_{m,m}$ can be constructed from the statistics when emitting the states of $\hat{\rho}_{\mu}^{Z}$ and $\hat{\rho}_{\mu}^{\varphi}$ with $\varphi\in\{2\pi k/m,2\pi k/m+\delta\}_{k=0}^{m-1}$. Notably, the extended decoy method allows estimating the gains with the number of parameters increasing only linearly in the photon number. In later discussions, a maximal two-photon components will be utilised. Specifically, for $m=2$,

$$\Pr_{\mu}(2)\left|\Psi_{2}^{\pm}\right\rangle\left\langle\Psi_{2}^{\pm}\right|=\hat{P}_{2}\left[\hat{\rho}_{\mu}^{Z}\pm\left(\frac{1}{2}\hat{\rho}_{\mu}^{0}+\frac{1}{2}\hat{\rho}_{\mu}^{\pi}\right)\mp\left(\frac{1}{2}\hat{\rho}_{\mu}^{\frac{\pi}{2}}+\frac{1}{2}\hat{\rho}_{\mu}^{\frac{3\pi}{2}}\right)\right]\hat{P}_{2}. \tag{6.40}$$

The parameter estimation can thus be done based on the homodyne tomography and extended decoy methods. In the experiment, given that they choose certain bases and light intensity, the users can collect data and evaluate the conditional probabilities for taking $(\varphi_{b}^{1},\varphi_{b}^{2})=\vec{\varphi}_{b}$ and observing $(q_{1},q_{2})=\vec{q}$ in the homodyne measurements, or the yields. For simplicity, the notations of $Y_{\mu_{a},(\vec{\varphi}_{b},\vec{q})}^{Z}$ and $Y_{\mu_{a},(\vec{\varphi}_{b},\vec{q})}^{\varphi}$ are adopted. In the subscript, μ_{a} denotes the light intensity, and $(\vec{\varphi}_{b},\vec{q})$ denotes the homodyne measurement results of Bob. When the superscript writes Z, it denotes that Alice chooses the Z-basis; when the superscript writes

φ, it denotes that Alice chooses the X-basis and $\varphi_a^2 - \varphi_a^1 = \varphi$. Via homodyne tomography, these values can be used to estimate $Y^Z_{\mu_a,\hat{O}}$ and $Y^{\varphi}_{\mu_a,\hat{O}}$, namely, the expected value of measuring observable $\hat{O}$ conditioned on the corresponding input settings. Following Eq. (6.30), the yields are given by

$$\begin{aligned} Y^Z_{\mu_a,\hat{O}} &= \int_0^{\pi} d\varphi_b^1 \int_0^{\pi} d\varphi_b^2 \int_{-\infty}^{\infty} dq_1 \int_{-\infty}^{\infty} dq_2 \mathscr{R}[\hat{O}](\vec{q},\vec{\varphi}_b) Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}, \\ Y^{\varphi}_{\mu_a,\hat{O}} &= \int_0^{\pi} d\varphi_b^1 \int_0^{\pi} d\varphi_b^2 \int_{-\infty}^{\infty} dq_1 \int_{-\infty}^{\infty} dq_2 \mathscr{R}[\hat{O}](\vec{q},\vec{\varphi}_b) Y^{\varphi}_{\mu_a,(\vec{\varphi}_b,\vec{q})}. \end{aligned} \tag{6.41}$$

In the second step, the extended decoy state methods are applied to estimate the gains and phase-error probabilities in Eq. (6.12), the key-rate formula. With finite decoy states, the users can obtain upper and lower bounds on these quantities (Ma, 2008).

Since the estimation procedure involves many quantities, for convenience, the estimation procedures and the involved quantities are listed in Table 6.2. Note that the original data can be re-used to estimate various quantities in homodyne tomography by varying the kernel function with respect to the observable under consideration.

Table 6.2 Parameter estimation with homodyne tomography and decoy states. In our work, the light intensity is chosen from the set $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$. For simplicity, denote the photon-number operator, $|n_1 n_2\rangle\langle n_1 n_2|$, as $|n_1 n_2\rangle$ in the subscripts of the yields, and similarly for $|\Psi_n^{\pm}\rangle$. Denote the lower and upper bounds with additional superscripts of L and U, respectively. Note that one can directly estimate $Q_{*,0}$ in the rounds of $\mu_a = \mu$. The estimation of $e^X_{2,2}$ involves statistics in the rounds that Alice chooses the Z-basis and X-basis with $\varphi = k\pi/2$.

Original data	Homodyne-tomography estimation	Decoy-state estimation
$Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^Z_{\mu,\|00\rangle}$	$Q_{*,0}$
	$Y^Z_{\mu_a,\|01\rangle}, Y^Z_{\mu_a,\|10\rangle}$	$Q^L_{1,1}, Q^U_{1,1}$
	$Y^Z_{\mu_a,\|02\rangle}, Y^Z_{\mu_a,\|20\rangle}, Y^Z_{\mu_a,\|11\rangle}$	$Q^L_{2,2}, Q^U_{2,2}$
$Y^{\varphi}_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^{\varphi=\pi}_{\mu_a,\|\Psi_1^+\rangle}, Y^{\varphi=0}_{\mu_a,\|\Psi_1^+\rangle}, Y^{\varphi=\pi}_{\mu_a,\|\Psi_1^-\rangle}, Y^{\varphi=0}_{\mu_a,\|\Psi_1^-\rangle}$	$e^{X,L}_{1,1}, e^{X,U}_{1,1}$
	$Y^{\varphi=k\pi/2}_{\mu_a,\|\Psi_2^+\rangle}, Y^{\varphi=k\pi/2}_{\mu_a,\|\Psi_2^-\rangle}, Y^{\varphi=k\pi/2}_{\mu_a,\|11\rangle}$	$e^{X,L}_{2,2}, e^{X,U}_{2,2}$
$Y^Z_{\mu_a,(\vec{\varphi}_b,\vec{q})}$	$Y^Z_{\mu_a,\|\Psi_2^+\rangle}, Y^Z_{\mu_a,\|\Psi_2^-\rangle}, Y^Z_{\mu_a,\|11\rangle}$	

C. General parameter estimation under the coherent attack

The security analysis and parameter estimation under the coherent attack case are briefly discussed. In the most general adversarial scenario, namely the coherent attack, Eve can

apply a joint quantum operation over the rounds for eavesdropping, which may correlate or even entangle the states transmitted to Bob. Eve collects all the side information leaked to her in the protocol and then guesses the legitimate users' keys. Under such an attack, the measurement statistics obtained by Bob are generally correlated over the rounds (Xu et al., 2020).

The complementarity-based security analysis remains valid with finite statistics under a coherent attack (Koashi, 2009). The information leakage is quantified via the number of phase errors, while the occurrence of a phase error in each round may be non-i.i.d. That is, one should interpret the gains and phase-error rates in Eq. (6.12) as frequencies in non-i.i.d. statistics. For instance, $Q_{1,1}$ should be regarded as the frequency of the events that Alice sends a single-photon state, and Bob accepts a single-photon state among key generation rounds in the virtual experiment. The remaining problem is to estimate these parameters via observed statistics.

To tackle the non-i.i.d. parameter estimation problem, a martingale-based analysis can be applied. The details can be found in the appendix of (Jin et al., 2023). As the starting point, in the i'th round, the users can evaluate the probability of choosing some experimental setting and observing a particular event conditioned on the experimental history, including the events of sending an m-photon state and accepting an n-photon state and the occurrence of a phase error if they choose the key generation setting, and observing a particular homodyne detection result if they choose to perform the parameter estimation operations. The events' correlations with the experimental history are inherently taken into account in the definitions of conditional probabilities. Martingales can be set up for a series of events, such as the occurrence of phase errors in each round of the virtual protocol, and link their frequencies with the associated conditional probabilities via concentration results like Azuma's inequality (Azuma, 1967). Note that such concentration results work for general non-i.i.d. correlations. Furthermore, the setting choices randomly chosen by Alice and Bob are independent of the experimental history and unknown to Eve. Therefore, conditioned on the experimental history, the probabilities of different possible events in a round are linked. For instance, the probability that the users take key generation measurements and a phase error occurs in a round is measurable via the probability that they instead take parameter estimation measurements and observe certain statistics. The relation is in the form of Eq. (6.20), while now the probabilities are interpreted as conditional ones that cover the correlations. The relations between conditional probabilities then link the martingales for the parameter estimation measurement with the ones for the gains and phase-error rates, completing the parameter estimation. In the end, the total number of keys that can be securely distilled from finite statistics under the coherent attack is given by a formula of the following form:

Theorem 3 (Informal) *The finite-size key rate r is lower bounded by:*

$$r \geq \bar{Q}^L_{*,0} + \sum_{m=1}^{\infty} \left(\bar{Q}^L_{m,m} \left\{ 1 - h[\bar{e}^{X(U)}_{m,m}] \right\} + \frac{1}{N^{zz}_{\mu}} \log \varepsilon^{\mathrm{pa}}_{m,m} \right) - f Q^Z h(e^Z), \tag{6.42}$$

where the barred notations specify that the quantities should be considered as average values of non-i.i.d. statistics and superscripts L and U represent the estimated lower and upper bounds. $\varepsilon^{\mathrm{pa}}_{m,m}$ *denotes the failure probability (Koashi, 2009; Fung et al., 2010) of the group sending m photons and accepting m photons.* N^{zz}_{μ} *is the number of key-generation rounds.*

Note that the failure probability $\varepsilon^{\mathrm{pa}}_{m,m}$ comes from the possible estimation inaccuracy of the decoy state method, homodyne tomography, and the convergence of the martingale-based concentration results, introducing an additional cost of $(-\log \varepsilon^{\mathrm{pa}}_{m,m})$ key bits. In the asymptotic limit where the number of key generation rounds $N^{zz}_{\mu} \to \infty$, the average cost of this term per round converges to zero, and the key rate formula degenerates to that in Eq. (6.12).

