博士論文

Digital Quantum Information Processing with Continuous-Variable Systems

（連続変量系を用いた離散的量子情報処理）

松浦　孝弥

Digital Quantum Information Processing with Continuous-Variable Systems

by

Takaya Matsuura

A Dissertation
Submitted for the Degree of

Doctor of Engineering

Department of Applied Physics
Graduate School of Engineering
The University of Tokyo

December 2021

Abstract

Continuous-variable quantum systems are characterized by physical quantities that can take continuous values. It appears in many physical systems, such as the position and momentum of oscillator modes of trapped ions and the complex amplitude of an optical mode. Especially, the quantum optical system is one of the most important continuous-variable systems for the quantum information application since light is an information carrier for telecommunication and behaves quantum mechanically even in the room-temperature environment. Furthermore, the complex amplitude of the optical mode can easily be manipulated. However, using a continuous variable, as it is, in quantum information processing does not work since a continuous variable is subject to continuous noises in the physical world, and such noises cannot completely be corrected. In order to perform reliable and fault-tolerant quantum information processing, information should be encoded in a digitized degree of freedom. In this thesis, digital quantum information processing with continuous-variables systems is studied in the quantum key distribution (QKD) and the quantum computation (QC), two major fields of quantum information processing.

For the QKD, the so-called continuous-variable QKD protocols, in which information is encoded on the complex amplitude of an optical pulse and the homodyne or heterodyne detector is used to measure it, are studied. More specifically, a continuous-variable QKD protocol that uses discretely modulated signals and the classical digital information processing is developed, and its security proof against general attacks in the finite-key case is established. This is achieved by virtually introducing the discrete-variable quantum system into the continuous-variable system and thereby reducing its security argument to that of discrete-variable QKDs, which is more mature. This is in sharp contrast to the previous security analyses on this kind of QKD protocol, where they directly use continuous variables in the security analyses and thus have difficulty in extending the analyses to the finite-key case. Another key to our security proof is the development of the method of estimating a lower bound on the fidelity to the coherent states, which eventually leads to the evaluation of how well the discrete-variable system can be approximated by the continuous-variable one. These security analyses are further elaborated, and a protocol whose key rate against the loss noise achieves almost optimal scaling is obtained.

For the QC with the continuous-variable system, the Gottesman-Kitaev-Preskill (GKP) code, which encodes discrete quantum information into a continuous-variable system, is studied. This code has many desirable properties for the optical implementation of QC; e.g., the universal QC is possible using only the Gaussian operations, which are relatively easy to implement in the quantum optical system, along with the GKP-encoded states. Because the ideal GKP-encoded state is unphysical, only

its approximation in some sense is realizable. Thus, several approximations of the GKP-encoded state have been developed since the first proposal of the GKP code. In this thesis, these conventionally used approximations are shown to be equivalent, and the explicit correspondences between the approximation parameters are given. This enables the direct comparison between the previous studies that were based on the different approximations. As the final result, an efficient method to implement the universal fault-tolerant QC using the Gaussian operations and only one type of the GKP-encoded state is developed. Contrary to the previous method of using the probabilistic state conversion and the costly distillation, our method can prepare the necessary elements deterministically. Based on the previous proposals of generating approximate GKP-encoded states, the physical systems suitable for our method of realizing the universal QC are investigated. The results in this thesis thus broaden the possibilities for reliable quantum information processing with continuous-variable systems.

Acknowledgement

I have received much support and advice during my Ph.D. studies. First, I would like to express my sincere thanks to my supervisor Masato Koashi for the instruction and all the constructive suggestions. He was always ready to listen to my questions and concerns for both academic and non-academic matters. From him, I learned the approaches to challenging problems and the importance of thorough consideration. I am grateful to all the collaborators, Kento Maeda, Toshihiko Sasaki, and Hayata Yamasaki, for the extensive discussions, which gave me fruitful ideas. Without their help, I could not complete the works presented in this thesis. I thank all the other group members, Yoshifumi Nakata, Wang Liao, Jingfang Zhou, Masanori Sumizaki, Shiro Tamiya, Shinichiro Yamano, Rei Tokami, and the former group members, Yui Kuramochi, Hongyi Zhou, Kenji Nishikawa, Khodai Kuroiwa, for valuable time having seminars and talking about scientific as well as everyday affairs. I especially thank Nakata-san for revising my application forms as well as presentations very carefully and Kuramochi-san for teaching me math.

I am grateful to Nicolas Menicucci and his group members, especially Ben Baragiola, for having accepted my visit to RMIT. It was my first time visiting the lab. overseas. I thank Christian Weedbrook and Ish Dhand for having given me an opportunity to work with people in Xanadu. I had fruitful discussions with Ish, Nick, Krishna Kumar Sabapathy, Rafael Alexander, Ilan Tzitrin, and all the other project members, which produced many results.

I have been financially supported by the ALPS program and the JSPS Research Fellowship for Young Scientists (DC2), which made my student life productive. I also thank my vice supervisor Akira Furusawa of the ALPS program for having given me lots of useful advice and put me in touch with Nick.

Many thanks to my parents for keeping me healthy in body and mind. They have been supporting me continuously since my birth. And finally, many thanks to my beloved, who is always with me and cheers me up. It is the future with her that makes me write this now.

支えてくださった皆様方に心より感謝申し上げます。

Contents

Chapter 1

Introduction

1.1 Background of the research

Quantum information processing is an emerging technology having distinct advantages over ordinary information processing that prevails in the real world (referred to as classical information processing). Quantum key distribution (QKD) [BB84], as an example, enables distant parties to share the keys that are secret to the adversary even when the adversary has unlimited computational power and arbitrary eavesdropping technology allowed in the law of physics. This type of strong security cannot be obtained by classical information processing in a similar setup. Quantum computation (QC) [Ben80, Fey82, DP85], as another example, can efficiently solve problems that are considered to be difficult to solve in the classical computer [Sho94]. Not limited to a matter of new technology, quantum information processing reveals plenty of essential aspects of quantum theory such as Bell non-locality [Bel64, FC72, ADR82] and entanglement, promoting our understanding of quantum theory. For these reasons, quantum information processing gathers growing interests and attention, and intensive studies have been made in this field for decades. Recently, the real-world implementation of quantum information technologies has been progressing. There are varieties of candidate materials and physical systems competing for realizing quantum information processing. Quantum optical system is one of the leading candidates for implementing quantum communication and quantum computation due to its retention ability of the quantum nature even in the room-temperature environment and its mobility with the propagating speed of light. Furthermore, technologies to control the wavy nature of light are established in the field of classical information processing.

The complex amplitude of the optical mode takes continuous values and is thus called a continuous-variable quantum system. The relation between quantum information processing with the continuous-variable system and that with the discrete-variable one (qubit or qudit) is similar to the relation between analog and digital classical information processing. Continuous-variable quantum information processing is fragile against noises compared to the discrete-variable one, as analog classical information processing is compared to the digital one. To circumvent this issue, we need to "digitize" information on the continuous-variable quantum system and leave an irrelevant continuous degree of freedom as a redundancy. The idea is general and natural in principle, but it is non-trivial how to consistently encode digital information on the

continuous-variable system and perform information processing on the encoded digital information with operations on the continuous-variable system. This thesis aims at developing quantum information processing on the digitized information encoded on the continuous-variable system.

1.2 What is studied in this thesis

As explained, the aim of the thesis is to develop digital quantum information processing with the continuous-variable system. We treat two topics; continuous-variable QKD and QC. For continuous-variable QKD, we develop a protocol that is adapted to digital information processing and prove the finite-size composable security for the protocol against general attacks. The complete security proof for the discrete-modulation continuous-variable QKD has been an open problem for a decade; we solve this problem by a newly developed estimation technique for the quantum state using the continuous-variable measurement. Our security analysis can easily incorporate the digitization of the signal processing and thus the finite resolution of the experimental apparatuses due to the adaptation to digital information processing. The security proof is further refined, and the protocol with almost optimal key rate scaling against transmission distance under the pure-loss channel is obtained.

For continuous-variable QC, we study the specific quantum error-correcting code called Gottesman-Kitaev-Preskill (GKP) code [GKP01]. The GKP code was developed to encode a qubit into a continuous-variable system, targeting the complex amplitude of an optical mode. It is suitable for optical QC for several reasons, one of which is that the important subset of the elementary gate operations on the GKP-encoded qubit can be realized by reliably implementable operations in the quantum optical experiment. The GKP code can be implemented on the physical system only approximately, and thus several conventional approximations for the GKP code have been developed. However, the correspondence between different approximations for the GKP code is still unclear. In this thesis, the conventional approximations for the GKP code are shown to be equivalent by the explicit correspondence between the approximation parameters. This enables the translation between researches based on the different approximations, which has been a problem for the analyses of the approximate GKP codes. Further properties of the approximate GKP codes are also shown. Another result is the development of a resource-efficient protocol to realize the universal QC with the GKP code. This protocol relies on direct preparation of only one type of the GKP-encoded state, the GKP magic state, and requires no probabilistic state conversion process. The feasibility for the direct preparation of the GKP magic state is discussed for several experimental proposals that aim to implement the GKP-encoded state.

1.3 The organization of this thesis

In Chapter 2, the basics of quantum information theory that this thesis is based on are listed (Section 2.1), and the distance measures for quantum states used throughout the thesis are defined (Section 2.2). In Chapter 3, the definitions and the properties of the continuous-variable quantum system are reviewed (Section 3.1) with the

quantum optical system as a prominent example (Section 3.2). Chapters 4 and 5 are the results of this thesis. In Chapter 4, after the review of the proof approach for the QKD and of the relevant probability theories, the security proof for a continuous-variable QKD protocol with digital information processing is developed (Section 4.4). The security proof is further refined based on the reverse reconciliation, a frequently used technique in the continuous-variable QKD, which results in the improvement of the protocol performance (Section 4.5). In Chapter 5, after reviewing the GKP code (Section 5.2.2), the equivalence of the conventionally-used approximate GKP codes is proved (Section 5.3). Furthermore, the resource-efficient protocol to realize the universal QC using the GKP code and experimentally feasible quantum optical operations is constructed (Section 5.4). Finally, Chapter 6 concludes the thesis.

Chapter 2

Preliminaries

2.1 The basic principles of quantum information theory

2.1.1 Linear operator and quantum state

In what follows, let $\mathcal{H}$ be a (possibly separable infinite-dimensional) Hilbert space. An element of $\mathcal{H}$ is denoted by a ket vector $|\psi\rangle$. An element of the dual $\mathcal{H}^*$ of $\mathcal{H}$ is denoted by a bra vector $\langle\psi|$. The inner product between two elements $|\psi\rangle$ and $|\phi\rangle$ in $\mathcal{H}$ is denoted by $\langle\psi|\phi\rangle$. Let $\mathfrak{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. The dagger operation $\dagger$ on $A \in \mathfrak{L}(\mathcal{H})$ is defined as follows. Let $\mathcal{D}$ be the set of vectors so that for $|\phi\rangle \in \mathcal{D}$, there exists $|\phi'\rangle \in \mathcal{H}$ such that $\langle\phi| A |\psi\rangle = \langle\phi'|\psi\rangle$ holds for all $|\psi\rangle \in \mathrm{dom}\, A$. Then, $A^\dagger$ is defined to satisfy $|\phi'\rangle = A^\dagger |\phi\rangle$ (i.e., $\mathcal{D} = \mathrm{dom}\, A^\dagger$). Such an $A^\dagger$ can be uniquely defined as long as $\mathrm{dom}\, A$ is dense in $\mathcal{H}$. An operator $A \in \mathfrak{L}(\mathcal{H})$ is called self-adjoint if $A = A^\dagger$. By definition, $\mathrm{dom}\, A = \mathrm{dom}\, A^\dagger$ in this case. A self-adjoint operator A is called positive and denoted by $A \geq 0$ if $\langle\psi| A |\psi\rangle \geq 0$ holds for all $|\psi\rangle \in \mathrm{dom}\, A$. An operator $A \in \mathfrak{L}(\mathcal{H})$ is called bounded if there exists a constant $M > 0$ such that $\|A|\psi\rangle\| \leq M\||\psi\rangle\|$ holds for all $|\psi\rangle \in \mathcal{H}$ (i.e., $\mathrm{dom}\, A = \mathcal{H}$). The set of bounded linear operators on $\mathcal{H}$ is denoted by $\mathfrak{B}(\mathcal{H})$. An operator $A \in \mathfrak{B}(\mathcal{H})$ is called isometry if $\|A|\psi\rangle\| = \||\psi\rangle\|$ for all $|\psi\rangle \in \mathcal{H}$, and called unitary if $A^\dagger A = AA^\dagger = I$, where I denotes an identity operator on $\mathcal{H}$. In quantum information theory, we frequently consider linear operators from $\mathcal{H}_1$ to $\mathcal{H}_2$, denoted by $\mathfrak{L}(\mathcal{H}_1, \mathcal{H}_2)$. The set $\mathfrak{B}(\mathcal{H}_1, \mathcal{H}_2)$ of bounded operators, an isometry, and a unitary from $\mathcal{H}_1$ to $\mathcal{H}_2$ can be defined analogously.

For a complete orthonormal system (CONS) $\{|e_j\rangle\}_{j\in\mathbb{N}} \subset \mathcal{H}$, the trace Tr of $A \in \mathfrak{B}(\mathcal{H})$ is defined as $\mathrm{Tr}(A) = \sum_{j\in\mathbb{N}} \langle e_j| A |e_j\rangle$ if it does not diverge. A bounded operator A with the trace of $\sqrt{A^\dagger A}$ convergent is called trace-class, and the set of trace-class operators is denoted by $\mathfrak{T}(\mathcal{H})$. A density operator $\rho \in \mathfrak{T}(\mathcal{H})$ is a positive and trace normalized operator, i.e.,

$$\rho^\dagger = \rho, \quad \rho \geq 0, \quad \mathrm{Tr}\rho = 1. \tag{2.1}$$

The set of density operators is denoted by $\mathfrak{D}(\mathcal{H})$.

A quantum state on a quantum mechanical system S can be uniquely determined by a density operator $\rho_S \in \mathfrak{D}(\mathcal{H}_S)$ on a Hilbert space $\mathcal{H}_S$ [NC10]. In the following, therefore, a quantum state is identified with its density operator. A quantum state is

called pure if the rank of its density operator ρ is equal to one, i.e. $\rho = |\psi\rangle\langle\psi|$ for a unit norm vector $|\psi\rangle \in \mathcal{H}$. The pure state is often denoted by the unit vector for brevity, e.g., $|\psi\rangle$ in the above case. A quantum state is referred to as mixed if it is not pure. A quantum state on a composite system of systems S_1 and S_2 are given by a density operator $\rho_{S_1S_2} \in \mathfrak{D}(\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2})$ on the tensor product $\mathcal{H}_{S_1} \otimes \mathcal{H}_{S_2}$ of Hilbert spaces. For any density operator $\rho_S \in \mathfrak{D}(\mathcal{H}_S)$, there exists a pure state $|\psi\rangle_{SR} \in \mathcal{H}_S \otimes \mathcal{H}_R$ with a reference system R such that $\mathrm{Tr}_R\, |\psi\rangle\langle\psi|_{SR} = \rho_S$, where Tr_R denotes the partial trace of the system R. $|\psi\rangle_{SR}$ is called the purification of the density operator ρ_S. $|\psi\rangle_{SR}$ is uniquely determined up to isometry [Kir06, Wat18].

2.1.2 Quantum operation and quantum channel

A quantum operation on a quantum state of the system S is defined as a completely-positive (CP) and trace-non-increasing (TNI) linear map (CPTNI map in short) $\mathcal{E} : \mathfrak{T}(\mathcal{H}_S) \to \mathfrak{T}(\mathcal{H}_S)$, which satisfies

$$^{\forall}\rho_{SE} \in \mathfrak{D}(\mathcal{H}_S \otimes \mathcal{H}_E), \quad \mathcal{E} \otimes \mathrm{Id}_E(\rho_{SE}) \geq 0, \qquad \text{(Completely-positive)}, \tag{2.2}$$

$$^{\forall}\rho_S \in \mathfrak{D}(\mathcal{H}_S), \quad \mathrm{Tr}\left[\mathcal{E}(\rho_S)\right] \leq 1, \qquad \text{(Trace-non-increasing)}, \tag{2.3}$$

where $\mathrm{Id}_E : A \mapsto A$, $^{\forall}A \in \mathfrak{B}(\mathcal{H}_E)$ denotes the identity map. These conditions are imposed to ensure the probabilistic interpretation of quantum states. The important subset of the quantum operations is the quantum channels, which are described as completely-positive and trace-preserving (TP) maps (CPTP maps in short). For CPTP maps, the inequality condition (2.3) of the CPTNI map is replaced with the equality. Roughly speaking, the quantum operation allows post-selection of the events while the quantum channel is non-selective. In general, the Hilbert spaces on which the input and the output trace-class operators of the CPTNI map are defined can be different. For a linear map $\mathcal{E} : \mathfrak{T}(\mathcal{H}_1) \to \mathfrak{T}(\mathcal{H}_2)$, the adjoint map of $\mathcal{E}$ denoted by $\mathcal{E}^\dagger$ from $\mathfrak{B}(\mathcal{H}_2)$ to $\mathfrak{B}(\mathcal{H}_1)$ is defined to satisfy

$$\mathrm{Tr}_{\mathcal{H}_2}[\mathcal{E}(\rho)A] = \mathrm{Tr}_{\mathcal{H}_1}[\rho\, \mathcal{E}^\dagger(A)], \quad \forall \rho \in \mathfrak{T}(\mathcal{H}_1),\ \forall A \in \mathfrak{B}(\mathcal{H}_2). \tag{2.4}$$

The adjoint of a CP map is also CP, the adjoint $\mathcal{F}$ of a TNI map is contractive, i.e., $\mathcal{F}(I) \leq I$, and the adjoint $\mathcal{F}$ of a TP map is unital, i.e., $\mathcal{F}(I) = I$. Thus, the adjoint of a CPTNI map (i.e., a quantum operation) is a contractive CP map, and the adjoint of a CPTP map (i.e., a quantum channel) is a unital CP map. For a unital CP map $\mathcal{F} : \mathfrak{B}(\mathcal{H}_2) \to \mathfrak{B}(\mathcal{H}_1)$, there exists a Hilbert space $\mathcal{K}$, an isometry $V \in \mathfrak{B}(\mathcal{H}_1, \mathcal{K})$, and a homomorphism $\pi : \mathfrak{B}(\mathcal{H}_2) \to \mathfrak{B}(\mathcal{K})$ such that $\mathcal{F}(A) = V^\dagger \pi(A) V$ for all $A \in \mathfrak{B}(\mathcal{H}_2)$ [Sti55]. This is called Stinespring dilation of the map $\mathcal{F}$, and the triple $(\pi, V, \mathcal{K})$ is unique up to isometry. For the adjoint map $\mathcal{E}^\dagger : \mathfrak{B}(\mathcal{H}_2) \to \mathfrak{B}(\mathcal{H}_1)$ of a CPTP map $\mathcal{E} : \mathfrak{T}(\mathcal{H}_1) \to \mathfrak{T}(\mathcal{H}_2)$, the Stinespring dilation takes a particularly simple form; $\mathcal{K} = \mathcal{H}_2 \otimes \mathcal{H}_R$ (where $\mathcal{H}_R$ can be chosen to be $\dim \mathcal{H}_R \leq \dim \mathcal{H}_1 \times \dim \mathcal{H}_2$ if $\mathcal{H}_1$ and $\mathcal{H}_2$ are finite dimensional [Cho75]), and $\pi(A) = A \otimes I_R$. Equivalently, the CPTP map $\mathcal{E} : \mathfrak{T}(\mathcal{H}_1) \to \mathfrak{T}(\mathcal{H}_2)$ can be written as

$$\mathcal{E}(\rho) = \mathrm{Tr}_R[V \rho V^\dagger], \quad \forall \rho \in \mathfrak{T}(\mathcal{H}_1), \tag{2.5}$$

which is (also) called Stinespring dilation of the CPTP map $\mathcal{E}$.

2.1.3 Quantum measurement and quantum instrument

For a Borel-measurable space (X, Σ), a map $E : \Sigma \to \mathfrak{B}(\mathcal{H})$ is called positive-operator-valued measure (POVM) if it satisfies

$$0 \leq E(\chi) \leq I, \qquad \forall \chi \in \Sigma, \tag{2.6}$$

$$E(\emptyset) = 0, \quad E(X) = I, \tag{2.7}$$

$$E\Big(\bigcup_{k\in\mathbb{N}} \chi_k\Big) = \sum_{k\in\mathbb{N}} E(\chi_k), \quad \forall \{\chi_k\}_{k\in\mathbb{N}} \subseteq \Sigma \text{ with } \chi_j \cap \chi_k = \emptyset \text{ for } j \neq k, \tag{2.8}$$

where the summation of the right-hand side of Eq. (2.8) converges σ-weakly, i.e., $\mathrm{Tr}[\rho \sum_{k=1}^{n} E(\chi_k)] \xrightarrow{n\to\infty} \mathrm{Tr}[\rho \sum_{k\in\mathbb{N}} E(\chi_k)]$ for all $\rho \in \mathfrak{D}(\mathcal{H})$ [Hol73, Hol11]. A quantum measurement with values in X is modeled by the above POVM if we do not care about the post-measurement state. Given a POVM $E : \Sigma \to \mathfrak{B}(\mathcal{H})$, the probability of observing $\chi \in \Sigma$ when the state of the system is prepared in ρ is given by

$$\Pr[\chi \in \Sigma \mid \rho] = \mathrm{Tr}[\rho E(\chi)], \qquad \text{(Born rule)}. \tag{2.9}$$

In other words, quantum measurement with values in X can be regarded as a (CPTP) map from the set of density operators to the set of probability distributions on X. For a POVM E, if $E(\chi)^2 = E(\chi)$ holds for all $\chi \in \Sigma$, then it is especially called projection-valued measure (PVM).

If we care about the post-measurement state, a quantum measurement should be treated as a quantum operation. Such quantum operations $\mathcal{E}_\chi$ ($\chi \in \Sigma$) called the quantum instrument is a map from a σ-algebra Σ to the collection of CPTNI maps that satisfies

$$\mathcal{E}_\chi^\dagger(I) = E(\chi), \tag{2.10}$$

with an identity operator I on the post-measurement space and a POVM E [DL70].

For a measurement with finite number of outcomes $\{0, \ldots, d-1\}$, one can associate the outcomes with mutually orthogonal pure states $\{|0\rangle\langle 0|, \ldots, |d-1\rangle\langle d-1|\}$ on $\mathbb{C}^d$ called the classical states. The quantum channel $\mathcal{I}$ composed of the instrument $\mathcal{E}$ and the register C of the outcomes can be defined as

$$\mathcal{I}(\rho) = \sum_{i=0}^{d-1} |i\rangle\langle i|_C \otimes \mathcal{E}_i(\rho), \tag{2.11}$$

which is often used in combination with the quantum instrument.

2.1.4 Qubit as an information unit

Qubit is a quantum system characterized by the two-dimensional Hilbert space. It is an elemental unit of the quantum information theory in analogy with the bit in the classical information theory. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis of a qubit. Throughout the thesis, the Pauli operators σ^X, σ^Y, and σ^Z are defined in this basis as

$$\sigma^X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma^Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma^Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.12}$$

In this thesis, $\{|0\rangle, |1\rangle\}$ is called the Z basis of the qubit and $\{|0_X\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |1_X\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$ is called the X basis of the qubit.

2.2 The distance measures of quantum states

In this section, the definitions and properties of the trace distance and the fidelity are listed. The proofs of them are given, for example, in the book [Wil13].

2.2.1 The trace norm and the trace distance

The trace distance is a distance measure of quantum states based on the trace norm defined below.

Definition 2.2.1 (Trace norm)**.** The trace norm $\|\cdot\|_1$ of a trace-class operator $A \in \mathfrak{T}(\mathcal{H})$ is defined as

$$\|A\|_1 \coloneqq \mathrm{Tr}\sqrt{A^\dagger A}. \tag{2.13}$$

As a norm, the trace norm satisfies the following properties.

- (Positive definiteness) The trace norm of a linear operator $A \in \mathfrak{T}(\mathcal{H})$ is positive semidefinite:
$$\|A\|_1 \geq 0. \tag{2.14}$$
The trace norm is null if and only if the operator A is null:
$$\|A\|_1 = 0 \Leftrightarrow A = 0. \tag{2.15}$$
- (Homogeneity) For any constant $c \in \mathbb{C}$,
$$\|cA\|_1 = |c|\|A\|_1. \tag{2.16}$$
.
- (Subaddtivity) For $A, B \in \mathfrak{T}(\mathcal{H})$. Then the following inequality holds:
$$\|A + B\|_1 \leq \|A\|_1 + \|B\|_1. \tag{2.17}$$

The following property is given as a corollary.

Corollary 2.2.2 (Convexity)**.** *For $A, B \in \mathfrak{T}(\mathcal{H})$ and $\lambda \in [0, 1]$, the following inequality holds:*

$$\|\lambda A + (1-\lambda)B\|_1 \leq \lambda\|A\|_1 + (1-\lambda)\|B\|_1. \tag{2.18}$$

The trace distance between quantum states ρ and σ is defined using the trace norm.

Definition 2.2.3 (Trace distance)**.** The trace distance $d(\rho, \sigma)$ between two density operators ρ and σ is defined as

$$d(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\mathrm{Tr}\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}. \tag{2.19}$$

From the subadditivity property of the trace norm, $0 \leq d(\rho, \sigma) \leq 1$ holds. Furthermore, the following also holds.

Corollary 2.2.4 (Triangle inequality)**.** *For $\rho, \sigma, \tau \in \mathfrak{D}(\mathcal{H})$, the following triangle inequality holds for trace distance:*

$$d(\rho, \sigma) \leq d(\rho, \tau) + d(\tau, \sigma). \tag{2.20}$$

The trace distance is a measure of how well two quantum states can be distinguished [Wil13]. The trace distance satisfies the following desirable property in terms of information processing.

Proposition 2.2.5 (Monotonicity)**.** *For any CPTP map $\mathcal{E} : \mathfrak{D}(\mathcal{H}) \to \mathfrak{D}(\mathcal{H})$ and for any quantum states $\rho, \sigma \in \mathfrak{D}(\mathcal{H})$, the following condition holds:*

$$d(\rho, \sigma) \geq d\left(\mathcal{E}(\rho), \mathcal{E}(\sigma)\right). \tag{2.21}$$

Monotonicity property of the trace distance reflects the fact that the distinguishability of two quantum states does not increase via any quantum channels. This property is crucial in the security proof of the QKD.

2.2.2 The quantum fidelity

The fidelity between two quantum states is defined as follows.

Definition 2.2.6 (Fidelity)**.** Let ρ, σ be quantum states. The fidelity $F(\rho, \sigma)$ between ρ and σ is defined as

$$F(\rho, \sigma) \coloneqq \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1^2. \tag{2.22}$$

As a direct consequence, the following proposition holds:

Proposition 2.2.7 (Expected fidelity)**.** *The fidelity between a pure state $|\psi\rangle$ and a mixed state ρ is given by*

$$F(|\psi\rangle, \rho) = \langle\psi| \rho |\psi\rangle. \tag{2.23}$$

The expected fidelity can be seen as the probability of observing "Yes" in the Yes/No measurement $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$ performed on the state ρ. One can also check that $0 \leq F(\rho, \sigma) \leq 1$. Although the fidelity is also a measure for the distinguishability of quantum states, one can notice that the distinguishability grows when the fidelity gets decreased, contrary to the trace distance. The followings are the useful properties of the fidelity.

Proposition 2.2.8 (Concavity)**.** *Let ρ_1, ρ_2, σ be the quantum states and $\lambda \in [0, 1]$. Then the following inequality holds:*

$$F(\lambda\rho_1 + (1-\lambda)\rho_2, \sigma) \geq \lambda F(\rho_1, \sigma) + (1-\lambda) F(\rho_2, \sigma) \tag{2.24}$$

Proposition 2.2.9 (Monotonicity)**.** *For any CPTP map $\mathcal{E} : \mathfrak{D}(\mathcal{H}) \to \mathfrak{D}(\mathcal{H})$ and for any quantum states $\rho, \sigma \in \mathfrak{D}(\mathcal{H})$, the following condition holds:*

$$F(\rho, \sigma) \leq F\left(\mathcal{E}(\rho), \mathcal{E}(\sigma)\right). \tag{2.25}$$

Theorem 2.2.10 (Uhlmann [Uhl76, HQ11]). *Let $\rho, \sigma \in \mathfrak{D}(\mathcal{H}_A)$ be quantum states on the system A, and R be the system with $\mathcal{H}_R \cong \mathcal{H}_A$. Then, the following expression holds for the fidelity:*

$$F(\rho, \sigma) = \max\{|\langle\psi|\phi\rangle|^2 : |\psi\rangle \in \mathcal{P}_\rho, |\phi\rangle \in \mathcal{P}_\sigma\}, \tag{2.26}$$

where $\mathcal{P}_\rho = \{|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_R : |\psi\rangle$ is a purification of $\rho\}$.

The following lemma is not very common, so a proof is given here for later use.

Lemma 2.2.11 (Lower bound of the fidelity in the extended system). *For any quantum state $\tau_{AE} \in \mathfrak{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$ and any pure state $|0\rangle\langle 0|_A \in \mathfrak{D}(\mathcal{H}_A)$,*

$$\left(F(\tau_A, |0\rangle\langle 0|_A)\right)^2 \leq F(\tau_{AE}, |0\rangle\langle 0|_A \otimes \tau_E) \leq F(\tau_A, |0\rangle\langle 0|_A) \tag{2.27}$$

holds, where $\tau_E \coloneqq \mathrm{Tr}_A \tau_{AE}$ and $\tau_A \coloneqq \mathrm{Tr}_E \tau_{AE}$.

Proof. The second inequality is the direct consequence of Lemma 2.2.9 applied on the partial trace Tr_E. In order ot prove the first inequality, let Q, R be auxiliary systems with $\mathcal{H}_R \cong \mathcal{H}_A$, and let $|\Psi\rangle_{AEQR}, |\Phi\rangle_{AEQR}$ be the purified states of τ_{AE} and $|0\rangle\langle 0|_A \otimes \tau_E$, respectively, which are given by

$$|\Psi\rangle_{AEQR} \coloneqq \sum_i |i\rangle_A |\psi_i\rangle_{EQ} |\tilde{0}\rangle_R \tag{2.28}$$

$$|\Phi\rangle_{AEQR} \coloneqq |0\rangle_A |\phi\rangle_{EQR}. \tag{2.29}$$

Here, $\{|i\rangle_A\}_i$ is a CONS in $\mathcal{H}_A$ that contains $|0\rangle_A$, $|\psi_i\rangle$s are subnormalized vectors satisfying $\sum_i \langle\psi_i|\psi_i\rangle = 1$, and $|\phi\rangle_{EQR}$ is given by

$$|\phi\rangle_{EQR} = \sum_i |\psi_i\rangle_{EQ} |\tilde{i}\rangle_R, \tag{2.30}$$

where $\{|\tilde{i}\rangle_R\}_i$ is a CONS in $\mathcal{H}_R$ that contains $|\tilde{0}\rangle_R$. One can ensure that $|\phi\rangle_{EQR}$ is a purification of τ_E because

$$\begin{aligned} \mathrm{Tr}_{QR}\left[|\phi\rangle\langle\phi|_{EQR}\right] &= \sum_{i,j} \mathrm{Tr}_{QR}\left[|\psi_i\rangle\langle\psi_j|_{EQ} \otimes |\tilde{i}\rangle\langle\tilde{j}|_R\right] && (2.31)\\ &= \sum_i \mathrm{Tr}_Q\left[|\psi_i\rangle\langle\psi_i|_{EQ}\right] && (2.32)\\ &= \tau_E, && (2.33) \end{aligned}$$

from the definition of τ_E and $|\psi_i\rangle$ in (2.28). By using Uhlmann's theorem (2.26), we have

$$\begin{aligned} F(\tau_{AE}, |0\rangle\langle 0|_A \otimes \tau_E) &\geq \left|\langle\Psi|_{AEQR} |\Phi\rangle_{AEQR}\right|^2 && (2.34)\\ &= \left|\langle\psi_0|_{EQ} \langle\tilde{0}|_R |\phi\rangle_{EQR}\right|^2 && (2.35)\\ &= \left|\langle\psi_0|\psi_0\rangle\right|^2, && (2.36) \end{aligned}$$

where we used Eq. (2.30) in the second equality. On the other hand, the following also holds:

$$\begin{aligned} F(\tau_A, |0\rangle\langle 0|_A) &= \langle 0|_A \operatorname{Tr}_{EQR}\left[|\Psi\rangle\langle\Psi|_{AEQR}\right]|0\rangle_A && (2.37)\\ &= \sum_{i,j} \langle 0|_A \operatorname{Tr}_{EQR}\left[|i\rangle\langle j|_A \otimes |\psi_i\rangle\langle\psi_j|_{EQ} \otimes |\tilde{0}\rangle\langle\tilde{0}|_R\right]|0\rangle_A && (2.38)\\ &= \operatorname{Tr}_{EQ} |\psi_0\rangle\langle\psi_0|_{EQ} && (2.39)\\ &= \langle\psi_0|\psi_0\rangle\,. && (2.40) \end{aligned}$$

Combining these two, the following inequality holds:

$$\left(F(\tau_A, |0\rangle\langle 0|_A)\right)^2 \leq F(\tau_{AE}, |0\rangle\langle 0|_A \otimes \tau_E). \tag{2.41}$$

□

Finally, the relation between the trace distance and the fidelity of quantum states is given as follows [NC10].

Proposition 2.2.12 (Relation between the trace distance and the fidelity)**.** *Let ρ, σ be quantum states. Then,*

$$1 - \sqrt{F(\rho,\sigma)} \leq d(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)}. \tag{2.42}$$

Chapter 3

Continuous-variable quantum system

Some physical systems, such as an oscillator mode of the trapped ion and a single optical mode, can be modeled by infinite-dimensional Hilbert spaces. Such a system has observables with a continuous spectrum, which are unique to the infinite dimension and can be used in quantum information processing [BvL05, EP03], and thus is called the continuous-variable quantum system. In this section, the basics of the continuous-variable quantum system are explained, and the theories of quantum optical systems are reviewed as a particular example of continuous-variable quantum systems.

3.1 Basics of the continuous-variable quantum system

3.1.1 Position and momentum operators

Let $L^2(\mathbb{R})$ be the (normed) space of complex square-integrable functions on the real line $\mathbb{R}$. $L^2(\mathbb{R})$ is a Hilbert space with the inner product $\langle\psi|\phi\rangle = \int_{-\infty}^{\infty} dq\, \overline{\psi(q)}\phi(q)$. Let $X(s)$ and $Z(t)$ be (strongly continuous) one-parameter unitary groups on $L^2(\mathbb{R})$ defined by

$$[X(s)\psi](q) = \psi(q-s), \quad [Z(t)\psi](q) = e^{itq}\psi(q), \qquad \forall t, s \in \mathbb{R},\ \forall \psi \in L^2(\mathbb{R}), \tag{3.1}$$

and therefore satisfying $X(s)Z(t) = e^{-ist}Z(t)X(s)$. Due to the Stone's theorem, $X(s)$ and $Z(t)$ can be denoted by

$$X(s) = \exp(-is\hat{p}) \quad \text{and} \quad Z(t) = \exp(it\hat{q}) \tag{3.2}$$

with self-adjoint operators $\hat{q}$ and $\hat{p}$ satisfying

$$[\hat{q}\,\psi](q) = q\psi(q), \qquad \psi \in \operatorname{dom}\hat{q}, \tag{3.3}$$

$$[\hat{p}\,\phi](q) = i^{-1}\frac{d}{dq}\phi(q), \qquad \phi \in \operatorname{dom}\hat{p}. \tag{3.4}$$

Self-adjoint operators $\hat{q}$ and $\hat{p}$ are called the position and the momentum operators, respectively, and can take continuous values. Written in terms of the Dirac's notation, they are

$$\hat{q} = \int_{-\infty}^{\infty} dq\, q\, |q\rangle\langle q|\,, \qquad \hat{p} = \int_{-\infty}^{\infty} dp\, p\, |p\rangle\langle p|\,, \tag{3.5}$$

$$X(s)^\dagger\, \hat{q}\, X(s) = \hat{q} + s, \qquad Z(t)^\dagger\, \hat{p}\, Z(t) = \hat{p} + t, \tag{3.6}$$

$$\langle q|q'\rangle = \delta(q-q'), \qquad \langle p|p'\rangle = \delta(p-p'), \qquad \langle q|p\rangle = \frac{1}{\sqrt{2\pi}} e^{iqp}, \tag{3.7}$$

$$\langle q|\psi\rangle = \psi(q), \qquad \langle p|\psi\rangle = \tilde{\psi}(p), \tag{3.8}$$

$$|\psi\rangle = \int_{-\infty}^{\infty} dq\, \psi(q)\, |q\rangle = \int_{-\infty}^{\infty} dp\, \tilde{\psi}(p)\, |p\rangle\,, \tag{3.9}$$

where $\delta(x)$ is the Dirac delta function and the $\tilde{\psi}$ is the Fourier transform of ψ. (Conventionally, $\psi(q)$ is called the position wave function and $\tilde{\psi}(p)$ is called the momentum wave function.) This particular Hilbert space and unitary groups $X(s)$ and $Z(t)$ on it play an important role, which is explained in the following. Let $U(s)$ and $W(t)$ $(s,t \in \mathbb{R})$ be one-parameter unitary groups satisfying $U(s)W(t) = e^{-ist}W(t)U(s)$. This is called Weyl-Segal canonical commutation relation (CCR). Equivalently, by introducing the vector $z = (s,t)$ and defining the unitary $V'(z) \coloneqq e^{ist/2}U(s)W(t)$, the CCR can be denoted by $V'(z_1)V'(z_2) = \exp(i(t_1s_2 - s_1t_2)/2)\, V'(z_1+z_2)$. The pair of the unitary groups $X(s)$ and $Z(t)$ in Eq. (3.1) is an irreducible representation of the CCR (called the Schrödinger representation). Likewise, the unitary $V(z)$ defined by

$$V(z) \coloneqq e^{ist/2}X(s)Z(t) = e^{-ist/2}Z(t)X(s) = \exp\left(it\hat{q} - is\hat{p}\right) \tag{3.10}$$

is the Schrödinger representation of $V'(z)$. The Stone-von Neumann theorem states that any irreducible representation of CCR is unitarily equivalent to the Schrödinger representation. Therefore, we can always use the Schrödinger representation to analyze the continuous variables obeying the CCR. The more commonly known CCR is the commutation relation $[\hat{q},\hat{p}] = i$ between the generators $\hat{q}$ and $\hat{p}$ (called Heisenberg CCR). Note that this commutation relation is meaningful only on a certain dense subset of the Hilbert space.

Now we turn to the multi-variable case. The Heisenberg CCR with N degrees of freedom can be written as $[\hat{q}_j,\hat{p}_k] = i\delta_{j,k}$, $[\hat{q}_j,\hat{q}_k] = 0$, and $[\hat{p}_j,\hat{p}_k] = 0$, where $\delta_{j,k}$ denotes the Kronecker delta. The corresponding Weyl form of the CCR is given as follows. Let $\boldsymbol{x} = (x_1,\ldots,x_N)$ and $\boldsymbol{y} = (y_1,\ldots,y_N)$ be N component row vectors. Define $X(\boldsymbol{x}) \coloneqq \exp(-i\sum_{k=1}^N x_k\hat{p}_k)$ and $Z(\boldsymbol{y}) \coloneqq \exp(i\sum_{k=1}^N y_k\hat{q}_k)$. Then, the Weyl CCR with N degrees of freedom is given by

$$X(\boldsymbol{x})Z(\boldsymbol{y}) = \exp\left(-i\sum_{k=1}^{N} x_k y_k\right) Z(\boldsymbol{y})X(\boldsymbol{x}). \tag{3.11}$$

For an alternative form of the above, let $\boldsymbol{z} = (x_1,y_1,x_2,y_2,\ldots,x_N,y_N)$ be a $2N$ component vector, and let $\Delta(\boldsymbol{z},\boldsymbol{z}')$ be a symplectic form defined as

$$\Delta(\boldsymbol{z},\boldsymbol{z}') = \sum_{k=1}^{N}(x'_k y_k - x_k y'_k). \tag{3.12}$$

Then, an alternative form of the Weyl CCR with N degrees of freedom is given by

$$V(\boldsymbol{z})V(\boldsymbol{z}') = e^{i\Delta(\boldsymbol{z},\boldsymbol{z}')/2}V(\boldsymbol{z}+\boldsymbol{z}'). \tag{3.13}$$

The generator $\hat{R}(\boldsymbol{z})$ of $V(\boldsymbol{z})$ (i.e., $V(\boldsymbol{z}) = e^{i\hat{R}(\boldsymbol{z})}$) can be given by

$$\hat{R}(\boldsymbol{z}) = \sum_k (y_k\hat{q}_k - x_k\hat{p}_k), \tag{3.14}$$

and satisfies

$$[\hat{R}(\boldsymbol{z}), \hat{R}(\boldsymbol{z}')] = i\Delta(\boldsymbol{z},\boldsymbol{z}')I. \tag{3.15}$$

3.1.2 Characteristic function and Wigner function

The quantum state in the continuous-variable system has convenient representations as a function of continuous variables. For $\rho \in \mathfrak{D}(\mathcal{H}^{\otimes N})$, its characteristic function $F_\rho(\boldsymbol{z})$ ($\boldsymbol{z} \in \mathbb{R}^{2N}$) is defined as

$$F_\rho(\boldsymbol{z}) = \mathrm{Tr}[\rho V(\boldsymbol{z})]. \tag{3.16}$$

The characteristic function $F_\rho(\boldsymbol{z})$ is continuous for all $\boldsymbol{z} \in \mathbb{R}^{2N}$ and satisfies $|F_\rho(\boldsymbol{z})| \leq 1$, $F_\rho(\boldsymbol{0}) = 1$, and $F_\rho(-\boldsymbol{z}) = (F_\rho(\boldsymbol{z}))^*$ [Hol11]. The Wigner function $W_\rho(\boldsymbol{r})$ ($\boldsymbol{r} \in \mathbb{R}^{2N}$) is defined as the (symplectic) Fourier transform of $F_\rho(\boldsymbol{z})$ given by [CG69]

$$W_\rho(\boldsymbol{r}) = \int_{-\infty}^{\infty} \frac{dz^{2N}}{(2\pi)^{2N}} F_\rho(\boldsymbol{z}) \exp[-i\Delta(\boldsymbol{r},\boldsymbol{z})]. \tag{3.17}$$

The characteristic function and the Wigner function has one-to-one correspondence to the density matrix. For the characteristic function, for example, the inverse transformation can be explicitly given by

$$\rho = \int_{-\infty}^{\infty} \frac{dz^{2N}}{(2\pi)^{N}} F_\rho(\boldsymbol{z}) V(-\boldsymbol{z}). \tag{3.18}$$

The Wigner function is real and satisfies a kind of normalization condition $\int d\boldsymbol{r}\, W_\rho(\boldsymbol{r}) = 1$. Thus, the Wigner function is called quasi-probability distribution; the only difference from the usual probability distribution is that the Wigner function can be negative while any probability distribution is nonnegative.

Similarly to probability distributions, the moment of the Wigner function can be defined. The first moment, the mean $\overline{\boldsymbol{r}}$, is defined as $\overline{\boldsymbol{r}} \coloneqq \int d\boldsymbol{r}\, \boldsymbol{r} W_\rho(\boldsymbol{r})$ if it does not diverge. The second moment, the covariance matrix $\boldsymbol{V} = (V_{ij})$ is the $2N \times 2N$ matrix defined as

$$V_{ij} = \mathrm{Re}\left[\int d\boldsymbol{r}\, (r_i - \overline{r}_i)(r_j - \overline{r}_j) W_\rho(\boldsymbol{r})\right], \tag{3.19}$$

where $\mathrm{Re}[\cdot]$ denotes the real part. The higher moment can be defined similarly.

The Wigner function for ρ has the following alternative form:

$$W_\rho(\boldsymbol{r}) = \frac{1}{(2\pi)^N} \int_{-\infty}^{\infty} d\boldsymbol{x}\, e^{i\boldsymbol{p}\boldsymbol{x}^\top} \left\langle \boldsymbol{q} - \frac{\boldsymbol{x}}{2} \middle| \rho \middle| \boldsymbol{q} + \frac{\boldsymbol{x}}{2} \right\rangle, \tag{3.20}$$

where $\top$ denotes the transposition. This transformation from the density operator to the function over $\mathbb{R}^{2N}$ can be extended to an arbitrary operator A on $\mathcal{H}^{\otimes N}$, which is also called the Wigner function of A.