D. Practical protocol

Combining the above ingredients, it is provided below the practical protocol 13 that utilizes up to the two-photon components. In the parameter estimation, Bob applies homodyne tomography to estimate the statistics of measuring photon-number observables, including $|00\rangle$, $(|01\rangle \pm |10\rangle)/\sqrt{2}$, $(|02\rangle \pm |20\rangle)/\sqrt{2}$, and $|11\rangle$, on various states transmitted from the source, originally $\hat{\rho}^Z_{\mu_a}$ and $\hat{\rho}^{\varphi_a}_{\mu}$. Afterward, the users can obtain upper and lower bounds on the gains and phase-error rates by applying the extended decoy-state method.

Protocol 13 ***Practical time-bin CV QKD with decoy states using up to two photons***

1. ***Encoding:***
   - *Z*-basis*:*
     (a) *Alice randomly selects a key bit* $k_a \in \{0,1\}$*, a phase factor* $\varphi_a \in \{2\pi j/D\}_{j=0}^{D-1}$*, and a light intensity* $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) *Alice prepares a coherent state of* $|0\rangle_{A1}\left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle_{A2}$ *for* $k_a = 0$ *or* $\left|\sqrt{\mu_a}e^{i\varphi_a}\right\rangle_{A1}|0\rangle_{A2}$ *for* $k_a = 1$.
   - *X*-basis*:*
     (a) *Alice randomly selects two phase factors* $\varphi^1_a, \varphi^2_a \in \{2\pi j/D\}_{j=0}^{D-1}$ *and a light intensity* $\mu_a \in \{\mu, \nu_1, \nu_2, 0\}$.
     (b) *Alice prepares a coherent state of* $\left|\sqrt{\mu_a/2}e^{i\varphi^1_a}\right\rangle\left|\sqrt{\mu_a/2}e^{i\varphi^2_a}\right\rangle$.

2. ***Transmission:*** *Alice sends the state through an authenticated channel to Bob.*

3. ***Detection:***

   - Z-basis*:*
     (a) *Bob randomly selects a phase factor* $\varphi_b \in \{2\pi j/D\}_{j=0}^{D-1}$.
     (b) *Bob uses homodyne detectors with LO phases* φ_b *to measure the modes and obtain quadratures* q_1 *and* q_2.
     (c) *Bob decodes the key bit as* 0 *if* $|q_1| < \tau \wedge |q_2| > \tau$, 1 *if* $|q_1| > \tau \wedge |q_2| < \tau$, *and* $\emptyset$ *otherwise.*
   - X-basis*:*
     (a) *Bob randomly selects two phases* $\varphi_b^1, \varphi_b^2 \in \{\pi j/D\}_{j=0}^{D-1}$.
     (b) *Bob uses homodyne detectors with LO phases* φ_b^1 *and* φ_b^2 *to measure the modes and obtain quadratures* q_1 *and* q_2.

4. ***Sifting:*** *Alice and Bob announce the basis in each round. Alice announces the light intensity in each round and relative phase between the two modes in X-basis states* $\varphi_a = \varphi_a^2 - \varphi_a^1$. *They obtain raw keys in the rounds where they both choose Z-basis with light intensity* $\mu_a = \mu$ *and* $k_b \neq \emptyset$.

5. ***Parameter estimation:*** *Bob estimates the gains and phase-error rates from the statistics in the rounds where Alice sends the Z-basis states* $\hat{\rho}_{\mu_a}^{Z}$ *or X-basis states* $\hat{\rho}_{\mu_a}^{\varphi_a}$ *with* $\varphi_a \in \{0, \pi/2, \pi, 3\pi/2\}$.

6. ***Information reconciliation and privacy amplification****: Alice and Bob perform reverse information reconciliation and privacy amplification to obtain final keys.*

In the end, some remarks on the protocol should be made. Alice's announcement of the relative phase does not reveal key information since the key is encoded in the relative intensity between the two modes. In addition, the discrete phase randomization are parameterised with the same value, D, for both state preparation and homodyne detection in different basis choices. This does not need to be the case in practice, and one can take different phase randomization precision in these procedures for higher accuracy or to compromise the devices' functioning.

6.2.4 Performances and comparison

This section demonstrates the key rate-distance performances of the time-bin CV QKD protocol. A thermal noise channel with a unit-efficiency homodyne detector is considered.

An inefficient detector with thermal electronic noise can be equated to a fiber section with transmittance equal to the detector efficiency, and the electronic noise absorbed into the channel excess noise (Eq. (B.12)). The fiber attenuation is 0.2 dB/km, and the error-correction efficiency f is taken to be 1. The simulation formulae can be found in Appendix B.3.

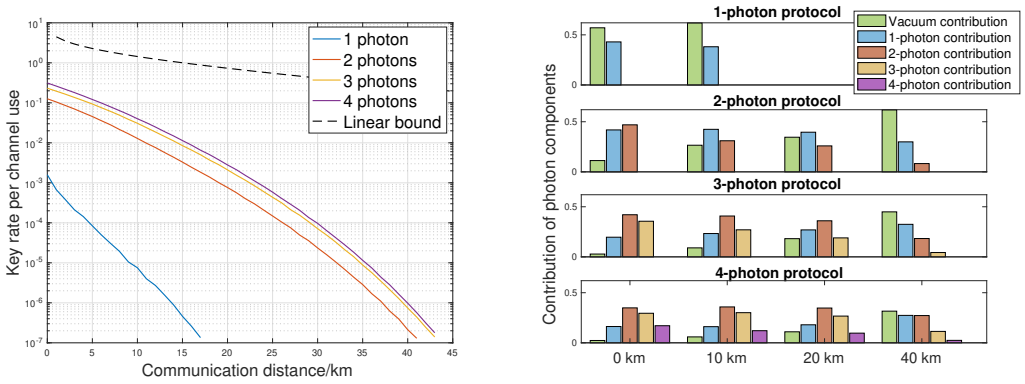
According to the key rate formula Eq. (6.12), the rounds where Alice sends m photons and Bob receives m photons can assure to generate secure keys. The asymptotic key rate of the i-photon protocol is plotted in Fig. 6.4a assuming perfect decoy estimation and no excess noise, where in an i-photon protocol secure keys are only extracted from a maximal i-photon components. In this ideal case, the phase error rates of all the protocols are zero. The optimized source intensities μ and the post-selection thresholds τ are listed in Table 6.3, as well as the resulted Z-basis error rate. Notice that the two-photon-protocol key rate derived from our DV method is similar to that from (Primaatmaja et al., 2022) using CV method, both reversely reconciled. This implies the connection between DV and CV security analysis, as well as the validity of the DV reverse reconciliation idea in Theorem 2. To facilitate the discussion, the contribution of each photon components to the key rate at different distances is also plotted in Fig. 6.4b . In each group of bars, the relative contribution of the vacuum, one, two, three, four-photon components are plotted respectively, where the m-photon contribution of the i-photon protocol is defined to be $Q_{m,m}/(Q_{*,0}+\sum_{m=1}^{i} Q_{m,m})$ and the vacuum contribution is $Q_{*,0}/(Q_{*,0}+\sum_{m=1}^{i} Q_{m,m})$, i.e., the relative contribution to the raw key rate.

Table 6.3 The optimized intensities and post-selection thresholds of protocols using one to four photons respectively at different distances. μ_i, τ_i and e_Z^i denote the optimized intensity, post-selection threshold and the Z-basis error rate of the i-photon protocol. These parameters generate the four key rate plots in Fig. 6.4a, assuming infinite decoy levels.

	μ_1	μ_2	μ_3	μ_4	τ_1	τ_2	τ_3	τ_4
0 km	0.356	1.487	2.395	2.395	1.437	1.641	1.845	1.845
10 km	0.137	0.924	1.887	2.395	3.476	2.253	2.457	2.457
20 km	—	0.728	1.487	1.887	—	3.068	3.068	3.272
40 km	—	0.356	0.728	1.172	—	4.495	4.495	4.699

e_Z^1	e_Z^2	e_Z^3	e_Z^4
30.95%	10.52%	5.31%	5.31%
29.80%	14.84%	5.66%	4.17%
—	15.48%	6.91%	3.85%
—	28.52%	17.07%	8.81%

It can be seen that the key rate improves as making use of the multi-photon components. The improvement is most remarkable between the one and two-photon protocols. This is



(a) (b)

Fig. 6.4 **(a)** The solid lines illustrate the asymptotic key rates of protocols using maximal one, two, three and four photons to generate keys. The dotted line is the linear key rate bound (Takeoka et al., 2014; Pirandola et al., 2017). The PLOB bound is plotted here. The channel and devices are assumed to be ideal with no excess noise and inefficiency. **(b)** The relative contribution of $Q_{m,m}$, i.e. the gain of the rounds where m photons are sent and m photons are received. The m-photon contribution of the i-photon protocol is relative to the raw key rate. Each group of bars illustrate the contribution of vacuum, one, two, three and four-photon components of the protocol at a certain distance.

reasonable since in the one-photon protocol, the multi-photon components are considered insecure, thus limiting the source intensity. The low source intensity would result in severe bit error rate and higher post-selection thresholds, which in turn suppress the key rate. Whilst in the two-photon protocol where the two-photon components are considered secure, the limit in the source intensity can be lifted, and the bit error rate would drop, resulting in higher key rates. This is manifested in Fig. 6.4b, where the single-photon protocol sees significant vacuum contribution, whilst the two-photon protocol, at short distances, does not. Since the vacuum component would yield 50% bit error rate, it can be seen that the lower bit error rate of the two-photon protocol than the single-photon protocol as in Table 6.3.