3.1.3 Gaussian states, Gaussian channels, and Gaussian measurements

The set of Gaussian states is a distinctive subset of the set of quantum states in continuous-variable systems; it is closed under the action of Gaussian channels, and a Gaussian state has lots of similarities to the classical probability distribution [CLP07, WPGP$^+$12].

A quantum state ρ in the continuous-variable system is called Gaussian if its characteristic function has a Gaussian form, i.e.,

$$F_\rho(\boldsymbol{z}) = \exp\left(-\frac{1}{2}\boldsymbol{z}\left(\boldsymbol{\Omega}^\top \boldsymbol{V}\boldsymbol{\Omega}\right)\boldsymbol{z}^\top + i\overline{\boldsymbol{r}}\boldsymbol{\Omega}\boldsymbol{z}^\top\right), \tag{3.21}$$

where $2N \times 2N$ matrix $\boldsymbol{\Omega}$ satisfies $\boldsymbol{x}\boldsymbol{\Omega}\boldsymbol{z}^\top = \Delta(\boldsymbol{x}, \boldsymbol{z})$. One can show that its Wigner function is also Gaussian [WPGP$^+$12], i.e.,

$$W_\rho(\boldsymbol{r}) = \frac{\exp\left[-\frac{1}{2}(\boldsymbol{r}-\overline{\boldsymbol{r}})\boldsymbol{V}^{-1}(\boldsymbol{r}-\overline{\boldsymbol{r}})^\top\right]}{(2\pi)^N\sqrt{\det \boldsymbol{V}}}. \tag{3.22}$$

Examples of the Gaussian states are the vacuum state, coherent states and thermal states in the quantum optics. The covariance matrix $\boldsymbol{V}$ must satisfy a physicality condition $\boldsymbol{V} \geq \frac{i}{2}\boldsymbol{\Omega}$, which is reduced to the Heisenberg uncertainty principle $(\Delta q)^2(\Delta p)^2 \geq \frac{1}{4}$ in the case of $N = 1$ [SMD94, EP03, CEGH08, WPGP$^+$12].

A Gaussian unitary U is a unitary that transforms the position and momentum operators linearly. It is generated by self-adjoint operators that are at most quadratic in the position and momentum operators. The Weyl unitary $V(\boldsymbol{z})$ is contained in the set of Gaussian unitary operators since it adds a constant vector to the position and momentum operators. Other than the addition of a constant vector, the (adjoint) action of a Gaussian unitary U on the Weyl unitary $V(\boldsymbol{z})$ leads to $U^\dagger V(\boldsymbol{z})U = V(\boldsymbol{z}S^{-1})$, where S denotes a symplectic matrix $S \in Sp(2N, \mathbb{R})$ that satisfies $\Delta(\boldsymbol{z}, \boldsymbol{z}') = \Delta(\boldsymbol{z}S, \boldsymbol{z}'S)$ or equivalently $S\boldsymbol{\Omega}S^\top = \boldsymbol{\Omega}$ [CEGH08, Hol11]. In other words, such unitary operators form a representation of $Sp(2N, \mathbb{R})$. Examples of the Gaussian unitaries are the phase rotations, squeezing, and beamsplitter coupling in quantum optics.

A Gaussian channel Φ is a CPTP map whose adjoint map $\Phi^\dagger$ acts on $V(\boldsymbol{z})$ as

$$\Phi^\dagger(V(\boldsymbol{z})) = V(\boldsymbol{z}K)\exp\left[-\frac{1}{2}\boldsymbol{z}\left(\boldsymbol{\Omega}^\top\Gamma\boldsymbol{\Omega}\right)\boldsymbol{z}^\top + i\boldsymbol{m}\boldsymbol{\Omega}\boldsymbol{z}^\top\right], \tag{3.23}$$

where K and Γ are $2N \times 2N$ real matrices and $\boldsymbol{m} \in \mathbb{R}^{2N}$ is a row vector [HW01, EP03, CGH06, Hol07, CEGH08]. Therefore, the characteristic function of a density operator ρ transforms into

$$F_{\Phi(\rho)}(\boldsymbol{z}) = F_\rho(\boldsymbol{z}K)\exp\left[-\frac{1}{2}\boldsymbol{z}\left(\boldsymbol{\Omega}^\top\Gamma\boldsymbol{\Omega}\right)\boldsymbol{z}^\top + i\boldsymbol{m}\boldsymbol{\Omega}\boldsymbol{z}^\top\right]. \tag{3.24}$$

For the Gaussian state ρ given in Eq. (3.21), the application of the Gaussian channel Φ on ρ leads to

$$\overline{\boldsymbol{r}} \to \overline{\boldsymbol{r}}K'^\top + \boldsymbol{m}, \tag{3.25}$$

$$\boldsymbol{V} \to K'\boldsymbol{V}K'^\top + \Gamma, \tag{3.26}$$

where K' denotes $K' = \mathbf{\Omega} K \mathbf{\Omega}^\top$. Therefore, a Gaussian state is transformed into a Gaussian state through the Gaussian channel. In fact, Eqs. (3.25) and (3.26) hold for general quantum states with the first and second moments given respectively by $\overline{\boldsymbol{r}}$ and $\boldsymbol{V}$. The complete positivity of the channel is equivalent to the following inequality for K' and Γ [HW01, CGH06, Hol07, CEGH08]:

$$\Gamma \geq \frac{i}{2}\mathbf{\Omega} - \frac{i}{2} K' \mathbf{\Omega} K'^{\top}. \tag{3.27}$$

A Gaussian channel is called quantum-limited when the equality in Eq. (3.27) is achieved [ISS11, GHGP15]. The Gaussian channel Φ can also be written as

$$\Phi(\rho) = \mathrm{Tr}_E \left[U(\rho \otimes \rho_E) U^\dagger \right], \tag{3.28}$$

where U is a Gaussian unitary and ρ_E is a Gaussian state [CG06, CGH06, CLP07, CEGH08, CEGH11]. Note that this is not the Stinespring dilation of the channel in general, since ρ_E can be a mixed state. If the state ρ_E is the vacuum state, the corresponding Gaussian channel is quantum-limited.

The classification of Gaussian channels in perspective of its information-theoretic characteristics has been intensively studied e.g. in Refs. [HW01, CGH06, CG06, Hol07, WPGG07, CEGH08, PGPBL09, ISS11, GPNBL$^+$12, WHG12, MGH14, GGPCH14, TGW14, GHGP15, DPTG16, PLOB17, DPTG17, QW17, WQ18, SWAT18, RMG18]. Among others, in the case of $N = 1$, the following channels are important in the application [CGH06, Hol07, GPNBL$^+$12].

- The quantum-limited loss (pure-loss) channel: the Gaussian channel with $\boldsymbol{m}$, K, and Γ in Eqs. (3.25) and (3.26) being

$$\boldsymbol{m} = (0,0), \qquad K = \begin{pmatrix} \sqrt{\eta} & 0 \\ 0 & \sqrt{\eta} \end{pmatrix}, \qquad \Gamma = \frac{1}{2}\begin{pmatrix} 1-\eta & 0 \\ 0 & 1-\eta \end{pmatrix}, \tag{3.29}$$

  where $0 \leq \eta \leq 1$. The parameter η is called the transmissivity of the loss channel.

- The quantum-limited amplifier channel: the Gaussian channel with $\boldsymbol{m}$, K, and Γ being

$$\boldsymbol{m} = (0,0), \qquad K = \begin{pmatrix} \sqrt{G} & 0 \\ 0 & \sqrt{G} \end{pmatrix}, \qquad \Gamma = \frac{1}{2}\begin{pmatrix} G-1 & 0 \\ 0 & G-1 \end{pmatrix}, \tag{3.30}$$

  where $G \geq 1$. The parameter G is called the gain of the amplifier.

- The Gaussian random displacement channel: the Gaussian channel with $\boldsymbol{m}$, K, and Γ being

$$\boldsymbol{m} = (0,0), \qquad K = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Gamma = \begin{pmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{pmatrix}. \tag{3.31}$$

  The parameter σ^2 is called the variance of the Gaussian random displacement.

In fact, any phase-covariant single-mode Gaussian channel, that is, the channel in which the phase rotation transforms covariantly from the input to the output, can be realized by a composition of the quantum-limited loss and amplifier channels [CGH06, GHGP15]. For example, the Gaussian random displacement channel with the variance σ^2 can be realized by a quantum-limited loss channel with the transmissivity $\eta = 1/(1+\sigma^2)$ followed by a quantum-limited amplifier channel with the gain $G = 1+\sigma^2$.

Finally, we introduce the Gaussian measurement. Let $M : \mathcal{B}(\mathbb{R}^m) \to \mathfrak{B}(\mathcal{H}^{\otimes N})$ be a POVM on the continuous-variable system with N degrees of freedom, where $\mathcal{B}(\mathbb{R}^m)$ denotes the Borel σ-algebra of $\mathbb{R}^m$. The probability $\Pr_\rho[\cdot]$ that the outcome of the measurement on ρ is in $A \in \mathcal{B}(\mathbb{R}^m)$ is thus given by

$$\Pr_\rho[A] = \mathrm{Tr}\left[\rho \int_A M(d^m\xi)\right]. \tag{3.32}$$

Define the operator characteristic function $\phi_M(\boldsymbol{\omega})$ as follows:

$$\phi_M(\boldsymbol{\omega}) = \int e^{i\boldsymbol{\omega}\boldsymbol{\xi}^\top} M(d^m\xi), \qquad \boldsymbol{\omega} \in \mathbb{R}^m. \tag{3.33}$$

The POVM M is called Gaussian if its operator characteristic function $\phi_M(\boldsymbol{\omega})$ has the form [Hol19, Hol21]

$$\phi_M(\boldsymbol{\omega}) = V(\boldsymbol{\omega}K\boldsymbol{\Omega}^\top)\exp\Big(-\frac{1}{2}\boldsymbol{\omega}\boldsymbol{\alpha}\boldsymbol{\omega}^\top\Big), \tag{3.34}$$

where K is a real $m \times 2N$ matrix and $\boldsymbol{\alpha}$ is a real symmetric $m \times m$ matrix satisfying

$$\boldsymbol{\alpha} \geq \pm\frac{i}{2}K\boldsymbol{\Omega}K^\top. \tag{3.35}$$

Let $r_{\boldsymbol{\alpha}}$ be the rank of the matrix $\boldsymbol{\alpha}$ and $r_{\boldsymbol{\Omega}_K}$ be the rank of $K\boldsymbol{\Omega}K^\top$, which is always even. Then, the Gaussian POVM M on the system A is known to be written, with the continuous-variable system C with $r_{\boldsymbol{\alpha}} - r_{\boldsymbol{\Omega}_K}/2$ degrees of freedom, in the following form [Hol19, Hol21]:

$$M(d^m\xi) = \mathrm{Tr}_C\left[(I \otimes \rho_C)\, E_{AC}(d^m\xi)\right]. \tag{3.36}$$

Here, ρ_C is the centered (i.e., mean zero) Gaussian state with the covariance matrix $\boldsymbol{\alpha}_C$ satisfying

$$KP\Lambda\boldsymbol{\alpha}_C\Lambda P^\top K^\top = \boldsymbol{\alpha}, \tag{3.37}$$

where Λ changes the signs of the entries corresponding to the momentum variables and P denotes the projection onto the subspace spanned by $\mathrm{supp}(\boldsymbol{\alpha})K$ (see [Hol19, Hol21] for more detail). The PVM E_{AC} is the spectral measure of the vector of self-adjoint operator:

$$\hat{X} = \hat{r}_A K^\top \otimes I_C + I_A \otimes \hat{r}_C \Lambda P^\top K^\top. \tag{3.38}$$

An example of the Gaussian measurement in the case of $N = 1$ is the PVM E that is the spectral measure of the position operator $\hat{q}$ given by

$$E(d\xi) = |(q =)\xi\rangle\langle(q =)\xi|\, d\xi, \tag{3.39}$$

where we followed the Dirac's notation in Eq. (3.5). It is the Gaussian measurement with $K = (1, 0)$ and $\boldsymbol{\alpha} = 0$ in its operator characteristic function (3.33) since

$$\phi_E(\omega) = \int e^{i\omega\xi} \, |(q =)\xi\rangle\langle(q =)\xi| \, d\xi = e^{i\omega\hat{q}} = V(0, \omega), \tag{3.40}$$

and

$$\boldsymbol{\Omega} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{3.41}$$

Such a single-outcome measurement with $\boldsymbol{\alpha} = 0$ is called the ideal homodyne measurement in the quantum optics [CD94]. A Gaussian measurement with $K = (1, 0)$ and $\boldsymbol{\alpha} > 0$ can be regarded as a noisy version of the homodyne measurement.

Another example of the Gaussian measurement for $N = 1$ is the two-outcome measurement F given by

$$F(d^2\xi) = V(\sqrt{2}\boldsymbol{\xi}) \, |0\rangle\langle 0| \, V(\sqrt{2}\boldsymbol{\xi})^\dagger \frac{d^2\xi}{\pi}, \tag{3.42}$$

where $|0\rangle$ denotes the vacuum state with its position wave function $\langle q|0\rangle$ given by

$$\langle q|0\rangle = \psi_0(q) = \pi^{-\frac{1}{4}} \exp(-q^2/2) \tag{3.43}$$

satisfying

$$[(\hat{q} + i\hat{p})\psi_0](q) = 0 \tag{3.44}$$

from Eqs. (3.3) and (3.4) and its Wigner function $W_{|0\rangle\langle 0|}(q, p)$ given by

$$W_{|0\rangle\langle 0|}(q, p) = \frac{1}{\pi} \exp(-q^2 - p^2). \tag{3.45}$$

The operator characteristic function (3.33) of the POVM F is given by

$$K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \boldsymbol{\alpha} = \frac{1}{4} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.46}$$

This can be checked as follows. Let us observe that, for $s \in \mathbb{C}$,

$$V(-is, s)V(\sqrt{2}\xi_R, \sqrt{2}\xi_I) \, |0\rangle = e^{\sqrt{2}is(\xi_R + i\xi_I)} V(\sqrt{2}\xi_R, \sqrt{2}\xi_I)V(-is, s) \, |0\rangle \tag{3.47}$$

$$= e^{\sqrt{2}is(\xi_R + i\xi_I)} V(\sqrt{2}\xi_R, \sqrt{2}\xi_I) \, |0\rangle \, , \tag{3.48}$$

where the last equality follows from $V(-is, s) = \exp(is(\hat{q} + i\hat{p}))$ and Eq. (3.44). Changing s to $-s$ in the above, we also have

$$V(is, -s)V(\sqrt{2}\xi_R, \sqrt{2}\xi_I) \, |0\rangle = e^{-\sqrt{2}is(\xi_R + i\xi_I)} V(\sqrt{2}\xi_R, \sqrt{2}\xi_I) \, |0\rangle \, . \tag{3.49}$$

Combining these with Eq. (3.42), we have

$$V(-is, s)F(d^2\xi)V(is, -s)^\dagger = e^{\sqrt{2}is(\xi_R + i\xi_I) + \sqrt{2}is^*(\xi_R - i\xi_I)} F(d^2\xi), \tag{3.50}$$

where * denotes the complex conjugate. Integrating over $\mathbb{R}^2$, we have

$$V(-is, s) \, I \, V(is, -s)^\dagger = \phi_F \left(2\sqrt{2} \, \mathrm{Re}[s], -2\sqrt{2} \, \mathrm{Im}[s] \right). \tag{3.51}$$

Using Eq. (3.13), the left-hand side can be reformulated as

$$V(-is,s)\,I\,V(is,-s)^\dagger = V(-is,s)V(is^*,s^*) \tag{3.52}$$
$$= e^{i(is^*s-(-is)s^*)/2}V(-is+is^*,s+s^*) \tag{3.53}$$
$$= e^{-|s|^2}V(2\mathrm{Im}[s],2\mathrm{Re}[s]). \tag{3.54}$$

Substituting $s=(\omega_R-i\omega_I)/(2\sqrt{2})$, we have

$$e^{-\frac{1}{8}(\omega_R^2+\omega_I^2)}V(-\omega_I/\sqrt{2},\omega_R/\sqrt{2}) = \phi_F(\omega_R,\omega_I), \tag{3.55}$$

and thus Eq. (3.34) for $M=F$ holds with $\boldsymbol{\Omega}$, K, and $\boldsymbol{\alpha}$ given in Eqs. (3.41) and (3.46). Using Eq. (3.36), we can rewrite this POVM with the ancillary state ρ_C being the vacuum state $|0\rangle$ and the PVM E_{AC} being the joint spectral measure of $(\hat{q}_A+\hat{q}_C)/\sqrt{2}$ and $(\hat{p}_A-\hat{p}_C)/\sqrt{2}$. This can be checked by comparing Eqs. (3.37) and (3.38) with

$$P=\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad \Lambda=\begin{pmatrix}1&0\\0&-1\end{pmatrix}, \tag{3.56}$$

and the covariance matrix $\boldsymbol{\alpha}_C$ of the vacuum being

$$\boldsymbol{\alpha}_C=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{3.57}$$

from its Wigner function (3.45). This type of measurement is called the heterodyne (or dual-homodyne) measurement in the quantum optics [CD94]. Again, a Gaussian measurement with the same K but a larger value of $\boldsymbol{\alpha}$ can be interpreted as a noisy heterodyne measurement. The set of Gaussian measurements is essentially composed of multi-variable generalization of (noisy) symplectic-transformed homodyne and heterodyne measurements [Hol19, Hol21].

3.1.4 Gaussian operations

Gaussian operations are the important subset of operations that can be performed on the continuous-variable quantum system. It is composed of the preparation of Gaussian states, the action of Gaussian unitaries, Gaussian measurements, and the ignorance of a subsystem. Gaussian channels are contained in Gaussian operations, which is obvious from the expression (3.28). Note that in terms of the transformation law as in Eq. (3.23), the ignorance Φ_{tr} of a subsystem is given by $\Phi_{\mathrm{tr}}^\dagger(V(\boldsymbol{z}))=V(\boldsymbol{z}\oplus(0,0))$, where $\oplus$ denotes the direct sum. Implementation of Gaussian operations in quantum optical systems is relatively easy, which will be explained in the next section.

3.2 Quantum optical system as a continuous-variable system

In this section, the quantum optical system is reviewed as a prominent example of the continuous-variable system. For detail, see e.g. [MW95, KL10].

3.2.1 Quantization of electromagnetic field

The vector potential $\boldsymbol{A}(\boldsymbol{r},t)$ of the free electromagnetic field satisfies the homogeneous wave equation

$$\nabla^2\boldsymbol{A}(\boldsymbol{r},t)-\frac{1}{c^2}\frac{\partial^2}{\partial t^2}\boldsymbol{A}(\boldsymbol{r},t)=0, \tag{3.58}$$

in the Coulomb gauge

$$\nabla\cdot\boldsymbol{A}=0,\qquad \Phi=0. \tag{3.59}$$

The electric field $\boldsymbol{E}(\boldsymbol{r},t)$ and the magnetic field $\boldsymbol{B}(\boldsymbol{r},t)$ are given by

$$\boldsymbol{E}(\boldsymbol{r},t)=-\frac{\partial}{\partial t}\boldsymbol{A}(\boldsymbol{r},t), \tag{3.60}$$

$$\boldsymbol{B}(\boldsymbol{r},t)=\nabla\times\boldsymbol{A}(\boldsymbol{r},t). \tag{3.61}$$

The Maxwell equation for electromagnetic fields follows from these equations. The solution of the wave equation (3.58) can be written as

$$\boldsymbol{A}(\boldsymbol{r},t)=\sum_\lambda\int\frac{d\boldsymbol{k}}{\sqrt{\varepsilon_0}}\left[\boldsymbol{e}_\lambda(\boldsymbol{k})A_\lambda(\boldsymbol{k})u(\boldsymbol{k};\boldsymbol{r},t)+\boldsymbol{e}_\lambda^*(\boldsymbol{k})A_\lambda^*(\boldsymbol{k})u^*(\boldsymbol{k};\boldsymbol{r},t)\right], \tag{3.62}$$

where $A_\lambda(\boldsymbol{k})$ denotes the amplitude of the mode with the wave vector $\boldsymbol{k}$ and polarization λ, $\boldsymbol{e}_\lambda$ denotes the direction of the polarization, and $u(\boldsymbol{k};\boldsymbol{r},t)$ denotes the "normalized" solution of the wave equation (3.58), i.e.,

$$u(\boldsymbol{k};\boldsymbol{r},t)=\frac{e^{i\boldsymbol{k}\cdot\boldsymbol{r}-i\omega_{\boldsymbol{k}}t}}{\sqrt{(2\pi)^3 2\omega_{\boldsymbol{k}}}}, \tag{3.63}$$

with $\omega_{\boldsymbol{k}}=c|\boldsymbol{k}|$. Due to the condition of Coulomb gauge (3.59), we have $\boldsymbol{k}\cdot\boldsymbol{e}_\lambda(\boldsymbol{k})=0$. When the electromagnetic fields are quantized, the classical amplitude $A_\lambda(\boldsymbol{k})$ and its complex conjugate $A_\lambda^*(\boldsymbol{k})$ is replaced with $\sqrt{\hbar}$ times the operators $\hat{a}_\lambda(\boldsymbol{k})$ and $\hat{a}_\lambda^\dagger(\boldsymbol{k})$ that satisfies

$$[\hat{a}_\lambda(\boldsymbol{k}),\hat{a}_{\lambda'}^\dagger(\boldsymbol{k}')]=\delta_{\lambda,\lambda'}\delta^3(\boldsymbol{k}-\boldsymbol{k}'). \tag{3.64}$$

(These are not operators in the usual sense but rather the operator-valued distributions.) The resulting quantized vector potential as well as electromagnetic fields are

given by

$$\hat{\boldsymbol{A}}(\boldsymbol{r},t) = \sum_{\lambda} \int d\boldsymbol{k} \sqrt{\frac{\hbar}{\varepsilon_0}} \left[\boldsymbol{e}_{\lambda}(\boldsymbol{k}) \hat{a}_{\lambda}(\boldsymbol{k}) u(\boldsymbol{k};\boldsymbol{r},t) + \boldsymbol{e}^*_{\lambda}(\boldsymbol{k}) \hat{a}^{\dagger}_{\lambda}(\boldsymbol{k}) u^*(\boldsymbol{k};\boldsymbol{r},t) \right], \tag{3.65}$$

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = \sum_{\lambda} \int d\boldsymbol{k}\, i \sqrt{\frac{\hbar}{\varepsilon_0}} \left[\boldsymbol{e}_{\lambda}(\boldsymbol{k}) \hat{a}_{\lambda}(\boldsymbol{k}) \omega_{\boldsymbol{k}} u(\boldsymbol{k};\boldsymbol{r},t) - \boldsymbol{e}^*_{\lambda}(\boldsymbol{k}) \hat{a}^{\dagger}_{\lambda}(\boldsymbol{k}) \omega_{\boldsymbol{k}} u^*(\boldsymbol{k};\boldsymbol{r},t) \right], \tag{3.66}$$

$$\hat{\boldsymbol{B}}(\boldsymbol{r},t) = \sum_{\lambda} \int d\boldsymbol{k}\, i \sqrt{\frac{\hbar}{\varepsilon_0}} \left[(\boldsymbol{k} \times \boldsymbol{e}_{\lambda}(\boldsymbol{k})) \hat{a}_{\lambda}(\boldsymbol{k}) u(\boldsymbol{k};\boldsymbol{r},t) - (\boldsymbol{k} \times \boldsymbol{e}^*_{\lambda}(\boldsymbol{k})) \hat{a}^{\dagger}_{\lambda}(\boldsymbol{k}) u^*(\boldsymbol{k};\boldsymbol{r},t) \right]. \tag{3.67}$$

The energy H of the (quantized) electromagnetic field is given by

$$H = \frac{\varepsilon_0}{2} \int d\boldsymbol{r} \left[\hat{\boldsymbol{E}}^2(\boldsymbol{r},t) + c^2 \hat{\boldsymbol{B}}^2(\boldsymbol{r},t) \right] \tag{3.68}$$

$$= \sum_{\lambda} \int d\boldsymbol{k}\, \frac{\hbar \omega_{\boldsymbol{k}}}{2} [\hat{a}_{\lambda}(\boldsymbol{k}) \hat{a}^{\dagger}_{\lambda}(\boldsymbol{k}) + \hat{a}^{\dagger}_{\lambda}(\boldsymbol{k}) \hat{a}_{\lambda}(\boldsymbol{k})], \tag{3.69}$$

where we used $\boldsymbol{e}^*_{\lambda}(\boldsymbol{k}) \cdot \boldsymbol{e}_{\lambda'}(\boldsymbol{k}) = \delta_{\lambda,\lambda'}$ and

$$2 \int d\boldsymbol{r}\, \omega_{\boldsymbol{k}} u^*(\boldsymbol{k};\boldsymbol{r},t) u(\boldsymbol{k}';\boldsymbol{r},t) = \delta^3(\boldsymbol{k} - \boldsymbol{k}'). \tag{3.70}$$

Next we construct a well-defined mode functions $\boldsymbol{v}_{j,\lambda}(\boldsymbol{r},t)$. This can be made by taking an orthonormal system of weight functions $f_j(\boldsymbol{k})$, and define the mode function $\boldsymbol{v}_{j,\lambda}(\boldsymbol{r},t)$ by

$$\boldsymbol{v}_{j,\lambda}(\boldsymbol{r},t) = \int d\boldsymbol{k}\, f^*_j(\boldsymbol{k}) \boldsymbol{e}_{\lambda}(\boldsymbol{k}) \omega_{\boldsymbol{k}} u(\boldsymbol{k};\boldsymbol{r},t) \tag{3.71}$$

and the mode annihilation operators $\hat{a}_{j,\lambda}$ by

$$\hat{a}_{j,\lambda} = \int d\boldsymbol{k}\, f_j(\boldsymbol{k}) \hat{a}_{\lambda}(\boldsymbol{k}). \tag{3.72}$$

Due to the relation $\sum_j f^*_j(\boldsymbol{k}) f_j(\boldsymbol{k}') = \delta^3(\boldsymbol{k} - \boldsymbol{k}')$, we have

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = i \sqrt{\frac{\hbar}{\varepsilon_0}} \sum_{\lambda} \sum_{j} \left[\boldsymbol{v}_{j,\lambda}(\boldsymbol{r},t) \hat{a}_{j,\lambda} - \boldsymbol{v}^*_{j,\lambda}(\boldsymbol{r},t) \hat{a}^{\dagger}_{j,\lambda} \right]. \tag{3.73}$$

The electromagnetic field can thus be decomposed into the well-defined mode functions. By carefully designing the weight function $f_j(\boldsymbol{k})$ and the polarization vector $\boldsymbol{e}_{\lambda}(\boldsymbol{k})$, we can obtain a pulse-shaped mode function. In this thesis, we assume that an optical pulse emitted by a light source can be treated as a single pulse-shaped mode. The mode annihilation and creation operators satisfy the commutation relation

$$[\hat{a}_{j,\lambda}, \hat{a}_{k,\lambda'}] = 0, \qquad [\hat{a}^{\dagger}_{j,\lambda}, \hat{a}^{\dagger}_{k,\lambda'}] = 0, \qquad [\hat{a}_{j,\lambda}, \hat{a}^{\dagger}_{k,\lambda'}] = \delta_{jk} \delta_{\lambda\lambda'}. \tag{3.74}$$

The electromagnetic field has the pure vacuum state $|0\rangle$ satisfying

$$\hat{a}_{j,\lambda} |0\rangle = 0, \quad \forall j, \lambda. \tag{3.75}$$

Since the electromagnetic field can be decomposed into the mode functions $\boldsymbol{v}_{j,\lambda}(\boldsymbol{r},t)$, the vacuum state $|0\rangle$ can be interpreted an infinite tensor product of the vacua $|0\rangle_{j,\lambda}$ for each mode j and the polarization λ satisfying $\hat{a}_{j,\lambda}|0\rangle_{j,\lambda}=0$. We can define the Fock state $|n\rangle_{j,\lambda}$ for the mode j and the polarization λ by

$$|n\rangle_{j,\lambda}=\frac{1}{\sqrt{n!}}(\hat{a}^\dagger_{j,\lambda})^n|0\rangle_{j,\lambda}\,, \tag{3.76}$$

that satisfies

$$\hat{n}_{j,\lambda}|n\rangle_{j,\lambda}=\hat{a}^\dagger_{j,\lambda}\hat{a}_{j,\lambda}|n\rangle_{j,\lambda}=n|n\rangle_{j,\lambda}\,, \tag{3.77}$$

where $\hat{n}_{j,\lambda}\coloneqq\hat{a}^\dagger_{j,\lambda}\hat{a}_{j,\lambda}$ is called the photon number operator. The set of vectors $\{|n\rangle_{j,\lambda}\}$ forms a CONS of the Hilbert space associated with the mode j and the polarization λ. Finally, by setting $\hat{q}_{j,\lambda}=\frac{1}{\sqrt{2}}(\hat{a}_{j,\lambda}+\hat{a}^*_{j,\lambda})$ and $\hat{p}_{j,\lambda}=-i\frac{1}{\sqrt{2}}(\hat{a}_{j,\lambda}-\hat{a}^*_{j,\lambda})$, we have the commutation relation

$$[\hat{q}_{j,\lambda},\hat{q}_{k,\lambda'}]=0,\qquad[\hat{p}_{j,\lambda},\hat{p}_{k,\lambda'}]=0,\qquad[\hat{q}_{j,\lambda},\hat{p}_{k,\lambda'}]=i\delta_{jk}\delta_{\lambda\lambda'}. \tag{3.78}$$

This is nothing but the multi-mode generalization of the Heisenberg CCR explained in the previous section. One can also check the consistency between $\hat{a}_{j,\lambda}|0\rangle_{j,\lambda}=0$ and Eq. (3.44) for the vacuum state. All the equations given in this section are formal and not mathematically rigorous. More rigorous treatments are given in e.g. [BCRV16].

3.2.2 Operations in quantum optics

In the following, we suppress the indices for the mode and polarization degrees of freedom and add them only when needed. Linear optics is composed of optical media that responds linearly to the electric field. Linear optical unitaries are unitaries that can be realized by the combination of beamsplitter $B_{ij}(\theta)$ and the phase shifter $R(\phi)$ [RZBB94], given respectively by

$$B_{ij}(\theta)\coloneqq\exp\left[-\theta(\hat{a}^\dagger_i\hat{a}_j-\hat{a}^\dagger_j\hat{a}_i)\right], \tag{3.79}$$

$$R(\phi)\coloneqq\exp(i\phi\hat{a}^\dagger\hat{a}). \tag{3.80}$$

They respectively transform the annihilation operators into

$$B_{ij}(\theta)^\dagger\begin{pmatrix}\hat{a}_i\\\hat{a}_j\end{pmatrix}B_{ij}(\theta)=\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}\begin{pmatrix}\hat{a}_i\\\hat{a}_j\end{pmatrix}, \tag{3.81}$$

$$R(\phi)^\dagger\hat{a}R(\phi)=e^{i\phi}\hat{a}, \tag{3.82}$$

by the adjoint actions. (Note that $B_{ij}(\theta)^\dagger=B_{ij}(-\theta)$ as well as $R(\phi)^\dagger=R(-\phi)$ holds.) In particular, $R(\pi/2)$ corresponds to the Fourier transform between quadrature operators, i.e.,

$$R(-\pi/2)\hat{q}R(\pi/2)=-\hat{p},\qquad R(-\pi/2)\hat{p}R(\pi/2)=\hat{q}. \tag{3.83}$$

For the beamsplitter B_{ij}, $\cos^2\theta$ and $\sin^2\theta$ are respectively called the transmissivity and the reflectivity. Contrary to linear optics, nonlinear optics can be realized by a

nonlinear optical media whose polarization density responds nonlinearly to the electric field. An example of the (second-order) nonlinear optical process is optical squeezing. The squeezing unitary $S(\xi)$ ($\xi \in \mathbb{C}$) is given by

$$S(\xi) \coloneqq \exp\left(\frac{1}{2}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2})\right). \tag{3.84}$$

The combination of linear optical unitary (that contains phase space displacement) and squeezing unitary forms the Gaussian unitary operations introduced in the previous section.

An example of the optical single-mode Gaussian state is the coherent state $|\alpha\rangle$ defined as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{3.85}$$

It is known that the laser light is well described by the coherent state. Its position wave function is given by

$$\langle q|\alpha\rangle = \pi^{-\frac{1}{4}} \exp\left[-\frac{(q-\sqrt{2}\alpha_R)^2}{2} + iq\sqrt{2}\alpha_I - i\alpha_R\alpha_I\right], \tag{3.86}$$

where $\alpha = \alpha_R + i\alpha_I$. The displacement operator $D(\alpha)$ transforms the vacuum state into a coherent state with the amplitude $\alpha \in \mathbb{C}$, i.e.,

$$D(\alpha)|0\rangle = |\alpha\rangle. \tag{3.87}$$

In terms of the creation and annihilation operators, it is given by

$$D(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}). \tag{3.88}$$

The operator $V(z)$ introduced in the previous section is related to the displacement operator by

$$V(x,y) = D\left((x+iy)/\sqrt{2}\right). \tag{3.89}$$

Using this, the POVM F of the heterodyne measurement Eq. (3.42) can be rewritten by the coherent state vector $|\alpha\rangle$ as

$$F(d^2\alpha) = |\alpha\rangle\langle\alpha| \frac{d^2\alpha}{\pi}. \tag{3.90}$$

Another example of the Gaussian state is the squeezed state given by

$$S(\xi)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \left(-e^{i\varphi}\tanh r\right)^n |2n\rangle, \tag{3.91}$$

where $\xi = re^{i\varphi}$. Written in terms of the position wave function, it is given by

$$\langle q|S(\xi)|0\rangle = \left(2\pi(\Delta q)^2\right)^{-\frac{1}{4}} \exp\left[-\frac{1+i\sinh(2r)\sin\varphi}{4(\Delta q)^2} q^2\right], \tag{3.92}$$

where

$$(\Delta q)^2 \coloneqq \frac{1}{2}\left[e^{2r}\sin^2(\varphi/2) + e^{-2r}\cos^2(\varphi/2)\right]. \tag{3.93}$$

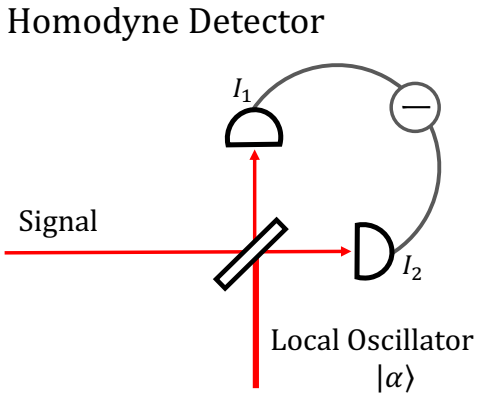

Figure 3.1: The schematics of the homodyne detector. The signal light is coupled with the local oscillator $|\alpha\rangle$ by the 50:50 beamsplitter and successively measured by the photo-diodes. The difference $I_1 - I_2$ of the photo-currents is the output of the detector.

A single-mode pure Gaussian state is in fact given by the squeezed coherent state $D(\alpha)S(\xi)\,|0\rangle$.

The homodyne detector is a detector that is frequently used in quantum optics and can be implemented by linear optical elements. The experimental setups of the homodyne detector are presented in Figure 3.1. First, the optical signal is coupled with the local oscillator (that is, the strong coherent light used as a phase reference) by the 50:50 beamsplitter. The coupled modes are successively put into the photo-diodes. In photo-diodes, the photo-currents proportional to the intensity of the input electric field are generated. Since the intensity of the electric field is proportional to the photon number $\hat{n}$, the photo-currents I_1 and I_2 are proportional to

$$I_1 \propto \hat{n}_1 = \frac{1}{2}(\hat{a}_s^\dagger + \alpha^*)(\hat{a}_s + \alpha), \tag{3.94}$$

$$I_2 \propto \hat{n}_2 = \frac{1}{2}(\hat{a}_s^\dagger - \alpha^*)(\hat{a}_s - \alpha), \tag{3.95}$$

where $\hat{a}_s$ denotes the annihilation operator of the signal mode. Taking the difference $I_1 - I_2$ of the photo currents, we have

$$I_1 - I_2 \propto |\alpha|(e^{-i\theta}\hat{a}_s + e^{i\theta}\hat{a}_s^\dagger) \tag{3.96}$$

$$\propto |\alpha|(\cos\theta\,\hat{q}_s + \sin\theta\,\hat{p}_s). \tag{3.97}$$

In the actual experiment, photo-diodes have electric noise, which makes the measurement carried out by the above setups unsharp. However, taking the intensity of the local oscillator infinitely strong, i.e., $|\alpha| \to \infty$, the homodyne measurement gets close to the quadrature measurement with its PVM given by $|q_\theta\rangle\langle q_\theta|\,dq_\theta$, where $\hat{q}_\theta := \cos\theta\,\hat{q}_s + \sin\theta\,\hat{p}_s$. (The case of $\theta = 0$ is exactly equal to the one in Eq. (3.39).) Another detector that is frequently used in quantum optics is the heterodyne detector (also known as the dual-homodyne detector) depicted in Figure 3.2. In this detector, the signal light is split into two by the 50:50 beamsplitter, and each of the two split modes is measured by the homodyne detector. One of the optical phases of the local

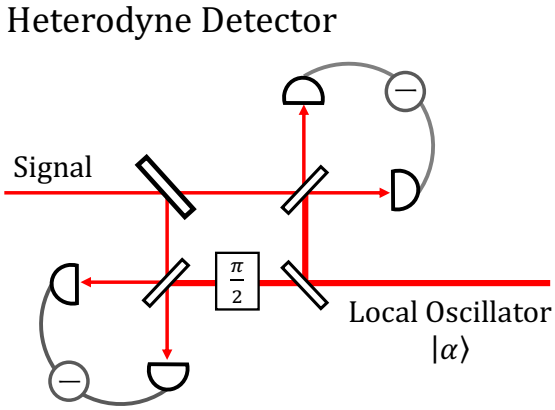

Figure 3.2: The schematics of the heterodyne (dual-homodyne) detector. The signal light is split into two (i.e., is coupled with the vacuum) by the 50:50 beamsplitter and then measured by the homodyne detectors. One of the optical phases of the local oscillators is $\pi/2$-rotated, and thus two homodyne detectors measure orthogonal quadratures.

oscillators for the homodyne detectors is $\pi/2$-rotated so that the two homodyne detectors measure the orthogonal quadratures, e.g., $\hat{q}$ and $\hat{p}$. Precisely speaking, the first 50:50 beamsplitter couples the signal light and the external vacuum. Since the 50:50 beamsplitter transforms quadrature operators as

$$B_{12}(-\pi/4)^\dagger \hat{q}_1 B_{12}(-\pi/4) = (\hat{q}_1 + \hat{q}_2)/\sqrt{2}, \quad B_{12}(-\pi/4)^\dagger \hat{p}_2 B_{12}(-\pi/4) = (\hat{p}_1 - \hat{p}_2)/\sqrt{2}, \tag{3.98}$$

the 50:50 beamsplitter followed by the homodyne measurements for $\hat{q}_1$ and $\hat{p}_2$ in Figure 3.2 is equivalent to the measurement for the joint spectral measure of $(\hat{q}_1 + \hat{q}_2)/\sqrt{2}$ and $(\hat{p}_1 - \hat{p}_2)/\sqrt{2}$. Combining these with Eq. (3.36), one can notice that the POVM for the detector in Figure 3.2 is equal to the heterodyne POVM in Eq. (3.42) or equivalently (3.90) as explained in Section 3.1.3. An alternative derivation for this fact is as follows. The operator characteristic function of the two homodyne measurements at the end in Figure 3.2 is given by $V(0, \omega_R, -\omega_I, 0)$. The transformation law for the operator $V(x_1, y_1, x_2, y_2)$ by the adjoint of the channel $\Phi_B(\rho) \coloneqq B(-\pi/4)\rho B(-\pi/4)^\dagger$ is given as follows:

$$\Phi_B^\dagger(V(x_1, y_1, x_2, y_2)) = V\left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{y_1 - y_2}{\sqrt{2}}, \frac{x_1 + x_2}{\sqrt{2}}, \frac{y_1 + y_2}{\sqrt{2}}\right). \tag{3.99}$$

Thus, the operator characteristic function before the first 50:50 beamsplitter that couples the signal light and the external vacuum $|0\rangle$ in Figure 3.2 is given by

$$\begin{aligned} \langle 0| V\left(\frac{\omega_I}{\sqrt{2}}, \frac{\omega_R}{\sqrt{2}}\right) |0\rangle V\left(-\frac{\omega_I}{\sqrt{2}}, \frac{\omega_R}{\sqrt{2}}\right) &= \exp\left[-\frac{1}{8}(\omega_R^2 + \omega_I^2)\right] V\left(-\frac{\omega_I}{\sqrt{2}}, \frac{\omega_R}{\sqrt{2}}\right) \\ &= \phi_F(\omega_R, \omega_I), \end{aligned} \tag{3.100}$$

where $\phi_F(\omega_R, \omega_I)$ is the operator characteristic function of the heterodyne POVM.

We finally comment on the photon detectors used in quantum optics. On-off detectors (also called threshold detectors) distinguish zero and non-zero photons. Photon-number-resolving detectors distinguish up to a few photons (with current technology). Both detectors should distinguish photons with sufficiently high probability; i.e., the efficiency of the detector should be high. These detectors respond to the input photon number very non-linearly and thus are non-Gaussian operations. An example of the high-efficiency on-off detector used in quantum optics experiments is the superconducting nanowire single-photon detector (SNSPD), and an example of the photon-number-resolving detector is the transition edge sensor (TES). Both detectors utilize the transition event of the superconductor when absorbing photons. For details, see e.g. [IH05, NTH12] and the references therein.

Chapter 4

Quantum key distribution with continuous-variable systems

4.1 Introduction for this chapter

Quantum key distribution (QKD) aims at generating a secret key shared between two remote legitimate parties with information-theoretic security. QKD combined with the one-time pad [Sha49] provides secure communication against an adversary with arbitrary computational power and hardware technology. Since the first proposal in 1984 [BB84], various QKD protocols have been proposed with many varieties of encoding and decoding schemes. These protocols are typically classified into two categories depending on the detection methods. One of them is called discrete-variable QKD, which uses photon detectors and includes earlier protocols such as BB84 [BB84] and B92 [Ben92] protocols. The other is called continuous-variable QKD, which uses homodyne and heterodyne measurements with photodetectors [Ral99, Hil00, GKP01, CLA01, GG02, GVAW$^+$03, WLB$^+$04]. See Refs. [XMZ$^+$20, PAB$^+$20] for recent comprehensive reviews on the topic.

Although discrete-variable QKD is more mature and achieves longer-distant key distribution if photon detectors with low dark count rates are available, continuous-variable QKD has its own distinct advantages for a short distance. It can be implemented with components common to coherent optical communication technology and is expected to be cost-effective. Excellent spectral filtering capability inherent in homodyne/heterodyne measurements suppresses crosstalk in wavelength division multiplexing (WDM) channels. This allows multiplexing of hundreds of QKD channels into a single optical fiber [ELP$^+$20] as well as co-propagation with classical data channels [HLW$^+$15, KQA15, HHL$^+$16, KCB$^+$17, KBF$^+$18, EHO$^+$18, EHP$^+$19, MVL$^+$20], which makes integration into an existing communication network easier.

One major obstacle in putting continuous-variable QKD to practical use is the gap between the employed continuous variables and mandatory digital signal processing. The continuous-variable QKD protocols using coherent states are divided into two branches depending on whether the modulation of the encoder is also continuous or discrete. The continuous modulation protocols usually adopts Gaussian modulation, in which the sender chooses the complex amplitude of a coherent-state pulse according to a Gaussian distribution [Ral99, Hil00, GG02, GVAW$^+$03, WLB$^+$04] (see Ref. [DL15,

LPF+18] for a review). This allows powerful theoretical tools of the de Finetti theorem [LKGC09, Lev17b], and complete security proofs for a finite-size key and against general attacks have been given [LGPRC13, Lev15, Lev17a]. In order to implement Gaussian protocols with a digital random-number generator and digital signal processing, it is necessary to approximate the continuous distribution with a constellation composed of a finite number of complex amplitudes. It turns out that an overwhelming number of coherent states is needed to directly approximate the Gaussian ensemble in order for the security condition to be satisfied [JKJDL12, Lup20]. If we try to mitigate the required number, additional assumptions are needed, which makes it difficult to apply it in the finite-size regime [KGW21]. The other branch gives priority to the simplicity of the modulation and uses a very small (usually two to four) number of amplitudes [SRLL02, HYA+03, LG09, LG11]. As for the security analysis, the status is more or less similar to the Gaussian constellation case, and current security proofs are either in the asymptotic regime against collective attacks [ZHRL09, BW18, LUL19, GGDL19, DBL21, LLX+21] or in the finite-size regime but against more restrictive attacks [PP21, POP21]. Hence, regardless of approaches, a complete security proof of continuous-variable QKD in the finite-size regime against general attacks has been a milestone yet to be achieved.

Here, we achieve the above milestone by proposing a binary phase-modulated continuous-variable QKD protocol with a composable security proof in the finite-size regime against general attacks. The key ingredient is an estimation method of the fidelity to the coherent states we develop here using the heterodyne measurement and the classical post-processing, which is suited for the analysis in the finite-size regime. Once the estimation method is developed, the security proof is accomplished by a reduction to the entanglement distillation, which is the established technique in the discrete-variable QKD.

The so-obtained security proof is further refined based on the reverse reconciliation, aiming at improving the performance of the protocol at the cost of more complexity in the security analysis. With a refined proof and no additional experimental requirement, we obtain a significant improvement in the key gain rate against loss. In fact, it achieves near-optimal scaling against transmission distance in the limit of infinite code length. These results accelerate the real-world implementation of reliable and provably-secure continuous-variable QKDs.

This chapter is organized as follows. In Section 4.2, the notations and preliminaries used in this chapter are summarized. In Section 4.3, the definition of the composable security of the QKD is stated, and an approach for the security proof is reviewed. Sections 4.4 and 4.5 are the results of this thesis. In Section 4.4, the composable security for a binary modulation continuous-variable QKD protocol is proved against general attacks in the finite-size regime. Our security proof is adapted to digital information processing and thus allows the use of the binned homodyne and heterodyne measurements (i.e., measurements with finite resolutions). The security proof is further refined in Section 4.5 based on the reverse reconciliation, and, as a result, the asymptotic key rate of the protocol achieves almost optimal scaling against transmission distance for the pure-loss channel. (Section 4.4 is based on the publication [MMSK21].)

4.2 Notations and preliminaries

In what follows, the base of the logarithm is taken to be 2.

4.2.1 Finite field $\mathbb{F}_2$

Classical information processing is done on binary numbers. Binary numbers $0, 1$ forms a finite field $\mathbb{F}_2$ with the addition $\oplus$ and the multiplication $\cdot$ that are defined as follows:

$$0 \oplus 0 = 1 \oplus 1 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1, \tag{4.1}$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1. \tag{4.2}$$

In what follows, arithmetics of binary numbers (i.e., bits) follow the above.

An N-bit row vector $\boldsymbol{u}$ is an element of $\mathbb{F}_2^N$. The inner product $\boldsymbol{u}\boldsymbol{v}^\top$ of two N-bit row vectors $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^N$ is defined as

$$\boldsymbol{u}\boldsymbol{v}^\top = \bigoplus_{i=1}^{N} u_i \cdot v_i. \tag{4.3}$$

For a $N \times N$ binary matrix C, $\boldsymbol{u}C$ is also an N-bit row vector. The Hamming weight $\mathrm{wt}(\boldsymbol{u})$ of $\boldsymbol{u} \in \mathbb{F}_2^N$ is defined as

$$\mathrm{wt}(\boldsymbol{u}) = \Big|\{i \in \{1, \ldots, N\} : u_i = 1\}\Big|. \tag{4.4}$$

4.2.2 Classical linear information processing as a quantum operation

Let $\boldsymbol{u}$ be an N-bit row vector and C be a $N \times N$ non-singular binary matrix. Let $|\boldsymbol{u}\rangle \coloneqq |u_1\rangle \otimes \cdots \otimes |u_N\rangle$ be the pure quantum state on the N qubit system, where each qubit is in one of the Z-basis states $\{|0\rangle, |1\rangle\}$. If $|\boldsymbol{u}\rangle$ is measured on the Z basis, the binary string $\boldsymbol{u}$ is obtained with unit probability. The unitary operation that corresponds to the action of C on the Z basis of $|\boldsymbol{u}\rangle$ is defined as

$$U(C) = \sum_{\boldsymbol{z} \in \{0,1\}^N} |\boldsymbol{z}C\rangle\langle \boldsymbol{z}| = \sum_{\boldsymbol{x} \in \{0,1\}^N} |\boldsymbol{x}(C^\top)^{-1}{}_X\rangle\langle \boldsymbol{x}_X|. \tag{4.5}$$

Then, if $U(C)|\boldsymbol{u}\rangle$ is measured on the Z basis, $\boldsymbol{u}C$ is obtained with unit probability. One can derive the second equality of Eq. (4.5) by the following Fourier transform between the Z- and X-basis:

$$|\boldsymbol{z}\rangle = \frac{1}{\sqrt{2^N}} \sum_{\boldsymbol{x} \in \{0,1\}^N} (-1)^{\boldsymbol{z}\boldsymbol{x}^\top} |\boldsymbol{x}_X\rangle. \tag{4.6}$$

An example of $U(C)$ is the Controlled-NOT (CNOT) operation with C being

$$C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = C^{-1}. \tag{4.7}$$

Let $|\boldsymbol{u}\rangle = |u_1\rangle\,|u_2\rangle$ and $|\boldsymbol{v}_X\rangle = |v_{1X}\rangle\,|v_{2X}\rangle$ be pure quantum states with the binary strings $\boldsymbol{u}$ and $\boldsymbol{v}$ encoded on the Z and X basis, respectively. Then, the above CNOT gate acts as

$$\mathrm{CNOT}\,|\boldsymbol{u}\rangle = |u_1\rangle\,|u_1 \oplus u_2\rangle\,, \tag{4.8}$$

where the first qubit is the control qubit and the second qubit is the target qubit. Using Eq. (4.5), we also have

$$\mathrm{CNOT}\,|\boldsymbol{v}_X\rangle = |(v_1 \oplus v_2)_X\rangle\,|v_{2X}\rangle\,. \tag{4.9}$$

Let $\boldsymbol{v}$ be another N-bit row vector. Then, $\boldsymbol{u} \oplus \boldsymbol{v}$ is also a N-bit row vector. The unitary that corresponds to the addition of $\boldsymbol{v}$ on the Z basis is given by

$$U^{\oplus}(\boldsymbol{v}) = \sum_{\boldsymbol{z}\in\{0,1\}^N} |\boldsymbol{z} \oplus \boldsymbol{v}\rangle\langle\boldsymbol{z}|\,, \tag{4.10}$$

If $U^{\oplus}(\boldsymbol{v})\,|\boldsymbol{u}\rangle$ is measured on the Z basis, $\boldsymbol{u} \oplus \boldsymbol{v}$ is obtained with unit probability. One can also check from (4.6) that this unitary acts as an identity on the X basis (up to the irrelevant global phase). In the same way, $U_X^{\oplus}(\boldsymbol{v}')$ is the unitary that corresponds to the addition of $\boldsymbol{v}'$ on the X basis. The simple examples of $U^{\oplus}(\boldsymbol{v})$ and $U_X^{\oplus}(\boldsymbol{v}')$ when $N = 1$ are the Pauli-X σ^X and the Pauli-Z σ^Z operators, which can be written respectively as

$$\sigma^X = |0\rangle\langle 1| + |1\rangle\langle 0|\,, \qquad \sigma^Z = |0_X\rangle\langle 1_X| + |1_X\rangle\langle 0_X|\,. \tag{4.11}$$

To sum up, one can rewrite classical linear information processing such as multiplying C and adding $\boldsymbol{v}$ on the binary sequence $\boldsymbol{u}$ as the unitary actions such as acting $U(C)$ and $U^{\oplus}(\boldsymbol{v})$ on the quantum state $|\boldsymbol{u}\rangle$ (followed by the Z-basis measurement).

4.2.3 Definitions and properties of the entropic quantities

The definitions and properties of the entropic quantities used in this chapter are listed. $\mathbb{E}_P[\check{X}]$ denotes the expectation value of $\check{X}$, where $\check{X} : \Omega \to \mathbb{R}$ denotes the random variable for the probability space (Ω, Σ, P). Throughout the chapter, random variables are denoted with the symbol $\check{}$. In this section, only the discrete random variable is treated, and thus P_X denotes the probability mass function of $\check{X}$ and satisfies $P_X(x) = P(\check{X} = x) = P(\check{X}^{-1}(x))$.

Definition 4.2.1 (Entropy function)**.** Let $\check{X}$ be a random variable with possible values in $\mathcal{X} \coloneqq \{x_1, \ldots, x_n\}$, and P_X be the probability mass function of $\check{X}$. Then, the entropy function $H(\check{X})_{P_X}$ of P_X is defined as

$$H(\check{X})_{P_X} \coloneqq \mathbb{E}_{P_X}[-\log P_X] = \sum_{i=1}^{n} -P_X(x_i)\log P_X(x_i). \tag{4.12}$$

The entropy function is non-negative. The entropy function is concave; i.e., for probability mass functions P_1, P_2 of $\check{X}$ and a number $p \in [0,1]$, the following inequality holds:

$$H(\check{X})_{pP_1+(1-p)P_2} \geq pH(\check{X})_{P_1} + (1-p)H(\check{X})_{P_2}. \tag{4.13}$$

Definition 4.2.2 (Binary entropy function)**.** The binary entropy function is defined as

$$h(p) \coloneqq -p \log p - (1-p) \log(1-p). \tag{4.14}$$

The binary entropy function $h(p)$ is a special case of the entropy function; i.e., for a binary random variable $\check{X}$ ($\mathcal{X} = \{0,1\}$) with $P_X(0) = p$, we have $H(\check{X})_{P_X} = h(p)$. It can be shown that $0 \leq h(p) \leq 1$. The following lemma with respect to the binary entropy function is proved here for later use.

Lemma 4.2.3 (Upper-bound on the number of possible patterns)**.** *Let $\boldsymbol{e} \in \{0,1\}^n$ be the n-bit sequence and $\mathrm{wt}(\boldsymbol{e})$ be the Hamming weight of $\boldsymbol{e}$. For $0 \leq m \leq n$, let $\mathcal{T}_m$ be the set of n-bit sequences defined as $\mathcal{T}_m \coloneqq \{\boldsymbol{e} \in \{0,1\}^n : \mathrm{wt}(\boldsymbol{e}) \leq m\}$. Then, the following inequality holds:*

$$|\mathcal{T}_m| \leq 2^{nh(p)}, \quad p \coloneqq \min\{m/n,\, 1/2\}, \tag{4.15}$$

where $|\mathcal{T}_m|$ denotes the cardinality of the set $\mathcal{T}_m$.

Proof. It is trivial when $p = 1/2$ (i.e., $m/n \geq 1/2$). Therefore, we prove the case $p = m/n < 1/2$. Let $\Pr(\boldsymbol{e})$ be defined as $\Pr(\boldsymbol{e}) \coloneqq p^{\mathrm{wt}(\boldsymbol{e})}(1-p)^{n-\mathrm{wt}(\boldsymbol{e})}$. Since, for $p < 1/2$, $\Pr(\boldsymbol{e})$ monotonically decreases with respect to $\mathrm{wt}(\boldsymbol{e})$, $\Pr(\boldsymbol{e}) \geq p^m(1-p)^{n-m} = 2^{-nh(m/n)}$ holds. From this, $1 \geq \sum_{\boldsymbol{e}\in\mathcal{T}_m} \Pr(\boldsymbol{e}) \geq |\mathcal{T}_m| 2^{-nh(m/n)}$ follows, which proves the statement of the proposition. □

Definition 4.2.4 (Kullback-Leibler divergence (relative entropy function))**.** Let $\check{X}$ be a random variable that takes value in the set $\mathcal{X} \coloneqq \{x_1, \ldots, x_n\}$. Let P_X and Q_X be probability mass functions of $\check{X}$. Then the Kullback-Leibler divergence $D(P_X \| Q_X)$ is defined as

$$D(P_X \| Q_X) \coloneqq \sum_{i=1}^{n} P_X(x_i) \log \frac{P_X(x_i)}{Q_X(x_i)} = -\sum_{i=1}^{n} P_X(x_i) \log \frac{Q_X(x_i)}{P_X(x_i)}. \tag{4.16}$$

Lots of important properties and inequalities for entropic functions can be derived from the properties of the Kullback-Leibler divergence. Examples of such properties are:

- (Asymmetry) $D(P_X \| Q_X)$ is in general asymmetric; i.e. $D(P_X \| Q_X) = D(Q_X \| P_X)$ does not necessarily hold. This is obvious from the definition.
- (Non-negativity) $D(P_X \| Q_X)$ satisfies $D(P_X \| Q_X) \geq 0$. This can be proved by applying Jensen's inequality to the logarithmic function:

$$D(P_X \| Q_X) = -\sum_{i=1}^{n} P_X(x_i) \log \frac{Q_X(x_i)}{P_X(x_i)} \geq -\log\left(\sum_{i=1}^{n} P_X(x_i) \frac{Q_X(x_i)}{P_X(x_i)}\right) = 0. \tag{4.17}$$

- (Joint convexity) For probability mass functions P_1, P_2, Q_1, Q_2 and a number $p \in [0,1]$, the Kullback-Leibler divergence satisfies the following inequality:

$$D\left(pP_1 + (1-p)P_2 \| pQ_1 + (1-p)Q_2\right) \leq pD(P_1 \| Q_1) + (1-p)D(P_2 \| Q_2). \tag{4.18}$$

  The proof of this property is given in e.g. [CT12].

- (Data processing) Let $\check{X}$ and $\check{Y}$ be random variables that take values in $\mathcal{X}$ and $\mathcal{Y}$, respectively, and let $(\Lambda(y \mid x))_{x\in\mathcal{X},y\in\mathcal{Y}}$ be the transition matrix for the stochastic process $\check{X} \to \check{Y}$, that is, each matrix element $\Lambda(y \mid x)$ is non-negative and $\sum_{y\in\mathcal{Y}} \Lambda(y \mid x) = 1$. Let P_X, Q_X be probability mass functions of $\check{X}$. Then the following inequality holds (data processing inequality):
$$D(P_X\|Q_X) \geq D(P_Y\|Q_Y), \tag{4.19}$$
where $P_Y(y) \coloneqq \sum_{x\in\mathcal{X}} \Lambda(y \mid x)P_X(x)$, $Q_Y(y) \coloneqq \sum_{x\in\mathcal{X}} \Lambda(y \mid x)Q_X(x)$. The proof is given in e.g. [CT12]. The data processing inequality is a very important property in information theory.

Now we move on to the quantum entropic quantities, which are not directly used in this chapter but nevertheless important in the theory of security proof of quantum key distribution. Here, we assume that the quantum system we treat is finite-dimensional. First, we define a generalization of the fidelity to subnormalized states.

Definition 4.2.5 (Generalized fidelity)**.** For subnormalized states ρ, σ (i.e., $\rho, \sigma \geq 0$ and $\mathrm{Tr}(\rho), \mathrm{Tr}(\rho) \leq 1$), the generalized fidelity $\tilde{F}(\rho, \sigma)$ is defined as
$$\tilde{F}(\rho, \sigma) \coloneqq \left(\|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \mathrm{Tr}(\rho))(1 - \mathrm{Tr}(\sigma))}\right)^2. \tag{4.20}$$
By definition, the generalized fidelity is reduced to the usual fidelity (Def. 2.2.6) when the states are normalized.

Definition 4.2.6 (Conditional min- and max-entropies [RK05, Ren08, KRS09, TCR09, Tom12])**.** Let ρ_{AB} be a subnormalized state on $\mathcal{H}_A \otimes \mathcal{H}_B$ (i.e., $\mathrm{Tr}[\rho_{AB}] \leq 1$). Then, the min- and max-entropies of A conditioned on B of ρ_{AB} are given respectively by
$$H_{\min}(A|B)_\rho \coloneqq \max_{\sigma\in\mathfrak{D}(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda} I_A \otimes \sigma_B\} \tag{4.21}$$
$$= -\log \min_{\sigma\geq 0}\{\mathrm{Tr}(\sigma) : \rho_{AB} \leq I_A \otimes \sigma_B\}, \tag{4.22}$$
$$H_{\max}(A|B)_\rho \coloneqq \max_{\sigma\in\mathfrak{D}(\mathcal{H}_B)} \log\left(d_A\, \tilde{F}(\rho_{AB}, d_A^{-1} I_A \otimes \sigma_B)\right), \tag{4.23}$$
where d_A denotes the dimension of $\mathcal{H}_A$.

In order to introduce the smoothed version of the conditional min- and max- entropies, we introduce another distance measure for the subnormalized states.

Definition 4.2.7 (Purified distance [Tom12])**.** For subnormalized states ρ, σ, the purified distance $P(\rho, \sigma)$ is defined as
$$P(\rho, \sigma) \coloneqq \sqrt{1 - \tilde{F}(\rho, \sigma)}. \tag{4.24}$$

Definition 4.2.8 (Smooth conditional min- and max-entropies [Tom12])**.** For a subnormalized state ρ_{AB} and $\varepsilon \geq 0$, the ε-smooth min- and max-entropies of A conditioned on B of ρ_{AB} are given respectively by
$$H^\varepsilon_{\min}(A|B)_\rho \coloneqq \max_{\tilde{\rho}\in\mathcal{B}^\varepsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}, \tag{4.25}$$
$$H^\varepsilon_{\max}(A|B)_\rho \coloneqq \max_{\tilde{\rho}\in\mathcal{B}^\varepsilon(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}, \tag{4.26}$$
where the ε-ball $\mathcal{B}^\varepsilon(\rho_{AB})$ is defined as
$$\mathcal{B}^\varepsilon(\rho_{AB}) \coloneqq \{\tau \in \mathfrak{T}(\mathcal{H}_{AB}) : \tau \geq 0, \mathrm{Tr}(\tau) \leq 1, P(\tau, \rho) \leq \varepsilon\}. \tag{4.27}$$

4.2.4 Concentration inequalities

In this section, concentration inequalities used in this thesis are listed. The probability space (Ω, Σ, P) and the associated random variable $\check{X}$ we treat here can be continuous. The first one is the so-called Chernoff bound, which is a tail bound for the binomial distribution.

Theorem 4.2.9 (Tail bound for the binomial distribution [Che52, Hoe63, Hoe94])**.** *Let $\check{X}_1, \ldots, \check{X}_n$ be independent and identically distributed binary random variables with $P(\check{X}_i = 1) = p$, for $i = 1, \ldots, n$. Then, for any $\delta \in [0, 1-p]$, the following inequality holds:*

$$P\left(\frac{1}{n}\sum_{i=1}^{n}\check{X}_i > p + \delta\right) < 2^{-nD(p+\delta\|p)}, \tag{4.28}$$

where $D(p+\delta\|p)$ denotes

$$D(p+\delta\|p) \coloneqq (p+\delta)\log\frac{p+\delta}{p} + (1-p-\delta)\log\frac{1-p-\delta}{1-p}. \tag{4.29}$$

The above is the bound of the probability for the upper tail. The bound for the lower tail can be obtained similarly by exchanging the values of the random variables as well as changing p to $1-p$. The following corollary of the above theorem is suitable for our applications.

Corollary 4.2.10 (Alternative form of the tail bound)**.** *Let $\check{X}_1, \ldots, \check{X}_n$ be independent and identically distributed binary random variables with $P(\check{X}_i = 1) = p$, for $i = 1, \ldots, n$. Given $\epsilon \in (0, 1)$, we have*

$$P\left(\frac{1}{n}\sum_{i=1}^{n}\check{X}_i > p + \delta(\epsilon; n)\right) < \epsilon, \tag{4.30}$$

where $\delta(\epsilon; n)$ is defined to satisfy

$$\begin{cases} D(p+\delta(\epsilon;n)\|p) = -\frac{1}{n}\log\epsilon & (\epsilon > p^n) \\ \delta(\epsilon;n) = 1-p & (\epsilon \le p^n) \end{cases}. \tag{4.31}$$

Proof. Since $D(p+\delta\|p)$ increases monotonically from 0 to $-\log p$ when δ varies from 0 to 1, Theorem 4.2.9 can be applied for $\epsilon > p^n$ by the suitable choice of $\delta(\epsilon; n)$. On the other hand, $P(\frac{1}{n}\sum_{i=1}^{n}\check{X}_i > 1) = 0 (< \epsilon)$ always holds. These prove the statement of the above Corollary. □

The Chernoff-type bound also holds for the hypergeometric distribution. The following is the statement.

Theorem 4.2.11 (Tail bound for the hypergeometric distribution [Chv79])**.** *Let $X_1, \ldots, X_N$ be a binary sequence, and M be the number of elements with $X_i = 1$, i.e, $M \coloneqq \sum_{i=1}^{N} X_i$. Let $\check{Y}_1, \ldots, \check{Y}_n$ be randomly sampled from $X_1, \ldots, X_N$ without replacement. Let $\check{m} \coloneqq \sum_{i=1}^{n}\check{Y}_i$ be the number of ones in $\check{Y}_1, \ldots, \check{Y}_n$. Then, for any $\delta \in [0, M/N]$, the following inequality holds:*

$$P\left(\frac{\check{m}}{n} \le \frac{M}{N} - \delta\right) \le 2^{-nD\left(\frac{M}{N}-\delta\middle\|\frac{M}{N}\right)}, \tag{4.32}$$

where $D(\cdot\|\cdot)$ is defined in Eq. (4.29).

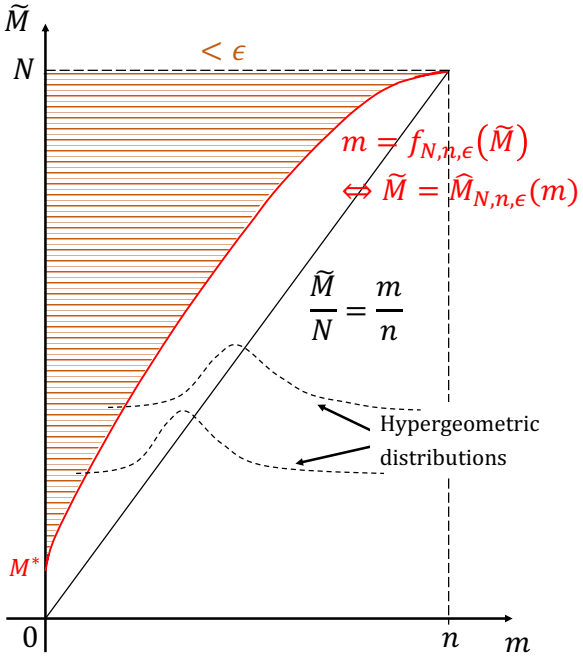

Figure 4.1: The definition of the function $f_{N,n,\epsilon}(\tilde{M})$ or equivalently $\hat{M}_{N,n,\epsilon}(m)$ in Corollary 4.2.12. The real number M^* is the intercept of the function $\hat{M}_{N,n,\epsilon}(m)$, i.e., $M^* = \hat{M}_{N,n,\epsilon}(0)$. Given N, n, and ϵ, the failure event for each M, i.e., $\hat{M}_{N,n,\epsilon}(\check{m}) \leq M$, occurs when $\check{m} \leq f_{N,n,\epsilon}(M)$. In order to bound the probability of such events, we can use the tail bound for the hypergeometric distribution in Theorem 4.2.11.

The above is the bound of the probability for the lower tail. The bound for the upper tail can be obtained similarly. The following corollary is useful for the bit error sampling.

Corollary 4.2.12 (Estimation by the simple random sampling without replacement)**.** *Let $X_1, \ldots, X_N$ be a binary sequence with $M \coloneqq \sum_{i=1}^{N} X_i$. Let $\check{Y}_1, \ldots, \check{Y}_n$ be randomly sampled from $X_1, \ldots, X_N$ without replacement, and define $\check{m} \coloneqq \sum_{i=1}^{n} \check{Y}_i$. Then, for any $\epsilon \in (0, 1)$, the following inequality holds:*

$$P\left(\lceil \hat{M}_{N,n,\epsilon}(\check{m}) \rceil \leq M\right) \leq \epsilon, \tag{4.33}$$

where the function $\hat{M}_{N,n,\epsilon}(m)$ is defined to satisfy

$$\frac{m}{n} \leq \frac{\hat{M}_{N,n,\epsilon}(m)}{N} \quad \text{and} \quad D\left(m/n \middle\| \hat{M}_{N,n,\epsilon}(m)/N\right) = -\frac{1}{n}\log\epsilon. \tag{4.34}$$

Proof. Let $f(M)$ be a function of M satisfying $0 \leq f(M)/n \leq M/N$. Then, from Theorem 4.2.11, we have

$$P\left(\frac{\check{m}}{n} \leq \frac{M}{N} - \left(\frac{M}{N} - \frac{f(M)}{n}\right)\right) \leq 2^{-nD\left(\frac{f(M)}{n} \middle\| \frac{M}{N}\right)}. \tag{4.35}$$

We set the function $f(M)$ to the restriction of the function $f_{N,n,\epsilon}(\tilde{M})$ of the real number $\tilde{M}$ that satisfies

$$D\left(f_{N,n,\epsilon}(\tilde{M})/n \| \tilde{M}/N\right) = -\frac{1}{n}\log\epsilon, \tag{4.36}$$

for $\tilde{M} \geq M^*(= (1-\sqrt[n]{\epsilon})N)$ (see Figure 4.1). (The case $\tilde{M} = N$ for $f_{N,n,\epsilon}(\tilde{M})$ is singular, so we take the limit of the case $\tilde{M} = N - \delta$, $\delta \to 0$, which leads to $f_{N,n,\epsilon}(N-\delta) \to n$.) The function $f_{N,n,\epsilon}(\tilde{M})$ is monotonically increasing, and its range lies in $[0, N]$. Thus, from Eq. (4.35), we have

$$P\left(f^{-1}_{N,n,\epsilon}(\check{m}) \leq M\right) \leq \epsilon \tag{4.37}$$

for any M. Combining these, defining $\hat{M}_{N,n,\epsilon}(m) \coloneqq f^{-1}_{N,n,\epsilon}(m)$ leads to Eq. (4.33) while $\hat{M}_{N,n,\epsilon}(m)$ satisfies Eq. (4.34) by construction. Note that, as has already been explained, $\hat{M}_{N,n,\epsilon}(n) \coloneqq \lim_{\delta\to 0}\hat{M}_{N,n,\epsilon}(n-\delta) = N$. □

The Chernoff-type bound is tight in many cases, but its applicability is restricted. The following inequality is looser than the Chernoff-type bound but can be applied to more general distributions.

Theorem 4.2.13 (Hoeffding's inequality [Hoe63, Hoe94])**.** *Let $\check{X}_1, \ldots, \check{X}_n$ be independent random variables with each $\check{X}_i$ bounded by the intervals $[a_i, b_i]$ almost surely. Then, for $t \geq 0$, we have*

$$P\left(\sum_{i=1}^{n}(\check{X}_i - \mathbb{E}[\check{X}_i]) \geq t\right) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^{n}(b_i-a_i)^2}\right). \tag{4.38}$$

Note that, for two random variables $\check{X}_1$ and $\check{X}_2$, the condition that $\check{X}_1 \geq \check{X}_2$ holds almost surely means that $P(\check{X}_1 \geq \check{X}_2) = 1$. Equivalently, $\check{X}_1 \geq \check{X}_2$ holds almost surely if and only if $\int_A(\check{X}_1 - \check{X}_2)dP \geq 0$ for any $A \in \Sigma$. Lots of refinement of the Hoeffding's inequality (e.g., by using the information of higher moments of the probability distributions) have been studied [Hoe63, Hoe94].

In the following, we explain Azuma's inequality, which has a wide range of applications since, contrary to the previous bounds, the random variable can be neither independent nor identically distributed. First, we introduce the following notion.

Definition 4.2.14 ($\mathcal{F}$-measurable)**.** Let (Ω, Σ, P) be a probability space. Let $\mathcal{F}$ be a σ-subalgebra of Σ. The random variable $\check{X}$ is called $\mathcal{F}$-measurable if, for any Borel set $A \in \mathcal{B}(\mathbb{R})$ (where $\mathcal{B}(\mathbb{R})$ denotes the Borel σ-algebra of $\mathbb{R}$), it satisfies

$$\check{X}^{-1}(A) \coloneqq \{y \in \Omega \mid \check{X}(y) \in A\} \in \mathcal{F}. \tag{4.39}$$

In the case of the discrete probability space, the following condition is equivalent to the above. For $x \in \Omega$, let $\mathcal{F}(x)$ be the smallest set in $\mathcal{F}$ containing x i.e.,

$$\mathcal{F}(x) \coloneqq \bigcap_{\substack{S\in\mathcal{F}\\ x\in S}} S. \tag{4.40}$$

Then, the random variable $\check{X}$ is $\mathcal{F}$-measurable if $\check{X}(x) = \check{X}(y)$ for any $x \in \Omega$ and $y \in \mathcal{F}(x)$. Note that, if $\check{X}$ is $\mathcal{G}$-measurable for $\mathcal{G} \subset \mathcal{F}$, then it is trivially $\mathcal{F}$-measurable. Note also that a constant random variable is measurable with respect to the trivial σ-algebra $\{\varnothing, \Omega\}$.

Next we introduce the conditional expectation.

Definition 4.2.15 (Conditional expectation)**.** Let (Ω, Σ, P) and $\mathcal{F}$ be the same as above. Let $\check{X} : \Omega \to \mathbb{R}$ be a random variable with a finite expectation. Then, the conditional expectation $\mathbb{E}[\check{X} \mid \mathcal{F}] : \Omega \to \mathbb{R}$ is defined as an $\mathcal{F}$-measurable function satisfying

$$\int_F \mathbb{E}[\check{X} \mid \mathcal{F}] dP = \int_F \check{X}\, dP, \qquad \forall F \in \mathcal{F}. \tag{4.41}$$

The definition of the conditional expectation is more tractable in the case of the discrete probability space; $\mathbb{E}[\check{X} \mid \mathcal{F}] : \Omega \to \mathbb{R}$ is given by

$$\mathbb{E}[\check{X} \mid \mathcal{F}](x) = \frac{1}{\sum_{y \in \mathcal{F}(x)} P(y)} \sum_{y \in \mathcal{F}(x)} \check{X}(y) P(y). \tag{4.42}$$

This can be regarded as a derivative form of Eq. (4.41). In fact, the conditional expectation can be given by the Radon-Nikodym derivative of probability measures. The conditional expectation has several important properties. Here we list some of them that are relevant to this thesis.

- (Linearity) For two random variables $\check{X}_1, \check{X}_2$, a σ-algebra $\mathcal{F}$, and $a \in \mathbb{R}$, the following holds:

$$\mathbb{E}[\check{X}_1 + a\check{X}_2 \mid \mathcal{F}] = \mathbb{E}[\check{X}_1 \mid \mathcal{F}] + a\,\mathbb{E}[\check{X}_2 \mid \mathcal{F}]. \tag{4.43}$$

- (Monotonicity) For $\check{X}_1 \leq \check{X}_2$ (almost surely), we have

$$\mathbb{E}[\check{X}_1 \mid \mathcal{F}] \leq \mathbb{E}[\check{X}_2 \mid \mathcal{F}]. \tag{4.44}$$

- (Stability) For an $\mathcal{F}$-measurable random variable $\check{X}$, we have

$$\mathbb{E}[\check{X} \mid \mathcal{F}] = \check{X}. \tag{4.45}$$

- (Tower property) For σ-algebras $\mathcal{G} \subset \mathcal{F}$, the following holds:

$$\mathbb{E}\left[\mathbb{E}[\check{X} \mid \mathcal{F}] \,\middle|\, \mathcal{G}\right] = \mathbb{E}[\check{X} \mid \mathcal{G}]. \tag{4.46}$$

  Note that $\mathbb{E}\left[\mathbb{E}[\check{X} \mid \mathcal{G}] \,\middle|\, \mathcal{F}\right] = \mathbb{E}[\check{X} \mid \mathcal{G}]$ also holds from the stability.

Now we introduce the following.

Definition 4.2.16 (Filtration)**.** A sequence of σ-algebras $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_n$ is called the filtration if

$$\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n. \tag{4.47}$$

We finally introduce the following notion.

Definition 4.2.17 (Martingale)**.** Let $\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n$ be a filtration. The sequence of random variables $(\check{X}_1, \ldots, \check{X}_n)$ is called a martingale with respect to this filtration if $\check{X}_i$ is $\mathcal{F}_i$-measurable, and

$$\mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}] = \check{X}_{i-1} \tag{4.48}$$

holds (almost surely) for $1 \leq i \leq n$. Here, $\check{X}_0$ is a constant function satisfying $\check{X}_0 = \mathbb{E}[\check{X}_1 \mid \mathcal{F}_0] = \mathbb{E}[\check{X}_1]$.

Eq. (4.48) is an equality as functions of Ω. An example of the $\mathcal{F}_i$-measurable sequence in the case of the discrete probability space is as follows. Let $\mathcal{Y}$ be a finite set. Let $\Omega = \mathcal{Y}^{\times n}$ be an n-ary Cartesian product and $\mathcal{F}_i = \{\mathcal{X} \times \mathcal{Y}^{\times(n-i)} \mid \mathcal{X} \in \mathcal{P}(\mathcal{Y}^{\times i})\}$ be a σ-subalgebra, where $\mathcal{P}(\mathcal{Y}^{\times i})$ is the power set of $\mathcal{Y}^{\times i}$. Given the sequence of outcomes $(y_1, \dots, y_n) \in \Omega$, the random variable $\check{X}_i$ should depend only on $(y_1, \dots, y_i)$ to be $\mathcal{F}_i$-measurable; that is, $\check{X}_i$ is fixed when given an element of $\mathcal{F}_i$. On the other hand, $\check{X}_i$ is in general still random when given an element of $\mathcal{F}_{i-1}$. Note that, by definition, $\check{X}_i$ is $\mathcal{F}_k$-measurable for $k \geq i$ if it is $\mathcal{F}_i$-measurable.

Now we can state Azuma's inequality as follows.

Theorem 4.2.18 (Azuma's inequality [Azu67, RS13, McD98])**.** *Let $(\check{X}_1, \dots, \check{X}_n)$ be a martingale sequence with respect to the filtration $\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n$. Suppose there are predictable processes $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ with respect to $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n$ (i.e., a_i and b_i are $\mathcal{F}_{i-1}$-measurable for $1 \leq i \leq n$), such that*

$$a_i \leq \check{X}_i - \check{X}_{i-1} \leq b_i \tag{4.49}$$

holds (almost surely). Then, for $t \geq 0$, we have

$$P(\check{X}_n - \check{X}_0 \geq t) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right). \tag{4.50}$$

The following corollary combines Azuma's inequality with the technique called the Doob decomposition.

Corollary 4.2.19 (Azuma's inequality combined with the Doob decomposition)**.** *Let $\{\varnothing, \Omega\} = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n$ be a filtration. Let $(a_1, \dots, a_n)$ and $(b_1, \dots, b_n)$ be predictable processes with respect to this filtration. Let $(\check{X}_1, \dots, \check{X}_n)$ be the sequence of random variables such that for $1 \leq i \leq n$, $\check{X}_i$ is $\mathcal{F}_i$-measurable and satisfies*

$$a_i \leq \check{X}_i \leq b_i, \qquad \textit{(almost surely).} \tag{4.51}$$

Then, for $t \geq 0$, we have

$$P\left(\sum_{i=1}^n (\check{X}_i - \mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}]) \geq t\right) \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right). \tag{4.52}$$

Proof. For $1 \leq i \leq n$, let $\check{Y}_i$ be defined as

$$\check{Y}_i := \sum_{k=1}^i (\check{X}_k - \mathbb{E}[\check{X}_k \mid \mathcal{F}_{k-1}]). \tag{4.53}$$

Then, the sequence $(\check{Y}_1, \dots, \check{Y}_n)$ is a martingale with respect to the filtration $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots \subseteq \mathcal{F}_n$, since $\check{Y}_i$ is $\mathcal{F}_i$-measurable and satisfies

$$\begin{aligned}
\mathbb{E}[\check{Y}_i \mid \mathcal{F}_{i-1}] &= \sum_{k=1}^i \Big(\mathbb{E}[\check{X}_k \mid \mathcal{F}_{i-1}] - \mathbb{E}\Big[\mathbb{E}[\check{X}_k \mid \mathcal{F}_{k-1}] \,\Big|\, \mathcal{F}_{i-1}\Big]\Big) && (4.54)\\
&= \sum_{k=1}^{i-1} (\check{X}_k - \mathbb{E}[\check{X}_k \mid \mathcal{F}_{k-1}]) && (4.55)\\
&= \check{Y}_{i-1}. && (4.56)
\end{aligned}$$

The second equality follows from the fact that $\check{X}_k$ is $\mathcal{F}_{i-1}$ measurable for $1 \leq k \leq i-1$ and the stability Eq. (4.45) of the conditional expectation. Note that $Y_0 \coloneqq 0$. Furthermore, $(\check{Y}_1, \ldots, \check{Y}_n)$ satisfies

$$a_i - \mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}] \leq \check{Y}_i - \check{Y}_{i-1} \leq b_i - \mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}], \tag{4.57}$$

(almost surely) for $1 \leq i \leq n$. Since $a_i - \mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}]$ and $b_i - \mathbb{E}[\check{X}_i \mid \mathcal{F}_{i-1}]$ are $\mathcal{F}_{i-1}$-measurable, we can apply Theorem 4.2.18 to the sequence $(\check{Y}_1, \ldots, \check{Y}_n)$ and prove the statement. □

At the cost of versatility, Azuma's inequality is not tight for most practical applications. The recent refinement of Azuma's inequality that is suitable for QKD applications is given in Ref. [Kat20].

4.3 The basics of the QKD

4.3.1 The goal of the QKD

The goal of the QKD is to distribute the secret key between the distant two parties connected by a quantum channel and an authenticated public classical channel while ensuring that the key is secure against any eavesdropping attacks allowed by the law of quantum mechanics. The "secret key" here means a shared sequence of random numbers, and the "security" needs to meet the following two conditions; (1) two parties share the coincident keys (correctness condition), and (2) the key is secret against all except two parties (secrecy condition). With these two conditions, the two parties can communicate in the information-theoretically secure way, using the one-time pad [Sha49].

4.3.2 The general procedures of the QKD

In what follows, "Alice" and "Bob" denote the two parties that carry out a quantum key distribution protocol, and "Eve" denotes the eavesdropper, following the convention of the information theory. The common procedures of QKD protocols are given as follows.

Setups: Alice and Bob share the quantum channel in which they transmit quantum states as well as the authenticated public classical channel for the announcement. Eve can perform arbitrary attacks allowed by the law of quantum mechanics in the quantum channel and listen to all the announcements in the public channel.

Protocol:

1. Quantum communication:
   Alice and Bob encode classical information onto quantum states, send them through the quantum channel, and perform measurement on the quantum states they receive to read out the encoded information. Eve may perform arbitrary attacks in the quantum channel.

2. Sifting:
   Alice and Bob generate the binary strings $\boldsymbol{z}_A$ and $\boldsymbol{z}_B$, which are selected or "sifted" from measurement outcomes according to the conditions defined in each protocol. $\boldsymbol{z}_A$ and $\boldsymbol{z}_B$ are called the sifted keys of Alice and Bob, respectively.

3. Information reconciliation:
   The obtained sifted keys $\boldsymbol{z}_A$ and $\boldsymbol{z}_B$ do not coincide in general due to noises or Eve's attacks in the quantum channel. Therefore, they have to correct the errors in their sifted keys. One way is that Alice sends the syndrome bits of her sifted key encrypted by a pre-shared secret key, and Bob corrects the errors on his sifted key $\boldsymbol{z}_B$ according to it. As a result, Bob obtains the reconciled key $\boldsymbol{z}_B^{\mathrm{rec}}$. This is called the "direct reconciliation". Alternatively, we can exchange the role of Alice and Bob in the above procedure. This alternative is called the "reverse reconciliation".

4. Privacy amplification:
   Eve may have part of the information of the (reconciled) keys $\boldsymbol{z}_A$ and $\boldsymbol{z}_B^{\mathrm{rec}}$. Alice and Bob estimate the amount of information leakage. Depending on the estimated leakage, they generate shorter keys $\boldsymbol{z}_A^{\mathrm{fin}}$ and $\boldsymbol{z}_B^{\mathrm{fin}}$ by acting a suitable linear hash function on $\boldsymbol{z}_A$ and $\boldsymbol{z}_B^{\mathrm{rec}}$ (in the case of the direct reconciliation). These are the final keys.

Note that $\boldsymbol{z}_A$, $\boldsymbol{z}_B$, $\boldsymbol{z}_B^{\mathrm{rec}}$, $\boldsymbol{z}_A^{\mathrm{fin}}$, and $\boldsymbol{z}_B^{\mathrm{fin}}$ are actually random variables and thus denoted with the symbol $\check{}$ in the following. Various types of QKD protocols mainly differ in the first line, i.e., the method of quantum communication. The sifting, the information reconciliation, and the privacy amplification after the quantum communication are referred to as (classical) post-processing. In most cases, the information reconciliation procedure does not differ so much among different QKD protocols. On the other hand, the privacy amplification procedure, or more precisely, the necessary amount of shortening the sifted key depends on which protocol to use. Thus, the development of the new QKD protocols requires both the procedure of quantum communication and the evaluation of the amount of privacy amplification.

4.3.3 The security condition of the key in the QKD

In this section, the definition of security in the QKD is given. Let $\mathcal{H}_{ABE} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ be the Hilbert space of the joint system of Alice's and Bob's final keys and Eve's quantum system. Let $\Pr(\cdot)$ be the probability distribution for all the random variables defined in the protocol and $\check{N}_{\mathrm{fin}}$ be the length of the final key. Let $\rho_{ABE|N}^{\mathrm{fin}} \in \mathfrak{D}(\mathcal{H}_{ABE})$ be the density operator of the state of Alice's and Bob's N-bit final keys as well as Eve's quantum state after all the attacks, given $\check{N}_{\mathrm{fin}} = N$. When Alice and Bob abort the protocol, the final key length $\check{N}_{\mathrm{fin}}$ is set to be zero. Then the definition of the ε-security is given by

$$\sum_{N \geq 1} \Pr(\check{N}_{\mathrm{fin}} = N)\, d(\rho_{ABE|N}^{\mathrm{fin}}, \rho_{ABE|N}^{\mathrm{ideal}}) \leq \varepsilon, \tag{4.58}$$

where $d(\cdot, \cdot)$ denotes the trace distance in Definition 2.2.3, and

$$\rho_{ABE|N}^{\mathrm{ideal}} \coloneqq \sum_{\boldsymbol{z} \in \{0,1\}^N} \frac{1}{2^N} |\boldsymbol{z}\boldsymbol{z}\rangle\langle\boldsymbol{z}\boldsymbol{z}|_{AB} \otimes \mathrm{Tr}_{AB}\left[\rho_{ABE|N}^{\mathrm{fin}}\right]. \tag{4.59}$$

The parameter ε is an arbitrary positive constant and is referred to as the security parameter. This condition means that the final keys obtained in the protocol are, measured by the trace distance, ε-close to the ideal secret keys in which Alice's and Bob's keys perfectly coincide and are completely random for Eve. The trace distance is used in the security condition to ensure the monotonicity and the composability [MQR09]. The monotonicity is necessary because the distinguishability between the final state of the protocol and the ideal state should not increase under quantum channels, i.e., CPTP maps. Since the trace distance is a CPTP monotone as shown in Proposition 2.2.5, the condition is satisfied. The composability is the requirement that, if Alice and Bob use an ε-secure key to perform an ε'-secure cryptographic protocol, the composite protocol should be at least $(\varepsilon + \varepsilon')$-secure. The composability is necessary

because the security of a complex composite cryptographic protocol should be ensured by the security of its component protocols. In QKD, the composability follows from the triangle inequality (Corollary 2.2.4) of the trace distance.