When further making use of the three-photon components, the key rate as well as the source intensity still increase, yet less obviously. This is mainly because the fraction of the rounds where three photons are sent and three photons are received, decaying cubically with the channel transmittance, are not dominating, especially at longer distances. For example, as in Fig. 6.4b that at 20 km, the contribution of the three-photon component is less than that of the single and two-photon components, and at 40 km the three-photon component rarely has contribution to the key rate. This trend is justified further in the four-photon protocol, where in Fig. 6.4b sees the four-photon-component contribution is quite small for longer distances, and in turn the key rate of the four-photon protocol only improves marginally

than that of the three-photon protocol. Simulation shows that resorting to higher-than-four photon-number components has negligible increase to the key rate. Hence, If considering the protocol with infinite photon-number components, the 0-km key rate is around 0.31 bit/channel, and the BB84 protocol with currently the best single-photon detector of 80% efficiency (Grünenfelder et al., 2020; Li et al., 2023) has 0-km key rate 0.29 bit/channel, based on the model by Ma et al. (2005). Our key rate thus matches the best BB84 key rate with practically favorable devices.

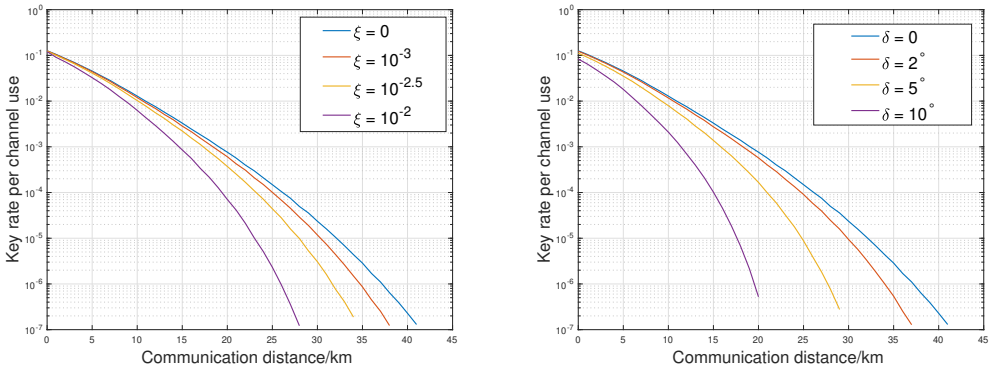
The practical performances of the two-photon time-bin CV QKD protocol are illustrated in Fig. 6.5. For a reasonable range of excess noise ξ from 10^{-3} to 10^{-2} with respect to channel output, the key rate decays mildly as shown in Fig. 6.5a. Notice that the key rate is almost unaffected at 0 km since no noise photon is introduced to give phase error, and the bit error is almost unchanged for a negligible increase in the shot-noise variance. This demonstrates the robustness of the phase-error analysis to the excess noise.

Fig. 6.5b illustrates the key rate against the mode reference misalignment, where the two optical modes generating the time-bin qubit differ by δ in the reference phases intrinsically. The misalignment in relative phases does not affect the Z basis as the key bits are encoded into the relative intensities, and it only affects the X basis where the phase error is defined as the flips in relative phases. Our protocol thus has robustness against misalignment.

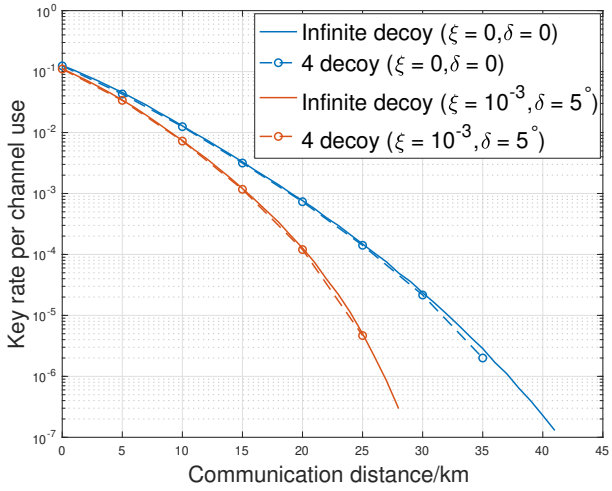
Fig. 6.5c illustrates the key rates of the practical decoy-state protocol 13. One decoy level is set at vacuum, and the two decoy intensities ν_1 and ν_2 and the signal intensity μ are heuristically optimised. The decoy estimations are done by linear programming with a cutoff photon number 10 (Ma et al., 2012; Xu et al., 2014). For both the noiseless setup, with no excess noise and misalignment, and the practical setup, with 10^{-3} excess noise and 5° misalignment, the 4-level decoy estimation is almost exact. This clearly surpassed the practical performance of the protocol by Primaatmaja et al. (2022), since our protocol uses simpler estimation of the phase error by identifying the principal components in key generation. The optimized parameters of the practical setup are listed in Table 6.4.

6.2.5 Concluding remarks

In summary, the time-bin-encoding CV QKD protocol is presented with a phase-error-based security analysis. Similar to the ideas in DV protocols (Beaudry et al., 2008) and other CV protocols (Matsuura et al., 2021), a squashing channel is introduced to "squash" the original privacy-estimation problem on two optical modes to a single qubit, enabling the definition of phase-error rate. The phase randomization on both the source and detector enables the introduction of the photon-number-tagging method, identifying the central components for key generation. Combined with the decoy-state estimation, our parameter estimation is made



(a) (b)



(c)

Fig. 6.5 Practical performances of the two-photon protocol. **(a)** Key rate against excess noise with respect to channel output, assuming infinite decoy levels. **(b)** Key rate against misalignment, i.e. the phase-reference difference between the two optical modes generating the time-bin qubit, assuming infinite decoy levels. **(c)** Key rate derived using decoy methods. The noiseless setup (blue curves) uses fixed decoy levels at 1.2×10^{-4}, 1×10^{-4} and vacuum, and the optimized protocol parameters of the practical setup (red curves) are listed in Table 6.4.

Table 6.4 Optimal protocol parameters in generating the key rate plot with 10^{-3} excess noise and 5° misalignment, using 4 decoy levels, as in Fig. 6.5c. The heuristically optimized signal intensity, post-selection threshold and the decoy intensities are as given. There is one more decoy intensity set to be vacuum. The decoy estimation is done by linear programming with cutoff photon number 10.

Distance (km)	Signal intensity μ	Threshold τ	Decoy intensity ν_1	Decoy intensity ν_2
0	1.487	1.641	1.737×10^{-1}	1.000×10^{-4}
5	1.172	2.049	3.406×10^{-3}	2.740×10^{-4}
10	0.924	2.457	2.993×10^{-2}	1.000×10^{-4}
15	0.924	3.068	1.861×10^{-2}	1.000×10^{-4}
20	0.728	3.476	1.355×10^{-2}	2.441×10^{-4}
25	0.728	4.291	1.355×10^{-2}	1.562×10^{-4}

simple and efficient. This methods of constructing squashing models and applying phase randomization are expected to be applied to many other CV protocols.

One of our major observation is that the coherent detectors can be used to estimate the privacy of the multi-photon signals. This may also be helpful to the protocols with DV detectors. In fact, a hybrid protocol may be considered: single-photon detectors for key generation and homodyne detectors for parameter estimation. The multi-photon components in this protocol can contribute to the key generation compared with the single-photon BB84 protocol.

A general framework for finite-size analysis based on martingale for this CV protocol is provided. Due to photon-number tagging method, the finite-size analysis is greatly simplified. A direct follow-up of this work is to complete the finite-size analysis, encompassing the effects on the distillable key rate, the decoy-method accuracy and the deviation of the homodyne tomography. In the literature, variants of Azuma's inequality have been applied for faster convergence of parameter estimation in quantum key distribution (Currás-Lorenzo et al., 2021; Zhang et al., 2023), such as Kato's inequality (Kato, 2020). One can borrow such techniques to the protocol in this work for better practicality.

It is tempting to enhance the key rate as well as the maximal distance of this protocol. The high-dimensional time-bin encoding may be considered, which is relatively easy to implement experimentally (Islam et al., 2017, 2019; Vagniluca et al., 2020). The high-dimensional complementarity security analysis (Jin et al., 2021) can be invoked, and the squashing channel should map the optical modes to a qudit. The trusted-noise model can also be applied to alleviate the effect of the detector noise (Usenko and Filip, 2016; Qi and Lim, 2018). This requires the modification of the detector POVM, which is shown to be still block-diagonal in Fock basis (Primaatmaja et al., 2022). One may also consider to use

squeezed states as the light source to reduce the shot noise in one quadrature and use the other quadrature for parameter estimation only. This may tackle the large bit error rate due to the shot noise, rendering our 0-km performance not as good as the usual CV QKD scheme. The measurement-device-independent-type schemes (Lo et al., 2012; Ma and Razavi, 2012) and their extensions, including the twin-field-type (Lucamarini et al., 2018; Ma et al., 2018; Wang et al., 2018b) and the mode-pairing schemes (Zeng et al., 2020; Xie et al., 2022), may also be helpful to enhance the long-distance performance of our protocol.

Chapter 7

Conclusion and outlooks

In this thesis, the state-of-the-art QKD-protocol designs are reviewed, focusing on both the theoretical soundness and the practicality. In the current noisy intermediate-scale quantum era (Preskill, 2018), without the possession of reliable quantum repeaters (Azuma et al., 2023), QKD protocols should be designed towards high key rate and long allowable distance using mainly linear optics. Three categories of protocols are discussed that are believed to be the suitable next-generation QKD types:

- *TF QKD*: this type of protocols invoke the entanglement between vacuum and single photon, thus able to break the linear key rate-transmittance bound (Pirandola et al., 2017; Takeoka et al., 2014) for the repeaterless QKD. The implementation of the TF QKD is still an outstanding research topic in search for stable phase interference between several hundreds kilometers.

- *Discrete-modulated CV QKD*: this type of protocols are highly practical utilising the standard coherent detectors and discrete modulation. The main drawbacks lie in the theoretical side, where it still lacks a reliable key rate formula under the most general coherent attacks.

- *Time-bin CV QKD*: this protocol is also highly practical as a coherent-detected protocol without the need for pilot references. What is more, the security can be derived under the coherent attacks with simple parameter estimations and finite-size analysis. The main drawback of the time-bin CV protocol is its limited allowable distance, largely due to the sensitivity of intensity encoding to the channel loss.