4.3.4 An approach to prove the security condition

There are several approaches to prove the security of the QKD [LC99, SP00a, Ren08, HHHO09, Koa09, Tsu20b, Tsu20a]. One of the approaches for the security proof is to use the leftover hash lemma [Ren08, Tsu20b], which utilizes the information-theoretic property of the universal$_2$ hash function [CW79, TH13]. In this approach, we aim to evaluate the ε-smooth conditional min-entropy in Definition 4.2.8 of Alice's or Bob's sifted key conditioned on the adversary Eve. An advantage of this approach is the applicability to protocols in which the sifted keys are not binary numbers; the Gaussian-modulation continuous-variable QKD is an example.

Another approach, which is the main topic in this thesis, proves the security using complementarity between the bit (Z) and phase (X) bases [Koa09]. By explicitly constructing a virtual procedure for correcting the phase errors of Alice's or Bob's sifted key that should be compatible with the actual protocol, we can ensure that the obtained final key is secret to Eve. Furthermore, if we find an optimal phase-error-correction procedure, the resulting key gain is optimal for the protocol [Tsu20b, Tsu20a]. In this section, we review the approach in Refs. [Koa09, MSK19] with a slight generalization. Without loss of generality, we here treat the direct reconciliation scenario. The case of reverse reconciliation can be treated similarly.

As shown in [Koa09], the condition (4.58) can be divided into the following two conditions by applying triangle inequality to the trace distance. The first condition, the $\varepsilon_{\rm cor}$-correctness condition, is the following:

$$\Pr(\check{\boldsymbol{z}}_A^{\rm fin} \neq \check{\boldsymbol{z}}_B^{\rm fin}) = \sum_{N\geq 1} \Pr(\check{N}_{\rm fin} = N) \sum_{\boldsymbol{z},\boldsymbol{z}'\in\{0,1\}^N, \boldsymbol{z}\neq\boldsymbol{z}'} \langle \boldsymbol{z}\boldsymbol{z}'|_{AB}\, \rho_{AB|N}^{\rm fin}\, |\boldsymbol{z}\boldsymbol{z}'\rangle_{AB} \leq \varepsilon_{\rm cor}, \quad (4.60)$$

where $\rho_{AB|N}^{\rm fin} \coloneqq {\rm Tr}_E[\rho_{ABE|N}^{\rm fin}]$. Eq. (4.60) means that the probability of disagreement of Alice's and Bob's final keys is required to be no larger than $\varepsilon_{\rm cor}$. The second condition, the $\varepsilon_{\rm sec}$-secrecy condition, is defined as follows:

$$\sum_{N\geq 1} \Pr(\check{N}_{\rm fin} = N)\, d(\rho_{AE|N}^{\rm fin}, \rho_{AE|N}^{\rm ideal}) \leq \varepsilon_{\rm sec}, \quad (4.61)$$

where $\rho_{AE|N}^{\rm fin} \coloneqq {\rm Tr}_B[\rho_{ABE|N}^{\rm fin}]$ and $\rho_{AE|N}^{\rm ideal} \coloneqq {\rm Tr}_B[\rho_{ABE|N}^{\rm ideal}]$. With these two conditions, the protocol is ensured to be $(\varepsilon_{\rm cor} + \varepsilon_{\rm sec})$-secure.

The $\varepsilon_{\rm cor}$-correctness condition is ensured if the failure probability of the information reconciliation is no larger than $\varepsilon_{\rm cor}$; i.e., the reconciled keys $\check{\boldsymbol{z}}_A$ and $\check{\boldsymbol{z}}_B^{\rm rec}$ satisfy the following:

$$\begin{aligned} &\Pr(\check{N}_{\rm fin} \geq 1, \check{\boldsymbol{z}}_A \neq \check{\boldsymbol{z}}_B^{\rm rec}) \\ &= \sum_{N'\geq 1} \sum_{\boldsymbol{z},\boldsymbol{z}'\in\{0,1\}^{N'},\, \boldsymbol{z}\neq\boldsymbol{z}'} \Pr(\check{N}_{\rm fin} \geq 1, \check{N}_{\rm sift} = N', \check{\boldsymbol{z}}_A = \boldsymbol{z}, \check{\boldsymbol{z}}_B^{\rm rec} = \boldsymbol{z}') \quad (4.62) \\ &\leq \varepsilon_{\rm cor}, \quad (4.63) \end{aligned}$$

where $\check{N}_{\text{sift}}$ is the length of the sifted key or equivalently the length of the reconciled key. In order for this condition to be satisfied, the protocol has to be aborted with a high probability when the reconciliation fails.

In order to prove the ε_{sec}-secrecy condition along with [Koa09], a compatible virtual protocol is constructed as follows. First, $\check{N}_{\text{sift}}$ (virtual) register qubits are introduced for Alice, and Alice's procedure of determining each bit of her sifted key in the actual protocol is replaced with the Z-basis measurement. The measurement is then postponed by replacing the privacy amplification procedure with the corresponding quantum operations as shown in Section 4.2.2. Thus Alice's $\check{N}_{\text{fin}}$-bit final key is generated by the Z-basis measurements on $\check{N}_{\text{fin}}$ qubits among Alice's register qubits in the virtual protocol. In constructing such a virtual protocol, Alice (and Bob) can do arbitrary quantum operations in the virtual protocol before the Z-basis measurements as long as the following condition is satisfied; for any attack by Eve in the actual protocol, there exists a corresponding attack in the virtual protocol such that the state on Alice's final key obtained by the Z-basis measurements and Eve's system is the same as that of the actual protocol; i.e., the probability $\Pr(\check{N}_{\text{fin}} = N)$ and $\rho^{\text{fin}}_{AE|N}$ are the same as the actual protocol. The condition for $\rho^{\text{fin}}_{AE|N}$ can be rephrased as follows. Given $\check{N}_{\text{fin}} = N$, let $\rho^{\text{virt}}_{AE|N}$ be a quantum state on Alice's N register qubits and Eve's system just before Alice's Z-basis measurement in the virtual protocol. Let $\mathcal{E}^{\text{meas}}_{A|N}$ be a CPTP map of Alice's Z-basis measurement in the virtual protocol given by

$$\mathcal{E}^{\text{meas}}_{A|N}(\rho) = \sum_{\boldsymbol{z}\in\{0,1\}^N} \langle \boldsymbol{z}|\rho|\boldsymbol{z}\rangle \, |\boldsymbol{z}\rangle\langle \boldsymbol{z}| \,. \tag{4.64}$$

Then, they must satisfy $\mathcal{E}^{\text{meas}}_{A|N} \otimes \mathrm{Id}_E(\rho^{\text{virt}}_{AE|N}) = \rho^{\text{fin}}_{AE|N}$ for Eve's corresponding attack in the virtual protocol. With $\mathcal{E}^{\text{meas}}_{A|N}$ and $\rho^{\text{virt}}_{AE|N}$, the secrecy condition (4.61) can be rewritten as follows:

$$\sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\, d\Big(\mathcal{E}^{\text{meas}}_{A|N} \otimes \mathrm{Id}_E(\rho^{\text{virt}}_{AE|N}), \mathcal{E}^{\text{meas}}_{A|N}\Big(|0_X\rangle\langle 0_X|^{\otimes N}_A\Big) \otimes \rho^{\text{fin}}_{E|N}\Big) \leq \varepsilon_{\text{sec}}, \tag{4.65}$$

where $\rho^{\text{fin}}_{E|N} \coloneqq \mathrm{Tr}_A\Big[\rho^{\text{fin}}_{AE|N}\Big]$.

Now we find a sufficient condition in order for Eq. (4.65) to hold. The left-hand side of Eq. (4.65) is bounded from above as follows:

$$\begin{aligned}
&(\text{L.H.S. of Eq. (4.65)}) && (4.66)\\
&\leq \sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\, d\Big(\rho^{\text{virt}}_{AE|N}, |0_X\rangle\langle 0_X|^{\otimes N}_A \otimes \rho^{\text{fin}}_{E|N}\Big) && (4.67)\\
&\leq \sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\sqrt{1 - F\Big(\rho^{\text{virt}}_{AE|N}, |0_X\rangle\langle 0_X|^{\otimes N}_A \otimes \rho^{\text{fin}}_{E|N}\Big)} && (4.68)\\
&\leq \Pr(\check{N}_{\text{fin}} = 0)\sqrt{1-1^2} + \sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\sqrt{1 - \Big[F\Big(\rho^{\text{virt}}_{A|N}, |0_X\rangle\langle 0_X|^{\otimes N}_A\Big)\Big]^2} && (4.69)\\
&\leq \sqrt{1 - \Big[\Pr(\check{N}_{\text{fin}} = 0) + \sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\, F\Big(\rho^{\text{virt}}_{A|N}, |0_X\rangle\langle 0_X|^{\otimes N}_A\Big)\Big]^2} && (4.70)\\
&= \sqrt{1 - \Big[1 - \sum_{N\geq 1} \Pr(\check{N}_{\text{fin}} = N)\, \Big(1 - \langle 0_X|^{\otimes N}_A \, \rho^{\text{virt}}_{A|N} \, |0_X\rangle^{\otimes N}_A\Big)\Big]^2} && (4.71)
\end{aligned}$$

where $\rho^{\mathrm{virt}}_{A|N} \coloneqq \mathrm{Tr}_E\left[\rho^{\mathrm{virt}}_{AE|N}\right]$. Here, the first inequality follows from Proposition 2.2.5, the second inequality follows from Proposition 2.2.12, the third inequality follows from Lemma 2.2.11, and the last inequality follows from the concavity of the function $f(x) = \sqrt{1-x^2}$. If

$$\sum_{N\geq 1} \Pr(\check{N}_{\mathrm{fin}} = N)\left(1 - \langle 0_X|_A^{\otimes N}\, \rho^{\mathrm{virt}}_{A|N}\, |0_X\rangle_A^{\otimes N}\right) \leq \eta' \tag{4.72}$$

is satisfied for a (small) parameter η', then the left-hand side of Eq. (4.61) (or equivalently Eq. (4.65)) is bounded from above by

$$\sum_{N\geq 1} \Pr(\check{N}_{\mathrm{fin}} = N)\, d\left(\rho^{\mathrm{fin}}_{AE|N}, \rho^{\mathrm{ideal}}_{AE|N}\right) \leq \sqrt{1-(1-\eta')^2} \leq \sqrt{2\eta'}, \tag{4.73}$$

and thus the protocol is $\varepsilon_{\mathrm{sec}} = \sqrt{2\eta'}$-secret. Furthermore, the inequality (4.72) means that, if Alice measured $\rho^{\mathrm{virt}}_{A|N}$ on the X bases and obtained a (random) sequence $\check{\boldsymbol{x}}^{\mathrm{fin}}_A$, it satisfies

$$\Pr(\check{N}_{\mathrm{fin}} \geq 1, \check{\boldsymbol{x}}^{\mathrm{fin}}_A \neq \boldsymbol{0}) \leq \eta'. \tag{4.74}$$

In other words, it suffices to show that Alice succeeded in correcting the "phase errors" on her register qubits with high probability. With these arguments, the privacy amplification can be regarded as the virtual phase-error-correction procedure on Alice's register qubits.

To sum up, in order to ensure the $(\varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}})$-security of the final key defined in Eq. (4.58), the following two conditions have to be satisfied. The first is the $\varepsilon_{\mathrm{cor}}$-correctness condition (4.60); Alice's sifted key $\check{\boldsymbol{z}}_A$ and Bob's reconciled key $\check{\boldsymbol{z}}^{\mathrm{rec}}_B$ after the information reconciliation coincides with probability no smaller than $1-\varepsilon_{\mathrm{cor}}$, i.e.,

$$\Pr(\check{N}_{\mathrm{fin}} \geq 1, \check{\boldsymbol{z}}_A \neq \check{\boldsymbol{z}}^{\mathrm{rec}}_B) \leq \varepsilon_{\mathrm{cor}} \tag{4.75}$$

The second is the $\varepsilon_{\mathrm{sec}}$-secrecy condition (4.61). This condition can be replaced with the condition (4.65) by constructing a compatible virtual protocol that satisfies the followings. For any attack by Eve in the actual protocol, there exists a corresponding attack by Eve in the virtual protocol and Alice's quantum operations that result in the state $\rho^{\mathrm{virt}}_{AE|N}$ satisfying

$$\mathcal{E}^{\mathrm{meas}}_{A|N} \otimes \mathrm{Id}_E\left(\rho^{\mathrm{virt}}_{AE|N}\right) = \rho^{\mathrm{fin}}_{AE|N} \tag{4.76}$$

and

$$\sum_{N\geq 1} \Pr(\check{N}_{\mathrm{fin}} = N)\left(1 - \langle 0_X|_A^{\otimes N}\, \rho^{\mathrm{virt}}_{A|N}\, |0_X\rangle_A^{\otimes N}\right) \leq \frac{\varepsilon^2_{\mathrm{sec}}}{2} (= \eta') \tag{4.77}$$

at the same time, where $\mathcal{E}^{\mathrm{meas}}_{A|N}$ is defined in Eq. (4.64). Note that the second condition (4.77) is equivalent to Eq. (4.74).

4.3.5 The privacy amplification using dual universal$_2$ hashing

In this section, the privacy amplification using dual universal$_2$ hashing is reviewed [TH13, MSK19]. Let N and N' be the length of the final key and the sifted key, respectively. For the privacy amplification, multiplying the (randomly generated) $N' \times N$ matrix $\check{G}$ on the sifted key $\check{\boldsymbol{z}}_A$ to obtain the final key $\check{\boldsymbol{z}}^{\mathrm{fin}}_A = \check{\boldsymbol{z}}_A\check{G}$ in the actual protocol is replaced with acting the unitary $U(\check{C})$ of Eq. (4.5) on Alice's register qubits

followed by the Z-basis measurements $\mathcal{E}^{\rm meas}_{A|N}$ on the first N qubits of the N'-qubit register. Here, $N' \times N'$ full-rank matrix $\check{C}$ satisfies $\check{G} = \check{C}(\boldsymbol{I}_N \ \boldsymbol{O})^\top$, where $\boldsymbol{I}_n$ denotes the $n \times n$ identity matrix and $\boldsymbol{O}$ denotes a zero matrix with the appropriate size. Let $\rho_{AE|N'}$ be the state of Alice's N'-qubit register and Eve's system just before the privacy amplification in the virtual protocol. Then for $N \geq 1$, we set

$$\rho^{\rm virt}_{AE|N} = \sum_{\boldsymbol{y}\in\{0,1\}^{N'-N}} U_X^{\oplus}(\boldsymbol{v}(\boldsymbol{y}))\mathrm{Tr}_{N'\backslash N}\Big[(I_N \otimes |\boldsymbol{y}_X\rangle\langle\boldsymbol{y}_X|)\, U(\check{C})\rho_{AE|N'}U(\check{C})^\dagger\Big]U_X^{\oplus}(\boldsymbol{v}(\boldsymbol{y}))^\dagger, \tag{4.78}$$

where $U_X^{\oplus}(\boldsymbol{v})$ is defined in Section 4.2.2, and all the unitaries act on Alice's N'-qubit register while act as identity on Eve's system. The state $\rho^{\rm virt}_{AE|N}$ in Eq. (4.78) satisfies the condition (4.76) since $U_X^{\oplus}(\boldsymbol{v})$ does not change the Z-basis values of Alice's N'-qubit register, i.e.,

$$\mathcal{E}^{\rm meas}_{A|N} \otimes \mathrm{Id}_E\left(\rho^{\rm virt}_{AE|N}\right) = \mathcal{E}^{\rm meas}_{A|N} \otimes \mathrm{Id}_E\left(\mathrm{Tr}_{N'\backslash N}\Big[U(\check{C})\rho_{AE|N'}U(\check{C})^\dagger\Big]\right). \tag{4.79}$$

The role of $U_X^{\oplus}(\boldsymbol{v})$ as well as the $\boldsymbol{y}$ dependency of $\boldsymbol{v}$ in Eq. (4.78) will be revealed in the following. At this point, we recall the condition (4.77) or equivalently (4.74) for the secrecy. Suppose we performed X-basis measurement on $\rho_{A|N'} \coloneqq \mathrm{Tr}_E[\rho_{AE|N'}]$ and obtained a random sequence $\check{\boldsymbol{x}}_A$. Then from Eqs. (4.5) and (4.78), it is related to the random sequence $\check{\boldsymbol{x}}^{\rm fin}_A$ in Eq. (4.74) with $\rho_{A|N'}$ not measured on the X basis by

$$\check{\boldsymbol{x}}^{\rm fin}_A = \check{\boldsymbol{x}}_A\check{H}' + \boldsymbol{v}(\check{\boldsymbol{x}}_A\check{H}), \tag{4.80}$$

where the matrices $\check{H}'$ and $\check{H}$ are defined as

$$\check{H}' \coloneqq (\check{C}^\top)^{-1}(\boldsymbol{I}_N \ \boldsymbol{O})^\top, \tag{4.81}$$

$$\check{H} \coloneqq (\check{C}^\top)^{-1}(\boldsymbol{O} \ \boldsymbol{I}_{N'-N})^\top. \tag{4.82}$$

Then, the condition (4.74) can be reinterpreted as

$$\Pr(\check{N}_{\rm fin} \geq 1, \check{\boldsymbol{x}}_A\check{H}' \neq \boldsymbol{v}(\check{\boldsymbol{x}}_A\check{H})) \leq \eta'. \tag{4.83}$$

We set $\boldsymbol{v}$ as follows. Given the $(N'-N)$-bit sequence $\check{\boldsymbol{x}}_A\check{H}$ and other random variables $\check{\boldsymbol{\zeta}}$ that can be defined in the virtual protocol (but not necessarily be observed in the actual protocol), we determine an estimate $\boldsymbol{x}^*_A(N', \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})$ of the sequence $\check{\boldsymbol{x}}_A$ and set $\boldsymbol{v} = \boldsymbol{x}^*_A(N', \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})\check{H}'$. (Thus, $\boldsymbol{v}$ also depends on N' and $\check{\boldsymbol{\zeta}}$.) Then, the condition (4.83) can be ensured if the following condition holds:

$$\Pr(\check{N}_{\rm fin} \geq 1, \check{\boldsymbol{x}}_A \neq \boldsymbol{x}^*_A(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})) \leq \eta'. \tag{4.84}$$

This condition is nothing but the identifiability of the random sequence $\check{\boldsymbol{x}}_A$, given the $(N'-N)$-bit syndrome $\check{\boldsymbol{x}}_A\check{H}$ with the hash function $\check{H}$ and other random variables $\check{\boldsymbol{\zeta}}$ that can be defined in the virtual protocol. As the next step, suppose that, given $\check{N}_{\rm sift}$ and $\check{\boldsymbol{\zeta}}$, we can find a set $\mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})$ of candidates of the sequence $\check{\boldsymbol{x}}_A$ so that $\check{\boldsymbol{x}}_A$ belongs to $\mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})$ with a high probability, i.e.,

$$\Pr(\check{N}_{\rm sift} \geq 1, \check{\boldsymbol{x}}_A \notin \mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})) \leq \eta. \tag{4.85}$$

In general, the random variables $\check{\boldsymbol{\zeta}}$ consist of ones that can be observed in the actual protocol denoted by $\check{\boldsymbol{\alpha}}$ and ones that cannot be in the actual protocol denoted by $\check{\boldsymbol{\beta}}$. Thus we write $\check{\boldsymbol{\zeta}} = (\check{\boldsymbol{\alpha}}, \check{\boldsymbol{\beta}})$. As will be shown later, the required amount of the privacy amplification is determined by the cardinality $|\mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}})|$ of the set $\mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}})$. Since we need to know the amount of the privacy amplification in the actual protocol, we define an integer-valued function $N_{\mathrm{PA}}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\alpha}})$ that depends on $\check{\boldsymbol{\alpha}}$ of $\check{\boldsymbol{\zeta}}$ and satisfies the following:

$$\Pr(\log|\mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}})| \leq N_{\mathrm{PA}}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\alpha}}) \mid \check{N}_{\mathrm{sift}} \geq 1) = 1. \tag{4.86}$$

Suppose further that for each final key length N and sifted key length N', the $N' \times N$ matrix $\check{H}$ is randomly chosen from the universal$_2$ hash function family; i.e., the following holds [CW79, Ren08, TH13]:

$$\forall \boldsymbol{x}, \boldsymbol{x}' \in \{0,1\}^{N'}, \boldsymbol{x} \neq \boldsymbol{x}', \qquad \Pr(\boldsymbol{x}\check{H} = \boldsymbol{x}'\check{H}) \leq 2^{-(N'-N)}. \tag{4.87}$$

We then construct $\boldsymbol{x}^*_A(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})$ as follows. Given the syndrome $\check{\boldsymbol{x}}_A\check{H}$, if there is only one element in $\mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}})$ that is consistent with the syndrome $\check{\boldsymbol{x}}_A\check{H}$, then that element is chosen as $\boldsymbol{x}^*_A(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})$. Otherwise, an arbitrary sequence is chosen as $\boldsymbol{x}^*_A(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})$. With this construction and in the case $\check{N}_{\mathrm{sift}} = N'$, $\check{N}_{\mathrm{fin}} = N$, $\check{\boldsymbol{\zeta}} = \boldsymbol{\zeta}' = (\boldsymbol{\alpha}', \boldsymbol{\beta}')$, and $\check{\boldsymbol{x}}_A = \boldsymbol{x} \in \mathcal{T}(N', \boldsymbol{\zeta}')$, the condition $\boldsymbol{x}^*_A(N', \boldsymbol{\zeta}', \boldsymbol{x}\check{H}) = \boldsymbol{x}$ holds if $\boldsymbol{x}\check{H} \neq \boldsymbol{y}\check{H}$ holds for any $\boldsymbol{y} \in \mathcal{T}(N', \boldsymbol{\zeta}') \setminus \{\boldsymbol{x}\}$. Combining this with Eq. (4.86), we have, for $\Pr(\check{N}_{\mathrm{sift}} = N', \check{\boldsymbol{\zeta}} = \boldsymbol{\zeta}') > 0$ and $\boldsymbol{x} \in \mathcal{T}(N', \boldsymbol{\zeta}')$,

$$\Pr(\boldsymbol{x} \neq \boldsymbol{x}^*_A(N', \boldsymbol{\zeta}', \boldsymbol{x}\check{H})) \leq 2^{N_{\mathrm{PA}}(N', \boldsymbol{\alpha}') - (N'-N)}. \tag{4.88}$$

Then, unless the protocol is aborted before the privacy amplification step, we set

$$\check{N}_{\mathrm{fin}} = \max\{\check{N}_{\mathrm{sift}} - N_{\mathrm{PA}}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\alpha}}) - s, 0\}, \tag{4.89}$$

which leads to

$$\Pr(\check{N}_{\mathrm{fin}} = \check{N}_{\mathrm{sift}} - N_{\mathrm{PA}}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\alpha}}) - s \mid \check{N}_{\mathrm{fin}} \geq 1) = 1. \tag{4.90}$$

Combining this with Eqs. (4.85) and (4.88), we have

$$\begin{aligned}
&\Pr(\check{N}_{\mathrm{fin}} \geq 1, \check{\boldsymbol{x}}_A \neq \boldsymbol{x}^*_A(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})) && (4.91)\\
&\leq \Pr\Big(\check{N}_{\mathrm{fin}} \geq 1, \check{\boldsymbol{x}}_A \notin \mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}) \cup \Big[\check{\boldsymbol{x}}_A \in \mathcal{T}(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}) \cap \check{\boldsymbol{x}}_A \neq \boldsymbol{x}^*_A(\check{N}_{\mathrm{sift}}, \check{\boldsymbol{\zeta}}, \check{\boldsymbol{x}}_A\check{H})\Big]\Big) && (4.92)\\
&\leq \eta + 2^{-s}. && (4.93)
\end{aligned}$$

Setting $\eta' = \eta + 2^{-s}$ leads to Eq. (4.84) and thus Eq. (4.74). Finally, it is known that randomly choosing $\check{H}$ from the universal$_2$ hash function family amounts to randomly choosing $\check{G}$ from the dual universal$_2$ hash function family [TH13]. (These two relate through the matrix $\check{C}$.) Therefore, we perform the dual universal$_2$ hashing in the privacy amplification step of the actual protocol in order for the argument in this section to hold. Note that $\check{H}$ can be chosen from the almost universal$_2$ hash function families, which is more general than the universal$_2$ hash function families, at the cost of the additional amount of the syndrome extraction in the virtual protocol. In this

case, the almost dual universal$_2$ hashing will be performed in the actual protocol at the cost of the additional amount of the privacy amplification. See Ref. [TH13] for more details.

To sum up, if all of the following conditions are satisfied, the privacy amplification using the dual universal$_2$ hashing ensures $\varepsilon_{\rm sec}$-secrecy with $\varepsilon_{\rm sec} = \sqrt{2(\eta + 2^{-s})}$.

- Given $\check{N}_{\rm sift} \geq 1$, let $\check{\boldsymbol{x}}_A$ be the outcome of the X-basis measurement on Alice's $\check{N}_{\rm sift}$-qubit register just before the privacy amplification step in the virtual protocol. There exists a set-valued function $\mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})$ and an integer-valued function $N_{\rm PA}(\check{N}_{\rm sift}, \check{\boldsymbol{\alpha}})$ of the sifted-key length $\check{N}_{\rm sift}$ and other random variables $\check{\boldsymbol{\zeta}} = (\check{\boldsymbol{\alpha}}, \check{\boldsymbol{\beta}})$ defined in the virtual protocol, where $\check{\boldsymbol{\alpha}}$ is observable in the actual protocol, such that
$$\Pr(\check{N}_{\rm sift} \geq 1, \check{\boldsymbol{x}}_A \notin \mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})) \leq \eta, \tag{4.94}$$
and
$$\Pr(\log |\mathcal{T}(\check{N}_{\rm sift}, \check{\boldsymbol{\zeta}})| \leq N_{\rm PA}(\check{N}_{\rm sift}, \check{\boldsymbol{\alpha}}) \mid \check{N}_{\rm sift} \geq 1) = 1. \tag{4.95}$$
- Unless the protocol is aborted before the privacy amplification step, the final key length is chosen to be
$$\check{N}_{\rm fin} = \max\{\check{N}_{\rm sift} - N_{\rm PA}(\check{N}_{\rm sift}, \check{\boldsymbol{\alpha}}) - s, 0\} \tag{4.96}$$
at the privacy amplification step.

4.3.6 Key rate of the QKD protocol

In general, secret keys may be consumed in the QKD protocol in order to, for example, authenticate the announcement or send encrypted messages such as the bit error syndromes. Therefore, if the number of the consumed secret keys in the whole protocol is denoted by $\check{N}_{\rm KC}$, the net key gain is given by $\check{N}_{\rm fin} - \check{N}_{\rm KC}$. If the total number of communication rounds between Alice and Bob is $N_{\rm tot}$, then the key rate per pulse is defined as $(\check{N}_{\rm fin} - \check{N}_{\rm KC})/N_{\rm tot}$. This quantity shows an efficiency for the key gain of the protocol and thus is the performance index for the QKD protocol. It is implied in the previous section that $(N_{\rm PA}(\check{N}_{\rm sift}, \check{\boldsymbol{\alpha}}) + s)$-bit privacy amplification is sufficient to ensure the secrecy condition when we use the dual universal$_2$ hashing. Therefore, the key rate can alternatively be given by
$$(\check{N}_{\rm sift} - \check{N}_{\rm KC} - N_{\rm PA}(\check{N}_{\rm sift}, \check{\boldsymbol{\alpha}}) - s)/N_{\rm tot}. \tag{4.97}$$

4.4 Finite-size security of continuous-variable QKD with digital signal processing

In this section, the composable security of a binary-modulation continuous-variable QKD protocol is proved against arbitrary attacks in the finite-size regime. The proposed security proof can be applied to the case in which the binned homodyne and heterodyne measurements are used (see also [LO21]). The key to our security proof is an estimation method we develop in Section 4.4.1 using the heterodyne measurement and classical post-processing, which is suited for analysis of confidence region in the finite-size regime. The outcome of the heterodyne measurement, which is unbounded, is converted to a bounded value by a smooth function such that its expectation is proved to be no larger than the fidelity of the input pulse to a coherent state. This allows us to use a standard technique to derive a lower bound on the fidelity with a required confidence level in the finite-size regime. The fidelity as a measure of disturbance in the binary modulation protocol is essentially the same as what is monitored through bit errors in the B92 protocol [Ben92, TKI03, Koa04]. Using this similarity, we derive an operator inequality through which we construct a security proof based on a reduction to the distillation of entangled qubit pairs [SP00b, LC99], a technique frequently used for discrete-variable QKD protocols.

4.4.1 Estimation of the fidelity to a coherent state

We first introduce a test scheme to estimate the fidelity between an optical state ρ and the vacuum state $|0\rangle\langle 0|$ through a heterodyne measurement. For a state ρ of a single optical mode, the heterodyne measurement (with its POVM defined in Eq. (3.90)) produces an outcome $\check{\alpha} \in \mathbb{C}$ with a probability density

$$q_\rho(\alpha)\, d^2\alpha \coloneqq \langle\alpha|\, \rho\, |\alpha\rangle\, \frac{d^2\alpha}{\pi}, \tag{4.98}$$

where the coherent state $|\alpha\rangle$ is defined in Eq. (3.85). We refer to the expectation associated with the distribution $q_\rho(\alpha)$ simply as $\mathbb{E}_\rho$. To construct a lower bound on the fidelity $\langle 0|\, \rho\, |0\rangle$ from $\check{\alpha}$, we will use the associated Laguerre polynomials which are given by

$$L_n^{(k)}(\nu) \coloneqq (-1)^k \frac{d^k L_{n+k}(\nu)}{d\nu^k}, \tag{4.99}$$

where

$$L_n(\nu) \coloneqq \frac{e^\nu}{n!}\frac{d^n}{d\nu^n}(e^{-\nu}\nu^n) \tag{4.100}$$

are the Laguerre polynomials. Our test scheme is based on the following theorem.

Theorem 4.4.1. *Let $\Lambda_{m,r}(\nu)$ $(\nu \geq 0)$ be a bounded function given by*

$$\Lambda_{m,r}(\nu) \coloneqq e^{-r\nu}(1+r)L_m^{(1)}((1+r)\nu), \tag{4.101}$$

for an integer $m \geq 0$ and a real number $r > 0$. Then, for any density operator ρ, we have

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\check{\alpha}|^2)] = \langle 0|\, \rho\, |0\rangle + \sum_{n=m+1}^{\infty} \frac{\langle n|\, \rho\, |n\rangle}{(1+r)^n} I_{n,m}, \tag{4.102}$$

where $I_{n,m}$ are constants satisfying $(-1)^m I_{n,m} > 0$.

Proof. From Eq. (4.98), the expectation value of $\Lambda_{m,r}(|\check{\alpha}|^2)$ when given a measured state ρ is given by

$$\begin{aligned}\mathbb{E}_\rho[\Lambda_{m,r}(|\check{\alpha}|^2)] &= \int_{\alpha\in\mathbb{C}} \Lambda_{m,r}\left(|\alpha|^2\right) q_\rho(\alpha)\, d^2\alpha \\ &= \int_0^\infty d\nu\, \Lambda_{m,r}(\nu) \left(\int_0^{2\pi} \frac{d\theta}{2\pi} \langle \sqrt{\nu} e^{i\theta}| \,\rho\, |\sqrt{\nu} e^{i\theta}\rangle \right) \\ &= \int_0^\infty d\nu\, \Lambda_{m,r}(\nu) \left(\sum_{n=0}^\infty \frac{\nu^n e^{-\nu}}{n!} \langle n|\,\rho\,|n\rangle \right) \\ &= \sum_{n=0}^\infty \frac{\langle n|\,\rho\,|n\rangle\, I_{n,m}}{(1+r)^n}, \end{aligned} \tag{4.103}$$

where

$$I_{n,m} \coloneqq \frac{1}{n!} \int_0^\infty d\nu\; e^{-\nu} \nu^n L_m^{(1)}(\nu) \tag{4.104}$$

for integers $n, m \geq 0$.

The following three properties hold for $I_{n,m}$:

(i) $I_{n,m} = 0$ for $m \geq n \geq 1$.

This results from orthogonality relations of the associated Laguerre polynomials, that is,

$$\int_0^\infty L_n^{(1)}(\nu) L_m^{(1)}(\nu) \nu e^{-\nu}\, d\nu = (n+1)\delta_{n,m}. \tag{4.105}$$

Since the polynomial ν^{n-1} can be written as a linear combination of lower order polynomials $\{L_l^{(1)}(\nu)\}_{0\leq l\leq n-1}$, $I_{n,m}$ vanishes whenever $m \geq n \geq 1$.

(ii) $(-1)^m I_{n,m} > 0$ for $n > m \geq 0$.

This property is shown as follows. First, the associated Laguerre polynomials satisfy the following recurrence relation for $m \geq 1$ [AS48]:

$$m L_m^{(1)}(\nu) = \nu \frac{dL_m^{(1)}}{d\nu}(\nu) + (m+1) L_{m-1}^{(1)}(\nu). \tag{4.106}$$

Substituting this to Eq. (4.104) and using integration by parts, we have

$$I_{n,m} = \frac{n+m}{n} I_{n-1,m} - \frac{m+1}{n} I_{n-1,m-1}. \tag{4.107}$$

for $n \geq 1$ and $m \geq 1$. The property (ii) is then proved by induction over m. For $m = 0$, it is true since $I_{n,0} = 1 > 0$. When $(-1)^{m-1} I_{n,m-1} > 0$ for $n > m-1$, we can prove $(-1)^m I_{n,m} > 0$ for $n > m$ by using Eq. (4.107) recursively with $I_{m,m} = 0$ from the property (i).

(iii) $I_{0,m} = 1$ for $m \geq 0$.

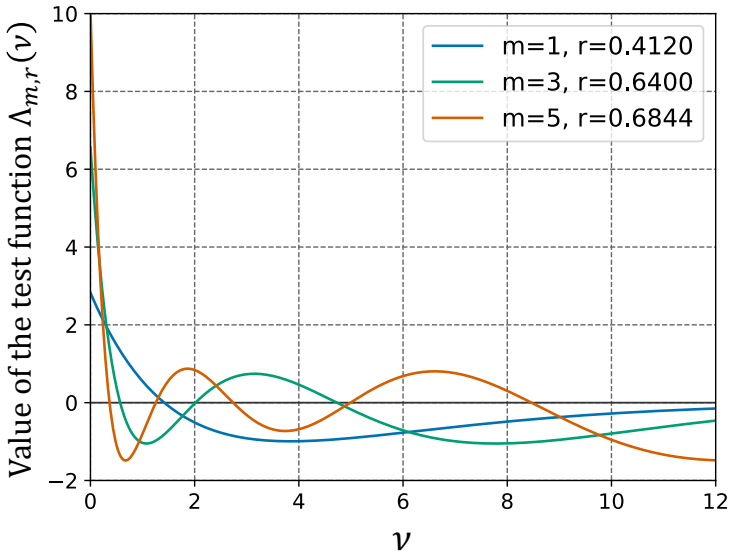

Figure 4.2: Example of the test functions $\Lambda_{m,r}$ used in the estimation. The values of r in the figure are chosen so that the range of $\Lambda_{m,r}$ is minimized for given m. In general, the minimum range of the function $\Lambda_{m,r}$ becomes larger as m increases. The pair $(m, r) = (1, 0.4120)$ was used in the numerical simulation of key rates below.

This also follows from property (i) and Eq. (4.107) for $n = 1$ and $m \geq 1$, which leads to $I_{0,m} = I_{0,0} = 1$.

Combining properties (i), (ii), and (iii) shows Eq. (4.102). □

Note that Eq. (4.102) can also be interpreted as an operator equality

$$\int_{\alpha\in\mathbb{C}} \frac{d^2\alpha}{\pi} \Lambda_{m,r}(|\alpha|^2) \, |\alpha\rangle\langle\alpha| = |0\rangle\langle 0| + \sum_{n=m+1}^{\infty} \frac{I_{n,m}}{(1+r)^n} \, |n\rangle\langle n| \,, \tag{4.108}$$

which converges σ-weakly.

As a corollary, we obtain the following.

Corollary 4.4.2. *Let $|\beta\rangle$ ($\beta \in \mathbb{C}$) be the coherent state with the amplitude β. Then, for any $\beta \in \mathbb{C}$ and for any odd positive integer m, we have*

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\check{\alpha} - \beta|^2)] \leq \langle\beta| \, \rho \, |\beta\rangle \,. \tag{4.109}$$

Proof. From Eq. (4.102) of Theorem 4.4.1, for any odd positive integer m, we have

$$\mathbb{E}_\rho[\Lambda_{m,r}(|\check{\alpha}|^2)] \leq \langle 0| \, \rho \, |0\rangle \,. \tag{4.110}$$

Let D_β be a displacement operator satisfying

$$D_\beta \, |0\rangle\langle 0| \, D_\beta^\dagger = |\beta\rangle\langle\beta| \,, \tag{4.111}$$

and $D_\beta^\dagger = D_{-\beta}$. With $\tilde{\rho} \coloneqq D_\beta \rho D_\beta^\dagger$, we have $q_{\tilde{\rho}}(\alpha) = q_\rho(\alpha - \beta)$ for probability density function of heterodyne measurement outcome, which implies that

$$\begin{aligned} \mathbb{E}_{\tilde{\rho}}[\Lambda_{m,r}(|\check{\alpha} - \beta|^2)] &= \mathbb{E}_\rho[\Lambda_{m,r}(|\check{\alpha}|^2)] \\ &\leq \langle 0| \rho |0\rangle \\ &= \langle \beta| \tilde{\rho} |\beta\rangle . \end{aligned} \tag{4.112}$$

Since this holds for any $\tilde{\rho}$, we proved Eq. (4.109). □

As seen in Figure 4.2, the absolute value and the slope of the function $\Lambda_{m,r}$ are moderate for small values of m and r, which is advantageous in executing the test in a finite duration with a finite resolution. Later we will see that the range of the function $\Lambda_{m,r}$ affects the speed of convergence to the expectation value in the case of a finite number of repetitions (i.e., a finite duration). Furthermore, when the outcome of the heterodyne measurement is digitized (i.e., has a finite resolution), assume that a digitized outcome $\check{\alpha}_{\mathrm{dig}}$ ensures that the true value $\check{\alpha}$ lies in a range $\Omega(\check{\alpha}_{\mathrm{dig}})$. Then, we need only to replace $\Lambda_{m,r}(|\check{\alpha} \pm \beta|^2)$ with its worst-case value, $\min\{\Lambda_{m,r}(|\check{\alpha} \pm \beta|^2) \mid \check{\alpha} \in \Omega(\check{\alpha}_{\mathrm{dig}})\}$, in order for the inequality (4.109) to be satisfied. As seen in Figure 4.2, the slope of the function $\Lambda_{m,r}(\nu)$ is moderate and goes to zero for $\nu \to \infty$. This means that the worst-case value can be made close to the true value, leading to a small influence on the tightness of the estimation.

Compared to a similar method proposed in [CDG+19], our method excels in its tightness for weak input signals; we see from Eq. (4.102) that, regardless of the value of r, the inequality (4.110) saturates when ρ has at most m photons. This is crucial for the use in the QKD protocols in which tightness directly affects the efficiency of the key generation. Furthermore, from Eq. (4.102), the inequality (4.109) can be made arbitrarily tight by taking arbitrarily large m and r. Therefore, our estimation method is asymptotically sharp. See Ref. [CGKM21] for further generalizations.

4.4.2 Proposed protocol

Based on this fidelity test, we propose the following discrete-modulation QKD protocol (see Figure 4.3). Prior to the protocol, Alice and Bob determine the number of rounds N, the acceptance probability of the homodyne measurement $f_{\mathrm{suc}}(q)$ for $q \in \mathbb{R}$ satisfying $f_{\mathrm{suc}}(q) + f_{\mathrm{suc}}(-q) \leq 1$, the parameters for the test function (m, r) with m being positive odd integer and r being positive real, and the protocol parameters $(\mu, p_{\mathrm{sig}}, p_{\mathrm{test}}, p_{\mathrm{trash}}, \beta, s)$ with $p_{\mathrm{sig}} + p_{\mathrm{test}} + p_{\mathrm{trash}} = 1$, where all the parameters are positive. Alice and Bob then run the following protocol.

— **Actual protocol** —

1. Alice generates a random bit $a \in \{0, 1\}$ and sends an optical pulse $\tilde{C}$ in a coherent state with an amplitude $(-1)^a\sqrt{\mu}$ to Bob. She repeats it N times.

2. For each of the received N pulses, Bob chooses a label from $\{\mathrm{signal}, \mathrm{test}, \mathrm{trash}\}$ with probabilities $p_{\mathrm{sig}}, p_{\mathrm{test}}$, and p_{trash}, respectively. According to the label, Alice and Bob do one of the following procedures.

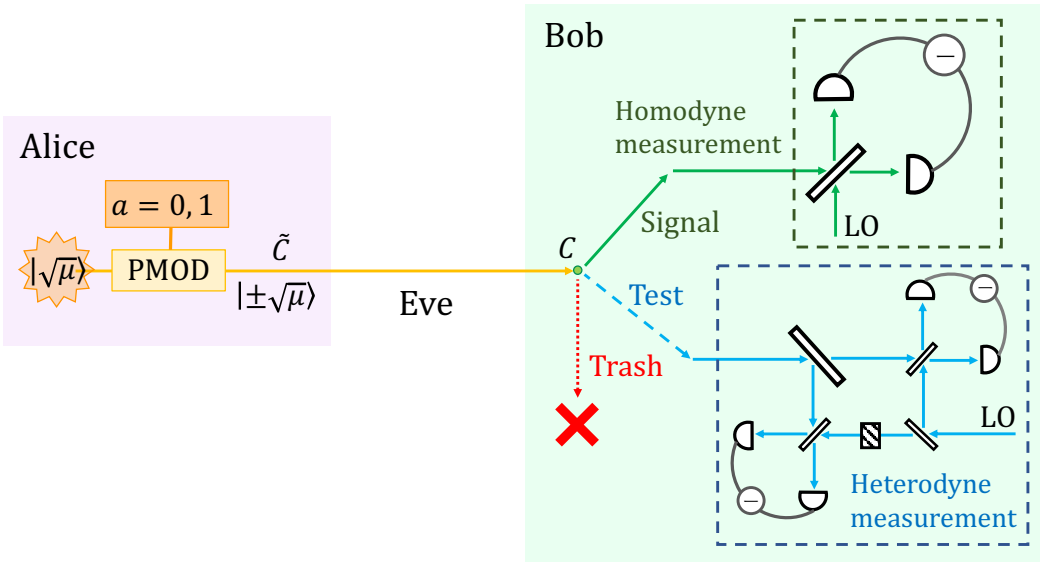

Figure 4.3: The proposed continuous-variable quantum key distribution protocol. Alice generates a random bit $a \in \{0, 1\}$ and sends a coherent state with an amplitude $(-1)^a\sqrt{\mu}$. Bob chooses one of the three measurements based on the predetermined probability. In the signal round, Bob performs the homodyne measurement on the received optical pulse and obtains an outcome $\check{q}$. In the test round, Bob performs the heterodyne measurement on the received optical pulse and obtains an outcome $\check{\alpha}$. In the trash round, he produces no outcome.

[signal] Bob performs the homodyne measurement (defined in Eq. (3.39)) on the received optical pulse C, and obtains an outcome $\check{q} \in \mathbb{R}$. Bob defines a bit b as $b = 0$ with a probability $f_{\rm suc}(\check{q})$ and $b = 1$ with a probability $f_{\rm suc}(-\check{q})$, and otherwise regards the round as "failure". The round in which Bob defines the bit b is regarded as "success". He announces success/failure of the detection. In the case of a success, Alice (resp. Bob) keeps a (b) as a sifted key bit.

[test] Bob performs the heterodyne measurement on the received optical pulse C, and obtains an outcome $\check{\alpha}$. Alice announces her bit a. Bob calculates the value of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$. (See Figure 4.4.)

[trash] Alice and Bob produce no outcomes.

3. We refer to the numbers of "success" and "failure" signal rounds, test rounds, and trash rounds as $\check{N}^{\rm suc}, \check{N}^{\rm fail}, \check{N}^{\rm test}$, and $\check{N}^{\rm trash}$, respectively. ($N = \check{N}^{\rm suc} + \check{N}^{\rm fail} + \check{N}^{\rm test} + \check{N}^{\rm trash}$ holds by definition. Note also that the sifted key length of this protocol is equal to $\check{N}^{\rm suc}$.) Bob calculates the sum of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$ obtained in the $\check{N}^{\rm test}$ test rounds, which is denoted by $\check{F}$.

4. For the information reconciliation, they use $(N_{\rm EC} + s')$-bits of encrypted communication consuming a pre-shared secret key to do the following. Alice sends Bob an $N_{\rm EC}$-bit syndrome of a linear code for her sifted key. Bob reconciles his sifted key accordingly. Alice and Bob verify the correction by comparing s' bits via universal$_2$ hashing [CW79].

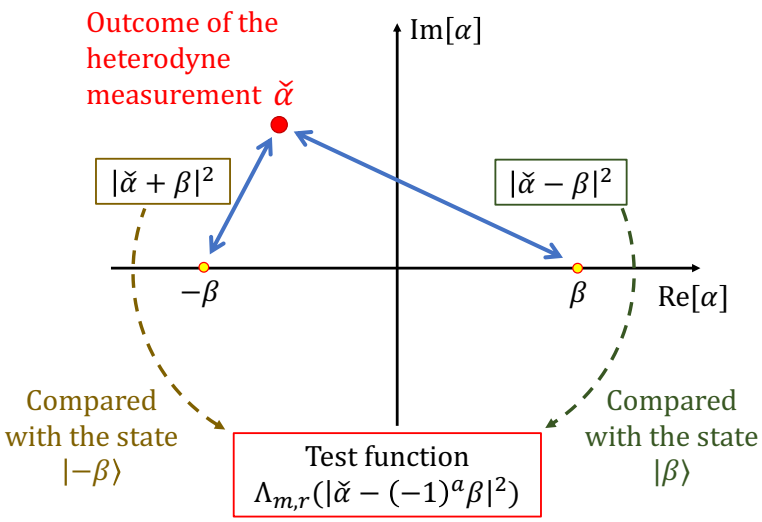

Figure 4.4: A schematic description of the usage of obtained outcomes in the heterodyne measurement. In order to estimate the lower bound on the fidelity to the coherent states $|\pm\beta\rangle$, the squared distance between the outcome $\check{\alpha}$ and the objective point $(-1)^a\beta$ (i.e., $|\check{\alpha}-(-1)^a\beta|^2$) is put into the test function $\Lambda_{m,r}$.

5. Bob computes and announces the final key length $\check{N}^{\rm fin}$ according to

$$\check{N}^{\rm fin} = \max\left\{\check{N}^{\rm suc} - \lceil \check{N}^{\rm suc} h(\check{p})\rceil - s, 0\right\} \tag{4.113}$$

with

$$\check{p} \coloneqq \min\{U(\check{F}, \check{N}^{\rm trash})/\check{N}^{\rm suc}, 1/2\}, \tag{4.114}$$

where $h(x) \coloneqq -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function, $\lceil\cdot\rceil$ is the ceiling function, and the function $U(\check{F}, \check{N}^{\rm trash})$ will be specified later. Alice and Bob then apply the privacy amplification with dual universal$_2$ hashing to obtain the final key. The net key gain $\check{G}$ per pulse is thus given by

$$\check{G} = (\check{N}^{\rm fin} - N_{\rm EC} - s')/N.$$

The acceptance probability $f_{\rm suc}(q)$ should be chosen to post-select the rounds with larger values of q, for which the bit error probability is expected to be lower. It is ideally a step function, but our security proof is applicable to any form of $f_{\rm suc}(q)$. The parameter β is typically chosen to be $\sqrt{\eta\mu}$ with η being a nominal transmissivity of the quantum channel, but the security proof itself holds for any choice of β. The parameters s and s' are related to the overall security parameter in the security proof below.

4.4.3 Security proof

We prove the security of this protocol based on the approach summarized in Section 4.3; i.e., prove the $\varepsilon_{\rm cor}$-correctness Eq. (4.75) and $\varepsilon_{\rm sec}$-secrecy Eq. (4.61) of the protocol, which results in $(\varepsilon_{\rm cor}+\varepsilon_{\rm sec})$-security in Eq. (4.58). Due to the property of the universal$_2$ hashing [CW79, Ren08, TH13] (see also Eq. (4.88)), our protocol achieves $\varepsilon_{\rm cor}$-correctness with $\varepsilon_{\rm cor} = 2^{-s'}$ via the verification in Step 4. In order to prove the $\varepsilon_{\rm sec}$-secrecy, we determine a sufficient amount of the privacy amplification according to Shor and Preskill [SP00b, HT12], which can be regarded as a special case of the security proof summarized in Section 4.3.4. We consider a coherent version of Steps 1 and 2, in which Alice and Bob share an entangled pair of qubits for each success signal round, such that their Z-basis-measurement outcomes correspond to the sifted key bits a and b. For Alice, we introduce a qubit A and assume that she entangles it with an optical pulse $\tilde{C}$ in a state

$$|\Psi\rangle_{A\tilde{C}} \coloneqq \frac{|0\rangle_A |\sqrt{\mu}\rangle_{\tilde{C}} + |1\rangle_A |-\sqrt{\mu}\rangle_{\tilde{C}}}{\sqrt{2}}. \tag{4.115}$$

Then, Step 1 is equivalent to the preparation of $|\Psi\rangle_{A\tilde{C}}$ followed by a measurement of the qubit A on Z basis $\{|0\rangle, |1\rangle\}$ to determine the bit value a. For Bob, we construct a process of probabilistically converting the received optical pulse C to a qubit B (See Figure 4.5). Consider a completely positive (CP) map defined by

$$\mathcal{F}_{C\to B}(\rho_C) \coloneqq \int_{-\infty}^{\infty} dq\, K^{(q)} \rho_C K^{(q)\dagger} \tag{4.116}$$

with

$$K^{(q)} \coloneqq \sqrt{f_{\rm suc}(q)}\, (|0\rangle_B\langle q|_C + |1\rangle_B\langle -q|_C), \tag{4.117}$$

where $\langle q|$ maps a state vector to the value of its wave function at q (see Eq. (3.8)). When the pulse C is in a state ρ_C, the corresponding process succeeds with a probability $p_{\rm suc}$ and then prepares the qubit B in a state ρ_B, where $p_{\rm suc}\rho_B = \mathcal{F}_{C\to B}(\rho_C)$. If the qubit B is further measured on Z basis, probabilities of the outcomes $b = 0, 1$ are given respectively by

$$p_{\rm suc} \langle 0| \rho_B |0\rangle = \int_{-\infty}^{\infty} f_{\rm suc}(q) dq\ \langle q| \rho_C |q\rangle, \tag{4.118}$$

$$p_{\rm suc} \langle 1| \rho_B |1\rangle = \int_{-\infty}^{\infty} f_{\rm suc}(q) dq\ \langle -q| \rho_C |-q\rangle, \tag{4.119}$$

which shows the equivalence to the signal round in Step 2. This is illustrated in Figure 4.5.

To clarify the above observation, we introduce an entanglement-sharing protocol defined in the following.

— Entanglement-sharing protocol —

1′. Alice prepares a qubit A and an optical pulse $\tilde{C}$ in a state $|\Psi\rangle_{A\tilde{C}}$ defined in (4.115). She repeats it N times.

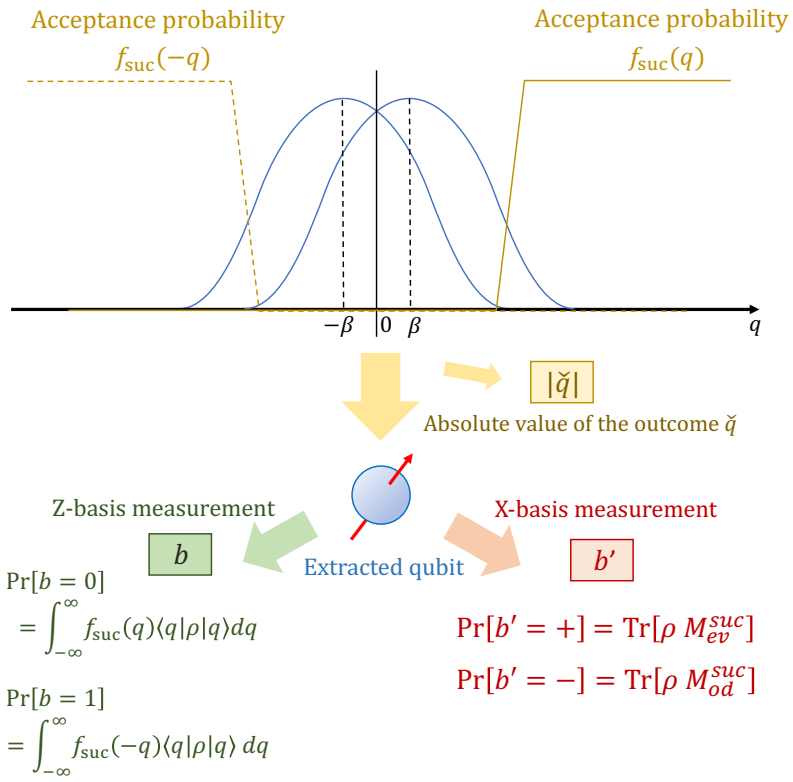

Figure 4.5: Bob's qubit extraction in the entanglement-sharing protocol. Bob performs on the optical pulse a non-demolition projective measurement with which the absolute value $|q|$ of the outcome of the homodyne measurement $\check{q}$ is determined. Then, Bob prepares a qubit B in a state determined by the operation $(K^{(|q|)}(\cdot)K^{(|q|)\dagger} + K^{(-|q|)}(\cdot)K^{(-|q|)\dagger})dq$ with $K^{(|q|)}$ defined in Eq. (4.117). The Z-basis measurement on this qubit gives the same sifted key bit b as that 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.

2′. For each of the received N pulses, Bob announces a label in the same way as that in Step 2. Alice and Bob do one of the following procedures according to the label.

[signal] Bob performs a quantum operation on the received pulse C specified by the CP map $\mathcal{F}_{C\to B}$ to determine success/failure of detection and to obtain a qubit B upon success. He announces success/failure of detection. In the case of a success, Alice keeps her qubit A.

[test] Bob performs a heterodyne measurement on the received optical pulse C, and obtains an outcome $\check{\alpha}$. Alice measures her qubit A on the Z basis and announces the outcome $a \in \{0,1\}$. Bob calculates the value of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$.

[trash] Alice measures her qubit A on the X basis to obtain $a' \in \{+,-\}$, where $+ := 0_X$ and $- := 1_X$.

3′. $\check{N}^{\mathrm{suc}}, \check{N}^{\mathrm{fail}}, \check{N}^{\mathrm{test}}, \check{N}^{\mathrm{trash}}$, and $\check{F}$ are defined in the same way as those in Step 3. Let $\check{Q}_-$ be the number of rounds in the $\check{N}^{\mathrm{trash}}$ trash rounds with $a' = -$.

This protocol leaves $\check{N}^{\mathrm{suc}}$ pairs of qubits shared by Alice and Bob. If they measure these qubits on the Z bases to define the sifted key bits, the whole procedure is equivalent to Steps 1 through 3 of the actual protocol (see Figure 4.6). Alice's measurements on the X basis $\{|\pm\rangle \coloneqq (|0\rangle + |1\rangle)/\sqrt{2}\}$ in the trash rounds are added for later security argument, and they do not affect the equivalence.

The Shor-Preskill argument proceeds the security proof as follows. Suppose that, after the entanglement-sharing protocol, the Controlled-NOT operation CNOT is applied on each pair of qubits, where $\mathrm{CNOT} \coloneqq |0\rangle\langle 0|_A \otimes I_B + |1\rangle\langle 1|_A \otimes \sigma_B^X$. Alice then performs the quantum-mechanical version of the privacy amplification in Step 5 of the actual protocol as in Section 4.2.2 and successively measures the qubits on the Z bases to obtain the final key. Since CNOT does not affect the Z-basis value of Alice's qubit, the resulting $\check{N}^{\mathrm{fin}}$-bit final key in this scenario is equivalent to that in the actual protocol. Although CNOT prevents Bob from obtaining an equivalent final key, he can still simulate the reconciliation and the verification process in Step 4 since the Z-basis value of each of his $\check{N}^{\mathrm{suc}}$ qubits corresponds to absence/presence of a bit error between Alice's and Bob's sifted key bits. Hence, Bob can equivalently carry out all the announcements in Steps 4 and 5 of the actual protocol. As a result, this scenario leads to exactly the same distribution $\Pr(\check{N}^{\mathrm{fin}} = N)$ and the same states $\rho_{AE|N}^{\mathrm{fin}}$ as those of the actual protocol, and thus corresponds to a virtual protocol in the sense of Section 4.3.4; i.e., Eq. (4.76) is satisfied with $\rho_{AE|N}^{\mathrm{virt}}$ being the state of Alice's qubits and Eve's system just before Alice's Z-basis measurement.

The secrecy condition (4.77) of Alice's final key can now be determined from the X-basis property of her $\check{N}^{\mathrm{suc}} = N'$ qubits after the application of CNOT, whose state is denoted by $\rho_{A|N'}$. Since CNOT can be rewritten as $\mathrm{CNOT} = I_A \otimes |+\rangle\langle +|_B + \sigma_A^Z \otimes |-\rangle\langle -|_B$, the X-basis values of $\rho_{A|N'}$ correspond to absence/presence of a phase error $\sigma_A^X \otimes \sigma_B^X = \pm 1$ just before the application of CNOT. Let $\check{\boldsymbol{x}}_A$ be the sequence obtained by the X-basis measurement on $\rho_{A|N'}$, and $\check{N}_{\mathrm{ph}}^{\mathrm{suc}}$ be the number of '$-$' symbols in $\check{\boldsymbol{x}}_A$. If we can have a good upper bound $\check{e}_{\mathrm{ph}}$ on the phase error rate $\check{N}_{\mathrm{ph}}^{\mathrm{suc}}/\check{N}^{\mathrm{suc}}$, shortening by fraction $h(\check{e}_{\mathrm{ph}})$ via privacy amplification in the actual protocol achieves the security in the asymptotic limit [SP00b].

To cover the finite-size case as well, we need a more rigorous statement on the upper bound. For that purpose, we define an estimation protocol in the following (see also Figure 4.6).

— **Estimation protocol** —

1″–3″. Same as Steps 1′, 2′, and 3′ of the entanglement-sharing protocol.

4″. Alice and Bob measure each of their $\check{N}^{\mathrm{suc}}$ pairs of qubits on the X basis and obtain outcomes a' and b', respectively. Let $\check{\boldsymbol{x}}_A$ be the binary sequence with each bit value being zero if $a' = b'$ and one otherwise. Define $\check{N}_{\mathrm{ph}}^{\mathrm{suc}} \coloneqq \mathrm{wt}(\check{\boldsymbol{x}}_A)$, where $\mathrm{wt}(\cdot)$ is defined in Eq. (4.4).

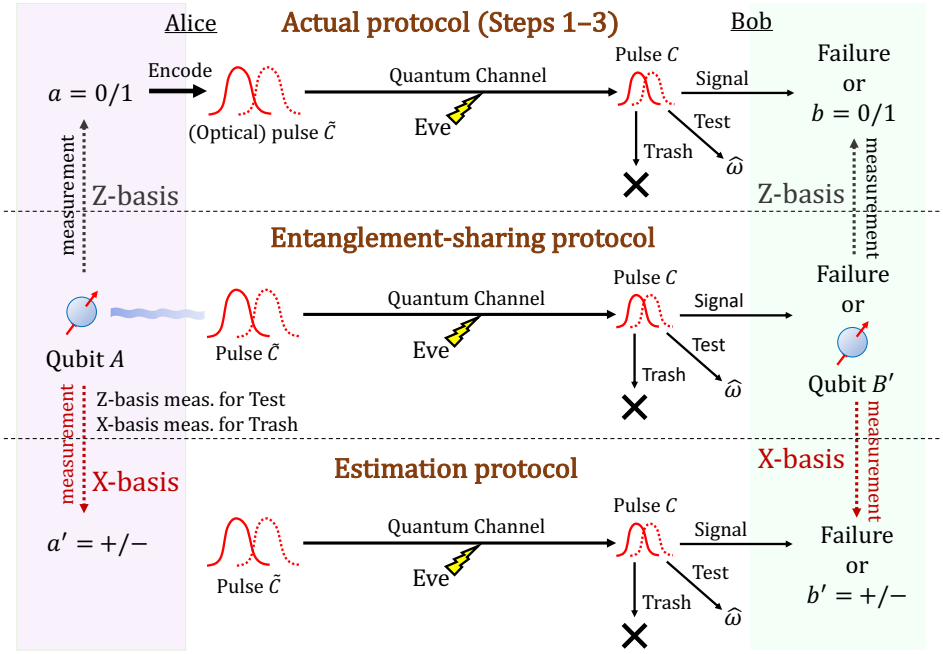

Figure 4.6: Relation between the three protocols. The actual protocol and the estimation protocol are related through the entanglement-sharing protocol. After the entanglement-sharing protocol, Alice and Bob are left with the observed data $(\check{N}^{\mathrm{suc}}, \check{N}^{\mathrm{fail}}, \check{N}^{\mathrm{test}}, \check{N}^{\mathrm{trash}}, \check{F}, \check{Q}_{-})$ and $\check{N}^{\mathrm{suc}}$ pairs of qubits. If Alice and Bob ignore $\check{Q}_{-}$ and measure their qubits on the Z basis to determine their $\check{N}^{\mathrm{suc}}$-bit sifted keys, it becomes equivalent to the actual protocol. On the other hand, if Alice and Bob measure their $\check{N}^{\mathrm{suc}}$ pairs of qubits on the X basis, they can count the number $\check{N}^{\mathrm{suc}}_{\mathrm{ph}}$ of phase errors, which we call the estimation protocol. If we can find a reliable upper bound U on $\check{N}^{\mathrm{suc}}_{\mathrm{ph}}$ in the estimation protocol, it restricts the property of the state of $\check{N}^{\mathrm{suc}}$ pairs of qubits after the entanglement-sharing protocol, which in turn limits the amount of leaked information on the sifted keys in the actual protocol. The security proof is thus reduced to finding such an upper bound U in the estimation protocol, represented as a function of the variables that are commonly available in the three protocols.

The task of proving the security of the actual protocol is then reduced to construction of a function $U(\check{F}, \check{N}^{\mathrm{trash}})$ that satisfies

$$\Pr\left[\check{N}^{\mathrm{suc}}_{\mathrm{ph}} \leq U(\check{F}, \check{N}^{\mathrm{trash}})\right] \geq 1 - \epsilon \tag{4.120}$$

for any attack in the estimation protocol. In fact, this condition implies

$$\Pr\left[\check{N}^{\mathrm{suc}} \geq 1, \check{\boldsymbol{x}}_A \notin \mathcal{T}(\check{N}^{\mathrm{suc}}, \check{F}, \check{N}^{\mathrm{trash}})\right] \leq \epsilon, \tag{4.121}$$

where $\mathcal{T}(\check{N}^{\mathrm{suc}}, \check{F}, \check{N}^{\mathrm{trash}})$ denotes the set of all the possible patterns with $\mathrm{wt}(\check{\boldsymbol{x}}_A) \leq U(\check{F}, \check{N}^{\mathrm{trash}})$. Furthermore, from Lemma 4.2.3, it satisfies

$$\log|\mathcal{T}(\check{N}^{\mathrm{suc}}, \check{F}, \check{N}^{\mathrm{trash}})| \leq \check{N}^{\mathrm{suc}} h(\check{p}) \leq \lceil \check{N}^{\mathrm{suc}} h(\check{p}) \rceil, \tag{4.122}$$

with

$$\check{p} := \min\left\{U(\check{F}, \check{N}^{\mathrm{trash}})/\check{N}^{\mathrm{suc}}, 1/2\right\}. \tag{4.123}$$

Therefore, from Eqs. (4.94), (4.95), and (4.96), setting the final key length to

$$\check{N}^{\mathrm{fin}} = \max\{\check{N}^{\mathrm{suc}} - \lceil \check{N}^{\mathrm{suc}} h(\check{p}) \rceil - s, 0\} \tag{4.124}$$

achieves the $\varepsilon_{\mathrm{sec}} = \sqrt{2(\epsilon + 2^{-s})}$-secrecy.

To construct the function $U(\check{F}, \check{N}^{\mathrm{trash}})$ that satisfies Eq. (4.120), it is beneficial to clarify what property of the optical pulse C is measured by Bob's X-basis measurement in the estimation protocol (see Figure 4.5). Let $\Pi_{\mathrm{ev(od)}}$ be the projection to the subspace with even (resp. odd) photon numbers. ($\Pi_{\mathrm{ev}} + \Pi_{\mathrm{od}} = I_C$ holds by definition.) Furthermore, since $\Pi_{\mathrm{ev}} - \Pi_{\mathrm{odd}}$ is the operator for an optical phase shift of π, we have $\langle q| (\Pi_{\mathrm{ev}} - \Pi_{\mathrm{odd}}) = \langle -q|$. Eq. (4.117) is then rewritten as

$$K^{(q)} = \sqrt{2 f_{\mathrm{suc}}(q)} \left(|+\rangle_B \langle q|_C \Pi_{\mathrm{ev}} + |-\rangle_B \langle q|_C \Pi_{\mathrm{od}} \right). \tag{4.125}$$

Therefore, when the state of the pulse C is ρ_C, the probability of obtaining $+(-)$ in the X-basis measurement in the estimation protocol is given by

$$\langle +(-)| \mathcal{F}_{C\to B}(\rho_C) |+(-)\rangle = \mathrm{Tr}\left(\rho_C M^{\mathrm{suc}}_{\mathrm{ev(od)}} \right), \tag{4.126}$$

where

$$M^{\mathrm{suc}}_{\mathrm{ev(od)}} \coloneqq \int_{-\infty}^{\infty} 2 f_{\mathrm{suc}}(q) dq \, \Pi_{\mathrm{ev(od)}} |q\rangle \langle q|_C \Pi_{\mathrm{ev(od)}}. \tag{4.127}$$

This shows that Bob's X-basis measurement distinguishes the parity of the photon number of the received pulse. In this sense, the secrecy of our protocol is assured by the complementarity between the sign of the quadrature and the parity of the photon number.

As an intermediate step toward our final goal of Eq. (4.120), let us first derive an upper bound on the expectation value $\mathbb{E}[\check{N}^{\mathrm{suc}}_{\mathrm{ph}}]$ in terms of those collected in the test and the trash rounds, $\mathbb{E}[\check{F}]$ and $\mathbb{E}[\check{Q}_-]$, in the estimation protocol. Let ρ_{AC} be the state of the qubit A and the received pulse C averaged over N pairs, and define relevant operators as

$$M^{\mathrm{suc}}_{\mathrm{ph}} \coloneqq |+\rangle\langle +|_A \otimes M^{\mathrm{suc}}_{\mathrm{od}} + |-\rangle\langle -|_A \otimes M^{\mathrm{suc}}_{\mathrm{ev}}, \tag{4.128}$$

$$\Pi^{\mathrm{fid}} \coloneqq |0\rangle\langle 0|_A \otimes |\beta\rangle\langle \beta|_C + |1\rangle\langle 1|_A \otimes |-\beta\rangle\langle -\beta|_C, \tag{4.129}$$

$$\Pi^{\mathrm{trash}}_- \coloneqq |-\rangle\langle -|_A \otimes I_C. \tag{4.130}$$

Then we immediately have

$$\mathbb{E}_\rho[\check{N}^{\mathrm{suc}}_{\mathrm{ph}}] = p_{\mathrm{sig}} N \, \mathrm{Tr}\left(\rho_{AC} M^{\mathrm{suc}}_{\mathrm{ph}} \right) \tag{4.131}$$

and

$$\mathbb{E}_\rho[\check{Q}_-] = p_{\mathrm{trash}} N \, \mathrm{Tr}\left(\rho_{AC} \Pi^{\mathrm{trash}}_- \right), \tag{4.132}$$

while application of the property of Eq. (4.109) leads to

$$\mathbb{E}_\rho[\check{F}] \le p_{\mathrm{test}} N \, \mathrm{Tr}\left(\rho_{AC} \Pi^{\mathrm{fid}} \right). \tag{4.133}$$

Let us denote $\mathrm{Tr}(\rho_{AC} M)$ simply by $\langle M \rangle$ for any operator M. The set of points $\left(\langle M^{\mathrm{suc}}_{\mathrm{ph}} \rangle, \langle \Pi^{\mathrm{fid}} \rangle, \langle \Pi^{\mathrm{trash}}_- \rangle \right)$ for all the density operators ρ_{AC} form a convex region. Rather

than directly deriving the boundary of the region, it is easier to pursue linear constraints in the form of

$$\langle M_{\rm ph}^{\rm suc}\rangle \le B(\kappa,\gamma) - \kappa\langle\Pi^{\rm fid}\rangle + \gamma\langle\Pi_-^{\rm trash}\rangle, \tag{4.134}$$

where $B(\kappa,\gamma),\kappa,\gamma\in\mathbb{R}$.

It is expected that a meaningful bound is obtained only for $\kappa,\gamma\ge 0$. Decreasing the fidelity $\langle\Pi^{\rm fid}\rangle$ should allow more room for eavesdropping, leading to a larger value of phase error rate $\langle M_{\rm ph}^{\rm suc}\rangle$. Hence Eq. (4.134) will give a good bound only when $\kappa\ge 0$. As for $\langle\Pi_-^{\rm trash}\rangle$, it only depends on the marginal state of Alice's qubit A, which is independent of the adversary's attack. We thus have

$$\langle\Pi_-^{\rm trash}\rangle = q_- := \| \langle -|_A |\Psi\rangle_{A\tilde{C}} \|^2 = (1-e^{-2\mu})/2. \tag{4.135}$$

Since Alice's use of a stronger pulse leads to more leaked information, $\gamma\ge 0$ should be chosen for a good bound.

To find a function $B(\kappa,\gamma)$ satisfying Eq. (4.134), let us define an operator

$$M[\kappa,\gamma] := M_{\rm ph}^{\rm suc} + \kappa\Pi^{\rm fid} - \gamma\Pi_-^{\rm trash}. \tag{4.136}$$

Then Eq. (4.134) is rewritten as

$$\mathrm{Tr}\left(\rho_{AC}M[\kappa,\gamma]\right) \le B(\kappa,\gamma). \tag{4.137}$$

This condition holds for any ρ_{AC} iff $M[\kappa,\gamma]$ satisfies an operator inequality

$$M[\kappa,\gamma] \le B(\kappa,\gamma) I_{AC}. \tag{4.138}$$

Since $M[\kappa,\gamma]$ is a bounded operator, such $B(\kappa,\gamma)$ always exists. If the operator $M[\kappa,\gamma]$ were represented by a matrix of small size, the tightest bound would be found by computing the largest eigenvalue of the matrix. But here, $M[\kappa,\gamma]$ may not be a finite-rank operator (not even be a compact operator), and therefore it is difficult to compute the tightest bound. We thus compromise and heuristically find a computable bound $B(\kappa,\gamma)$ which is not necessarily tight; we reduce the problem to finding the largest eigenvalues of small-size matrices by replacing $M[\kappa,\gamma]$ with a constant upper bound except in a relevant finite-dimensional subspace spanned by $|\pm\beta\rangle$ and $M_{\rm ev(od)}^{\rm suc}|\pm\beta\rangle$. For the detailed derivation of $B(\kappa,\gamma)$, see the next section, Section 4.4.4.

With $B(\kappa,\gamma)$ computed, we can rewrite Eq. (4.134) using Eqs. (4.131)–(4.133) to obtain a relation between $\mathbb{E}[\check{N}_{\rm ph}^{\rm suc}]$, $\mathbb{E}[\check{F}]$, and $\mathbb{E}[\check{Q}_-]$. It is concisely written as

$$\mathbb{E}\left[\check{T}[\kappa,\gamma]\right] \le NB(\kappa,\gamma) \tag{4.139}$$

with

$$\check{T}[\kappa,\gamma] := p_{\rm sig}^{-1}\check{N}_{\rm ph}^{\rm suc} + p_{\rm test}^{-1}\kappa\check{F} - p_{\rm trash}^{-1}\gamma\check{Q}_-. \tag{4.140}$$

This relation leads to an explicit bound on the phase error rate as $\mathbb{E}[\check{N}_{\rm ph}^{\rm suc}]/p_{\rm sig}N \le B(\kappa,\gamma)+\gamma q_- - \kappa\,\mathbb{E}[\check{F}]/p_{\rm test}N$, which is enough for the computation of asymptotic key rates.

The security in the finite-size regime is proved by evaluating the fluctuations of $\check{T}[\kappa,\gamma]$ around the expectation value as follows. In the estimation protocol, the following random variables labeled by the number i of the round can be defined;

(i) $\check{N}_{\rm ph}^{{\rm suc},(i)}$ is defined to be unity only when "signal" is chosen in the i-th round, the detection is a "success", and a pair of outcomes (a',b') is $(+,-)$ or $(-,+)$. Otherwise, $\check{N}_{\rm ph}^{{\rm suc},(i)}=0$. We have

$$\check{N}_{\rm ph}^{{\rm suc},(i)}=\begin{cases}1 & \Big(\text{signal, success, } (+,-) \text{ or } (-,+)\Big)\\ 0 & \text{(otherwise)}\end{cases}, \tag{4.141}$$

and $\check{N}_{\rm ph}^{\rm suc}=\sum_{i=1}^{N}\check{N}_{\rm ph}^{{\rm suc},(i)}$.

(ii) $\check{F}^{(i)}$ is defined to be $\Lambda_{m,r}(|\check{\alpha}-(-1)^a\beta|^2)$ only when "test" is chosen in the i-th round. We have

$$\check{F}^{(i)}=\begin{cases}\Lambda_{m,r}(|\check{\alpha}-(-1)^a\beta|^2) & \text{(test)}\\ 0 & \text{(otherwise)}\end{cases}, \tag{4.142}$$

and $\check{F}=\sum_{i=1}^{N}\check{F}^{(i)}$.

(iii) $\check{Q}_{-}^{(i)}$ is defined to be unity only when "trash" is chosen in the i-th round and $a'=-$. Otherwise, $\check{Q}_{-}^{(i)}=0$. We have

$$\check{Q}_{-}^{(i)}=\begin{cases}1 & \text{(trash, } -)\\ 0 & \text{(otherwise)}\end{cases}, \tag{4.143}$$

and $\check{Q}_{-}=\sum_{i=1}^{N}\check{Q}_{-}^{(i)}$.

(iv) We also define

$$\check{T}^{(i)}:=p_{\rm sig}^{-1}\check{N}_{\rm ph}^{{\rm suc},(i)}+p_{\rm test}^{-1}\kappa\check{F}^{(i)}-p_{\rm trash}^{-1}\gamma\check{Q}_{-}^{(i)}, \tag{4.144}$$

which leads to $\check{T}[\kappa,\gamma]=\sum_{i=1}^{N}\check{T}^{(i)}$.

Let $\sigma(\boldsymbol{Y})$ be a σ-algebra generated by a random vector $\boldsymbol{Y}$ (composed of n random variables), i.e.,

$$\sigma(\boldsymbol{Y}):=\{\boldsymbol{Y}^{-1}(A)\mid A\in\mathcal{B}(\mathbb{R}^n)\}. \tag{4.145}$$

Let

$$\{\varnothing,\Omega\}\subseteq\sigma(\check{T}^{(\le 1)})\subseteq\cdots\subseteq\sigma(\check{T}^{(\le N)}) \tag{4.146}$$

be a filtration, where $\check{T}^{(\le i)}:=\left(\check{T}^{(1)},\ldots,\check{T}^{(i)}\right)$ are random vectors. Then, we can apply Corollary 4.2.19 to the sequence $\left(\check{T}^{(1)},\ldots,\check{T}^{(N)}\right)$ with respect to the filtration (4.146) if we can find constants $c_{\min}$ and $c_{\max}$ that satisfy

$$c_{\min}\le\check{T}^{(i)}\le c_{\max} \tag{4.147}$$

for any $i\in\{1,\ldots,N\}$. We define $c_{\min}$ and $c_{\max}$ as follows. In each round, at most one of $\check{N}_{\rm ph}^{{\rm suc},(i)}$, $\check{F}^{(i)}$, and $\check{Q}_{-}^{(i)}$ takes non-zero value; $\check{N}_{\rm ph}^{{\rm suc},(i)}$ and $\check{Q}_{-}^{(i)}$ are either zero or unity,

and $\inf \Lambda_{m,r} \leq \check{F}^{(i)} \leq \sup \Lambda_{m,r}$. Since $\kappa, \gamma \geq 0$, Eq. (4.147) holds when $c_{\min}$ and $c_{\max}$ are defined as

$$c_{\min} \coloneqq \min\{p_{\text{test}}^{-1}\kappa \inf \Lambda_{m,r},\ -p_{\text{trash}}^{-1}\gamma\}, \tag{4.148}$$

$$c_{\max} \coloneqq \max\{p_{\text{sig}}^{-1},\ p_{\text{test}}^{-1}\kappa \sup \Lambda_{m,r}\}. \tag{4.149}$$

Applying Corollary 4.2.19 to the sequence $\left(\check{T}^{(1)}, \ldots, \check{T}^{(N)}\right)$ with respect to the filtration (4.146), we have, with a probability no smaller than $1 - \epsilon/2$,

$$\check{T}[\kappa, \gamma] \leq \sum_{i=1}^{N} \mathbb{E}\left[\check{T}^{(i)} \,\middle|\, \sigma(\check{T}^{(\leq i-1)})\right] + \delta_1(\epsilon/2), \tag{4.150}$$

where

$$\delta_1(\epsilon) \coloneqq (c_{\max} - c_{\min})\sqrt{\frac{N}{2}\ln\left(\frac{1}{\epsilon}\right)}. \tag{4.151}$$

Furthermore, for any state ρ_{AC}, we have

$$\mathbb{E}_\rho[\check{N}_{\text{ph}}^{\text{suc},(i)}] = p_{\text{sig}}\text{Tr}\left(\rho_{AC} M_{\text{ph}}^{\text{suc}}\right), \tag{4.152}$$

$$\mathbb{E}_\rho[\check{Q}_{-}^{(i)}] = p_{\text{trash}}\text{Tr}\left(\rho_{AC} \Pi_{-}^{\text{trash}}\right), \tag{4.153}$$

$$\mathbb{E}_\rho[\check{F}^{(i)}] \leq p_{\text{test}}\text{Tr}\left(\rho_{AC} \Pi^{\text{fid}}\right), \tag{4.154}$$

and thus

$$\mathbb{E}_\rho[\check{T}^{(i)}] \leq \text{Tr}(\rho_{AC} M[\kappa, \gamma]) \leq B(\kappa, \gamma), \tag{4.155}$$

for $i \in \{1, \ldots, N\}$. Since the above inequality holds for any state ρ_{AC}, the following holds for each $i \in \{1, \ldots, N\}$ and for any $D \in \sigma(\check{T}^{(\leq i-1)})$:

$$\int_D \mathbb{E}\left[\check{T}^{(i)} \,\middle|\, \sigma(\check{T}^{(\leq i-1)})\right](x)\, P^{(\leq i-1)}(dx) \leq \text{Tr}\left[\left(E^{(\leq i-1)}(D) \otimes M[\kappa, \gamma] \otimes I^{\otimes(N-i)}\right)\rho^{\text{tot}}\right] \tag{4.156}$$

$$\leq B(\kappa, \gamma) \int_D P^{(\leq i-1)}(dx), \tag{4.157}$$

where $E^{(\leq i-1)}$ denotes the POVM for the random variables $\check{T}^{(\leq i-1)}$, ρ^{tot} denotes the density operator for the total round with which the probability measure for Azuma's inequality is defined, and the probability measure $P^{(\leq i-1)}(dx)$ is defined as

$$P^{(\leq i-1)}(dx) \coloneqq \text{Tr}\left[\left(E^{(\leq i-1)}(dx) \otimes I^{\otimes(N-i+1)}\right)\rho^{\text{tot}}\right]. \tag{4.158}$$

The inequality (4.157) implies that the following inequality holds almost surely:

$$\mathbb{E}\left[\check{T}^{(i)} \,\middle|\, \sigma(\check{T}^{(\leq i-1)})\right] \leq B(\kappa, \gamma). \tag{4.159}$$

Combining this with Eq. (4.150), we have

$$\check{T}[\kappa, \gamma] \leq NB(\kappa, \gamma) + \delta_1(\epsilon/2), \tag{4.160}$$

which holds with a probability no smaller than $1 - \epsilon/2$. We remark that the reason for including the trash rounds in the actual protocol is to circumvent a technical issue

which would arise in this step. Without measurement of $\check{Q}_-$ in the estimation protocol, we would obtain an inequality $\mathbb{E}[p_{\rm sig}^{-1}\check{N}_{\rm ph}^{\rm suc} + p_{\rm test}^{-1}\kappa\check{F}] \leq NB(\kappa,\gamma) + \gamma q_-$. In contrast to Eq. (4.139), the new inequality is true only when ρ_{AC} satisfies $\langle \Pi_-^{\rm trash}\rangle = q_-$, which is too stringent for the application of Azuma's inequality.

Although Eq. (4.140) includes $\check{Q}_-$ which is inaccessible in the actual protocol, we can derive an upper bound by noticing that it is an outcome from Alice's qubits and is independent of the adversary's attack. In fact, given $\check{N}^{\rm trash} = n$, it is the tally of n Bernoulli trials with a probability q_-, i.e., $\Pr(\check{Q}_- \mid \check{N}^{\rm trash} = n)$ is a binomial distribution. Thus from Corollary 4.2.10, the following inequality holds with a probability no smaller than $1 - \epsilon/2$:

$$\check{Q}_- \leq \check{N}^{\rm trash} q_- + \delta_2(\epsilon/2; \check{N}^{\rm trash}), \tag{4.161}$$

where

$$\delta_2(\epsilon/2; \check{N}^{\rm trash}) \coloneqq \check{N}^{\rm trash}\delta(\epsilon/2; \check{N}^{\rm trash}) \tag{4.162}$$

with $\delta(\epsilon, n)$ defined in Corollary 4.2.10. Note that when $\check{N}^{\rm trash}$ is equal to zero, $\check{Q}_-$ is also equal to zero, and thus Eq. (4.161) also holds.

Combining Eqs. (4.140), (4.160), and (4.161), we obtain $U(\check{F}, \check{N}^{\rm trash})$, satisfying Eq. (4.120) by the union bound, as follows:

$$U(\check{F}, \check{N}^{\rm trash}) = p_{\rm sig}(NB(\kappa,\gamma) + \delta_1(\epsilon/2)) - \frac{p_{\rm sig}}{p_{\rm test}}\kappa\check{F} + \frac{p_{\rm sig}}{p_{\rm trash}}\gamma\left(\check{N}^{\rm trash}q_- + \delta_2(\epsilon/2; \check{N}^{\rm trash})\right). \tag{4.163}$$

We finally remark that the encryption of $M \coloneqq N_{\rm EC} + s'$ bits in Step 4 can be omitted as long as each bit linearly depends on Alice's sifted key over GF(2). In such a case, the virtual and the estimation protocol must include measurements on Alice's qubits to simulate the announcement of the M bits in Step 4. (Otherwise, the condition (4.76) cannot be met.) The back-action on the X basis caused by the measurement for each bit amounts to doubling the number of probable patterns $\check{\boldsymbol{x}}_A$. We can thus redefine the set $\mathcal{T}(\check{N}^{\rm suc}, \check{F}, \check{N}^{\rm trash})$ by enlarging its size by factor of 2^M so that Eq. (4.121) holds. This leads to adding M to $N_{\rm PA} \coloneqq \lceil \check{N}^{\rm suc} h(p) \rceil$, which eventually reduces the length of $\check{N}^{\rm fin}$ by M-bits. This means that we achieve the same net key gain rate $\check{G}$ with the same level of security.

4.4.4 Derivation of the operator inequality

The goal of this section is to explicitly construct $B(\kappa,\gamma)$ satisfying (4.138), which was the heuristic part of the security proof in the previous section. Let $\lambda_{\rm sup}(O)$ denote the supremum of the spectrum of a bounded self-adjoint operator O. Although $B(\kappa,\gamma) = \lambda_{\rm sup}(M[\kappa,\gamma])$ would give the tightest bound satisfying Eq. (4.138), it is hard to compute it numerically since system C has an infinite-dimensional Hilbert space. Instead, we derive a looser but simpler bound. We first prove the following lemma.

Lemma 4.4.3. *Let $\Pi_\pm$ be orthogonal projections satisfying $\Pi_+\Pi_- = 0$. Suppose that the rank of $\Pi_\pm$ is no smaller than two or infinite. Let $M_\pm$ be self-adjoint operators satisfying $\Pi_\pm M_\pm \Pi_\pm = M_\pm \leq \alpha_\pm \Pi_\pm$, where $\alpha_\pm$ are real constants. Let $|\psi\rangle$ be an unnormalized vector satisfying $(\Pi_+ + \Pi_-)|\psi\rangle = |\psi\rangle$ and $\Pi_\pm|\psi\rangle \neq 0$. Define the*

following quantities with respect to $|\psi\rangle$*:*

$$C_\pm \coloneqq \langle\psi|\,\Pi_\pm\,|\psi\rangle\,(>0), \tag{4.164}$$
$$D_\pm \coloneqq C_\pm^{-1}\,\langle\psi|\,M_\pm\,|\psi\rangle\,, \tag{4.165}$$
$$V_\pm \coloneqq C_\pm^{-1}\,\langle\psi|\,M_\pm^2\,|\psi\rangle - D_\pm^2. \tag{4.166}$$

Then, for any real numbers γ_+ *and* γ_-*, we have*

$$\lambda_{\sup}\Big(M_+ + M_- + |\psi\rangle\langle\psi| - \gamma_+\Pi_+ - \gamma_-\Pi_-\Big) \le \lambda_{\sup}\Big(M_{4\mathrm{d}}\Big), \tag{4.167}$$

where four dimensional matrix $M_{4\mathrm{d}}$ *is defined as*

$$M_{4\mathrm{d}} \coloneqq \begin{pmatrix} \alpha_+ - \gamma_+ & \sqrt{V_+} & 0 & 0 \\ \sqrt{V_+} & C_+ + D_+ - \gamma_+ & \sqrt{C_+C_-} & 0 \\ 0 & \sqrt{C_+C_-} & C_- + D_- - \gamma_- & \sqrt{V_-} \\ 0 & 0 & \sqrt{V_-} & \alpha_- - \gamma_- \end{pmatrix}. \tag{4.168}$$

Proof. We choose orthonormal vectors $\left\{|e_\pm^{(1)}\rangle\,, |e_\pm^{(2)}\rangle\right\}$ in the domain of $\Pi_\pm$, respectively, to satisfy

$$\sqrt{C_\pm}\,|e_\pm^{(1)}\rangle = \Pi_\pm\,|\psi\rangle\,, \tag{4.169}$$
$$M_\pm\,|e_\pm^{(1)}\rangle = D_\pm\,|e_\pm^{(1)}\rangle + \sqrt{V_\pm}\,|e_\pm^{(2)}\rangle\,, \tag{4.170}$$

which is well-defined due to Eqs. (4.164)–(4.166) and $\Pi_\pm M_\pm \Pi_\pm = M_\pm$. From $(\Pi_+ + \Pi_-)\,|\psi\rangle = |\psi\rangle$, we have

$$|\psi\rangle = \sqrt{C_+}\,|e_+^{(1)}\rangle + \sqrt{C_-}\,|e_-^{(1)}\rangle\,. \tag{4.171}$$

Let us define the following projection operators:

$$\Pi_\pm^{(j)} \coloneqq |e_\pm^{(j)}\rangle\langle e_\pm^{(j)}| \quad (j=1,2), \tag{4.172}$$
$$\Pi_\pm^{(\ge 2)} \coloneqq \Pi_\pm - \Pi_\pm^{(1)}, \tag{4.173}$$
$$\Pi_\pm^{(\ge 3)} \coloneqq \Pi_\pm^{(\ge 2)} - \Pi_\pm^{(2)}. \tag{4.174}$$

Since Eq. (4.170) implies $\Pi_\pm^{(\ge 3)} M_\pm \Pi_\pm^{(1)} = 0$, we have

$$M_\pm = \Pi_\pm^{(1)} M_\pm \Pi_\pm^{(1)} + \Pi_\pm^{(\ge 2)} M_\pm \Pi_\pm^{(\ge 2)} + \Pi_\pm^{(1)} M_\pm \Pi_\pm^{(2)} + \Pi_\pm^{(2)} M_\pm \Pi_\pm^{(1)}. \tag{4.175}$$

The second term in the right-hand side of Eq. (4.175) is bounded as

$$\Pi_\pm^{(\ge 2)} M_\pm \Pi_\pm^{(\ge 2)} \le \alpha_\pm \Pi_\pm^{(\ge 2)}, \tag{4.176}$$

since $M_\pm \le \alpha_\pm \Pi_\pm$. Combining Eqs. (4.165), (4.175), and (4.176), we have

$$\begin{aligned} M_\pm - \gamma_\pm\Pi_\pm \le{}& (D_\pm - \gamma_\pm)\,|e_\pm^{(1)}\rangle\langle e_\pm^{(1)}| + (\alpha_\pm - \gamma_\pm)\,|e_\pm^{(2)}\rangle\langle e_\pm^{(2)}| \\ &+ \sqrt{V_\pm}\Big(|e_\pm^{(1)}\rangle\langle e_\pm^{(2)}| + |e_\pm^{(2)}\rangle\langle e_\pm^{(1)}|\Big) + (\alpha_\pm - \gamma_\pm)\Pi_\pm^{(\ge 3)}. \end{aligned} \tag{4.177}$$

Combining Eqs. (4.171) and (4.177), we have

$$\begin{aligned} &M_+ + M_- + |\psi\rangle\langle\psi| - \gamma_+\Pi_+ - \gamma_-\Pi_- \\ &\leq M_{4\mathrm{d}} \oplus (\alpha_+ - \gamma_+)\Pi_+^{(\geq 3)} \oplus (\alpha_- - \gamma_-)\Pi_-^{(\geq 3)}, \end{aligned} \tag{4.178}$$

where $M_{4\mathrm{d}}$ is given in Eq. (4.168) with the basis $\{|e_+^{(2)}\rangle, |e_+^{(1)}\rangle, |e_-^{(1)}\rangle, |e_-^{(2)}\rangle\}$. Since $\alpha_\pm - \gamma_\pm = \langle e_\pm^{(2)}| M_{4\mathrm{d}} |e_\pm^{(2)}\rangle \leq \lambda_{\sup}\Big(M_{4\mathrm{d}}\Big)$, supremum of the spectrum of the right-hand side of Eq. (4.178) is equal to the largest eigenvalue of the four-dimensional matrix $M_{4\mathrm{d}}$. We thus obtain Eq. (4.167). □

As a corollary, we derive Eq. (4.138) as follows.