It can thus be concluded that the field of QKD is still under-developed mainly in the practicality of DV protocols and the theoretical soundness of CV protocols. There are several possible future directions extending the works in this thesis:

- *High-dimensional discrete-modulated CV QKD*: As is shown in Section 5.3 the high-dimensional DM CV QKD using more than two constellations can greatly improve the key-rate performance with mild experimental requirements. Its security is however incomplete. In Section 6.1, it is mentioned that Matsuura et al. (2021) proposed a phase-error-based security analysis to the DM CV QKD. Their security analysis is robust covering coherent attacks and finite size, yet only restricted to binary dimension. It is thus tempting to extend the security analysis of binary DM CV QKD to higher dimensions. The author's work on high-dimensional complementarity-based security analysis introduced in Section 3.1 can be applied, with the squashing channel and operator bound methods extended trivially to high dimensions.

- *Mode-pairing scheme of time-bin CV QKD*: The time-bin CV QKD in Section 6.2 encodes the key bits onto the relative intensities between two optical modes, and estimates parameters based on the relative phases. The two-mode encoding removes the need for global references and invalidates phase randomisation, yet it also gives up the merits of single-mode encoding such as loss tolerance and protocol flexibility. A possible approach to retain these features is the mode-pairing scheme (Zeng et al., 2022; Xie et al., 2022), where optical pulses are first prepared and processed independently, and paired together later based on the statistics to obtain relative information. The original mode-pairing QKD is upon the MDI setup, and it is possible to borrow the techniques to the prepared-and-measure time-bin CV QKD, or revise it to an MDI version.

- *Experimental reference-frame-independent PM QKD*: The RFI design of PM QKD introduced in Section 4.4 eliminates the need for phase calibration and post compensation in realistic experiments. It is helpful to deploy this technique with the practical mode-pairing scheme (Zhou et al., 2023) to completely remove the need for global references without much experimental complexity.

- *Experimental time-bin CV QKD*: The time-bin CV QKD introduced in Section 6.2 is claimed to be both theoretically robust and experimentally simple. This claim would be supported if demonstrative experiments and even field trials were to be carry out. One of the difficulties in the implementation would be the homodyne tomography technique, which would be affected by device imperfections such as detector inefficiency and electronic noise. Apart from characterising the devices carefully, algorithms from existed demonstrations (Lobino et al., 2008; Grandi et al., 2017; Kiesel et al., 2008, 2011) can be borrowed to improve the tomography accuracy and efficiency.

One of the ultimate applications of quantum information processing techniques is the realisation of quantum internet (Wehner et al., 2018), where each user holds a fault-tolerant quantum computer and communicates quantum states via quantum channels secured by quantum cryptography. It is thus crucial to prepare the QKD technologies to match this future advance. Apart from improving QKD performances from the protocol-wise, the design of practical quantum repeaters is another feasible route to ultimately lift the distance limits of QKD. Researches have been devoted in this direction, studying, for instance, the all-photonic design of quantum repeaters (Azuma et al., 2015) with graph states and the compatible tree-graph quantum error correction codes (Varnava et al., 2006).

References

Artin, M. (2011). Finite fields. In *Algebra*, chapter 15.7, pages 459–462. Pearson Education.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M. P., Hartmann, M. J., Ho, A., Hoffmann, M., Huang, T., Humble, T. S., Isakov, S. V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P. V., Knysh, S., Korotkov, A., Kostritsa, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrà, S., McClean, J. R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M. Y., Ostby, E., Petukhov, A., Platt, J. C., Quintana, C., Rieffel, E. G., Roushan, P., Rubin, N. C., Sank, D., Satzinger, K. J., Smelyanskiy, V., Sung, K. J., Trevithick, M. D., Vainsencher, A., Villalonga, B., White, T., Yao, Z. J., Yeh, P., Zalcman, A., Neven, H., and Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510.

Azuma, K. (1967). Weighted sums of certain dependent random variables. *Tohoku Math. J. Second Ser.*, 19(3):357–367.

Azuma, K., Economou, S. E., Elkouss, D., Hilaire, P., Jiang, L., Lo, H.-K., and Tzitrin, I. (2023). Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.*, 95(4):045006.

Azuma, K., Tamaki, K., and Lo, H.-K. (2015). All-photonic quantum repeaters. *Nature communications*, 6(1):1–7.

Beaudry, N. J., Moroder, T., and Lütkenhaus, N. (2008). Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601.

Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D., and Oppenheim, J. (2005). The universal composable security of quantum key distribution. In *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings 2*, pages 386–406. Springer.

Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York. IEEE Press.

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899.

Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851.

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330–1333.

Bunandar, D., Govia, L. C. G., Krovi, H., and Englund, D. (2020). Numerical finite-key analysis of quantum key distribution. *npj Quantum Information*, 6(1):104.

Calderbank, A. R. and Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105.

Cao, Z., Zhang, Z., Lo, H.-K., and Ma, X. (2015). Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.*, 17(5):053014.

Chau, H. (2005). Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Transactions on Information Theory*, 51(4):1451–1468.

Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhang, W.-J., Han, Z.-Y., Ma, S.-Z., Hu, X.-L., Li, Y.-H., Liu, H., Zhou, F., Jiang, H.-F., Chen, T.-Y., Li, H., You, L.-X., Wang, Z., Wang, X.-B., Zhang, Q., and Pan, J.-W. (2021). Twin-field quantum key distribution over a 511-km optical fibre linking two distant metropolitan areas. *Nature Photonics*, 15(8):570–575.

Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhao, D.-F., Zhang, W.-J., Chen, F.-X., Li, H., You, L.-X., Wang, Z., Chen, Y., Wang, X.-B., Zhang, Q., and Pan, J.-W. (2022). Quantum key distribution over 658 km fiber with distributed vibration sensing. *Physical Review Letters*, 128(18):180502.

Coles, P. J. (2012). Unification of different views of decoherence and discord. *Physical Review A*, 85(4):042103.

Coles, P. J., Metodiev, E. M., and Lütkenhaus, N. (2016). Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7(1):11712.

Currás-Lorenzo, G., Navarrete, Á., Azuma, K., Kato, G., Curty, M., and Razavi, M. (2021). Tight finite-key security for twin-field quantum key distribution. *npj Quantum Information*, 7(1):22.

Curty, M., Azuma, K., and Lo, H.-K. (2019). Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information*, 5(1):64.

D'Ariano, G. (1995). Tomographic measurement of the density matrix of the radiation field. *J. Eur. Opt. Soc. B*, 7(4):693.

D'Ariano, G. M., Leonhardt, U., and Paul, H. (1995). Homodyne detection of the density matrix of the radiation field. *Phys. Rev. A*, 52(3):R1801–R1804.

D'Ariano, G. M., Macchiavello, C., and Paris, M. G. A. (1994). Detection of the density matrix through optical homodyne tomography without filtered back projection. *Phys. Rev. A*, 50(5):4298–4302.

D'Ariano, G. M., Maccone, L., and Sacchi, M. F. (2007). Homodyne tomography and the reconstruction of quantum states of light. In *Quantum Information With Continuous Variables of Atoms and Light*, pages 141–158. World Scientific.

Denys, A., Brown, P., and Leverrier, A. (2021). Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540.

Devetak, I. and Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235.

Durt, T., Englert, B.-G., Bengtsson, I., and Życzkowski, K. (2010). On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640.

Eriksson, T. A., Hirano, T., Puttnam, B. J., Rademacher, G., Luís, R. S., Fujiwara, M., Namiki, R., Awaji, Y., Takeoka, M., Wada, N., and Sasaki, M. (2019). Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. *Communications Physics*, 2(1):9.

Fang, X.-T., Zeng, P., Liu, H., Zou, M., Wu, W., Tang, Y.-L., Sheng, Y.-J., Xiang, Y., Zhang, W., Li, H., Wang, Z., You, L., Li, M.-J., Chen, H., Chen, Y.-A., Zhang, Q., Peng, C.-Z., Ma, X., Chen, T.-Y., and Pan, J.-W. (2020). Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nature Photonics*, 14(7):422–425.

Ferrero, V. and Camatel, S. (2008). Optical phase locking techniques: an overview and a novel method based on single side sub-carrier modulation. *Optics Express*, 16(2):818.

Fung, C.-H. F., Ma, X., and Chau, H. F. (2010). Practical issues in quantum-key-distribution postprocessing. *Physical Review A*, 81(1):012318.

García-Patrón, R. and Cerf, N. J. (2006). Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97(19):190503.

Ghorai, S., Grangier, P., Diamanti, E., and Leverrier, A. (2019). Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Physical Review X*, 9(2):021059.

Gong, Y., Jin, A., Li, H., Wonfor, A., and Penty, R. (2021). Security analysis of continuous-variable quantum key distribution using m-psk classical modulation schemes. In *Quantum Information and Measurement*, pages W3B–3. Optica Publishing Group.

Gottesman, D., Lo, H.-K., Lütkenhaus, N., and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.*, 4(5):325–360.

Gottesman, D. and Preskill, J. (2001). Secure quantum key distribution using squeezed states. *Physical Review A*, 63(2):317–356.

Grandi, S., Zavatta, A., Bellini, M., and Paris, M. G. A. (2017). Experimental quantum tomography of a homodyne detector. *New Journal of Physics*, 19(5):053015.

Grosshans, F., Assche, G. V., Wenger, J., Brouri, R., Cerf, N. J., and Grangier, P. (2003). Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241.

Grosshans, F. and Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902.

Grünenfelder, F., Boaron, A., Rusca, D., Martin, A., and Zbinden, H. (2020). Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. *Applied Physics Letters*, 117(14):144003.

Hansen, H., Aichele, T., Hettich, C., Lodahl, P., Lvovsky, A. I., Mlynek, J., and Schiller, S. (2001). Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements. *Opt. Lett.*, 26(21):1714–1716.

Hirano, T., Ichikawa, T., Matsubara, T., Ono, M., Oguri, Y., Namiki, R., Kasai, K., Matsumoto, R., and Tsurumaru, T. (2017). Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, 2(2):024010.