Corollary 4.4.4. *Let $|\beta\rangle$ be a coherent state. Let $\Pi_{\mathrm{ev(od)}}$, $M_{\mathrm{ev(od)}}^{\mathrm{suc}}$, and $M[\kappa,\gamma]$ be as defined in the main text, and define following quantities:*

$$C_{\mathrm{ev}} \coloneqq \langle\beta|\,\Pi_{\mathrm{ev}}\,|\beta\rangle = e^{-|\beta|^2}\cosh|\beta|^2, \tag{4.179}$$

$$C_{\mathrm{od}} \coloneqq \langle\beta|\,\Pi_{\mathrm{od}}\,|\beta\rangle = e^{-|\beta|^2}\sinh|\beta|^2, \tag{4.180}$$

$$D_{\mathrm{ev(od)}} \coloneqq C_{\mathrm{ev(od)}}^{-1}\,\langle\beta|\,M_{\mathrm{ev(od)}}^{\mathrm{suc}}\,|\beta\rangle\,, \tag{4.181}$$

$$V_{\mathrm{ev(od)}} \coloneqq C_{\mathrm{ev(od)}}^{-1}\,\langle\beta|\,\Big(M_{\mathrm{ev(od)}}^{\mathrm{suc}}\Big)^2\,|\beta\rangle - D_{\mathrm{ev(od)}}^2. \tag{4.182}$$

Let $M_{4\mathrm{d}}^{\mathrm{err}}[\kappa,\gamma]$ and $M_{2\mathrm{d}}^{\mathrm{cor}}[\kappa,\gamma]$ be defined as follows:

$$M_{4\mathrm{d}}^{\mathrm{err}}[\kappa,\gamma] \coloneqq \begin{pmatrix} 1 & \sqrt{V_{\mathrm{od}}} & & \\ \sqrt{V_{\mathrm{od}}} & \kappa\,C_{\mathrm{od}} + D_{\mathrm{od}} & \kappa\sqrt{C_{\mathrm{od}}\,C_{\mathrm{ev}}} & \\ & \kappa\sqrt{C_{\mathrm{od}}\,C_{\mathrm{ev}}}, & \kappa\,C_{\mathrm{ev}} + D_{\mathrm{ev}} - \gamma & \sqrt{V_{\mathrm{ev}}} \\ & & \sqrt{V_{\mathrm{ev}}} & 1-\gamma \end{pmatrix}, \tag{4.183}$$

$$M_{2\mathrm{d}}^{\mathrm{cor}}[\kappa,\gamma] \coloneqq \begin{pmatrix} \kappa\,C_{\mathrm{ev}} & \kappa\sqrt{C_{\mathrm{ev}}\,C_{\mathrm{od}}} \\ \kappa\sqrt{C_{\mathrm{ev}}\,C_{\mathrm{od}}} & \kappa\,C_{\mathrm{od}} - \gamma \end{pmatrix}. \tag{4.184}$$

Define a convex function

$$B(\kappa,\gamma) \coloneqq \max\Big\{\lambda_{\sup}\Big(M_{4\mathrm{d}}^{\mathrm{err}}[\kappa,\gamma]\Big), \lambda_{\sup}\Big(M_{2\mathrm{d}}^{\mathrm{cor}}[\kappa,\gamma]\Big)\Big\}. \tag{4.185}$$

Then, for $\kappa,\gamma \geq 0$, we have

$$M[\kappa,\gamma] \leq B(\kappa,\gamma) I_{AC}. \tag{4.186}$$

Proof. Let us first observe that the operator Π^{fid} defined in Eq. (4.129) can be rewritten as follows:

$$\Pi^{\mathrm{fid}} = |\phi_{\mathrm{err}}\rangle\langle\phi_{\mathrm{err}}|_{AC} + |\phi_{\mathrm{cor}}\rangle\langle\phi_{\mathrm{cor}}|_{AC}\,, \tag{4.187}$$

where orthogonal vectors $|\phi_{\mathrm{err}}\rangle_{AC}$ and $|\phi_{\mathrm{cor}}\rangle_{AC}$ are defined as

$$|\phi_{\mathrm{err}}\rangle_{AC} \coloneqq |+\rangle_A \otimes \Pi_{\mathrm{od}}\,|\beta\rangle_C + |-\rangle_A \otimes \Pi_{\mathrm{ev}}\,|\beta\rangle_C\,, \tag{4.188}$$

$$|\phi_{\mathrm{cor}}\rangle_{AC} \coloneqq |+\rangle_A \otimes \Pi_{\mathrm{ev}}\,|\beta\rangle_C + |-\rangle_A \otimes \Pi_{\mathrm{od}}\,|\beta\rangle_C\,. \tag{4.189}$$

Next, using Eqs. (4.187), (4.128), and (4.130), we rearrange the operator $M[\kappa,\gamma]$ defined in Eq. (4.136) as follows:

$$M[\kappa,\gamma] = M^{\mathrm{err}}[\kappa,\gamma] \oplus M^{\mathrm{cor}}[\kappa,\gamma], \tag{4.190}$$

where

$$\begin{aligned} M^{\mathrm{err}}[\kappa,\gamma] \coloneqq |+\rangle\langle+|_A \otimes M_{\mathrm{od}}^{\mathrm{suc}} + |-\rangle\langle-|_A \otimes M_{\mathrm{ev}}^{\mathrm{suc}} \\ + \kappa\,|\phi_{\mathrm{err}}\rangle\langle\phi_{\mathrm{err}}|_{AC} - \gamma\,|-\rangle\langle-|_A \otimes \Pi_{\mathrm{ev}}, \end{aligned} \tag{4.191}$$

$$M^{\mathrm{cor}}[\kappa,\gamma] \coloneqq \kappa\,|\phi_{\mathrm{cor}}\rangle\langle\phi_{\mathrm{cor}}|_{AC} - \gamma\,|-\rangle\langle-|_A \otimes \Pi_{\mathrm{od}}. \tag{4.192}$$

We can apply Lemma 4.4.3 to $M^{\mathrm{err}}[\kappa,\gamma]$ by the following substitutions

$$M_\pm = |\pm\rangle\langle\pm|_A \otimes M_{\mathrm{od(ev)}}^{\mathrm{suc}}, \tag{4.193}$$

$$|\psi\rangle = \sqrt{\kappa}\,|\phi_{\mathrm{err}}\rangle_{AC}\,, \tag{4.194}$$

$$\Pi_\pm = |\pm\rangle\langle\pm|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{4.195}$$

$$\alpha_\pm = 1, \tag{4.196}$$

$$\gamma^+ = 0, \quad \gamma^- = \gamma. \tag{4.197}$$

Here, $M_\pm \leq \Pi_\pm$ (i.e., $\alpha_\pm = 1$) holds because $M_{\mathrm{od(ev)}}^{\mathrm{suc}}$ are POVM elements. The other prerequisites of Lemma 4.4.3 are easy to be confirmed. Thus, we obtain

$$\lambda_{\sup}\Big(M^{\mathrm{err}}[\kappa,\gamma]\Big) \leq \lambda_{\sup}\Big(M_{\mathrm{4d}}^{\mathrm{err}}[\kappa,\gamma]\Big). \tag{4.198}$$

In the same way, we can apply Lemma 4.4.3 to $M^{\mathrm{cor}}[\kappa,\gamma]$ via

$$M_\pm = 0, \tag{4.199}$$

$$|\psi\rangle = \sqrt{\kappa}\,|\phi_{\mathrm{cor}}\rangle_{AC}\,, \tag{4.200}$$

$$\Pi_\pm = |\pm\rangle\langle\pm|_A \otimes \Pi_{\mathrm{ev(od)}}, \tag{4.201}$$

$$\alpha_\pm = 0, \tag{4.202}$$

$$\gamma^+ = 0, \quad \gamma^- = \gamma. \tag{4.203}$$

Since $M_\pm = 0$ implies $D_\pm = V_\pm = 0$ in Lemma 4.4.3, this time we can reduce the dimension of relevant matrix Eq. (4.168) by separating known eigenvalues 0 and $-\gamma$. Therefore, we have

$$\lambda_{\sup}\Big(M^{\mathrm{cor}}[\kappa,\gamma]\Big) \leq \max\Big\{\lambda_{\sup}\Big(M_{\mathrm{2d}}^{\mathrm{cor}}[\kappa,\gamma]\Big), 0, -\gamma\Big\} = \lambda_{\sup}\Big(M_{\mathrm{2d}}^{\mathrm{cor}}[\kappa,\gamma]\Big), \tag{4.204}$$

where the last inequality holds since $\gamma \geq 0$ and $\kappa C_{\mathrm{ev}} \geq 0$. We then obtain Eq. (4.186) from Eqs. (4.190), (4.198), and (4.204). Since $M_{\mathrm{4d}}^{\mathrm{err}}[\kappa,\gamma]$ and $M_{\mathrm{2d}}^{\mathrm{cor}}[\kappa,\gamma]$ are symmetric and their elements linearly depend on κ and γ, $\lambda_{\sup}\Big(M_{\mathrm{4d}}^{\mathrm{err}}[\kappa,\gamma]\Big)$ and $\lambda_{\sup}\Big(M_{\mathrm{2d}}^{\mathrm{cor}}[\kappa,\gamma]\Big)$ are convex functions over κ and γ, and so is $B(\kappa,\gamma)$. □

4.4.5 Numerical simulations

We simulated the net key gain per pulse $\check{G}$ as a function of the transmission distance L in the optical channel. We assume a channel model with a loss with the transmissivity $\eta = 10^{-0.02L}$ (including the efficiency of Bob's apparatus) and an excess noise at channel output; Bob receives Gaussian states obtained by randomly displacing coherent states $|\pm\sqrt{\eta\mu}\rangle$ to increase their variances by a factor of $(1+\xi)$ [NH04, HIM+17]. The states that Bob receives dependent on Alice's bit value a are thus given by

$$\rho_{\mathrm{model}}^{(a)} \coloneqq \int_{\mathbb{C}} p_\xi(\gamma)\,|(-1)^a\sqrt{\eta\mu}+\gamma\rangle\langle(-1)^a\sqrt{\eta\mu}+\gamma|\,d^2\gamma, \tag{4.205}$$

where $p_\xi(\gamma)$ is given by

$$p_\xi(\gamma) \coloneqq \frac{1}{\pi\xi} e^{-|\gamma|^2/\xi}. \tag{4.206}$$

The parameter ξ is the excess noise relative to the vacuum, i.e.,

$$\left\langle (\Delta\hat{q})^2 \right\rangle_{\rho^{(\mathrm{a})}_{\mathrm{model}}} = (1+\xi)/2, \tag{4.207}$$

where $\langle(\Delta\hat{q})^2\rangle = 1/2$ for the vacuum state from Eq. (3.86). The expected amplitude of coherent state β is chosen to be $\sqrt{\eta\mu}$. The actual fidelity between Bob's objective state $|(-1)^a\sqrt{\eta\mu}\rangle$ and the model state $\rho^{(a)}_{\mathrm{model}}$ is given by

$$\begin{aligned} &F(\rho^{(a)}_{\mathrm{model}}, |(-1)^a\sqrt{\eta\mu}\rangle\langle(-1)^a\sqrt{\eta\mu}|) \\ &= \int_{\mathbb{C}} p_\xi(\gamma) |\left\langle (-1)^a\sqrt{\eta\mu}|(-1)^a\sqrt{\eta\mu}-\gamma\right\rangle|^2 d\gamma \\ &= \frac{1}{1+\xi/2}. \end{aligned} \tag{4.208}$$

We assume a step function with a threshold $q_{\mathrm{th}}(>0)$ as the acceptance probability, i.e., $f_{\mathrm{suc}}(q) = \Theta(q-q_{\mathrm{th}})$. In this case, the quantities defined in Eqs. (4.181) and (4.182) are given by

$$D_{\mathrm{ev}} = \int_{-\infty}^{\infty} 2C_{\mathrm{ev}}^{-1} f_{\mathrm{suc}}(q) \left|\langle q| \Pi_{\mathrm{ev}} |\beta\rangle\right|^2 dq \tag{4.209}$$

$$= \frac{1}{4C_{\mathrm{ev}}}\left[\mathrm{erfc}\Big(q_{\mathrm{th}}-\sqrt{2}\beta\Big) + \mathrm{erfc}\Big(q_{\mathrm{th}}+\sqrt{2}\beta\Big) + 2e^{-2\beta^2}\mathrm{erfc}\Big(q_{\mathrm{th}}\Big)\right], \tag{4.210}$$

$$D_{\mathrm{od}} = \int_{-\infty}^{\infty} 2C_{\mathrm{od}}^{-1} f_{\mathrm{suc}}(q) \left|\langle q| \Pi_{\mathrm{od}} |\beta\rangle\right|^2 dq \tag{4.211}$$

$$= \frac{1}{4C_{\mathrm{od}}}\left[\mathrm{erfc}\Big(q_{\mathrm{th}}-\sqrt{2}\beta\Big) + \mathrm{erfc}\Big(q_{\mathrm{th}}+\sqrt{2}\beta\Big) - 2e^{-2\beta^2}\mathrm{erfc}\Big(q_{\mathrm{th}}\Big)\right], \tag{4.212}$$

$$V_{\mathrm{ev(od)}} = \int_{-\infty}^{\infty} 2C_{\mathrm{ev(od)}}^{-1} \Big(f_{\mathrm{suc}}(q)\Big)^2 \left|\langle q| \Pi_{\mathrm{ev(od)}} |\beta\rangle\right|^2 dq - D_{\mathrm{ev(od)}}^2 \tag{4.213}$$

$$= D_{\mathrm{ev(od)}} - D_{\mathrm{ev(od)}}^2, \tag{4.214}$$

where $\beta = \sqrt{\eta\mu}$ and the complementary error function $\mathrm{erfc}(x)$ is defined as

$$\mathrm{erfc}(x) \coloneqq \frac{2}{\sqrt{\pi}} \int_x^{\infty} dt\ e^{-t^2}. \tag{4.215}$$

For the derivation of Eq. (4.213), we used the fact that $\Pi_{\mathrm{ev}} + \Pi_{\mathrm{od}} = I$ and $(\Pi_{\mathrm{ev}} - \Pi_{\mathrm{od}})|\beta\rangle = |-\beta\rangle$.

We assume that the number of "success" signal rounds $\check{N}^{\mathrm{suc}}$ is equal to its expectation value,

$$\begin{aligned} \mathbb{E}[\check{N}^{\mathrm{suc}}] &= \left(\int_{-\infty}^{\infty} f(q) \langle q| \rho^{(a)}_{\mathrm{model}} |q\rangle\, dq\right) p_{\mathrm{sig}} N \\ &= p_{\mathrm{sig}} N (P^+ + P^-), \end{aligned} \tag{4.216}$$

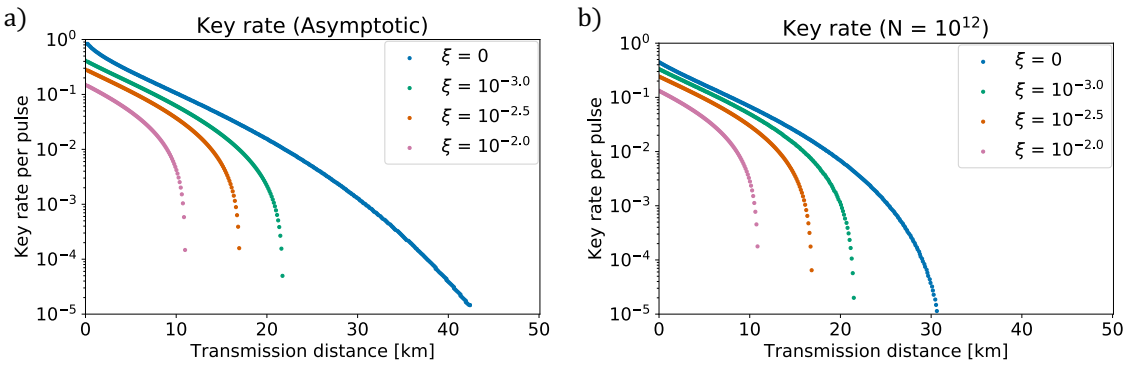

Figure 4.7: The net key gain per pulse $\check{G}$ (key rate) vs. the transmission distance L of the optical channel. We assumed that the optical pulse that Bob receives is given by randomly displacing a coherent state to increase its variance by a factor of $(1+\xi)$. a) The asymptotic key rate for various values of ξ. b) The key rate for various values of ξ when the pulse number is finite ($N = 10^{12}$).

where

$$P^{\pm} := \int_{q_{\rm th}}^{\infty} \langle \pm(-1)^a q| \, \rho^{(a)}_{\rm model} \, |\pm(-1)^a q\rangle \, dq \tag{4.217}$$

$$= \frac{1}{2} \operatorname{erfc}\left((q_{\rm th} \mp \sqrt{2}\sqrt{\eta\mu}) \sqrt{\frac{1}{1+\xi}} \right). \tag{4.218}$$

We also assume that the number of test rounds $\check{N}^{\rm test}$ is equal to $p_{\rm test}N$ and the number of trash rounds $\check{N}^{\rm trash}$ is equal to $p_{\rm trash}N$. The test outcome $\check{F}$ is assumed to be equal to its expectation value $\mathbb{E}[\check{F}]$, which is given by

$$\begin{aligned}
\mathbb{E}[\check{F}] &= p_{\rm test} N \, \mathbb{E}_{\rho^{(a)}_{\rm model}} [\Lambda_{m,r}(|\check{\alpha} - (-1)^a \sqrt{\eta\mu}|^2)] \\
&= p_{\rm test} N \int_{\mathbb{C}} \frac{d^2\alpha}{\pi} \, \langle \alpha| \, \rho^{(a)}_{\rm model} \, |\alpha\rangle \, \Lambda_{m,r}(|\alpha - (-1)^a \sqrt{\eta\mu}|^2) \\
&= \frac{p_{\rm test} N}{1+\xi/2} \left[1 - (-1)^{m+1} \left(\frac{\xi/2}{1 + r(1+\xi/2)} \right)^{m+1} \right].
\end{aligned} \tag{4.219}$$

We adopted $m = 1$ and $r = 0.4120$ for $\Lambda_{m,r}$, which leads to $(\sup \Lambda_{m,r}, \inf \Lambda_{m,r}) = (2.824, -0.9932)$. The cost of the bit error correction $N_{\rm EC}$ is assumed to be $1.1 \times \check{N}^{\rm suc} h(e_{\rm bit})$, where the bit error rate $e_{\rm bit}$ is given by

$$e_{\rm bit} = \frac{P^-}{P^+ + P^-}. \tag{4.220}$$

We set $\varepsilon_{\rm sct} (:= \varepsilon_{\rm cor} + \varepsilon_{\rm sec}) = 2^{-50}$ for the overall security parameter, and set $\epsilon = 2^{-s} = \varepsilon_{\rm sec}^2/4 = \varepsilon_{\rm sct}^2/16$ and $2^{-s'} = \varepsilon_{\rm cor} = \varepsilon_{\rm sct}/2$. We thus have two coefficients (κ, γ) and four protocol parameters $(\mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$ to be determined. For each transmission distance L, we determined (κ, γ) via a convex optimization using the CVXPY 1.0.25 [DB16, AVDB18] and $(\mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$ via the Nelder-Mead in the scipy.minimize library in Python, in order to maximize the key rate.

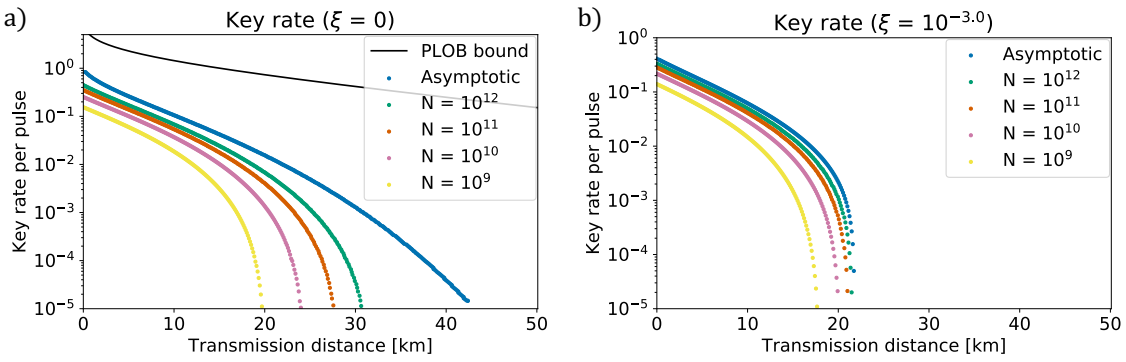

Figure 4.8: The net key gain per pulse $\check{G}$ (key rate) vs. the transmission distance L of the optical channel. We assumed that the optical pulse that Bob receives is given by randomly displacing a coherent state to increase its variance by a factor of $(1+\xi)$. a) The key rate in a pure-loss channel ($\xi = 0$) for various pulse numbers N. The solid black line shows the fundamental limitation of the one-way repeater-less secure key distribution called the PLOB bound [PLOB17]. b) The key rate in a channel with the excess noise $\xi = 10^{-3.0}$ for various pulse numbers N.

Figures 4.7 and 4.8 show the key rates of our protocol in the asymptotic limit $N \to \infty$ and finite-size cases with $N = 10^9$–10^{12} for $\xi = 10^{-2.0}$–$10^{-3.0}$ and 0. (Note that from the results of the recent experiments [JKJL+13, HIM+17, ELP+20], excess noise with $\xi = 10^{-2.0}$–$10^{-3.0}$ at the channel output seems reasonable. Furthermore, the state-of-the-art experiments [ELP+20] work at 0.5 GHz repetition rate, which implies that total number of rounds $N = 10^9$–10^{12} can be achieved in a realistic duration.) For the noiseless model ($\xi = 0$) in Figure 4.7 a, the asymptotic rate reaches 8 dB. In the case of $\xi = 10^{-3.0}$, it reaches 4 dB, which is comparable to the result of a similar binary modulation protocol proposed in Ref. [ZHRL09].

As for finite-size key rates, we see that the noiseless model shows a significant finite-size effect even for $N = 10^{12}$ in Figure 4.8 a. On the other hand, with the presence of noises ($\xi = 10^{-3.0}$), the effect becomes milder, and $N = 10^{11}$ is enough to achieve a rate close to the asymptotic case, as can be seen in Figure 4.8 b. This may be ascribed to the cost of the fidelity test. In order to make sure that the fidelity is no smaller than $1-\delta$, the statistical uncertainty of the fidelity test must be reduced to $O(\delta)$. As a result, approaching the asymptotic rate of $\xi = 0$ will require many rounds for the fidelity test.

Examples of optimized parameters are shown in Table 4.1. Typical optimized values of the threshold q_{th} range from 0.7 to 2.0. They are larger than those in other analyses of protocols with post-selection (e.g., [LUL19]). A possible reason is that the latter protocols use more than two states to monitor the eavesdropping action, which may lead to a lower cost of privacy amplification and higher tolerance against bit errors.

4.4.6 Discussion

Numerically simulated key rates above were computed on the implicit assumption that Bob's observed quantities are processed with infinite precision. Even when these are approximated with a finite set of discrete points, we can still prove the security with minimal degradation of key rates. We have already explained in Section 4.4.1 the capability to incorporate finite precision for the heterodyne measurement used for the test in the protocol. For the homodyne measurement used for the signal, finite precision can be treated through appropriate modification of the acceptance probability $f_{\mathrm{suc}}(q)$. Aside from a small change in the success rate and the bit error rate, this function affects the key rate only through integrals in Eqs. (4.209), (4.211), and (4.213) in the previous section, and hence influence on the key rate is expected to be small. We thus believe that the fundamental obstacles associated with the analog nature of the continuous-variable protocol have been settled by our approach.

In comparison with recent asymptotic analyses [GGDL19, LUL19] of continuous-variable QKD with the discrete modulation, our protocol achieves lower key rates and much shorter distance. Since ours is the first attempt to apply the proof technique of discrete-variable QKD to continuous-variable QKD, there is much room for possible improvement. We sacrificed the optimality for simplicity in deriving the operator inequality. The definition of the phase error is not unique, and there may be a better choice, which will be sought in the next section. The trash rounds were introduced for technical reasons, but we are not sure whether they are really necessary. The protocols considered in Ref. [GGDL19, LUL19] use four or more states in signal or test modes, while ours use only two states. In fact, the binary protocol analyzed in Ref. [ZHRL09] has the key rate comparable to ours when the excess noise ξ is around 10^{-3}.

In order to improve the presented finite-size key rate especially under the existence of excess noise, a promising route may be increasing the number of states from two. Our fidelity test can be straightforwardly generalized to the monitoring for such a larger constellation of signals, and we will be able to confine the adversary's attacks more tightly than in the present binary protocol. As for the proof techniques to determine the amount of privacy amplification, there are two possible directions. One is to generalize the present discrete-variable-QKD-inspired approach of estimating the number of phase errors in qubits to the case of qudits. The other direction is to seek a way to combine the existing analyses [GGDL19, LUL19, DW05] of discrete-modulation continuous-variable QKD protocols, which have been reported to yield high key rates in the asymptotic regime, to our fidelity test. Although either of the approaches is nontrivial, we believe that the present results will open up a new direction toward exploiting the expected high potential of continuous-variable QKD with an improved security level.

Table 4.1: Examples of optimized parameters

Parameters for $N = 10^{11}$ and $\xi = 0$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.38×10^{-1}	$(32.4, 1.38)$	0.514	0.752	0.821	0.172
10	5.36×10^{-2}	$(20.3, 0.741)$	0.442	1.02	0.831	0.160
15	1.75×10^{-2}	$(14.6, 0.381)$	0.451	1.21	0.767	0.227
20	4.15×10^{-3}	$(12.6, 0.175)$	0.442	1.46	0.624	0.371
25	3.23×10^{-4}	$(9.98, 0.059)$	0.438	1.77	0.370	0.626
Parameters for $N = 10^{11}$ and $\xi = 10^{-3.0}$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.13×10^{-1}	$(17.9, 1.19)$	0.466	0.802	0.853	0.138
10	4.07×10^{-2}	$(11.9, 0.666)$	0.442	1.02	0.831	0.160
15	1.02×10^{-2}	$(8.85, 0.345)$	0.440	1.27	0.758	0.233
20	5.29×10^{-4}	$(6.70, 0.147)$	0.463	1.57	0.484	0.505
Parameters for $N = 10^{12}$ and $\xi = 0$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.69×10^{-1}	$(54.9, 1.56)$	0.556	0.713	0.874	0.123
10	6.76×10^{-2}	$(31.3, 0.798)$	0.493	0.948	0.868	0.128
15	2.41×10^{-2}	$(23.2, 0.408)$	0.466	1.18	0.829	0.168
20	6.93×10^{-3}	$(17.7, 0.184)$	0.443	1.43	0.772	0.226
25	1.14×10^{-3}	$(14.6, 0.065)$	0.427	1.71	0.596	0.402
30	3.23×10^{-5}	$(10.8, 0.017)$	0.421	2.05	0.240	0.759
Parameters for $N = 10^{12}$ and $\xi = 10^{-3.0}$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.32×10^{-1}	$(21.7, 1.25)$	0.482	0.783	0.909	0.086
10	4.92×10^{-2}	$(13.8, 0.689)$	0.450	1.01	0.899	0.096
15	1.36×10^{-2}	$(9.82, 0.355)$	0.442	1.25	0.858	0.137
20	1.17×10^{-3}	$(7.13, 0.151)$	0.458	1.56	0.701	0.293

Examples of the parameters for a given pair of the total pulse number N and the excess noise parameter ξ defined in Eq. (4.207). The variance of the quadrature operator $\hat{q}$ for the vacuum state is $\langle(\Delta\hat{q})^2\rangle = 1/2$. Given (N, ξ), protocol parameters $(\kappa, \gamma, \mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$ are optimized for each transmission distance L [km] so that the net key gain per pulse (key rate) $\check{G}$ is maximized.

4.5 Finite-size analysis for the binary-modulation protocol based on the reverse reconciliation

Although the security proof developed in the previous section, Section 4.4, realizes the finite-size security against general attacks in a composable fashion, the obtained key rate has very bad scaling against transmission distance. A possible reason for this bad performance is the way of security proof based on the entanglement distillation [SP00b, LC99]. There are alternative types of security proofs [Ren08, Koa09, Tsu20a] that can approach necessary and sufficient conditions for security. In particular, for continuous-variable QKD protocols, it has been shown that the security proof based on the reverse reconciliation provides better performance than that based on the direct reconciliation [SRLL02].

In this section, we develop a refined security proof based on the reverse reconciliation (see Section 4.3 for its definition) for the binary-modulation protocol proposed in the previous section. With a refined proof and no additional experimental requirement, we obtain a significant improvement in the key gain against pure loss; in fact, it achieves near-optimal scaling against transmission distance in the asymptotic limit.

4.5.1 Alternative protocol

Our refined security proof is for almost the same protocol as that in Section 4.4.2 but with a slight change. Prior to the protocol, Alice and Bob determine the number N of total rounds, the acceptance probability $f_{\rm suc}(q)$ ($q \in \mathbb{R}$) of the homodyne measurement satisfying $f_{\rm suc}(q) + f_{\rm suc}(-q) \leq 1$, the parameters for the test function (m, r), and the protocol parameters $(\mu, p_{\rm sig}, p_{\rm test}, p_{\rm trash}, \beta, s)$ with $p_{\rm sig} + p_{\rm test} + p_{\rm trash} = 1$, where all the parameters are positive. Alice and Bob then run the protocol described in the following.

— Actual protocol —

1. Alice generates a random bit $a \in \{0, 1\}$ and sends an optical pulse $\tilde{C}$ in a coherent state with an amplitude $(-1)^a\sqrt{\mu}$ to Bob. She repeats it N times.

2. For each of the received N pulses, Bob chooses a label from $\{\text{signal}, \text{test}, \text{trash}\}$ with probabilities $p_{\rm sig}, p_{\rm test}$, and $p_{\rm trash}$, respectively. According to the label, Alice and Bob do one of the following procedures.

[signal] Bob performs a homodyne measurement on the received optical pulse C, and obtains an outcome $\check{q} \in \mathbb{R}$. Bob defines a bit b as $b = 0$ with a probability $f_{\rm suc}(\check{q})$ and $b = 1$ with a probability $f_{\rm suc}(-\check{q})$, and otherwise regards the round as "failure". The round in which Bob defines the bit b is regarded as "success". He announces success or failure of the detection. In the case of a success, Alice (resp. Bob) records a (b) as a sifted key bit.

[test] Bob performs a heterodyne measurement on the received optical pulse C, and obtains an outcome $\check{\alpha}$. Alice announces her bit a. Bob calculates the value of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$.

[trash] Alice and Bob produce no outcomes.

3. We refer to the numbers of "success" and "failure" signal rounds, test rounds, and trash rounds as $\check{N}^{\rm suc}, \check{N}^{\rm fail}, \check{N}^{\rm test}$, and $\check{N}^{\rm trash}$, respectively. ($N = \check{N}^{\rm suc} + \check{N}^{\rm fail} + \check{N}^{\rm test} + \check{N}^{\rm trash}$ holds by definition. Note also that the sifted key length of this protocol is equal to $\check{N}^{\rm suc}$.) Bob calculates the sum of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$ obtained in the $\check{N}^{\rm test}$ test rounds, which is denoted by $\check{F}$.

4. For the information reconciliation, they use $\check{N}_{\rm EC}$-bits of encrypted communication consuming a pre-shared secret key to do the following. According to (the upper bound on) the bit error rate $\check{e}_{\rm ub}$, Bob randomly chooses an error-correcting code and sends it with $\check{N}_{\rm EC}$ bits of syndrome to Alice. Alice reconciles her sifted key accordingly.

5. Bob computes and announces the final key length $\check{N}^{\rm fin}$ according to
$$\check{N}^{\rm fin} = \max\left\{\check{N}^{\rm suc} - \lceil \check{N}^{\rm suc} h(\check{p}')\rceil - s, 0\right\}, \tag{4.221}$$
where
$$\check{p}' \coloneqq \min\left\{U'(\check{F}, \check{N}^{\rm trash})/\check{N}^{\rm suc}, 1/2\right\}. \tag{4.222}$$
The function $U'(\check{F}, \check{N}^{\rm trash})$ will be specified later. Alice and Bob apply the privacy amplification using the dual universal$_2$ hashing to obtain the final key.

For simplicity, we omitted the bit error sampling rounds in the above protocol. In order to estimate an upper bound $\check{e}_{\rm ub}$ on the bit error rate with required correctness, Alice and Bob randomly insert $N_{\rm smp}$ sampling rounds among N rounds in which Bob performs the same measurement as that of the signal round. According to the observed discrepancies between Alice's and Bob's bits in the sampling rounds, Bob estimates the upper bound $\check{e}_{\rm ub}$ on the bit error rate with a failure probability no more than $\varepsilon_{\rm cor}/2$ and decides whether he aborts the protocol or not. The required amount of the error syndrome, $\check{N}_{\rm EC}$, that Bob sends to Alice in the information reconciliation step (Step 4) depends on the error correction method. Here we assume
$$\check{N}_{\rm EC} = \check{N}^{\rm suc}\left(f h(\check{e}_{\rm ub}) + (1-f)\right), \tag{4.223}$$
where $f \in [0,1]$ denotes a reconciliation efficiency of an error-correcting code [LBGP$^+$07, JEKJ14, GGDL19, LUL19, LLX$^+$21, WLM$^+$21] that succeeds with a probability no smaller than $1-\varepsilon_{\rm cor}/2$, when given the upper bound $\check{e}_{\rm ub}$ on the bit error rate. (To satisfy the condition, the error-correcting code with which one can show an upper bound on the failure probability has to be used.) The net key gain $\check{G}$ per pulse is thus given by
$$\check{G} = (\check{N}^{\rm fin} - \check{N}_{\rm EC})/(N + N_{\rm smp}). \tag{4.224}$$
We do not use verification in the post-processing, unlike Section 4.4, due to subtleties to incorporate it in our security proof. The acceptance probability $f_{\rm suc}(q)$ should be chosen to post-select the rounds with larger values of q, for which the bit error probability is expected to be lower. Note that the encryption of the $\check{N}_{\rm EC}$-bit syndrome at the information reconciliation step can be replaced with the $\check{N}_{\rm EC}$-bit additional privacy amplification as long as the syndrome bits Bob sends to Alice in the protocol linearly depend on Bob's sifted key. See the previous section for a detailed explanation.

4.5.2 Security proof based on the reverse reconciliation

We determine a sufficient amount of the privacy amplification according to the complementarity summarized in Sections 4.3.4 and 4.3.5 with the reverse reconciliation. To do so, we consider a virtual protocol in which Bob has a qubit for each success signal round such that the outcome of the Z-basis measurement on it coincides with his sifted key bit b. Alice can do arbitrary quantum operations in the virtual protocol as long as all the statistics and available information to the adversary Eve are the same as those in the actual protocol.

For Alice, we assume that a qubit A is introduced and the state in Eq. (4.115) is prepared in each round of the virtual protocol. Then, the optical quantum state emitted by Alice is the same as that in the actual protocol. For Bob, we adopt the same CP map $\mathcal{F}_{C\to B}$ defined in Eq. (4.116) to obtain a qubit B from the receive optical pulse C.

If the qubit B is successively measured on the Z basis, the obtained bit is equivalent to that in the signal round of the actual protocol.

At this point, one has the degree of freedom to perform quantum operations that do not change the value of the Z basis of the qubit B. Suppose that, after the qubit extraction map $\mathcal{F}_{C\to B}$ defined in Eq. (4.116), Alice and Bob performed a controlled-isometry $V_{BA\to BA'}$ that is defined as

$$V_{BA\to BA'} \coloneqq |0\rangle\langle 0|_B \otimes V^{(0)}_{A\to A'} + |1\rangle\langle 1|_B \otimes V^{(1)}_{A\to A'}, \tag{4.225}$$

where $V^{(i)}_{A\to A'}$ denotes an isometry from the system A to another system A' that is no smaller than A [1]. (Note that this corresponds to the twisting operation on the shield system [HLLO06, RS07, HHH$^+$08, HHHO09, BPLL20] since what we will show in the following is equivalent to showing that the system B is private (i.e., secret) to Eve with the shield system A'.) We thus introduce a virtual protocol in the sense of Section 4.3.4 that explicitly incorporates the action of $V_{BA\to BA'}$ in the following.

— Virtual protocol —

1′. Alice prepares a qubit A and an optical pulse $\tilde{C}$ in a state $|\Psi\rangle_{A\tilde{C}}$ defined in (4.115). She repeats it N times.

2′. For each of the received N pulses, Bob announces a label in the same way as that in Step 2. Alice and Bob do one of the following procedures according to the label.

[signal] Bob performs a quantum operation on the received pulse C specified by the CP map $\mathcal{F}_{C\to B}$ to determine success or failure of detection and to obtain qubit B upon success. He announces success or failure of detection. In the case of a success, Alice keeps her qubit A. Alice and Bob perform the controlled-isometry $V_{BA\to BA'}$ defined in Eq. (4.225).

[1] Here, the subtleties for using the verification come in. In order to know whether verification succeeds or not, Alice has to confirm the syndrome bits for the verification. However, this confirmation procedure may not commute with the action of $V_{BA\to BA'}$. Therefore, unless we evaluate how much the verification affects the secrecy condition, we cannot use the verification in this security proof.

[test] Bob performs a heterodyne measurement on the received optical pulse C, and obtains an outcome $\check{\alpha}$. Alice measures her qubit A on Z basis and announces the outcome $a \in \{0,1\}$. Bob calculates the value of $\Lambda_{m,r}(|\check{\alpha} - (-1)^a\beta|^2)$.

[trash] Alice measures her qubit A on X basis to obtain $a' \in \{+,-\}$.

3′. $\check{N}^{\rm suc}, \check{N}^{\rm fail}, \check{N}^{\rm test}, \check{N}^{\rm trash}$, and $\check{F}$ are defined in the same way as those in Step 3. Let $\check{Q}_-$ be the number of rounds in the $\check{N}^{\rm trash}$ trash rounds with $a' = -$.

4′. According to (the upper bound on) the bit error rate $\check{e}_{\rm ub}$, Bob uses $\check{N}_{\rm EC}$ bits of encrypted communication consuming a pre-shared secret key to send a dummy message to Alice.

5′. Bob computes and announces the final key length $\check{N}^{\rm fin}$ according to Eq. (4.221). Bob acts a randomly chosen unitary on his qubits and measures the first $\check{N}^{\rm fin}$ qubits on the Z bases.

To follow the security proof in Sections 4.3.4 and 4.3.5, suppose that, at the end of Step 3′ in the virtual protocol, Bob measured his $\check{N}^{\rm suc}$ qubits on the X basis $\{|+\rangle, |-\rangle\}$, and obtained a sequence $\check{\boldsymbol{x}}$ of '+' and '−'. The '−' in $\check{\boldsymbol{x}}$ is regarded as a phase error. If we can bound the number of possible phase-error patterns, then we can show the security from the argument in Section 4.3.5. In order to make the argument more rigorous, we define an estimation protocol as follows.

— **Estimation protocol** —

1″–3″. Same as Steps 1′, 2′, and 3′ of the virtual protocol.

4″. For every success signal round, Bob measures his qubit on the X basis and obtain an outcome $b' \in \{+,-\}$. Regarding + as zero and − as unity in the $\check{N}^{\rm suc}$ outcomes, define the $\check{N}^{\rm suc}$-bit sequence $\check{\boldsymbol{x}}$. Let $\check{N}'^{\rm suc}_{\rm ph} := {\rm wt}(\check{\boldsymbol{x}})$, where ${\rm wt}(\cdot)$ is defined in Eq. (4.4).

The task of proving the security of the actual protocol is then reduced to the construction of a function $U'(\check{F}, \check{N}^{\rm trash})$ that satisfies

$$\Pr\left[\check{N}'^{\rm suc}_{\rm ph} \le U'(\check{F}, \check{N}^{\rm trash})\right] \ge 1 - \epsilon \tag{4.226}$$

for any attack in the estimation protocol. In order to show that this is sufficient for the security proof, let $\mathcal{T}(\check{N}^{\rm suc}, \check{F}, \check{N}^{\rm trash})$ be the set of all the possible patterns for $\check{\boldsymbol{x}}$ with ${\rm wt}(\check{\boldsymbol{x}}) \le U'(\check{F}, \check{N}^{\rm trash})$. Then from Lemma 4.2.3, we have $\log|\mathcal{T}(\check{N}^{\rm suc}, \check{F}, \check{N}^{\rm trash})| \le N_{\rm PA}(\check{N}^{\rm suc}, \check{F}, \check{N}^{\rm trash})$ with

$$N_{\rm PA}(\check{N}^{\rm suc}, \check{F}, \check{N}^{\rm trash}) = \lceil \check{N}^{\rm suc} h(\check{p}') \rceil, \tag{4.227}$$

where $\check{p}'$ is defined in Eq. (4.222). With the same reasoning as the previous section, the condition (4.226) implies $\varepsilon_{\rm sec} = \sqrt{2(\epsilon + 2^{-s})}$-secrecy. Therefore, from now on, we focus on the estimation protocol.

4.5.3 Phase error operator

The number of phase errors depends on the choice of the controlled-isometry $V_{BA\to BA'}$ in the virtual and estimation protocol, and thus we aim to reduce the number of phase errors with a good choice of $V_{BA\to BA'}$. Here we heuristically choose $V_{BA\to BA'}$ so that the probability of the phase error event $b'=-$ in the estimation protocol is minimized for an ideal pure-loss channel (introduced in Section 3.1.3), which can be analytically investigated. We then use the same $V_{BA\to BA'}$ under the existence of excess noises, which is suboptimal but may still be a good choice when the excess noise is small.