Holevo, A. S., Sohma, M., and Hirota, O. (1999). Capacity of quantum gaussian channels. *Physical Review A*, 59(3):1820–1828.

Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901.

Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., and Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science advances*, 3(11):e1701491.

Islam, N. T., Lim, C. C. W., Cahall, C., Qi, B., Kim, J., and Gauthier, D. J. (2019). Scalable high-rate, high-dimensional time-bin encoding quantum key distribution. *Quantum Science and Technology*, 4(3):035008.

Jin, A., Zeng, P., Penty, R. V., and Ma, X. (2021). Reference-frame-independent design of phase-matching quantum key distribution. *Physical Review Applied*, 16(3):034017.

Jin, A., Zhang, X., Jiang, L., Penty, R. V., and Zeng, P. (2023). Pilot-reference-free continuous-variable quantum key distribution with efficient decoy-state analysis. *arXiv preprint arXiv:2309.03789*.

Kato, G. (2020). Concentration inequality using unconfirmed knowledge. *arXiv preprint arXiv:2002.04357*.

Kaur, E., Guha, S., and Wilde, M. M. (2021). Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, 103(1):012412.

Kiesel, T., Vogel, W., Hage, B., and Schnabel, R. (2011). Direct sampling of negative quasiprobabilities of a squeezed state. *Physical Review Letters*, 107(11):113604.

Kiesel, T., Vogel, W., Parigi, V., Zavatta, A., and Bellini, M. (2008). Experimental determination of a nonclassical glauber-sudarshan p function. *Physical Review A*, 78(2):021804.

Kim, Y., Eddins, A., Anand, S., Wei, K. X., van den Berg, E., Rosenblatt, S., Nayfeh, H., Wu, Y., Zaletel, M., Temme, K., and Kandala, A. (2023). Evidence for the utility of quantum computing before fault tolerance. *Nature*, 618(7965):500–505.

Koashi, M. (2009). Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018.

Konig, R., Renner, R., and Schaffner, C. (2009). The operational meaning of min-and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347.

Kumar, R., Qin, H., and Alléaume, R. (2015). Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics*, 17(4):043027.

Laing, A., Scarani, V., Rarity, J. G., and O'Brien, J. L. (2010). Reference-frame-independent quantum key distribution. *Phys. Rev. A*, 82(1):012304.

Landau, L. and Lifshitz, E. (1981). *Quantum Mechanics: Non-Relativistic Theory*, volume 3. Elsevier.

Laudenbach, F., Pacher, C., Fung, C.-H. F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., and Hübel, H. (2018). Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011.

Lee, D., Hong, S., Cho, Y.-W., Lim, H.-T., Han, S.-W., Jung, H., Moon, S., Lee, K. J., and Kim, Y.-S. (2020). Reference-frame-independent, measurement-device-independent quantum key distribution using fewer quantum states. *Optics Letters*, 45(9):2624.

Leonhardt, U. and Paul, H. (1995). Measuring the quantum state of light. *Prog. Quantum Electron.*, 19(2):89–130.

Leonhardt, U., Paul, H., and D'Ariano, G. M. (1995). Tomographic reconstruction of the density matrix via pattern functions. *Phys. Rev. A*, 52(6):4899–4907.

Leverrier, A. (2017). Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Physical Review Letters*, 118(20):200501.

Leverrier, A., Alleaume, R., Boutros, J., Zemor, G., and Grangier, P. (2008). Multidimensional reconciliation for continuous-variable quantum key distribution. In *2008 IEEE International Symposium on Information Theory*, pages 1020–1024.

Leverrier, A. and Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102(18):180504.

Leverrier, A. and Grangier, P. (2011). Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Physical Review A*, 83(4):042312.

Li, W., Zhang, L., Tan, H., Lu, Y., Liao, S.-K., Huang, J., Li, H., Wang, Z., Mao, H.-K., Yan, B., Li, Q., Liu, Y., Zhang, Q., Peng, C.-Z., You, L., Xu, F., and Pan, J.-W. (2023). High-rate quantum key distribution exceeding 110 mb s–1. *Nature Photonics*, 17(5):416–421.

Lin, J., Upadhyaya, T., and Lütkenhaus, N. (2019). Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 9(4):041064.

Liu, Y., Zhang, W.-J., Jiang, C., Chen, J.-P., Zhang, C., Pan, W.-X., Ma, D., Dong, H., Xiong, J.-M., Zhang, C.-J., Li, H., Wang, R.-C., Wu, J., Chen, T.-Y., You, L., Wang, X.-B., Zhang, Q., and Pan, J.-W. (2023). Experimental twin-field quantum key distribution over 1000 km fiber distance. *Physical Review Letters*, 130(21):210801.

Lo, H. K. and Chau, H. F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050.

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

Lo, H.-K., Ma, X., and Chen, K. (2005). Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504.

Lobino, M., Korystov, D., Kupchak, C., Figueroa, E., Sanders, B. C., and Lvovsky, A. I. (2008). Complete characterization of quantum-optical processes. *Science*, 322(5901):563–566.

Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403.

Lütkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304.

Ma, J., Zhou, Y., Yuan, X., and Ma, X. (2019). Operational interpretation of coherence in quantum key distribution. *Physical Review A*, 99(6):062325.

Ma, X. (2008). *Quantum cryptography: from theory to practice*. PhD thesis, University of Toronto. also available in arXiv:0808.1385.

Ma, X., Fung, C.-H. F., and Razavi, M. (2012). Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Physical Review A*, 86(5):052305.

Ma, X., Qi, B., Zhao, Y., and Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72(1):012326.

Ma, X. and Razavi, M. (2012). Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A*, 86(6):062319.

Ma, X., Zeng, P., and Zhou, H. (2018). Phase-matching quantum key distribution. *Physical Review X*, 8(3):031043.

Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M., Zhou, Y.-L., and Liang, L.-M. (2014). Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Physical Review A*, 89(3):032310.

Ma, X.-C., Sun, S.-H., Jiang, M.-S., and Liang, L.-M. (2013). Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Physical Review A*, 88(2):022339.

Maeda, K., Sasaki, T., and Koashi, M. (2019). Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nature communications*, 10(1):3140.

Marand, C. and Townsend, P. D. (1995). Quantum key distribution over distances as long as 30 km. *Optics Letters*, 20(16):1695.

Matsuura, T., Maeda, K., Sasaki, T., and Koashi, M. (2021). Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature Communications*, 12(1):252.

Matsuura, T., Yamano, S., Kuramochi, Y., Sasaki, T., and Koashi, M. (2023). Refined finite-size analysis of binary-modulation continuous-variable quantum key distribution. *Quantum*, 7:1095.

Minder, M., Pittaluga, M., Roberts, G. L., Lucamarini, M., Dynes, J. F., Yuan, Z. L., and Shields, A. J. (2019). Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics*, 13(5):334–338.

Navascués, M., Grosshans, F., and Acín, A. (2006). Optimality of gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97(19):190502.

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

Pan, Y., Wang, H., Shao, Y., Pi, Y., Li, Y., Liu, B., Huang, W., and Xu, B. (2022). Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Optics Letters*, 47(13):3307.

Papanastasiou, P. and Pirandola, S. (2021). Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective gaussian attacks. *Physical Review Research*, 3(1):013047.

Pirandola, S., Laurenza, R., Ottaviani, C., and Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):1–15.

Pittaluga, M., Minder, M., Lucamarini, M., Sanzaro, M., Woodward, R. I., Li, M.-J., Yuan, Z., and Shields, A. J. (2021). 600-km repeater-like quantum communications with dual-band stabilization. *Nature Photonics*, 15(7):530–535.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2:79.

Primaatmaja, I. W., Liang, C. C., Zhang, G., Haw, J. Y., Wang, C., and Lim, C. C.-W. (2022). Discrete-variable quantum key distribution with homodyne detection. *Quantum*, 6:613.

Qi, B. (2021). Bennett-brassard 1984 quantum key distribution using conjugate homodyne detection. *Physical Review A*, 103(1):012606.

Qi, B. and Lim, C. C. W. (2018). Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. *Physical Review Applied*, 9(5):054008.

Qi, B., Lougovski, P., and Williams, B. P. (2020). Characterizing photon number statistics using conjugate optical homodyne detection. *Optics Express*, 28(2):2276.

Qi, B., Zhu, W., Qian, L., and Lo, H.-K. (2010). Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, 12(10):103042.

Renner, R. (2007). Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649.

Renner, R. (2008). SECURITY OF QUANTUM KEY DISTRIBUTION. *International Journal of Quantum Information*, 06(01):1–127.

Renner, R. and König, R. (2005). Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer Berlin Heidelberg.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126.

Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Diamanti, E., and Grangier, P. (2021). High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM. In *2021 European Conference on Optical Communication (ECOC)*. IEEE.

Roumestan, F., Ghazisaeidi, A., Renaudier, J., Vidarte, L. T., Leverrier, A., Diamanti, E., and Grangier, P. (2022). Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution. *arXiv preprint arXiv:2207.11702*.

Sakurai, J. J. and Napolitano, J. (2020). *Modern Quantum Mechanics*. Cambridge University Press.

Sanchez, R. G.-P. (2007). *Quantum information with optical continuous variables: from Bell tests to key distribution*. PhD thesis, Université libre de Bruxelles.

Santarelli, G., Clairon, A., Lea, S., and Tino, G. (1994). Heterodyne optical phase-locking of extended-cavity semiconductor lasers at 9 GHz. *Optics Communications*, 104(4-6):339–344.

Scarani, V. and Renner, R. (2008). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20):200501.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715.

Sheridan, L. and Scarani, V. (2010). Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82(3):030301.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Shor, P. W. and Preskill, J. (2000). Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441.

Smithey, D. T., Beck, M., Raymer, M. G., and Faridani, A. (1993). Measurement of the wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum. *Phys. Rev. Lett.*, 70(9):1244–1247.

Steane, A. M. (1996). Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741–4751.

Takeoka, M., Guha, S., and Wilde, M. M. (2014). Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5(1):5235.

Tamaki, K., Lo, H.-K., Wang, W., and Lucamarini, M. (2018). Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv preprint arXiv:1805.05511*.

Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1):634.

Tomamichel, M. and Renner, R. (2011). Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11):110506.

Usenko, V. and Filip, R. (2016). Trusted noise in continuous-variable quantum key distribution: A threat and a defense. *Entropy*, 18(1):20.

Vagniluca, I., Lio, B. D., Rusca, D., Cozzolino, D., Ding, Y., Zbinden, H., Zavatta, A., Oxenløwe, L. K., and Bacco, D. (2020). Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Physical Review Applied*, 14(1):014051.

Varnava, M., Browne, D. E., and Rudolph, T. (2006). Loss tolerance in one-way quantum computation via counterfactual error correction. *Physical Review Letters*, 97(12):120501.

Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, XLV:295–301.

Vogel, K. and Risken, H. (1989). Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Phys. Rev. A*, 40(5):2847–2849.

Wang, H., Li, Y., Pi, Y., Pan, Y., Shao, Y., Ma, L., Zhang, Y., Yang, J., Zhang, T., Huang, W., and Xu, B. (2022a). Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. *Communications Physics*, 5(1):162.

Wang, H., Pi, Y., Huang, W., Li, Y., Shao, Y., Yang, J., Liu, J., Zhang, C., Zhang, Y., and Xu, B. (2020). High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Optics Express*, 28(22):32882.

Wang, P., Zhang, Y., Lu, Z., Wang, X., and Li, Y. (2023). Discrete-modulation continuous-variable quantum key distribution with a high key rate. *New Journal of Physics*, 25(2):023019.

Wang, S., Yin, Z.-Q., He, D.-Y., Chen, W., Wang, R.-Q., Ye, P., Zhou, Y., Fan-Yuan, G.-J., Wang, F.-X., Chen, W., Zhu, Y.-G., Morozov, P. V., Divochiy, A. V., Zhou, Z., Guo, G.-C., and Han, Z.-F. (2022b). Twin-field quantum key distribution over 830-km fibre. *Nature Photonics*, 16(2):154–161.

Wang, T., Huang, P., Zhou, Y., Liu, W., Ma, H., Wang, S., and Zeng, G. (2018a). High key rate continuous-variable quantum key distribution with a real local oscillator. *Optics Express*, 26(3):2794.

Wang, X.-B. (2005). Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94(23):230503.

Wang, X.-B., Yu, Z.-W., and Hu, X.-L. (2018b). Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A*, 98(6):062323.

Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., and Lloyd, S. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621–669.

Wehner, S., Elkouss, D., and Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288.

Wilde, M. M. (2011). From classical to quantum shannon theory. *arXiv preprint arXiv:1106.1445*.

Winick, A., Lütkenhaus, N., and Coles, P. J. (2018). Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77.

Wootters, W. K. and Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886):802–803.

Xie, Y.-M., Lu, Y.-S., Weng, C.-X., Cao, X.-Y., Jia, Z.-Y., Bao, Y., Wang, Y., Fu, Y., Yin, H.-L., and Chen, Z.-B. (2022). Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum*, 3(2):020315.

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., and Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92(2):025002.

Xu, F., Xu, H., and Lo, H.-K. (2014). Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A*, 89(5):052333.

Yuan, X., Zhou, H., Cao, Z., and Ma, X. (2015). Intrinsic randomness as a measure of quantum coherence. *Physical Review A*, 92(2):022124.

Yuan, Z., Plews, A., Takahashi, R., Doi, K., Tam, W., Sharpe, A. W., Dixon, A. R., Lavelle, E., Dynes, J. F., Murakami, A., Kujiraoka, M., Lucamarini, M., Tanizawa, Y., Sato, H., and Shields, A. J. (2018). 10-mb/s quantum key distribution. *Journal of Lightwave Technology*, 36(16):3427–3433.

Zeng, P., Wu, W., and Ma, X. (2020). Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel. *Physical Review Applied*, 13(6):064013.

Zeng, P., Zhou, H., Wu, W., and Ma, X. (2022). Mode-pairing quantum key distribution. *Nature Communications*, 13(1):3903.

Zhang, X., Zeng, P., Ye, T., Lo, H.-K., and Ma, X. (2023). Quantum complementarity approach to device-independent security. *Physical Review Letters*, 131(14):140801.

Zhang, Z., Zhao, Q., Razavi, M., and Ma, X. (2017). Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Physical Review A*, 95(1):012333.

Zhao, Y.-B., Heid, M., Rigas, J., and Lütkenhaus, N. (2009). Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307.

Zhou, L., Lin, J., Xie, Y.-M., Lu, Y.-S., Jing, Y., Yin, H.-L., and Yuan, Z. (2023). Experimental quantum communication overcomes the rate-loss limit without global phase tracking. *Physical Review Letters*, 130(25):250801.

Appendix A

Quantum information in finite fields

A.1 Finite field structure

The finite field, or Galois field, is the algebraic structure that lies in the discrete-value information processing. In a general d-dimensional information processing task, the set $\{0,1,\cdots,d-1\}$ are the symbols. In order to construct an algebra on this set, we need to define properly addition $\oplus$ and multiplication $\odot$ operations such that they follow the usual associative, commutative and distributive laws and each has identity and inverse. In other words, we need to make the symbol set a finite field, denoted by GF(d), by defining the addition and multiplication operations.

For prime dimension p, the set $\{0,1,\cdots,p-1\}$ can be made a finite field trivially equipped with the usual modulus p addition and multiplication. This is the finite field $\mathbf{Z}_p$, and it can be seen that every GF(p) is isomorphic to $\mathbf{Z}_p$.

Next, consider the prime power dimension $d = p^r$. We define the canonical addition on the set $\{0,1,\cdots,d-1\}$ such that:

$$\begin{aligned} a &= \sum_{m=0}^{r-1} a_m p^m \quad b = \sum_{m=0}^{r-1} b_m p^m \\ a \oplus b &= \sum_{m=0}^{r-1} (a_m \oplus_p b_m) p^m, \end{aligned} \tag{A.1}$$

where $\oplus_p$ is the p-modulus addition and a_m, b_m are the p-ary decompositions of a and b. This is a valid field addition for GF(p^r). In fact, the field multiplication can also be constructed for GF(p^r), and it can be shown that the set $\{0,1,\cdots,d-1\}$ can be made a field if and only if $d = p^r$, i.e only prime power degree finite fields exist (Artin, 2011).

The convenience of adopting the canonical addition defined above is its compatibility with exponential operations. We will encounter frequently the complex exponential γ_p^a, where γ_p is the complex number such that $\gamma_p^p = 1$ and $a \in$GF(d). The value of γ_p^a is a complex number calculated as if a were the usual integer. Note that the exponential multiplication rule follows:

$$\gamma_p^a \gamma_p^b = \gamma_p^{a+b} = \gamma_p^{a\oplus b}, \tag{A.2}$$

where $+$ is the integer addition and $\oplus$ is the canonical field addition. It can also be seen that the canonical field addition is also compatible with conjugation and distributive law in the way that:

$$\begin{aligned}(\gamma_p^a)^* &= \gamma_p^{(-a)} = \gamma_p^{(\ominus a)} \\ \gamma_p^{a\odot c}\gamma_p^{b\odot c} &= \gamma_p^{a\odot c + b\odot c} = \gamma_p^{a\odot c\oplus b\odot c} = \gamma_p^{(a\oplus b)\odot c}\end{aligned} \tag{A.3}$$

Since we are always working with the complex exponential γ_p^a in the security proof next section, we will use $+$ in replace of $\oplus$ as they are equivalent. The field multiplication is not compatible with complex exponential in the sense that $(\gamma_p^a)^b \neq \gamma_p^{a\odot b}$ (except for $\mathbf{Z}_p$). However, in the following discussions, we do not need operations like $(\gamma_p^a)^b$, and hence we will still replace $a \odot b$ as ab.

A.2 The Heisenberg-Weyl group: high-dimensional Pauli operators

We introduce the Heisenberg-Weyl group as a generalization of the two-dimensional Pauli group. A detailed revision is provided by (Durt et al., 2010). For a prime-power-dimensional space, i.e. $d = p^r$, with computational basis $\{|l\rangle\}_{l=0}^{d-1}$, we define

$$\begin{aligned}Z &= \sum_{l=0}^{d-1} \gamma_p^l |l\rangle\langle l|, \\ X &= \sum_{l=0}^{d-1} |l+1\rangle\langle l|, \text{ with respect to GF}(d).\end{aligned} \tag{A.4}$$

A natural mutually-unbiased basis (MUB) of Z-basis is given by the eigenbasis of X,

$$\begin{aligned}|\tilde{l}\rangle &:= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \gamma_p^{-lj} |j\rangle, \\ |j\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \gamma_p^{lj} |\tilde{l}\rangle.\end{aligned} \tag{A.5}$$

Note that $X\big|\tilde{l}\big\rangle = \gamma_p^l\big|\tilde{l}\big\rangle$. This is the basis complementary to the computational basis.

The Heisenberg-Weyl operator $W(u,v)$ is defined to be

$$W(u,v) = \sum_{l=0}^{d-1} |l+u\rangle\gamma_p^{lv}\langle l|, \tag{A.6}$$

with $u,v = 0,1,...,d-1$. It is easy to verify that

$$W(u,0)W(0,v) = \gamma_p^{-uv}W(0,v)W(u,0) \tag{A.7}$$

In prime dimension this reduces to the usual identity:

$$X^uZ^v = \gamma_p^{-uv}Z^vX^u \tag{A.8}$$

From the Heisenberg-Weyl operators, we can generate the Bell basis in prime power dimensions. Define $\big|\Phi_{0,0}\big\rangle = |\Phi_+\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jj\rangle$. Write $\Phi_{0,0}$ in X-basis,

$$\begin{aligned}\big|\Phi_{0,0}\big\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jj\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k,l=0}^{d-1}\sum_{j=0}^{d-1}\gamma_p^{j(k+l)}\big|\tilde{k}\tilde{l}\big\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\Big|\tilde{k},\widetilde{-k}\Big\rangle.\end{aligned} \tag{A.9}$$

The generalized qudit Bell states (Bennett et al., 1993) are

$$\begin{aligned}|\Phi_{u,v}\rangle &:= (I\otimes W(u,v))|\Phi_+\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\gamma_p^{lv}|l\rangle_A\otimes|l+u\rangle_B,\end{aligned} \tag{A.10}$$

Denote $\Phi_{u,v} := |\Phi_{u,v}\rangle\langle\Phi_{u,v}|$. The qudit Bell states $\{\Phi_{u,v}\}_{u,v=0}^{d-1}$ form an orthonormal basis,

$$\begin{aligned}\big\langle\Phi_{u,v}\big|\Phi_{u',v'}\big\rangle &= \frac{1}{d}\sum_{m,l=0}^{d-1}\gamma_p^{-lv}\gamma_p^{mv'}\langle l,l+u|m,m+u'\rangle \\ &= \frac{1}{d}\sum_{l=0}^{d-1}\gamma_p^{-l(v-v')}\delta_{u_d,0} \\ &= \delta_{u_d,0}\delta_{v_d,0}\end{aligned} \tag{A.11}$$

where $u_d := u' - u, v_d := v' - v$.