When the state $|\Psi\rangle_{A\tilde{C}}$ in Eq. (4.115) is put into a pure-loss channel and the channel output is $|\pm\beta\rangle_C$, the resulting state $|\Phi\rangle_{ACE}$ on systems A, C, and an adversary's system E (i.e., environment of the pure-loss channel) is given by

$$|\Phi\rangle_{ACE}=\frac{1}{\sqrt{2}}\left(|0\rangle_A|\beta\rangle_C\left|\sqrt{\mu-\beta^2}\right\rangle_E+|1\rangle_A|-\beta\rangle_C\left|-\sqrt{\mu-\beta^2}\right\rangle_E\right). \tag{4.228}$$

Tracing out the system E, the reduced state Φ_{AC} is given by

$$\begin{aligned}\Phi_{AC}=&\frac{e^{-(\mu-\beta^2)}}{2}\Big(\cosh(\mu-\beta^2)\,\hat{P}\Big(|0\rangle_A|\beta\rangle_C+|1\rangle_A|-\beta\rangle_C\Big)\\&\qquad+\sinh(\mu-\beta^2)\,\hat{P}\Big(|0\rangle_A|\beta\rangle_C-|1\rangle_A|-\beta\rangle_C\Big)\Big)\end{aligned} \tag{4.229}$$

$$\begin{aligned}=&e^{-(\mu-\beta^2)}\Big(\cosh(\mu-\beta^2)\,\hat{P}\Big(|+\rangle_A\Pi_{\rm ev}|\beta\rangle_C+|-\rangle_A\Pi_{\rm od}|\beta\rangle_C\Big)\\&\qquad+\sinh(\mu-\beta^2)\,\hat{P}\Big(|+\rangle_A\Pi_{\rm od}|\beta\rangle_C+|-\rangle_A\Pi_{\rm ev}|\beta\rangle_C\Big)\Big),\end{aligned} \tag{4.230}$$

where $\hat{P}(\phi):=\phi\phi^\dagger$ (and thus $\hat{P}(|\phi\rangle)=|\phi\rangle\langle\phi|$). After Bob acts the qubit-extraction map $\mathcal{F}_{C\to B}$ defined in (4.116) to the state Φ_{AC} and obtains the subnormalized state $\tau_{AB}:=\mathcal{F}_{C\to B}(\Phi_{AC})$ with $p_{\rm suc}:=\mathrm{Tr}(\tau_{AB})$, he performs a controlled-isometry $V_{BA\to BA'}$ on τ_{AB}. The phase error probability can thus be given by

$$\mathrm{Tr}[|-\rangle\langle-|_B V_{BA\to BA'}\tau_{AB}V_{BA\to BA'}^\dagger] \tag{4.231}$$

$$\begin{aligned}=&\frac{1}{2}\mathrm{Tr}\Big[\langle0|_B\tau_{AB}|0\rangle_B+\langle1|_B\tau_{AB}|1\rangle_B\\&\quad-V_{A\to A'}^{(1)\dagger}V_{A\to A'}^{(0)}\langle0|_B\tau_{AB}|1\rangle_B-\langle1|_B\tau_{AB}|0\rangle_B V_{A\to A'}^{(1)}V_{A\to A'}^{(0)\dagger}\Big]\end{aligned} \tag{4.232}$$

$$=\frac{1}{2}p_{\rm suc}-\mathrm{Re}\left[\mathrm{Tr}\left(V_{A\to A'}^{(1)\dagger}V_{A\to A'}^{(0)}\langle0|_B\tau_{AB}|1\rangle_B\right)\right] \tag{4.233}$$

$$\geq\frac{1}{2}p_{\rm suc}-\|\langle0|_B\tau_{AB}|1\rangle_B\|_1, \tag{4.234}$$

where $V_{A\to A'}^{(i)}$ $(i=0,1)$ are defined in Eq. (4.225), and the last inequality follows from the matrix Hölder inequality. If we write the polar decomposition of $\langle0|_B\tau_{AB}|1\rangle_B$ by $W_A\left|\langle0|_B\tau_{AB}|1\rangle_B\right|$, the equality in (4.234) can be achieved by setting $V_{A\to A'}^{(1)\dagger}V_{A\to A'}^{(0)}=W_A^\dagger$. One can also check that $\langle0|_B\tau_{AB}|1\rangle_B$ is a real matrix on the Z basis, and therefore, W_A can be taken to be an orthogonal matrix on the Z basis (and thus on the X basis).

We will derive an explicit form of W_A as a function of μ and β. We first observe

that

$$\begin{aligned}
&\sigma_A^X \langle 0|_B \tau_{AB} |1\rangle_B \\
&= \frac{1}{2\sqrt{\pi}} \int_{-\infty}^{\infty} f_{\mathrm{suc}}(q) dq \left[e^{-2(\mu-\beta^2)} (e^{-(q+\sqrt{2}\beta)^2} |0\rangle\langle 0|_A + e^{-(q-\sqrt{2}\beta)^2} |1\rangle\langle 1|_A) \right. \\
&\qquad \left. + e^{-q^2-2\beta^2} (|1\rangle\langle 0|_A + |0\rangle\langle 1|_A) \right] \qquad (4.235) \\
&= \frac{1}{2} \left[a(\mu,\beta) |0\rangle\langle 0|_A + b(\mu,\beta) |1\rangle\langle 1|_A + c(\beta) (|1\rangle\langle 0|_A + |0\rangle\langle 1|_A) \right] \qquad (4.236)
\end{aligned}$$

with real positive functions $a(\mu,\beta)$, $b(\mu,\beta)$, and $c(\beta)$ defined as

$$a(\mu,\beta) = e^{-2(\mu-\beta^2)} G_{\frac{1}{2}} * f_{\mathrm{suc}}(-\sqrt{2}\beta), \qquad (4.237)$$

$$b(\mu,\beta) = e^{-2(\mu-\beta^2)} G_{\frac{1}{2}} * f_{\mathrm{suc}}(\sqrt{2}\beta), \qquad (4.238)$$

$$c(\beta) = e^{-2\beta^2} G_{\frac{1}{2}} * f_{\mathrm{suc}}(0), \qquad (4.239)$$

where $G_{\frac{1}{2}}(q) \coloneqq \exp(-q^2)/\sqrt{\pi}$ denotes the normal distribution with variance $1/2$, and $f * g$ denotes the convolution of the functions f and g. The matrix $\sigma_A^X \langle 0|_B \tau_{AB} |1\rangle_B$ is thus hermitian. If $a(\mu,\beta)b(\mu,\beta) - c(\beta)^2 \geq 0$ or equivalently $\mu \leq \mu_{\mathrm{th}}(\beta)$ with

$$\mu_{\mathrm{th}}(\beta) \coloneqq 2\beta^2 - \frac{1}{4} \ln \left(\frac{\left[G_{\frac{1}{2}} * f_{\mathrm{suc}}(0) \right]^2}{\left[G_{\frac{1}{2}} * f_{\mathrm{suc}}(\sqrt{2}\beta) \right] \left[G_{\frac{1}{2}} * f_{\mathrm{suc}}(-\sqrt{2}\beta) \right]} \right), \qquad (4.240)$$

then the matrix $\sigma_A^X \langle 0|_B \tau_{AB} |1\rangle_B$ is positive, which leads us to setting $W_A = \sigma_A^X$. When $W_A = \sigma_A^X$, the controlled-isometry $V_{BA\to BA'}$ is chosen to be the CNOT, and thus the security proof is completely reduced to the previous analysis in Section 4.4 with the operator inequality (4.253) given by Corollary 4.4.4. On the other hand, when $\mu > \mu_{\mathrm{th}}(\beta)$ (i.e., $a(\mu,\beta)b(\mu,\beta) - c(\beta)^2 < 0$), we rewrite Eq. (4.236) as

$$\sigma_A^X \langle 0|_B \tau_{AB} |1\rangle_B = \frac{D(\mu,\beta)}{4} \left[\frac{a(\mu,\beta) + b(\mu,\beta)}{D(\mu,\beta)} I_A + \cos\theta(\mu,\beta)\, \sigma_A^X + \sin\theta(\mu,\beta)\, \sigma_A^Z \right], \qquad (4.241)$$

where $D(\mu,\beta) \coloneqq \sqrt{[a(\mu,\beta) - b(\mu,\beta)]^2 + 4c(\beta)^2} (> 0)$, $[a(\mu,\beta) + b(\mu,\beta)]/D(\mu,\beta) < 1$, and $\theta(\mu,\beta)$ satisfies

$$|\theta(\mu,\beta)| < \pi/2 \quad \text{and} \quad \tan\theta(\mu,\beta) = \frac{a(\mu,\beta) - b(\mu,\beta)}{2c(\beta)}. \qquad (4.242)$$

It shows that we may choose W_A as

$$W_A = \sigma_A^X \left(\cos\theta(\mu,\beta) \sigma_A^X + \sin\theta(\mu,\beta) \sigma_A^Z \right) = \cos\theta(\mu,\beta) I_A - i \sin\theta(\mu,\beta) \sigma_A^Y \qquad (4.243)$$

because

$$\begin{aligned}
&W_A^\dagger \langle 0|_B \tau_{AB} |1\rangle_B \\
&= \frac{a(\mu,\beta) + b(\mu,\beta)}{4} \left[\frac{D(\mu,\beta)}{a(\mu,\beta) + b(\mu,\beta)} I_A + \cos\theta(\mu,\beta)\, \sigma_A^X + \sin\theta(\mu,\beta)\, \sigma_A^Z \right] \qquad (4.244)
\end{aligned}$$

is positive. From Eq. (4.242), the condition $\theta(\mu,\beta)=0$ and thus $W_A=I_A$ holds only when $a(\mu,\beta)=b(\mu,\beta)$, i.e.,

$$G_{\frac{1}{2}} * f_{\rm suc}(\sqrt{2}\beta) = G_{\frac{1}{2}} * f_{\rm suc}(-\sqrt{2}\beta), \tag{4.245}$$

which is false for reasonable choices of the acceptance probability $f_{\rm suc}(q)$ that post-select larger values of q. Thus, in the following, we consider the case $\mu>\mu_{\rm th}(\beta)$ and $0<|\theta(\mu,\beta)|<\pi/2$.

As we explained previously, we set $V^{(1)\dagger}_{A\to A'}V^{(0)}_{A\to A'}=W_A^\dagger$ also for arbitrary channels, i.e., arbitrary coherent attacks by Eve. This choice of $V_{BA\to BA'}$ is not optimal for general channels but is expected to be close to the optimal for channels that are close to the pure loss. Now that the controlled-isometry $V_{BA\to BA'}$ is fixed, we can clarify using Eq. (4.231) what combination of measurement events on Alice's qubit A and the optical pulse C leads to the phase error $b'=-$ in the estimation protocol. The operator $M'^{\rm suc}_{\rm ph}$ on the system A and C that corresponds to the phase error event is given by

$$M'^{\rm suc}_{\rm ph} \coloneqq \mathcal{F}^\dagger_{C\to B}\Big(V^\dagger_{BA\to BA'}(|-\rangle\langle -|_B\otimes I_{A'})V_{BA\to BA'}\Big), \tag{4.246}$$

where $\mathcal{F}^\dagger_{C\to B}$ denotes the adjoint map of $\mathcal{F}_{C\to B}$ given explicitly by

$$\mathcal{F}^\dagger_{C\to B}(M_B)=\int_{-\infty}^{\infty} dq\, K^{(q)\dagger}M_BK^{(q)}. \tag{4.247}$$

Using the expression (4.117) of $K^{(q)}$, we have

$$\begin{aligned}
M'^{\rm suc}_{\rm ph} &= \frac{1}{2}\mathcal{F}^\dagger_{C\to B}\left(\hat{P}\Big(V^{(0)\dagger}_{A\to A'}\otimes|0\rangle_B - V^{(1)\dagger}_{A\to A'}\otimes|1\rangle_B\Big)\right) && (4.248)\\
&= \frac{1}{2}\mathcal{F}^\dagger_{C\to B}\left(I_{AB}-W_A\otimes|0\rangle\langle 1|_B - W_A^\dagger\otimes|1\rangle\langle 0|_B\right) && (4.249)\\
&= \frac{1}{4}\mathcal{F}^\dagger_{C\to B}\left(\hat{P}\Big(I_A\otimes(|+\rangle_B+|-\rangle_B)-W_A^\dagger\otimes(|+\rangle_B-|-\rangle_B)\Big)\right) && (4.250)\\
&= \int_{-\infty}^{\infty}2f_{\rm suc}(q)dq\,\hat{P}\left(\frac{I_A-W_A^\dagger}{2}\otimes\Pi_{\rm ev}|q\rangle_C+\frac{I_A+W_A^\dagger}{2}\otimes\Pi_{\rm od}|q\rangle_C\right). && (4.251)
\end{aligned}$$

Once the phase error operator can be defined on systems A and C, we can follow essentially the same analysis as that in Section 4.4, replacing $M^{\rm suc}_{\rm ph}$ with $M'^{\rm suc}_{\rm ph}$. This also leads to replacing $M[\kappa,\gamma]$ with $M'[\kappa,\gamma]$ defined as

$$M'[\kappa,\gamma]\coloneqq M'^{\rm suc}_{\rm ph}+\kappa\Pi^{\rm fid}-\gamma\Pi^{\rm trash}_-, \tag{4.252}$$

where $\Pi^{\rm fid}$ and $\Pi^{\rm trash}_-$ are defined in Eqs. (4.129) and (4.130). Then, the only difference to proceed the security proof is the operator inequality (4.138); we alternatively need to show

$$M'[\kappa,\gamma]\le B'(\kappa,\gamma)I_{AC}, \tag{4.253}$$

with a computable function $B'(\kappa,\gamma)$. Eq. (4.253) will be shown in the next section.

Once we obtain $B'(\kappa,\gamma)$, following the same line of argument as that in Section 4.4 leads to the definition of

$$U'(\check{F},\check{N}^{\rm trash})=p_{\rm sig}(NB'(\kappa,\gamma)+\delta_1(\epsilon/2))-\frac{p_{\rm sig}}{p_{\rm test}}\kappa\check{F}+\frac{p_{\rm sig}}{p_{\rm trash}}\gamma\Big(\check{N}^{\rm trash}q_-+\delta_2(\epsilon/2;\check{N}^{\rm trash})\Big), \tag{4.254}$$

which achieves $\sqrt{2(\epsilon+2^{-s})}$-secrecy. Thus, we complete the finite-size security proof based on the reverse reconciliation for this alternative protocol.

4.5.4 Proof of the operator inequality

In this section, we prove the inequality (4.253) used in the security proof. We first prove the following lemma.

Lemma 4.5.1. *Let $\Pi_\pm$ be orthogonal projections which have rank no smaller than three or infinite. Let M be a self-adjoint operator satisfying $M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-) \leq \alpha(\Pi_+ + \Pi_-)$, where α is a real constant. Let $|\psi\rangle$ be a vector satisfying $(\Pi_+ + \Pi_-)|\psi\rangle = |\psi\rangle$ and $\Pi_\pm|\psi\rangle \neq 0$. Assume $\Pi_+|\psi\rangle$ is not proportional to the eigenvectors of $\Pi_\pm M \Pi_+$ (if they have). Define the following quantities with respect to $|\psi\rangle$:*

$$C_\pm \coloneqq \langle\psi|\Pi_\pm|\psi\rangle \ (>0), \tag{4.255}$$

$$\lambda_{\pm\pm} \coloneqq C_\pm^{-1}\langle\psi|M_{\pm\pm}|\psi\rangle, \tag{4.256}$$

$$\lambda_{+-} \coloneqq (C_+C_-)^{-\frac{1}{2}}\langle\psi|M_{+-}|\psi\rangle, \qquad \lambda_{-+} \coloneqq \lambda_{+-}^*, \tag{4.257}$$

$$\sigma_{\pm+} \coloneqq \left(C_+^{-1}\|M_{\pm+}|\psi\rangle\|^2 - |\lambda_{\pm+}|^2\right)^{\frac{1}{2}} \ (>0), \tag{4.258}$$

$$\sigma_{\pm-} \coloneqq \sigma_{\pm+}^{-1}\left((C_+C_-)^{-\frac{1}{2}}\langle\psi|M_{+\pm}M_{\pm-}|\psi\rangle - \lambda_{+-}\lambda_{\pm\pm}\right), \tag{4.259}$$

$$\Delta_{\pm-} \coloneqq \left(C_-^{-1}\|M_{\pm-}|\psi\rangle\|^2 - |\lambda_{\pm-}|^2 - |\sigma_{\pm-}|^2\right)^{\frac{1}{2}}, \tag{4.260}$$

where M_{++}, M_{--}, M_{+-}, and M_{-+} are given respectively by

$$M_{\pm\pm} \coloneqq \Pi_\pm M \Pi_\pm, \quad M_{+-} \coloneqq \Pi_+ M \Pi_-, \quad M_{-+} \coloneqq M_{+-}^\dagger. \tag{4.261}$$

Then, for any real numbers $\gamma_\pm$, we have

$$\lambda_{\sup}(M + |\psi\rangle\langle\psi| - \gamma_+\Pi_+ - \gamma_-\Pi_-) \leq \lambda_{\sup}(M_{6\mathrm{d}}), \tag{4.262}$$

where $M_{6\mathrm{d}}$ is given by

$$M_{6\mathrm{d}} \coloneqq \begin{pmatrix} \alpha-\gamma_+ & 0 & 0 & \Delta_{+-} & 0 & 0 \\ 0 & \alpha-\gamma_+ & \sigma_{++} & \sigma_{+-} & 0 & 0 \\ 0 & \sigma_{++} & C_+ + \lambda_{++} - \gamma_+ & \sqrt{C_+C_-} + \lambda_{+-} & \sigma_{-+} & 0 \\ \Delta_{+-} & \sigma_{+-}^* & \sqrt{C_+C_-} + \lambda_{-+} & C_- + \lambda_{--} - \gamma_- & \sigma_{--}^* & \Delta_{--} \\ 0 & 0 & \sigma_{-+} & \sigma_{--} & \alpha-\gamma_- & 0 \\ 0 & 0 & 0 & \Delta_{--} & 0 & \alpha-\gamma_- \end{pmatrix}. \tag{4.263}$$

Proof. We choose orthonormal vectors $\{|e_\pm^{(1)}\rangle, |e_\pm^{(2)}\rangle, |e_\pm^{(3)}\rangle\}$ in the domains of $\Pi_\pm$, respectively, to satisfy

$$\sqrt{C_\pm}\left|e_\pm^{(1)}\right\rangle = \Pi_\pm|\psi\rangle, \tag{4.264}$$

$$M\left|e_+^{(1)}\right\rangle = (M_{++}+M_{-+})\left|e_+^{(1)}\right\rangle = \lambda_{++}\left|e_+^{(1)}\right\rangle + \sigma_{++}\left|e_+^{(2)}\right\rangle + \lambda_{-+}\left|e_-^{(1)}\right\rangle + \sigma_{-+}\left|e_-^{(2)}\right\rangle, \tag{4.265}$$

$$M\left|e_-^{(1)}\right\rangle = (M_{+-}+M_{--})\left|e_-^{(1)}\right\rangle = \lambda_{+-}\left|e_+^{(1)}\right\rangle + \sigma_{+-}\left|e_+^{(2)}\right\rangle + \Delta_{+-}\left|e_+^{(3)}\right\rangle \tag{4.266}$$

$$+ \lambda_{--}\left|e_-^{(1)}\right\rangle + \sigma_{--}\left|e_-^{(2)}\right\rangle + \Delta_{--}\left|e_-^{(3)}\right\rangle, \tag{4.267}$$

which is well-defined due to Eqs. (4.255)–(4.261) and $M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-)$. Actually, Eqs. (4.258)–(4.260) are derived by taking inner product of appropriate pairs among $M_{\pm\pm}|\psi\rangle$ and $M_{\pm\mp}|\psi\rangle$. Overall phases of $|e_\pm^{(2)}\rangle$ and $|e_\pm^{(3)}\rangle$ are taken so that $\sigma_{\pm+}$ and $\Delta_{\pm-}$ are non-negative. Since $\Pi_+|\psi\rangle$ is not proportional to the eigenvectors of $\Pi_\pm M \Pi_+$ by assumption, we have $\sigma_{\pm+} > 0$. From $(\Pi_+ + \Pi_-)|\psi\rangle = |\psi\rangle$, we have

$$|\psi\rangle = \sqrt{C_+}\left|e_+^{(1)}\right\rangle + \sqrt{C_-}\left|e_-^{(1)}\right\rangle. \tag{4.268}$$

Let us now define following projection operators:

$$\Pi_\pm^{(j)} := \left|e_\pm^{(j)}\right\rangle\!\left\langle e_\pm^{(j)}\right| \quad (j = 1, 2, 3), \tag{4.269}$$

$$\Pi_\pm^{(\geq 2)} := \Pi_\pm - \Pi_\pm^{(1)}, \tag{4.270}$$

$$\Pi_\pm^{(\geq 4)} := \Pi_\pm^{(\geq 2)} - \Pi_\pm^{(2)} - \Pi_\pm^{(3)}. \tag{4.271}$$

Since Eqs. (4.265) and (4.267) imply $(\Pi_+^{(\geq 4)} + \Pi_-^{(\geq 4)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) = 0$, we have

$$M = (\Pi_+ + \Pi_-)M(\Pi_+ + \Pi_-) \tag{4.272}$$

$$\begin{aligned} &= (\Pi_+^{(1)} + \Pi_-^{(1)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) + (\Pi_+^{(2)} + \Pi_+^{(3)} + \Pi_-^{(2)} + \Pi_-^{(3)})M(\Pi_+^{(1)} + \Pi_-^{(1)}) \\ &\quad + (\Pi_+^{(1)} + \Pi_-^{(1)})M(\Pi_+^{(2)} + \Pi_+^{(3)} + \Pi_-^{(2)} + \Pi_-^{(3)}) + (\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)})M(\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)}) \end{aligned} \tag{4.273}$$

$$\begin{aligned} &\leq \lambda_{++}\Pi_+^{(1)} + \lambda_{--}\Pi_-^{(1)} + \lambda_{+-}\left|e_+^{(1)}\right\rangle\!\left\langle e_-^{(1)}\right| + \lambda_{-+}\left|e_-^{(1)}\right\rangle\!\left\langle e_+^{(1)}\right| \\ &\quad + \Big(\sigma_{++}\left|e_+^{(2)}\right\rangle\!\left\langle e_+^{(1)}\right| + \sigma_{-+}\left|e_-^{(2)}\right\rangle\!\left\langle e_+^{(1)}\right| + \sigma_{+-}\left|e_+^{(2)}\right\rangle\!\left\langle e_-^{(1)}\right| \\ &\qquad + \Delta_{+-}\left|e_+^{(3)}\right\rangle\!\left\langle e_-^{(1)}\right| + \sigma_{--}\left|e_-^{(2)}\right\rangle\!\left\langle e_-^{(1)}\right| + \Delta_{--}\left|e_-^{(3)}\right\rangle\!\left\langle e_-^{(1)}\right|\Big) + (\quad \text{h.c.} \quad) \\ &\quad + \alpha(\Pi_+^{(\geq 2)} + \Pi_-^{(\geq 2)}), \end{aligned} \tag{4.274}$$

where h.c. denotes the hermitian conjugates of the terms in the preceding parenthesis. The last inequality comes from $M \leq \alpha(\Pi_+ + \Pi_-)$. Using Eq. (4.274), we have

$$M + |\psi\rangle\langle\psi| - \gamma_+\Pi_+ - \gamma_-\Pi_- \leq M_{6\mathrm{d}} \oplus (\alpha - \gamma_+)\Pi_+^{(\geq 4)} \oplus (\alpha - \gamma_-)\Pi_-^{(\geq 4)}, \tag{4.275}$$

where $M_{6\mathrm{d}}$ is given in Eq. (4.263) with the basis $\{|e_+^{(3)}\rangle, |e_+^{(2)}\rangle, |e_+^{(1)}\rangle, |e_-^{(1)}\rangle, |e_-^{(2)}\rangle, |e_-^{(3)}\rangle\}$. Since $\alpha - \gamma_\pm = \langle e_\pm^{(3)}| M_{6\mathrm{d}} |e_\pm^{(3)}\rangle \leq \lambda_{\sup}(M_{6\mathrm{d}})$, the supremum of the spectrum of the right-hand side of Eq. (4.275) is equal to the maximum eigenvalue of the six-dimensional matrix $M_{6\mathrm{d}}$. We then obtain Eq. (4.262). □

As a corollary of this lemma, we obtain the following.

Corollary 4.5.2. *Let $|\beta\rangle$ be a coherent state. Let $\mu_{\mathrm{th}}(\beta)$ and $\theta(\mu, \beta)$ be as defined in Eqs.* (4.240) *and* (4.242)*, respectively. Suppose $\mu > \mu_{\mathrm{th}}(\beta)$ and $\theta(\mu, \beta) \neq 0$. Let $\Pi_{\mathrm{ev(od)}}$ and $M'[\kappa, \gamma]$ be as defined in Section 4.5.3 with W_A given in Eq.* (4.243)*. Let $M_{\mathrm{ee}}^{\mathrm{suc}}$, $M_{\mathrm{oo}}^{\mathrm{suc}}$, $M_{\mathrm{eo}}^{\mathrm{suc}}$, and $M_{\mathrm{oe}}^{\mathrm{suc}}$ be defined as follows:*

$$M_{\mathrm{ee}}^{\mathrm{suc}} := \int_{-\infty}^{\infty} 2f_{\mathrm{suc}}(q)dq\, \Pi_{\mathrm{ev}}|q\rangle\langle q|\Pi_{\mathrm{ev}}, \tag{4.276}$$

$$M_{\mathrm{oo}}^{\mathrm{suc}} := \int_{-\infty}^{\infty} 2f_{\mathrm{suc}}(q)dq\, \Pi_{\mathrm{od}}|q\rangle\langle q|\Pi_{\mathrm{od}}, \tag{4.277}$$

$$M_{\mathrm{eo}}^{\mathrm{suc}} := \int_{-\infty}^{\infty} 2f_{\mathrm{suc}}(q)dq\, \Pi_{\mathrm{ev}}|q\rangle\langle q|\Pi_{\mathrm{od}}, \tag{4.278}$$

$$M_{\mathrm{oe}}^{\mathrm{suc}} := M_{\mathrm{eo}}^{\mathrm{suc}\dagger}. \tag{4.279}$$

Define the following (real) parameters:

$$w_+ \coloneqq \frac{1+\cos\theta(\mu,\beta)}{2}, \quad w_- \coloneqq \frac{1-\cos\theta(\mu,\beta)}{2}, \quad w_z \coloneqq \frac{\sin\theta(\mu,\beta)}{2}, \tag{4.280}$$

$$C_{\rm o} \coloneqq \langle\beta|\,\Pi_{\rm od}\,|\beta\rangle = e^{-|\beta|^2}\sinh|\beta|^2, \quad C_{\rm e} \coloneqq \langle\beta|\,\Pi_{\rm ev}\,|\beta\rangle = e^{-|\beta|^2}\cosh|\beta|^2, \tag{4.281}$$

$$\lambda_{\rm oo} \coloneqq \frac{w_+}{C_{\rm o}}\langle\beta|\,M_{\rm oo}^{\rm suc}\,|\beta\rangle, \quad \lambda_{\rm ee} \coloneqq \frac{w_-}{C_{\rm e}}\langle\beta|\,M_{\rm ee}^{\rm suc}\,|\beta\rangle, \tag{4.282}$$

$$\lambda_{\rm oe} \coloneqq \frac{w_z}{\sqrt{C_{\rm o}C_{\rm e}}}\langle\beta|\,M_{\rm oe}^{\rm suc}\,|\beta\rangle, \quad \lambda_{\rm eo} \coloneqq \frac{w_z}{\sqrt{C_{\rm o}C_{\rm e}}}\langle\beta|\,M_{\rm eo}^{\rm suc}\,|\beta\rangle = \lambda_{\rm oe}^*, \tag{4.283}$$

$$\sigma_{\rm oo} \coloneqq \left(\frac{w_+^2}{C_{\rm o}}\|M_{\rm oo}^{\rm suc}\,|\beta\rangle\,\|^2 - \lambda_{\rm oo}^2\right)^{\frac{1}{2}}, \quad \sigma_{\rm eo} \coloneqq \left(\frac{w_z^2}{C_{\rm o}}\|M_{\rm eo}^{\rm suc}\,|\beta\rangle\,\|^2 - \lambda_{\rm eo}^2\right)^{\frac{1}{2}}, \tag{4.284}$$

$$\sigma_{\rm oe} \coloneqq \sigma_{\rm oo}^{-1}\left(\frac{w_+w_z}{\sqrt{C_{\rm o}C_{\rm e}}}\langle\beta|\,M_{\rm oo}^{\rm suc}M_{\rm oe}^{\rm suc}\,|\beta\rangle - \lambda_{\rm oo}\lambda_{\rm oe}\right), \tag{4.285}$$

$$\sigma_{\rm ee} \coloneqq \sigma_{\rm eo}^{-1}\left(\frac{w_-w_z}{\sqrt{C_{\rm o}C_{\rm e}}}\langle\beta|\,M_{\rm oe}^{\rm suc}M_{\rm ee}^{\rm suc}\,|\beta\rangle - \lambda_{\rm oe}\lambda_{\rm ee}\right), \tag{4.286}$$

$$\Delta_{\rm oe} \coloneqq \left(\frac{w_z^2}{C_{\rm e}}\|M_{\rm oe}^{\rm suc}\,|\beta\rangle\,\|^2 - \lambda_{\rm oe}^2 - \sigma_{\rm oe}^2\right)^{\frac{1}{2}}, \quad \Delta_{\rm ee} \coloneqq \left(\frac{w_-^2}{C_{\rm e}}\|M_{\rm ee}^{\rm suc}\,|\beta\rangle\,\|^2 - \lambda_{\rm ee}^2 - \sigma_{\rm ee}^2\right)^{\frac{1}{2}}. \tag{4.287}$$

Define the following two matrices $M_{\rm 6d}^{(0)}$ and $M_{\rm 6d}^{(1)}$.

$$M_{\rm 6d}^{(0)} \coloneqq \begin{pmatrix} 1 & 0 & 0 & \Delta_{\rm oe} & 0 & 0 \\ 0 & 1 & \sigma_{\rm oo} & \sigma_{\rm oe} & 0 & 0 \\ 0 & \sigma_{\rm oo} & \kappa C_{\rm o}+\lambda_{\rm oo} & \kappa\sqrt{C_{\rm o}C_{\rm e}}+\lambda_{\rm oe} & \sigma_{\rm eo} & 0 \\ \Delta_{\rm oe} & \sigma_{\rm oe} & \kappa\sqrt{C_{\rm o}C_{\rm e}}+\lambda_{\rm eo} & \kappa C_{\rm e}+\lambda_{\rm ee}-\gamma & \sigma_{\rm ee} & \Delta_{\rm ee} \\ 0 & 0 & \sigma_{\rm eo} & \sigma_{\rm ee} & 1-\gamma & 0 \\ 0 & 0 & 0 & \Delta_{\rm ee} & 0 & 1-\gamma \end{pmatrix}, \tag{4.288}$$

$$M_{\rm 6d}^{(1)} \coloneqq \begin{pmatrix} 1-\gamma & 0 & 0 & \Delta_{\rm oe} & 0 & 0 \\ 0 & 1-\gamma & \sigma_{\rm oo} & -\sigma_{\rm oe} & 0 & 0 \\ 0 & \sigma_{\rm oo} & \kappa C_{\rm o}+\lambda_{\rm oo}-\gamma & \kappa\sqrt{C_{\rm o}C_{\rm e}}-\lambda_{\rm oe} & \sigma_{\rm eo} & 0 \\ \Delta_{\rm oe} & -\sigma_{\rm oe} & \kappa\sqrt{C_{\rm o}C_{\rm e}}-\lambda_{\rm eo} & \kappa C_{\rm e}+\lambda_{\rm ee} & -\sigma_{\rm ee} & \Delta_{\rm ee} \\ 0 & 0 & \sigma_{\rm eo} & -\sigma_{\rm ee} & 1 & 0 \\ 0 & 0 & 0 & \Delta_{\rm ee} & 0 & 1 \end{pmatrix}. \tag{4.289}$$

Define a convex function

$$B'(\kappa,\gamma) \coloneqq \max\{\lambda_{\rm sup}(M_{\rm 6d}^{(0)}), \lambda_{\rm sup}(M_{\rm 6d}^{(1)})\}. \tag{4.290}$$

Then, for $\kappa,\gamma \geq 0$, we have

$$M'[\kappa,\gamma] \leq B'(\kappa,\gamma)I_{AC}. \tag{4.291}$$

Proof. From the form of W_A in Eq. (4.243), we have

$$\left\| \frac{I+W_A}{2} |+\rangle \right\|^2 = \left\| \frac{I+W_A}{2} |-\rangle \right\|^2 = \frac{1+\cos\theta(\mu,\beta)}{2} = w_+, \tag{4.292}$$

$$\left\| \frac{I-W_A}{2} |-\rangle \right\|^2 = \left\| \frac{I-W_A}{2} |+\rangle \right\|^2 = \frac{1-\cos\theta(\mu,\beta)}{2} = w_-, \tag{4.293}$$

$$\begin{aligned} &- \langle -| \frac{I+W_A^\dagger}{2} \frac{I-W_A}{2} |+\rangle = - \langle +| \frac{I-W_A^\dagger}{2} \frac{I+W_A}{2} |-\rangle \\ &= \langle +| \frac{I+W_A^\dagger}{2} \frac{I-W_A}{2} |-\rangle = \langle -| \frac{I-W_A^\dagger}{2} \frac{I+W_A}{2} |+\rangle = \frac{\sin\theta(\mu,\beta)}{2} = w_z, \end{aligned} \tag{4.294}$$

where $w_\pm$ are positive due to $0 < |\theta(\mu,\beta)| < \pi/2$. Since $\sigma_A^X W_A = W_A^\dagger \sigma_A^X$ holds, the operator acted by $\mathcal{F}_{C\to B}^\dagger(\cdot)$ in Eq. (4.249) commutes with $\sigma_A^X \otimes \sigma_B^X$. Due to the form of $\mathcal{F}_{C\to B}^\dagger(\cdot)$, this means that $M'^{\mathrm{suc}}_{\mathrm{ph}}$ commutes with $\sigma_A^X \otimes \exp(\pi i \hat{n}_C)$, and so does $M'[\kappa,\gamma]$. Therefore, we have

$$M'[\kappa,\gamma] = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} + \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}, \tag{4.295}$$

where two orthogonal projections $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$ are defined as

$$\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} \coloneqq |+\rangle\langle+|_A \otimes \Pi_{\mathrm{od}} + |-\rangle\langle-|_A \otimes \Pi_{\mathrm{ev}} \tag{4.296}$$

$$\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} \coloneqq |-\rangle\langle-|_A \otimes \Pi_{\mathrm{od}} + |+\rangle\langle+|_A \otimes \Pi_{\mathrm{ev}}. \tag{4.297}$$

Then we apply Lemma 4.5.1 to the operators $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$ and $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$, respectively. For $\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})}$, we set

$$\Pi_\pm = |\pm\rangle\langle\pm|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{4.298}$$

$$M = \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{suc}} \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} \tag{4.299}$$

$$= w_+ |+\rangle\langle+| \otimes M_{\mathrm{oo}}^{\mathrm{suc}} + w_- |-\rangle\langle-| \otimes M_{\mathrm{ee}}^{\mathrm{suc}} + w_z \left(|+\rangle\langle-| \otimes M_{\mathrm{oe}}^{\mathrm{suc}} + |-\rangle\langle+| \otimes M_{\mathrm{eo}}^{\mathrm{suc}} \right), \tag{4.300}$$

$$|\psi\rangle = \sqrt{\kappa} |\phi_{\mathrm{err}}\rangle_{AC}, \tag{4.301}$$

$$\alpha = 1, \quad \gamma_+ = 0, \quad \gamma_- = \gamma, \tag{4.302}$$

where $|\phi_{\mathrm{err}}\rangle_{AC}$ is defined in Eq. (4.188). Since so-defined M only has continuous spectrum, we can apply Lemma 4.5.1 and obtain

$$\lambda_{\sup}\left(\Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(+,\mathrm{od}),(-,\mathrm{ev})} \right) \leq \lambda_{\sup}(M_{\mathrm{6d}}^{(0)}). \tag{4.303}$$

In the same way, we apply Lemma 4.5.1 to $\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M'[\kappa,\gamma] \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}$ by setting

$$\Pi_\pm = |\mp\rangle\langle\mp|_A \otimes \Pi_{\mathrm{od(ev)}}, \tag{4.304}$$

$$M = \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M_{\mathrm{ph}}^{\mathrm{suc}} \Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} \tag{4.305}$$

$$= w_- |-\rangle\langle-| \otimes M_{\mathrm{oo}}^{\mathrm{suc}} + w_+ |+\rangle\langle+| \otimes M_{\mathrm{ee}}^{\mathrm{suc}} - w_z \left(|-\rangle\langle+| \otimes M_{\mathrm{oe}}^{\mathrm{suc}} + |+\rangle\langle-| \otimes M_{\mathrm{eo}}^{\mathrm{suc}} \right), \tag{4.306}$$

$$|\psi\rangle = \sqrt{\kappa} |\phi_{\mathrm{cor}}\rangle_{AC}, \tag{4.307}$$

$$\alpha = 1, \quad \gamma_+ = \gamma, \quad \gamma_- = 0, \tag{4.308}$$

where $|\phi_{\rm cor}\rangle_{AC}$ is defined in Eq. (4.189). Then, we observe

$$\lambda_{\sup}\Big(\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})} M'[\kappa,\gamma]\Pi_{AC}^{(-,\mathrm{od}),(+,\mathrm{ev})}\Big) \leq \lambda_{\sup}(M_{\mathrm{6d}}^{(1)}). \tag{4.309}$$

Combining inequalities (4.303) and (4.309) completes the proof. □

4.5.5 Numerical simulations

We compute (the lower bound of) the net key gain per pulse (i.e., key rate $\check{G}$) against the transmission distance L with various values of excess noise ξ at the channel output. The channel model is the same as that in Section 4.4. For simplicity, the number $N_{\rm smp}$ of the sampling rounds is set to be $N/100$, and the bit error correction efficiency f is to be 0.95. The acceptance probability $f_{\rm suc}(q)$ is assumed to be a step function with the threshold $q_{\rm th}(>0)$, i.e., $\Theta(q-q_{\rm th})$. The expected amplitude of coherent state β is chosen to be $\sqrt{\eta\mu}$. We set the security parameter $\varepsilon_{\rm sct}=2^{-50}$, and set $\varepsilon_{\rm cor}=\varepsilon_{\rm sec}=\varepsilon_{\rm sct}/2$ and $\epsilon=2^{-s}=\varepsilon_{\rm sec}^2/4$.

We set $\check{N}^{\rm suc}$, $\check{F}$, $\check{N}^{\rm test}$, and $\check{N}^{\rm trash}$ in the same way as in Section 4.4. We adopted $m=1$ and $r=0.4120$ for the function $\Lambda_{m,r}$, which leads to $(\sup\Lambda_{m,r},\inf\Lambda_{m,r})=(2.824,-0.9932)$. We assume that the number of "success" sampling rounds $\check{N}_{\rm smp}^{\rm suc}$ is equal to its expectation value $(P^+ + P^-)N_{\rm smp}$, where $P^{\pm}$ are defined in Eq (4.217). We further assume that the number of bit errors $\check{E}_{\rm obs}$ observed in the sampling rounds is equal to its expectation value $P^- N_{\rm smp}$. The upper bound $\check{e}_{\rm ub}$ on the bit error rate is thus set to be

$$\check{e}_{\rm ub} = \Big(\lceil \hat{M}_{\check{N}^{\rm suc}+\check{N}_{\rm smp}^{\rm suc},\check{N}_{\rm smp}^{\rm suc},\varepsilon_{\rm cor}/2}(\check{E}_{\rm obs})\rceil - \check{E}_{\rm obs}\Big)/\check{N}^{\rm suc}, \tag{4.310}$$

where $\hat{M}_{N,n,\epsilon}$ is defined in Corollary 4.2.12.

Under these assumptions, remaining parameters to be determined are two coefficients (κ,γ) and four protocol parameters $(\mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$, which is the same as in Section 4.4. We determined (κ,γ) via a convex optimization using CVXPY 1.0.25 and $(\mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$ via the Nelder-Mead in the scipy.minimize library in Python, for each transmission distance L.

Figures 4.9 and 4.10 show the key rates against transmission distance over an optical fiber with the attenuation rate η assumed to be $10^{-0.02L}$. Figure 4.9 shows that under the condition of low excess noise ($\xi=0$–$10^{-4.0}$), our refined analysis offers higher key rates and longer transmission distance than that of the previous section even in the finite-key case. Furthermore, as shown in Figure 4.10 a, the logarithm of the asymptotic key rate in the pure-loss case (i.e., $\xi=0$) achieves almost linear scaling against transmission distance, which is known to be an optimal scaling allowed in the pure-loss channel. However, when the excess noise ξ is as high as $10^{-3.0}$, the improvements in our refined analysis are almost lost as shown in Figures 4.9 b and 4.10 b. Compared to four-state variants of the protocol that are previously studied [GGDL19, LUL19, LLX+21], our binary-modulation protocol is still fragile against excess noises.

Examples of optimized parameters are shown in Table 4.2. Overall, the key rates in Table 4.2 are better than those in Table 4.1 especially for the long transmission distances. Typical optimized values of the threshold $q_{\rm th}$ range from 0.7 to 1.2, which are larger than those of other analyses of protocols with post-selection (e.g., [LUL19])

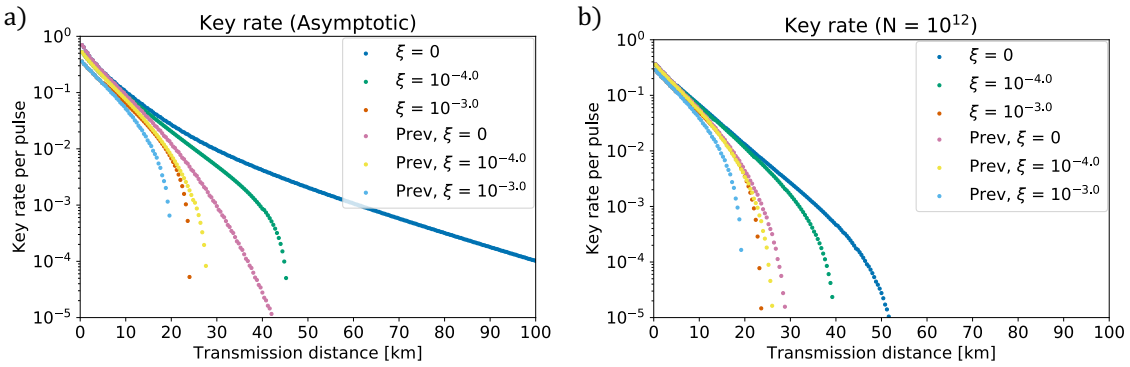

Figure 4.9: The net key gain per pulse $\check{G}$ (key rate) against the transmission distance L of the optical channel with the refined security analysis in this section and the previous analysis in Section 4.4. We assumed that the optical pulse that Bob receives is given by randomly displacing a coherent state to increase its variance by a factor of $(1+\xi)$. a) The asymptotic key rate for various values of ξ. In the figure, "Prev" denotes the key rate computed with the previous analysis in Section 4.4 while $\check{N}_{\mathrm{EC}}$ is given in Eq. (4.223). b) The key rate for various values of ξ when the pulse number is finite ($N = 10^{12}$). "Prev" denotes that with the previous analysis.

but smaller than those in Section 4.4. The intensities μ of the input coherent states are smaller in Table 4.2 than those in Table 4.1 for the longer transmission distances. Taking smaller intensities for longer transmission distances may be the characteristic feature of this analysis; optimal intensities for other asymptotic analyses are around 0.1–0.4 for over 100 km transmission distances [GGDL19, LUL19, LLX+21].

4.5.6 Discussion

We proposed a refined security analysis for the protocol proposed in Section 4.4 based on the reverse reconciliation. The motivating ideas of our refinement come from the facts that the secret key can be distilled from the states from which the entanglement cannot be distilled [HLLO06, RS07, HHH+08, Ren08, HHHO09, Koa09] and the reverse reconciliation can increase the key rate for continuous-variable QKD protocols [SRLL02]. To exploit the ideas, we developed the procedure of "twisting" Alice's system with the isometry $V_{BA\to BA'}$ controlled by the Z basis of Bob's qubit, while the techniques derived from similar ideas have already appeared in previous works [HLLO06, Ren08, HHH+08, HHHO09, Koa09, BPLL20]. Our finding is that, by using the twisting operation that minimizes the phase error probability for the pure-loss channel, the protocol has asymptotically almost optimal scaling in the key rates. This is the clear distinction from the result in Section 4.4; there, the logarithm of the asymptotic key rate non-linearly decreases against transmission distance. The improvement in the performance remains in the finite-key case but is lost under the existence of excess noise as high as $\xi = 10^{-3.0}$ at the channel output. This may limit the feasibility of our binary-modulation protocol. In fact, weakness against excess noises may be universal for binary-modulation continuous-variable QKD protocols [ZHRL09].