A.3 Parity check in GF(d)

We discuss the parity check operations for qudits since it plays a central role in the security proof. A length-N GF(d) string $\mathbf{x}$ is an ordered N-tuple:

$$\mathbf{x} = [x_0, x_1, \cdots, x_{N-1}], \tag{A.12}$$

where each element belongs to GF(d). For two length-N GF(d) strings $\mathbf{x}$ and $\mathbf{y}$, define the dot product as

$$\mathbf{x} \cdot \mathbf{y} = \sum_{k=0}^{N-1} x_k y_k, \tag{A.13}$$

where the additions and multiplications are defined on GF(d).

We focus on non-zero parity check as zero parity check would give a zero result for sure. For a fixed non-zero $\mathbf{y}$, the dot product $\mathbf{x} \cdot \mathbf{y}$ gives d different results uniformly, i.e. there are d^{N-1} string $\mathbf{x}$ giving the same $\mathbf{x} \cdot \mathbf{y}$. We call this dot product the parity check of $\mathbf{x}$, and it can be seen that one praity-check equation divides the overall string space into d cosets, each represented by the dot product result, which is a member of GF(d).

According to linear algebra, in order to completely determine an unknown length-N GF(d) string $\mathbf{x}$, it takes N linearly independent praity-check equations. This idea can be extended to quantum systems. Define the Z-parity measurement channel as the Kraus representation:

$$\mathscr{M}_Z(\mathbf{v})\{\rho\} = \sum_{l=0}^{d-1} P_l(\mathbf{v}) \rho P_l(\mathbf{v})^\dagger, \tag{A.14}$$

where $\mathbf{v}$ is a length-N GF(d) string and ρ is any density operator on $\mathscr{H}_d^{\otimes N}$. The Kraus operator $P_l(\mathbf{v})$ is given as the projector onto the space of parity check result $\mathbf{z} \cdot \mathbf{v} = l$:

$$P_l(\mathbf{v}) = \sum_{\mathbf{z} \cdot \mathbf{v} = l} |\mathbf{z}\rangle\langle\mathbf{z}| \tag{A.15}$$

Similarly, we can define the X-parity measurement $\mathscr{M}_X(\mathbf{v})$ with respect to the X basis. The output of the parity measurement is a mixture of d parity states, i.e.

$$\begin{aligned}\mathscr{M}_Z(\mathbf{v})\{\rho\} &= \sum_{l=0}^{d-1} P_l(\mathbf{v})\rho P_l(\mathbf{v})^\dagger \\ &= \sum_{l=0}^{d-1} \sum_{\mathbf{z},\mathbf{z}'\cdot\mathbf{v}=l} |\mathbf{z}\rangle\langle\mathbf{z}|\rho|\mathbf{z}'\rangle\langle\mathbf{z}'| \\ &= \sum_{l=0}^{d-1} p_l\rho_l,\end{aligned} \tag{A.16}$$

where

$$\begin{aligned}p_l &= \sum_{\mathbf{z}\cdot\mathbf{v}=l} \langle\mathbf{z}|\rho|\mathbf{z}\rangle \\ \rho_l &= \sum_{\mathbf{z},\mathbf{z}'\cdot\mathbf{v}=l} \frac{\langle\mathbf{z}|\rho|\mathbf{z}'\rangle}{p_l}|\mathbf{z}\rangle\langle\mathbf{z}'|, \text{ having parity } l.\end{aligned} \tag{A.17}$$

It can be seen that it takes N linearly independent Z/X-parity measurements to determine the Z/X measurement results of an unknown state in $\mathscr{H}_d^{\otimes N}$.

Appendix B

Simulation formulae

B.1 Simulation formulae for high-dimensional PM QKD

We present the formulae used to simulate the key rate performance of high-dimensional PM QKD in Fig. 4.6 and 4.7. The channel is assumed to be pure-loss and symmetric for Alice and Bob with transmittance η (with detector efficiency taken into account). The single-photon detectors have dark count rate p_d. The calculations below are for single L-click events, and can be easily altered for R-click events.

To calculate the bit-error rate vector $\vec{E}_{bit}^{\mu}$, assume Alice and Bob send coherent states of amplitude $\mu/2$ with phase difference $\phi+\delta$, where ϕ is the encoding difference and δ is the reference-frame misalignment. As computed in (Ma et al., 2018), the single-click probabilities of the L and R detector given phase difference $\phi+\delta$ are

$$\begin{aligned} P_{\mu}^{\phi+\delta}(L) &= 1-(1-p_d)\exp(-\eta\mu\cos^2((\phi+\delta)/2)) \\ P_{\mu}^{\phi+\delta}(R) &= 1-(1-p_d)\exp(-\eta\mu\sin^2((\phi+\delta)/2)). \end{aligned} \tag{B.1}$$

Given reference misalignment δ, when Alice and Bob have encoding difference $\phi_k = \frac{2\pi}{d}k$, the probability of a single L-click is

$$P_{\mu}(L|\phi_k,\delta) = P_{\mu}^{\phi_k+\delta}(L)[1-P_{\mu}^{\phi_k+\delta}(R)]. \tag{B.2}$$

Since the misalignment is independent of the encoding, by the Bayesian formula, the probability of encoding difference ϕ_k given a single L-click event with misalignment δ is

$$P_{\mu}(\phi_k|L,\delta) = \frac{P_{\mu}(L|\phi_k,\delta)P(\phi_k)}{Q_{\mu}^{\delta}}, \tag{B.3}$$

where $P(\phi_k) = \frac{1}{d}$ for uniform encoding. The gain Q_μ^δ given misalignment δ can be calculated by

$$Q_\mu^\delta = \sum_{k=0}^{d-1} P_\mu(L|\phi_k, \delta) P(\phi_k). \tag{B.4}$$

The k-th entry of the bit-error rate vector is therefore given by

$$\vec{E}_{bit}^{\mu}(k) = P_\mu(\phi_k|L) = \mathbb{E}_\delta[P_\mu(\phi_k|L, \delta)], \tag{B.5}$$

where the expectation is taken over the distribution of misalignment δ, which is deterministic for fixed misalignment and uniform for fluctuating misalignment. The total gain is the expectation

$$Q_\mu = \mathbb{E}_\delta[Q_\mu^\delta]. \tag{B.6}$$

To calculate the phase-error rate vector $\vec{q}_\mu$, given encoding difference ϕ_k and misalignment δ, when Alice and Bob send the n-photon state, the probability of a single L-click is (Ma et al., 2018)

$$P_n(L|\phi_k, \delta) = (1 - p_d)(1 - \eta \cos^2((\phi_k + \delta)/2))^n - (1 - p_d)^2(1 - \eta)^n. \tag{B.7}$$

Averaging over the encoding, the yield of n-photon states under misalignment δ is given by

$$Y_n^\delta = \sum_{k=0}^{d-1} P_n(L|\phi_k, \delta) P(\phi_k). \tag{B.8}$$

The total yield is therefore the expectation

$$Y_n = \mathbb{E}_\delta[Y_n^\delta]. \tag{B.9}$$

We can therefore calculate the detection fraction q_n^μ of the n-photon states by Eq. (4.19) with yield Y_n and gain Q_μ.

B.2 Simulation formulae for DM CV QKD

We list in this section the simulated statistics of a thermal-noise channel for the optimisation Eq. (5.19). For the transmitted states $\alpha_j \in \{\alpha \exp(j2\pi i/m)\}_{j=0}^{m-1}$, the simulated statistics of

a channel with transmittance η and thermal noise ξ are given by:

$$\begin{aligned}
\langle \hat{q} \rangle_j &= \sqrt{2\eta}\mathrm{Re}(\alpha_j) \\
\langle \hat{p} \rangle_j &= \sqrt{2\eta}\mathrm{Im}(\alpha_j) \\
\langle \hat{n} \rangle_j &= \eta|\alpha_j|^2 + \frac{\eta\xi}{2} \\
\langle \hat{d} \rangle_j &= \eta((\alpha_j)^2 + (\alpha_j^*)^2).
\end{aligned} \tag{B.10}$$

B.3 Simulation formulae for time-bin CV QKD under thermal-noise channel

We present the simulation formulae of the asymptotic time-bin CV QKD under a thermal-noise channel with excess noise ξ from the output. A thermal noise channel is characterized as a Gaussian completely positive map transforming the first and second moment $(\bar{r}, V)$, representing the mean vector and covariance matrix of the quadrature operators, of the input state as (Weedbrook et al., 2012):

$$\begin{aligned}
&\bar{r} \mapsto \sqrt{\eta}\bar{r}, \\
&V \mapsto \eta V + (1-\eta)\mathbb{I} + \xi\mathbb{I},
\end{aligned} \tag{B.11}$$

where η is the channel transmittance. Two thermal channels with transmittance η and η' and excess noise ξ and ξ' concatenate to another thermal channel with transmittance $\eta\eta'$ and excess noise $(\eta'\xi + \xi')$ since

$$\begin{aligned}
&\bar{r} \mapsto \sqrt{\eta'\eta}\bar{r}, \\
&V \mapsto \eta'(\eta V + (1-\eta)\mathbb{I} + \xi\mathbb{I}) + (1-\eta')\mathbb{I} + \xi'\mathbb{I} \\
&= \eta'\eta V + (1-\eta'\eta)\mathbb{I} + (\eta'\xi + \xi')\mathbb{I}.
\end{aligned} \tag{B.12}$$

On the bit-error side, the thermal noise can be seen as adding ξ to the unity variance of the coherent states. Hence, if Alice transmits a coherent state $\left|\sqrt{\mu}e^{i\theta}\right\rangle$ through a thermal-noise channel with transmittance η and excess noise ξ, and Bob applies homodyne detection with LO phase φ, the detection result q will follow a distribution

$$\Pr(q|\mu, \theta-\varphi) = \frac{1}{\sqrt{2\pi}} \exp\left\{ -\frac{[q - 2\sqrt{\eta\mu}\cos(\theta-\varphi)]^2}{2(1+\xi)} \right\}. \tag{B.13}$$

Since both the signal states and the receiver LO are uniformly phase randomized, $(\theta - \varphi)$ is also uniformly randomized with $[0, 2\pi)$ in a cyclic manner. The bit error rate e_μ^Z and the

Z-basis gain Q_μ^Z can thus be calculated according to the post-selection threshold τ, uniformly randomizing over $[0, 2\pi)$.

The calculation of the vacuum gain $Q_{*,0}$, according to Eq. (6.27), requires the probability of sending the Z-basis state whilst receiving vacuum. This can be calculated via the Wigner function for Gaussian state, and in specific

$$\mathrm{Tr}\left[\hat{P}_0^{B_1B_2}\mathscr{N}_E^{A_1A_2\to B_1B_2}\left(\hat{\rho}^Z\right)\hat{P}_0^{B_1B_2}\right] = \left(\frac{2}{2+\xi}\right)^2 \exp\left(-\frac{2\eta\mu}{2+\xi}\right). \tag{B.14}$$

The single- and two-photon gains, $Q_{1,1}$ and $Q_{2,2}$, and phase-error rates, $e_{1,1}^X$ and $e_{2,2}^X$, are more complicated in calculation. In the infinite-decoy setup, we calculate the photon gains directly. We decompose the thermal noise $\hat{\rho}_{\mathrm{th}}$ into Fock states,

$$\hat{\rho}_{\mathrm{th}} = \sum_{k=0}^{\infty} \frac{\bar{k}^k}{(\bar{k}+1)^{k+1}} |k\rangle\langle k|, \tag{B.15}$$

where $\bar{k} = \xi/2(1-\eta)$ is the average photon number of the thermal noise. The optical mode from Alice can be seen as mixing with the thermal noise through an η-transmittance beam splitter. We calculate the effect of the thermal noise in an ensemble manner, that is, we calculate the case where the channel injects k and l noise photons to the two consecutive optical modes respectively, and mix the results according to the noise photon-number distribution in Eq. (B.15). We set a cutoff photon-number at $N_c = 3$ since the thermal noise is relatively low. Simulation shows that higher cutoffs have negligible effects on the key rate. We also account for the effects of the misalignment angle δ, which introduces a $\sin^2(m\delta/2)$ error to the m-photon phase error rate. We ignore the correlation between the misalignment and thermal noise photon as a second-order small quantity.

The calculations of the quantities of interest are listed below. The notation of (k,l) represents the conditional probability that the thermal sources emit k and l photons respectively to the two optical modes:

1. The probability of sending $(|01\rangle\langle 01| + |01\rangle\langle 01|)/2$ whilst accepting one photon in total (Eq. (6.23)):

$$Q_{1,1}(k,l) = c_1 \mathrm{Pr}(1)\eta^{k+l-1}\left\{[(k+1)\eta - k]^2 + l(k+1)(1-\eta)^2\right\}, \tag{B.16}$$

$$Q_{1,1} = \sum_{k=0,l=0}^{N_c} \mathrm{P}_{\mathrm{th}}(k)\mathrm{P}_{\mathrm{th}}(l)Q_{1,1}(k,l), \tag{B.17}$$

where

$$\mathrm{P_{th}}(k) = \frac{\bar{k}^k}{(\bar{k}+1)^{k+1}} \text{ with } \bar{k} = \frac{\xi}{2(1-\eta)}. \tag{B.18}$$

2. The probability of sending $(|01\rangle \pm |10\rangle)/\sqrt{2}$ whilst receiving $(|01\rangle \mp |10\rangle)/\sqrt{2}$ (Eq. (6.21)):

$$\frac{e^X_{1,1}(k,l)Q_{1,1}}{\Pr(1)} = \frac{c_1}{4}\eta^{k+l-1}(1-\eta)^2(k^2+l^2+k+l) + c_1 \sin^2\left(\frac{\delta}{2}\right), \tag{B.19}$$

$$e^X_{1,1} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)e^X_{1,1}(k,l). \tag{B.20}$$

3. The probability of sending $(|02\rangle\langle 02| + |20\rangle\langle 20|)/2$ whilst accepting within the $(|02\rangle\langle 02| + |20\rangle\langle 20|)$ and $|11\rangle\langle 11|$ subspace (Eq. (6.26)):

$$Q^{02}_{2,2}(k,l) = \frac{1}{2}c_2^{02}\Pr(2)\eta^{k+l-2}\Big\{[\eta^2 - 2k\eta(1-\eta) + \frac{1}{2}k(k-1)(1-\eta)^2]^2 + \frac{1}{4}l^2(l-1)^2(1-\eta)^4\Big\} + \{k \leftrightarrow l\}, \tag{B.21}$$

$$Q^{11}_{2,2}(k,l) = \frac{1}{2}c_2^{11}\Pr(2)\eta^{k+l-2}\left[\sqrt{2(k+1)l}\eta(1-\eta) - \sqrt{\frac{1}{2}kl(k+1)}(1-\eta)^2\right]^2 + \{k \leftrightarrow l\}, \tag{B.22}$$

$$Q_{2,2} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)\left[Q^{02}_{2,2}(k,l) + Q^{11}_{2,2}(k,l)\right], \tag{B.23}$$

where the expression $\{k \leftrightarrow l\}$ denotes exchanging the k's and l's in the term ahead.

4. The probability of sending $(|02\rangle \pm |20\rangle)/\sqrt{2}$ whilst receiving $(|02\rangle \mp |20\rangle)/\sqrt{2}$ and $|11\rangle$ (Eq. (6.24)).

$$\frac{e^{02,X}_{2,2}(k,l)Q_{2,2}}{\Pr(2)} = \frac{c_2^{02}}{4}\eta^{k+l-2}\left[2(k-l)(1-\eta)\eta + (k^2-k-l^2-l)(1-\eta)^2\right]^2 + c_2^{02}\sin^2(\delta), \tag{B.24}$$

$$\frac{e^{11,X}_{2,2}(k,l)Q_{2,2}}{\Pr(2)} = c_2^{11}\eta^{k+l-2}(1-\eta)^2\left\{l(k+1)\left[\eta - \frac{1}{2}k(1-\eta)\right]^2 + k(l+1)\left[\eta - \frac{1}{2}l(1-\eta)\right]^2\right\}, \tag{B.25}$$

$$\frac{e^X_{2,2}Q_{2,2}}{\Pr(2)} = \sum_{k=0,l=0}^{N_c} \mathrm{P_{th}}(k)\mathrm{P_{th}}(l)\left[e^{02,X}_{2,2}(k,l) + e^{11,X}_{2,2}(k,l)\right]. \tag{B.26}$$

In the finite-decoy setup, the estimations of photon gains are derived from the statistics of coherent-state gains. We need to calculate the probability of transmitting certain coherent states whilst receiving certain photon states. This can be also be done by the Gaussian-state Wigner function. Let $\kappa = 2/(2+\xi)$. Denote the output of a thermal noise channel when transmitting the coherent state $|\alpha\rangle$ as ρ_α. Its Fock-basis matrix elements are:

$$\langle 0|\rho_\alpha|0\rangle = \kappa \exp(-\kappa|\alpha|^2), \tag{B.27}$$

$$\langle 1|\rho_\alpha|1\rangle = \kappa(\kappa^2|\alpha|^2 + 1 - \kappa)\exp(-\kappa|\alpha|^2), \tag{B.28}$$

$$\langle 0|\rho_\alpha|1\rangle = -\kappa^2\alpha^* \exp(-\kappa|\alpha|^2), \tag{B.29}$$

$$\langle 2|\rho_\alpha|2\rangle = \kappa(\frac{1}{2}\kappa^4|\alpha|^4 + 2(\kappa^2-\kappa^3)|\alpha|^2 + (1-\kappa^2))\exp(-\kappa|\alpha|^2), \tag{B.30}$$

$$\langle 0|\rho_\alpha|2\rangle = \frac{1}{\sqrt{2}}\kappa^3(\alpha^*)^2 \exp(-\kappa|\alpha|^2). \tag{B.31}$$

The statistics required by the decoy method are all based on the gains of separable coherent states. For example, the probability of sending $|\alpha\rangle \otimes |\beta\rangle$ whilst receiving $(|02\rangle + |20\rangle)/\sqrt{2}$ can be computed by

$$\begin{aligned}
&\frac{1}{2}(\langle 02| + \langle 20|)\rho_\alpha \otimes \rho_\beta(|02\rangle + |20\rangle) \\
&= \frac{1}{2}\left(\langle 0|\rho_\alpha|0\rangle\langle 2|\rho_\beta|2\rangle + \langle 2|\rho_\alpha|2\rangle\langle 0|\rho_\beta|0\rangle + \langle 0|\rho_\alpha|2\rangle\langle 2|\rho_\beta|0\rangle + \langle 2|\rho_\alpha|0\rangle\langle 0|\rho_\beta|2\rangle\right).
\end{aligned} \tag{B.32}$$