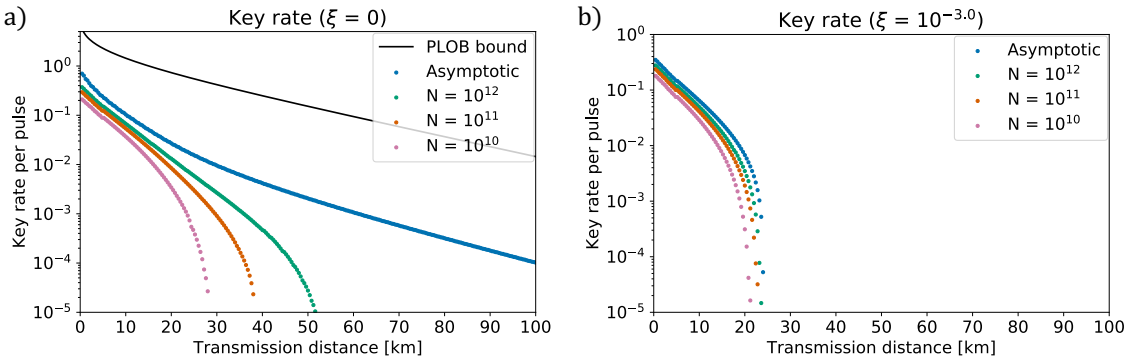

Figure 4.10: The net key gain per pulse $\check{G}$ (key rate) against the transmission distance L of the optical channel with our refined security analysis. We assumed that the optical pulse that Bob receives is given by randomly displacing a coherent state to increase its variance by a factor of $(1+\xi)$. a) The key rate in a pure-loss channel ($\xi = 0$) for various pulse numbers N. The solid black line shows the PLOB bound [PLOB17]. b) The key rate in a channel with the excess noise $\xi = 10^{-3.0}$ for various pulse numbers N.

Current theoretical progress in the continuous-variable QKD reveals that the discrete-modulation continuous-variable QKD protocols with four types of modulation have more tolerance against excess noise than those with binary modulation [GGDL19, LUL19, LLX+21]. What is important is that our security proof can be extended to the four-state protocols with binary outcomes, such as Protocol 2 in Ref. [LUL19] and a protocol in Ref. [LLX+21], by replacing the bit-extracting measurements of these protocols with the qubit-extracting maps as shown in Eq. (4.116) and defining the corresponding phase error operator. This is, however, much more complicated than the previous analysis, and we leave the problem as future work.

About the practicality of the protocol, reducing the total number 10^{12} of rounds may be desired to save the cost of classical information processing. The finite-size performance of our protocol may be improved by applying recently developed refinement [Kat20] of the Azuma's inequality [Azu67] that utilizes unconfirmed knowledge. What is non-trivial for applying this is that the random variable in our application of Azuma's inequality can not directly be observed even at the end of the protocol. Whether we can obtain a tighter bound using the refined concentration inequality [Kat20] with the information accessible in our protocol is an open problem.

Table 4.2: Examples of optimized parameters for the reverse reconciliation

Parameters for $N = 10^{11}$ and $\xi = 0$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.25×10^{-1}	$(25.8, 1.09)$	0.435	0.714	0.824	0.169
10	5.38×10^{-2}	$(14.6, 0.527)$	0.327	0.851	0.811	0.182
15	2.22×10^{-2}	$(10.4, 0.262)$	0.240	0.964	0.759	0.235
20	8.48×10^{-3}	$(8.07, 0.129)$	0.161	1.04	0.661	0.334
25	2.99×10^{-3}	$(6.25, 0.068)$	0.104	1.07	0.548	0.448
30	9.07×10^{-4}	$(5.03, 0.039)$	0.072	1.09	0.413	0.582
35	1.77×10^{-4}	$(4.22, 0.024)$	0.053	1.12	0.248	0.748
Parameters for $N = 10^{11}$ and $\xi = 10^{-3.0}$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.03×10^{-1}	$(14.9, 0.949)$	0.389	0.750	0.849	0.142
10	4.10×10^{-2}	$(9.14, 0.492)$	0.305	0.890	0.830	0.162
15	1.31×10^{-2}	$(6.47, 0.252)$	0.233	1.03	0.765	0.226
20	1.91×10^{-3}	$(4.80, 0.122)$	0.164	1.15	0.561	0.428
Parameters for $N = 10^{12}$ and $\xi = 0$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.53×10^{-1}	$(42.2, 1.21)$	0.473	0.692	0.878	0.119
10	6.72×10^{-2}	$(21.3, 0.553)$	0.343	0.833	0.878	0.119
15	2.94×10^{-2}	$(13.0, 0.266)$	0.244	0.949	0.879	0.119
20	1.32×10^{-2}	$(11.4, 0.132)$	0.164	1.01	0.782	0.215
25	5.87×10^{-3}	$(8.48, 0.070)$	0.107	1.04	0.733	0.265
30	2.67×10^{-3}	$(7.09, 0.040)$	0.076	1.05	0.367	0.709
35	1.17×10^{-3}	$(5.91, 0.025)$	0.057	1.07	0.538	0.460
40	4.68×10^{-4}	$(4.96, 0.016)$	0.045	1.09	0.454	0.544
45	1.58×10^{-4}	$(4.45, 0.011)$	0.038	1.11	0.306	0.692
50	2.76×10^{-5}	$(3.90, 0.0074)$	0.032	1.13	0.165	0.834
Parameters for $N = 10^{12}$ and $\xi = 10^{-3.0}$						
L [km]	Key rate $\check{G}$	(κ, γ)	μ	$q_{\rm th}$	$p_{\rm sig}$	$p_{\rm test}$
5	1.20×10^{-1}	$(17.9, 0.996)$	0.405	0.735	0.908	0.087
10	4.94×10^{-2}	$(10.3, 0.502)$	0.311	0.878	0.909	0.087
15	1.73×10^{-2}	$(7.09, 0.255)$	0.234	1.01	0.864	0.132
20	3.48×10^{-3}	$(5.03, 0.123)$	0.162	1.13	0.769	0.225

Examples of the parameters for a given pair of the total pulse number N and the excess noise parameter ξ in the refined security analysis. The variance of the quadrature operator $\hat{q}$ for the vacuum state is $\langle(\Delta\hat{q})^2\rangle = 1/2$. Given (N, ξ), protocol parameters $(\kappa, \gamma, \mu, q_{\rm th}, p_{\rm sig}, p_{\rm test})$ are optimized for each transmission distance L [km] so that the net key gain per pulse (key rate) $\check{G}$ is maximized.

4.6 Conclusion for this chapter

In this chapter, the finite-size security of the binary-modulation continuous-variable QKD protocol is established. The key to our achievement is the newly developed fidelity estimation for the channel output using the heterodyne measurement in Section 4.4.1. The fidelity as a measure of disturbance is essentially the same as what is monitored through bit errors in the B92 protocol [Ben92, TKI03, Koa04], and thus we can apply the proof techniques of the discrete-variable QKDs. This reduction has, however, non-triviality in the operator inequality (4.138) or (4.253) due to its infinite dimensionality. This is circumvented in Section 4.4.4 or 4.5.4 by constructing the heuristic but fairly good upper bound that is essentially finite-dimensional on the considered operator. These analyses are adapted to the digitization of the classical information processing; the detectors with finite resolution can be treated in our security analysis with minimal degradation to the protocol performance. In this sense, our security analysis is for digital information processing while the information itself is carried by the continuous-variable system.

While it is simple, the entanglement-distillation-based security proof developed in Section 4.4 turns out not to be tight. A tighter analysis with improved performance for the same protocol can be obtained via the reverse reconciliation in Section 4.5 at the cost of an additional complication for the operator inequality (Section 4.5.4). This refined analysis gives an almost optimal scaling of the asymptotic key rate against transmission distance. Our refined analysis is still fragile against the excess noise; Figure 4.10 b shows that the improvement of the performance with our refined analysis is lost by the excess noise as high as $\xi = 10^{-3.0}$ at the channel output. The key rates under the higher excess noise shown in Figure 4.7 are not practical. This may be a fate of the binary modulation protocol; the similar protocol considered in Ref. [ZHRL09] shows similar behaviors under the existence of the excess noise.

To improve the performance under the existence of the excess noise, therefore, we need to extend our finite-size analysis to protocols with more constellations. Among other things, the four-state protocols have been shown to be more robust against the excess noise [GGDL19, GGDL19, LLX$^+$21]. Our analysis can, in principle, be extended to the four-state protocols with binary outputs [LUL19, LLX$^+$21], i.e., protocols that use homodyne measurement to distinguish signals, by replacing the bit extraction with the qubit extraction as shown in Eqs. (4.116). However, developing the operator inequalities that keep the robustness against excess noise of these protocols still has non-triviality. A more challenging problem is to apply our finite-size security proof to the four-state protocols with more than two outputs, such as a protocol in Ref. [GGDL19] and Protocol 1 in Ref. [LUL19]. In this case, the definition of phase errors is already non-trivial as opposed to those with binary outputs, and we have to develop more elaborated finite-size security proof. Whether we can extend our techniques to these protocols or protocols with even more constellations is still open. The results in this chapter can thus be regarded as a first step for the complete security proofs for the continuous-variable QKD with digitized information processing.

Chapter 5

Quantum computation with continuous-variable systems

5.1 Introduction for this chapter

Quantum computation (QC) brings advantages over conventional classical computation in terms of computational speedups [HM17, AAB+19, BGK18] and stronger security [BFK09, BFK10]. Continuous-variable systems, especially quantum optical systems, have attracted growing interest as promising candidates for implementing QC. Compared to other matter-based candidates for implementing QC such as superconducting qubits [Wen17, KKY+19] and ion traps [HRB08, BCMS19], characteristics of the quantum optical architectures are scalability in generating quantum entanglement among more than one million photonic modes [YYK+16] and flexibility in interacting photons that fly in space, being free from geometrical constraints of two-dimensional surfaces of the matters.

For fault-tolerant quantum computing, one needs to construct an error-correcting routine to fight against the inevitable noise in the real world. Intensive research has thus been made on continuous-variable error-correcting codes [LS98, Bra98, GKP01, Men14, KKW+16, CMM99, NAC08, LKV+13, LRS16, LRS17, CLY97, KLM01, RHG05, WB07, BvL16, MSB+16, NCS18, AND+18]. Among them, the Gottesman-Kitaev-Preskill (GKP) code [GKP01], which encodes a qudit into an oscillator, gathers much attention in terms of both fault-tolerant continuous-variable QC [Men14, DMK+17, FTO17, FTOF18, VAW+19, WMBM19, Wan19, NC20, TBMS20, HHK20] and continuous-variable quantum communication [HP01, AND+18, NAJ18]. It needs only Gaussian operations, which is tractable in the quantum optical experiments, to implement Clifford gates (or even the universal gate set using protocols with a single type of GKP-encoded state [BPA+19]), and it is highly robust against loss errors as well as random displacement errors [FTO17, NAJ18].

In this chapter, we first show the equivalence between different conventional approximations of the GKP code. (The reason why approximations are needed will be explained in detail later.) This bridges the gap of previous studies that were based on different approximations. We then develop the strategy of efficiently implementing the universal QC with the GKP code and Gaussian operations, which is suited for optical systems. The chapter is organized as follows. Section 5.2.2 summarizes

the preliminaries about the GKP code. Sections 5.3 and 5.4 are the results of this thesis. In Section 5.3, the equivalence between the conventional approximations of the GKP code is proved, and the standard form of the approximate GKP codes is introduced. Furthermore, the explicit forms of the normalization constants and the average photon numbers of the approximate GKP code are derived in terms of the standard form. In Section 5.4, a resource-efficient implementation of the universal QC with a single type of GKP-encoded state and the Gaussian operations is constructed. A comparison between our construction and the previous proposal is discussed from a resource-theoretic perspective. Especially, the degree of non-Gaussianity of the approximate GKP-encoded state is computed numerically using the standard form developed in Section 5.3. Based on the existing proposals of preparing GKP-encoded states, we further discuss the feasibility of our constructed protocol. (Sections 5.3 and 5.4 are based on the publications [MYK20] and [YMK20] [1].)

5.2 Notations and preliminaries

5.2.1 Qudit, the Pauli group, and the Clifford group

Qudit is a quantum system characterized by the d-dimensional Hilbert space. It is the generalization of the qubit. Let $\{|j\rangle : j = 0, \ldots, d-1\}$ be an orthonormal basis of a qubit. Then, we can define the (generalized) Pauli-Z and -X operators by

$$Z|j\rangle = \exp(2\pi ij/d)|j\rangle, \qquad X|j\rangle = |j+1\rangle, \tag{5.1}$$

where the summation is modulo d. The commutation relation between Z and X are thus given by $ZX = \exp(2\pi i/d)XZ$. The group generated by Z, X, and iI is called the (generalized) Pauli group. Note that the global phase factor iI is irrelevant in quantum theory.

In QC, the normalizer of the Pauli group called the Clifford group plays an important role. In the case of the qubit, the Clifford group is generated by the Hadamard gate H, the phase gate S, and the CNOT gate given respectively by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5.2}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{5.3}$$

$$\mathrm{CNOT} = |0\rangle\langle 0|_1 \otimes I_2 + |1\rangle\langle 1|_1 \otimes \sigma_2^X. \tag{5.4}$$

These gates transform the Pauli-Z and -X operators by the adjoint actions as follows:

$$H^\dagger \sigma^Z H = \sigma^X, \qquad H^\dagger \sigma^X H = \sigma^Z, \tag{5.5}$$

$$S^\dagger \sigma^Z S = \sigma^Z, \qquad S^\dagger \sigma^X S = -\sigma^Y = i\sigma^Z\sigma^X, \tag{5.6}$$

$$\mathrm{CNOT}^\dagger(\sigma_1^Z \otimes I_2)\mathrm{CNOT} = \sigma_1^Z \otimes I_2, \qquad \mathrm{CNOT}^\dagger(\sigma_1^X \otimes I_2)\mathrm{CNOT} = \sigma_1^X \otimes \sigma_2^X, \tag{5.7}$$

$$\mathrm{CNOT}^\dagger(I_1 \otimes \sigma_2^Z)\mathrm{CNOT} = \sigma_1^Z \otimes \sigma_2^Z, \qquad \mathrm{CNOT}^\dagger(I_1 \otimes \sigma_2^X)\mathrm{CNOT} = I_1 \otimes \sigma_2^X. \tag{5.8}$$

[1] Copyright (2020) by The American Physical Society

It is known that all the unitaries on an N-qudit system can be approximately generated by the combination of Clifford gates and a non-Clifford gate in an arbitrary accuracy [NC10, KSVV02, DN05], while cannot be by only Clifford gates [Got98, AG04]. The set of gates that can approximately generate an arbitrary N-qudit unitary is called the universal gate set.

5.2.2 The Gottesman-Kitaev-Preskill code

In this chapter, we add a subscript of the basis choice instead of the system to a state vector for clarity, e.g., $|\psi\rangle_f$ for the Fock basis and $|q\rangle_{\hat{q}}$ for the quadrature "basis" in the sense of Eq. (3.9). (Strictly speaking, $|\cdot\rangle_{\hat{q}}$ is not an element of the Hilbert space for the oscillator mode, so it should be regarded as a weak limit of the squeezed coherent state as the squeezing parameter, i.e., ξ in Eq. (3.91), goes to infinity.) Exceptionally, the state vector with no subscripts denotes the GKP-encoded state. The GKP code [GKP01] is an error-correcting code that encodes a qudit into an oscillator mode. It has a lattice-like periodic structure when represented in the phase space; the Wigner function of the code states $|j\rangle$ and $|j+1\rangle$ have the same period, but $|j+1\rangle$ is shifted from $|j\rangle$ by $\frac{1}{d}$ of the period in position, where $j \in \{0, \dots, d-1\}$. The ideal (square lattice) GKP logical basis states $\{|j^{(\mathrm{ideal})}\rangle : j = 0, \dots, d-1\}$ are defined as [GKP01]

$$|j^{(\mathrm{ideal})}\rangle \coloneqq \sqrt{\alpha d} \sum_{s\in\mathbb{Z}} |\alpha(ds+j)\rangle_{\hat{q}}\,, \tag{5.9}$$

where $|\cdot\rangle_{\hat{q}}$ denotes the position "basis", and the pre-factor $\sqrt{\alpha d}$ is for later convenience. It is not actually an element of the Hilbert space; how to treat it is explained later. In the position wave function representation, it has a comb-like shape consisting of the Dirac delta functions (i.e., a Dirac comb) at intervals αd, and $|j+1^{(\mathrm{ideal})}\rangle$ is shifted from $|j^{(\mathrm{ideal})}\rangle$ by α. In the momentum representation, the logical basis states are given by

$$\begin{aligned}
|j^{(\mathrm{ideal})}\rangle &= \int dy\, \sqrt{\alpha d} \sum_{s\in\mathbb{Z}} |y\rangle\langle y|_{\hat{p}}\, |\alpha(ds+j)\rangle_{\hat{q}} && (5.10)\\
&= \sqrt{\frac{\alpha d}{2\pi}} \int dy \sum_{s\in\mathbb{Z}} e^{-i\alpha(ds+j)p}\, |y\rangle_{\hat{p}} && (5.11)\\
&= \sqrt{2\pi\alpha d} \int dy \sum_{t\in\mathbb{Z}} \delta(\alpha dy - 2\pi t) e^{-ij\alpha p}\, |y\rangle_{\hat{p}} && (5.12)\\
&= \sqrt{\frac{2\pi}{\alpha d}} \sum_{t\in\mathbb{Z}} e^{-i\frac{2\pi jt}{d}}\, |2\pi t/(\alpha d)\rangle_{\hat{p}}\,, && (5.13)
\end{aligned}$$

where we used the Poisson summation formula $\sum_{s\in\mathbb{Z}} e^{-isx} = 2\pi \sum_{t\in\mathbb{Z}} \delta(x - 2\pi t)$. The parameter α is often chosen to be

$$\alpha = \sqrt{\frac{2\pi}{d}} =: \alpha_d, \tag{5.14}$$

in order to symmetrize the code space in position and momentum coordinates in the phase space [GKP01], where the "symmetric code" is defined as follows.

Definition 5.2.1 (The code that is symmetric in position and momentum coordinates in the phase space)**.** Let $\{|j\rangle : j = 0, \ldots, d-1\}$ be the logical qudit basis encoded in an oscillator mode. The code is symmetric in position and momentum coordinates if it satisfies

$$\mathrm{span}\{|j\rangle : j = 0, \ldots, d-1\} = \mathrm{span}\{R(\pi/2)\,|j\rangle : j = 0, \ldots, d-1\}, \tag{5.15}$$

where $R(\pi/2)$ denotes the Fourier transform defined in Eq. (3.83).

Note that we can use $R(-\pi/2)$ instead of $R(\pi/2)$ in the definition. We also adopt Eq. (5.14) in the following. The symmetric code is beneficial if we aim at not biasing logical-level errors caused by physical-level phase-insensitive errors, that is, errors that occur symmetrically in position and momentum coordinates in the phase space. Furthermore, this definition implies that the Fourier transform $R(\pi/2)$ is an element of the stabilizer or a logical operator of the code since it preserves the code space. This symmetrization of the code is meaningful even when the logical basis states are nonorthogonal, which is the case in approximate GKP codes.

The ideal GKP code can be regarded as a stabilizer code. The stabilizer generators are given by the two commuting displacement operators $X_{\mathrm{st}} \coloneqq X(\alpha_d d)$ and $Z_{\mathrm{st}} \coloneqq Z(2\pi/\alpha_d) = Z(\alpha_d d)$, where $X(s) \coloneqq \exp(-is\hat{p})$ and $Z(t) \coloneqq \exp(it\hat{q})$ are introduced in Eq. (3.2). The logical Pauli-X and Z operators can be defined as $X_L \coloneqq X(\alpha_d)$ and $Z_L \coloneqq Z(2\pi/(\alpha_d d)) = Z(\alpha_d)$, which satisfy $Z_L X_L = \exp(2\pi i/d) X_L Z_L$ as expected. The GKP-encoded states defined in Eq. (5.9) are stabilized by X_{st} and Z_{st}, and are the eigenstates of the logical operator Z_L. The logical Clifford operators on the GKP code can be realized by the (symplectic) linear transformation of the quadrature operators $\hat{q}$ and $\hat{p}$ since logical Pauli operators are of the form $\exp[i(a\hat{q} + b\hat{p})]$ $(a, b \in \mathbb{R})$ up to a global phase. As explained in Section 3.1, the symplectic linear transformation of the quadrature gates can be implemented by Gaussian unitaries. Therefore, the logical Clifford gates on the GKP-encoded states can be realized by the Gaussian unitaries, which are reliably implementable in the quantum optical system. This is one of the advantages of using the GKP code in quantum optical systems.

For the GKP code with $d = 2$, the Gaussian unitaries that correspond to the logical H, S, and CNOT gates are given respectively by [GKP01]

$$H \longrightarrow \exp(\pi i \hat{n}/2)(= R(\pi/2)), \tag{5.16}$$

$$S \longrightarrow \exp(i\hat{q}^2/2), \tag{5.17}$$

$$\mathrm{CNOT} \longrightarrow \exp(-i\hat{q}_1\hat{p}_2). \tag{5.18}$$

These relations are understood by noticing that the following transformation rules hold:

$$R(-\pi/2) Z_L R(\pi/2) = X_L, \quad R(-\pi/2) X_L R(\pi/2) = Z(-\alpha_d) = Z_L^\dagger = Z_L Z_{\mathrm{st}}^\dagger, \tag{5.19}$$

$$e^{-i\hat{q}^2/2} Z_L e^{i\hat{q}^2/2} = Z_L, \quad e^{-i\hat{q}^2/2} X_L e^{i\hat{q}^2/2} = e^{-i\alpha_d\hat{q} - i\alpha_d\hat{p}} = i Z_L X_L^\dagger = i Z_L X_L X_{\mathrm{st}}^\dagger, \tag{5.20}$$

$$e^{i\hat{q}_1\hat{p}_2}(Z_L \otimes I_L)e^{-i\hat{q}_1\hat{p}_2} = Z_L \otimes I_L, \quad e^{i\hat{q}_1\hat{p}_2}(X_L \otimes I_L)e^{-i\hat{q}_1\hat{p}_2} = X_L \otimes X_L^\dagger = X_L \otimes X_L X_{\mathrm{st}}^\dagger, \tag{5.21}$$

$$e^{i\hat{q}_1\hat{p}_2}(I_L \otimes Z_L)e^{-i\hat{q}_1\hat{p}_2} = Z_L \otimes Z_L, \quad e^{i\hat{q}_1\hat{p}_2}(I_L \otimes X_L)e^{-i\hat{q}_1\hat{p}_2} = I_L \otimes X_L, \tag{5.22}$$

where we used Eqs. (3.6) and (3.83). We see that they are equivalent to Eqs. (5.5)–(5.8) up to the stabilizer elements $X_{\rm st}$ and $Z_{\rm st}$. The logical Z-basis measurement for the GKP code should distinguish $|0^{(\rm ideal)}\rangle$ and $|1^{(\rm ideal)}\rangle$ state. This can be achieved by performing the q-homodyne measurement, which always outputs an integer multiple of $\sqrt{\pi}$ for the GKP-encoded state. If the outcome is an even(odd) integer multiple of $\sqrt{\pi}$, then we know that $|0(1)^{(\rm ideal)}\rangle$ is observed. In fact, all the Pauli measurements can be realized by the homodyne measurements with appropriate directions in the phase space.

Using the stabilizer generators and logical Pauli operators, we have an alternative expression of the ideal GKP logical state as follows [GKP01, AND+18]:

$$|j^{(\rm ideal)}\rangle = \frac{(2d)^{-\frac{1}{4}}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2\in\mathbb{Z}}} X(\alpha_d(ds_1+j))Z(\alpha_d s_2)\,|0\rangle_f \tag{5.23}$$

$$= \frac{(2d)^{-\frac{1}{4}}}{\vartheta(0,id)} {X_L}^j \left(\sum_{l=0}^{d-1} {Z_L}^l\right) \sum_{\substack{s_1\in\mathbb{Z}\\ s_2\in\mathbb{Z}}} {X_{\rm st}}^{s_1} {Z_{\rm st}}^{s_2}\,|0\rangle_f \tag{5.24}$$

$$=: {X_L}^j \left(\sum_{l=0}^{d-1} {Z_L}^l\right) P_{\rm GKP}\,|0\rangle_f\,, \tag{5.25}$$

where $\vartheta(0,id) = \sum_{s\in\mathbb{Z}} \exp(-\pi d s^2)$ is the theta function, which will be explained later, and the last line defines an operator $P_{\rm GKP}$, which is interpreted as the projection onto the code space ignoring the normalization. The consistency with Eq. (5.9) can be confirmed as follows [AND+18]:

$$\frac{(2d)^{-\frac{1}{4}}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2\in\mathbb{Z}}} X(\alpha_d(ds_1+j))Z(\alpha_d s_2)\,|0\rangle_f$$

$$= \frac{(2d)^{-\frac{1}{4}}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2\in\mathbb{Z}}} \int dq\, e^{iq\alpha_d s_2}\,|q+\alpha_d(ds_1+j)\rangle\langle q|_{\hat q}\,|0\rangle_f \tag{5.26}$$

$$= \frac{(2\pi d)^{-\frac{1}{4}}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2\in\mathbb{Z}}} \int dq\, e^{-\frac{1}{2}q^2+iq\alpha_d s_2}\,|q+\alpha_d(ds_1+j)\rangle_{\hat q} \tag{5.27}$$

$$= \frac{\sqrt{2\pi\alpha_d}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2'\in\mathbb{Z}}} \int dq\, e^{-\frac{1}{2}q^2} \delta(q\alpha_d+2\pi s_2')\,|q+\alpha_d(ds_1+j)\rangle_{\hat q} \tag{5.28}$$

$$= \frac{\sqrt{\alpha_d d}}{\vartheta(0,id)} \sum_{\substack{s_1\in\mathbb{Z}\\ s_2'\in\mathbb{Z}}} e^{-\pi d s_2'^2} \Big|q+\alpha_d\Big(d(s_1-s_2')+j\Big)\Big\rangle_{\hat q} \tag{5.29}$$

$$= \sqrt{\alpha_d d} \sum_{s_1'\in\mathbb{Z}} |q+\alpha_d(ds_1'+j)\rangle_{\hat q} \tag{5.30}$$

$$= |j^{(\rm ideal)}\rangle\,, \tag{5.31}$$

where we used $\langle q|0\rangle_f = \pi^{-\frac{1}{4}}\exp(-q^2/2)$ in the second equality, used the Poisson summation formula $\sum_{s_2\in\mathbb{Z}} e^{-is_2 x} = 2\pi\sum_{s_2'\in\mathbb{Z}}\delta(x-2\pi s_2')$ in the third equality, and defined $s_1' \coloneqq s_1 - s_2'$ in the fifth equality.

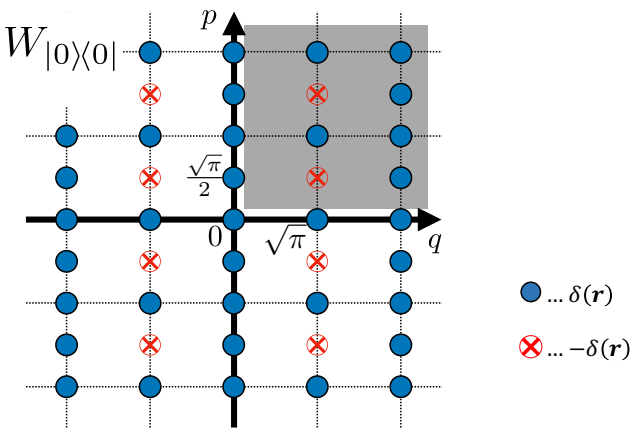

Figure 5.1: The Wigner function of the ideal GKP state $|0^{(\mathrm{ideal})}\rangle$, where each blue filled circle represents a positive delta function $\delta(\boldsymbol{r})$ with $\boldsymbol{r} = (q, p)$ and each red circled X represents a negative delta function $-\delta(\boldsymbol{r})$. This Wigner function has periodicity, where the gray region shows a period.

In the phase space, the Wigner function of the state $|j^{(\mathrm{ideal})}\rangle$ is given by [GKP01]

$$
\begin{aligned}
&W_{|j^{(\mathrm{ideal})}\rangle\langle j^{(\mathrm{ideal})}|}(q,p) \\
&= \frac{1}{2}\sum_{\substack{t\in\mathbb{Z}\\ t'\in\mathbb{Z}}} e^{-\pi i t t'}\,\delta\left(p-\frac{\alpha_d t}{2}\right)\delta\left(q-\frac{\alpha_d d t'}{2}-\alpha_d j\right) \qquad (5.32)\\
&= \frac{1}{2}\sum_{\substack{t\in\mathbb{Z}\\ t'\in\mathbb{Z}}} \delta\left(p+\frac{\alpha_d t}{2}\right)\left[\delta\left(q-\alpha_d d\left(t'+\frac{j}{d}\right)\right)+(-1)^t\,\delta\left(q-\alpha_d d\left(t'+\frac{j}{d}+\frac{1}{2}\right)\right)\right]. \qquad (5.33)
\end{aligned}
$$

Figure 5.1 shows the schematics of the ideal GKP logical basis state $|0^{(\mathrm{ideal})}\rangle$. This shows that the Wigner function of the ideal logical basis states forms a square lattice consisting of Dirac delta functions, which has half the period of the Dirac comb in the position and momentum representations. Since its sublattice formed of the odd periods starting from $(q, p) = (\alpha_d j, 0)$ consists of the Dirac delta functions with negative signs, the comb for the odd periods in position cancels out when integrated over momentum, and vice versa.

5.3 On the equivalence of approximate Gottesman-Kitaev-Preskill codes

As defined so far, the ideal GKP-encoded states are non-normalizable and thus unphysical. (All the relations described so far are formal.) The ideal GKP code should be regarded as a limit of physically meaningful approximate codes. Various approximations of the GKP-encoded states are considered in the past literature [GKP01, PMVT04, GK06, VSG10, Men14, AND+18, NAJ18, WT18]. The following three approximations are conventionally used.

(Approximation 1)

$$|j^{(1)}_{\kappa,\Delta}\rangle \coloneqq \frac{1}{\sqrt{N^{(1)}_{\kappa,\Delta,j}}} \sum_{s\in\mathbb{Z}} e^{-\frac{1}{2}\kappa^2\alpha_d^2(ds+j)^2} X(\alpha_d(ds+j))S(-\ln\Delta)\,|0\rangle_f\,, \tag{5.34}$$

where $\kappa, \Delta > 0$, $N^{(1)}_{\kappa,\Delta,j}$ is a normalization constant, and $S(\xi)$ is the squeezing operator defined in Eq. (3.84). This approximate code state approaches the ideal one as the limit of $\kappa, \Delta \to 0$. This approximation first appeared in the original paper of the GKP code [GKP01]. The idea of this approximation is to replace the position "eigenstates" with squeezed coherent states with a squeezing parameter $\ln(1/\Delta)$ and superpose them with a Gaussian weight of the width $1/\kappa$. This gives us an insight on how to generate the GKP-encoded state experimentally [MBGM17].

(Approximation 2)

$$|j^{(2)}_{\gamma,\delta}\rangle \coloneqq \frac{1}{\sqrt{N^{(2)}_{\gamma,\delta,j}}} \iint \frac{dr_1 dr_2}{2\pi\gamma\delta}\; e^{-\frac{r_1^2}{2\gamma^2}-\frac{r_2^2}{2\delta^2}} V(\boldsymbol{r})\,|j^{(\mathrm{ideal})}\rangle\,, \tag{5.35}$$

where γ and δ satisfy $0 < \gamma\delta < 2$, and $V(\boldsymbol{r}) \coloneqq \exp(-ir_1r_2/2)Z(r_1)X(r_2)$. This approximate code state approaches the ideal one as $\gamma, \delta \to 0$. This approximation also appeared in the original paper to regard the approximation as an error, and treat $\frac{1}{2\pi\gamma\delta}e^{-\frac{r_1^2}{2\gamma^2}-\frac{r_2^2}{2\delta^2}}$ as an error "wave function" [GKP01]. They use the term "wave function" because the state given in Eq. (5.35) is not an ideal code state subject to the error caused by the random displacement channel, but a coherent superposition of randomly displaced ideal code states. The error "wave function" later turned out to have more profound meanings; it is actually a wave function in the "grid representation" [GM96, KKW+16, TW16, DTW17, WT18], which is an analogous representation to the position representation, but with respect to the so-called "shifted grid states" instead of position eigenstates. In Appendix A, we make remarks on the "grid representation" in terms of the representation theory of the Heisenberg group.

(Approximation 3)

$$|j^{(3)}_{\beta}\rangle \coloneqq \frac{1}{\sqrt{N^{(3)}_{\beta,j}}} e^{-\beta\left(\hat{n}+\frac{1}{2}\right)}\,|j^{(\mathrm{ideal})}\rangle\,, \tag{5.36}$$

where β satisfies $\beta > 0$, and it approaches the ideal code state as $\beta \to 0$. Contrary to the former two approximations, Approximation 3, first appearing in Ref. [Men14],

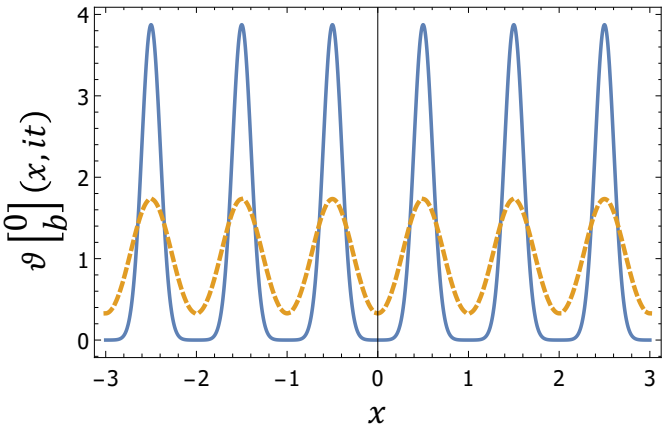

Figure 5.2: The theta function in the form of Eq. (5.39) with respect to x when $b = 1/2$ and $t = 1/15$ (blue solid line), and when $b = 1/2$ and $t = 1/3$ (yellow dashed line). The theta function in this form is a sequence of the same Gaussian functions with respect to x which has peaks at $b, b\pm1, b\pm2, \ldots$, and the width of each Gaussian is determined by t as shown in the figure. Note that Eq. (5.39) approaches the Dirac comb as $t \to 0$.

only deals with symmetric envelope in position and momentum coordinates. Since the approximation factor $e^{-\beta\left(\hat{n}+\frac{1}{2}\right)}$ is diagonal in the Fock basis, this approximation may be useful for computing the statistical properties of operators which are diagonal in the Fock basis, as shown in Ref. [Men14]. On the other hand, though this approximate code state could conceptually be prepared by feeding the ideal code states to the beamsplitter followed by post-selecting the vacuum click at the idler port [NAJ18], it provides few implications about their realistic experimental generation.

In this section, we prove that all the three approximations listed above are equivalent up to the squeezing. Before going into the proofs, we summarize the relevant functions used in this chapter. For $z \in \mathbb{C}$ and $\tau \in \mathbb{C}$ satisfying $\mathrm{Im}(\tau) > 0$, let $\vartheta(z,\tau) := \sum_{s\in\mathbb{Z}} \exp(\pi i\tau s^2 + 2\pi i z s)$ be the theta function (we follow the notation in Ref. [MM07]), and

$$\vartheta\begin{bmatrix}a\\b\end{bmatrix}(z,\tau) := \sum_{s\in\mathbb{Z}} \exp[\pi i\tau(s+a)^2 + 2\pi i(z+b)(s+a)] \tag{5.37}$$

$$= \exp[\pi i\tau a^2 + 2\pi i a(z+b)]\,\vartheta(z+\tau a+b,\tau) \tag{5.38}$$

be the theta function with rational characteristics (a,b) [MM07]. The theta functions which we mainly use are in the form

$$\vartheta\begin{bmatrix}0\\b\end{bmatrix}(x,it), \tag{5.39}$$

where $x, t \in \mathbb{R}$, and $b \in \mathbb{Q}$. The theta function in this form is a sequence of the same Gaussian functions with respect to x which has peaks at $b, b\pm1, b\pm2, \ldots$, and the width of each Gaussian is determined by t as shown in Fig. 5.2. Note that Eq. (5.39) approaches the Dirac comb as $t \to 0$. Let $G_{\sigma^2}(x)$ be a probability density function of the normal distribution with variance σ^2, which is defined as

$$G_{\sigma^2}(x) := \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{2\sigma^2}\right). \tag{5.40}$$

Finally, let $f * g(x) \coloneqq \int dy\, f(y)g(x-y)$ denote the convolution of two functions $f(x)$ and $g(x)$.

5.3.1 Position and momentum representations

In order to determine the relationship among the three approximations, we derive the position and momentum representations of the approximate code states. Note that the position and momentum representations of Approximation 1 have already appeared in the past literature [GKP01, TM02, PMVT04, VSG10, KKW+16, TW16, MBGM17, DMK+17, WT18, PBM20], but we rewrite them for completeness. For this purpose, we define the following functions.

Definition 5.3.1. Define $E_{\mu,\Gamma,a}(x)$ and $\tilde{E}_{\mu,\Gamma,a}(x)$ as

$$E_{\mu,\Gamma,a}(x) \coloneqq \sum_{s\in\mathbb{Z}} \exp\left(-\frac{(s+a)^2\Gamma^2}{2\mu}\right)\delta(x-(s+a)\Gamma)\,, \tag{5.41}$$

$$\tilde{E}_{\mu,\Gamma,a}(x) \coloneqq \sum_{s\in\mathbb{Z}} \exp\left(-\frac{s^2\Gamma^2}{2\mu}+2\pi i a s\right)\delta(x+s\Gamma)\,. \tag{5.42}$$

The function $E_{\mu,\Gamma,a}(x)$ is a Dirac comb with its interval given by Γ, which is shifted by the rational a of the interval from the origin and weighted by the Gaussian $\exp(-x^2/(2\mu))$ of the width μ. It can also be interpreted as a Fourier transform of the theta function in the form of $\frac{1}{\sqrt{2\pi}}\vartheta\begin{bmatrix}a\\0\end{bmatrix}\left(\frac{\Gamma}{2\pi}x, \frac{i\Gamma^2}{2\pi\mu}\right)$ with respect to x, which can be confirmed by its definition Eq. (5.37). On the other hand, the function $\tilde{E}_{\mu,\Gamma,a}(x)$, a Dirac comb with the Gaussian weight which has a phase factor for each peak, is a Fourier transform of the theta function in the form of $\frac{1}{\sqrt{2\pi}}\vartheta\begin{bmatrix}0\\a\end{bmatrix}\left(-\frac{\Gamma}{2\pi}x, \frac{i\Gamma^2}{2\pi\mu}\right)$, which can also be confirmed by Eq. (5.37).

Now, under Definition 5.3.1, we show the following proposition.

Proposition 5.3.2 (The position representation)**.** *Let $\kappa, \Delta, \beta > 0$ and $0 < \gamma\delta < 2$. Define $\lambda(\gamma,\delta) \coloneqq 1 + \frac{\gamma^2\delta^2}{4}$. Then, the position representations of the states Eqs.* (5.34)*,* (5.35)*, and* (5.36) *are given as follows:*

- *(Approximation 1)*

$$\langle q|j^{(1)}_{\kappa,\Delta}\rangle = \left(\frac{2\sqrt{\pi\Delta^2}}{N^{(1)}_{\kappa,\Delta,j}}\right)^{\frac{1}{2}} E_{\frac{1}{\kappa^2},\alpha_d d,\frac{j}{d}} * G_{\Delta^2}(q) \tag{5.43}$$

$$= \left(\frac{2\sqrt{\pi\Delta^2}}{\kappa^2 d N^{(1)}_{\kappa,\Delta,j}}\right)^{\frac{1}{2}} G_{\frac{1+\kappa^2\Delta^2}{\kappa^2}}(q)\ \vartheta\begin{bmatrix}0\\j/d\end{bmatrix}\left(-\frac{q}{\alpha_d d(1+\kappa^2\Delta^2)}, \frac{i\Delta^2}{d(1+\kappa^2\Delta^2)}\right). \tag{5.44}$$

- *(Approximation 2)*

$$\langle q|j^{(2)}_{\gamma,\delta}\rangle = \left(\frac{\alpha_d d}{\lambda(\gamma,\delta)N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} E_{\frac{\lambda(\gamma,\delta)}{\gamma^2}\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^2,\alpha_d d\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right),\frac{j}{d}} * G_{\frac{\delta^2}{\lambda(\gamma,\delta)}}(q) \tag{5.45}$$

$$= \left(\frac{\alpha_d \gamma^{-2}}{N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} G_{\frac{\lambda(\gamma,\delta)}{\gamma^2}}(q)\ \vartheta\begin{bmatrix}0\\ j/d\end{bmatrix}\left(-\frac{q}{\alpha_d d}\left[1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right], \frac{i\delta^2}{d\lambda(\gamma,\delta)}\right). \tag{5.46}$$

- *(Approximation 3)*

$$\langle q|j^{(3)}_{\beta}\rangle = \left(\frac{\alpha_d d}{\cosh\beta\, N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} E_{\frac{1}{\sinh\beta\cosh\beta},\frac{\alpha_d d}{\cosh\beta},\frac{j}{d}} * G_{\tanh\beta}(q) \tag{5.47}$$

$$= \left(\frac{\alpha_d}{\sinh\beta\, N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} G_{\frac{1}{\tanh\beta}}(q)\ \vartheta\begin{bmatrix}0\\ j/d\end{bmatrix}\left(-\frac{q}{\alpha_d d\cosh\beta}, \frac{i\tanh\beta}{d}\right). \tag{5.48}$$

For each approximation, we gave the two expressions in which we smear the Dirac delta functions in the definition of the ideal GKP-encoded state with the Gaussian functions in different orders. In the expressions (5.43), (5.45), and (5.47), each peak of the Dirac comb, which is weighted by a Gaussian as shown in the definition of $E_{\mu,\Gamma,a}$, is convoluted with another Gaussian $G_\nu(q)$. In the alternative expressions (5.44), (5.46), and (5.48), the infinite sequence of Gaussian spikes as defined in $\vartheta\begin{bmatrix}0\\ a\end{bmatrix}(q,it)$ is multiplied by another Gaussian function $G_{\nu'}(q)$ which works as an overall envelope. The expressions (5.43), (5.45), and (5.47) are suited for understanding the physical structure of the approximation such as the interval of the neighboring Gaussian peaks. The alternative expressions (5.44), (5.46), and (5.48) are convenient for numerical calculations because algorithms to calculate the theta function with arbitrary precision are well known [DHB+04].

Sketch of the proof. We derive Eqs. (5.43), (5.45), and (5.47) with straightforward but cumbersome calculations, and then apply the following lemma to derive Eqs. (5.44), (5.46), and (5.48).

Lemma 5.3.3. *For $\mu,\nu>0$, $\Gamma\in\mathbb{R}$, and $a\in\mathbb{Q}$, the following equality holds:*

$$E_{\mu,\Gamma,a} * G_\nu(q) = \sqrt{\frac{2\pi\mu}{\Gamma^2}}\ G_{\mu+\nu}(q)\ \vartheta\begin{bmatrix}0\\ a\end{bmatrix}\left(-\frac{q}{(1+\nu/\mu)\Gamma}, \frac{2\pi i\nu}{(1+\nu/\mu)\Gamma^2}\right), \tag{5.49}$$

$$\tilde{E}_{\mu,\Gamma,a} * G_\nu(q) = \sqrt{\frac{2\pi\mu}{\Gamma^2}}\ G_{\mu+\nu}(q)\ \vartheta\begin{bmatrix}a\\ 0\end{bmatrix}\left(-\frac{q}{(1+\nu/\mu)\Gamma}, \frac{2\pi i\nu}{(1+\nu/\mu)\Gamma^2}\right) \tag{5.50}$$

The full proof of Proposition 5.3.2 as well as the proof of Lemma 5.3.3 is in Appendix B.1. □

Under Definition 5.3.1, the momentum representations of the approximate code states can also be given by the following corollary.

Corollary 5.3.4 (The momentum represenation)**.** *Let $\kappa,\Delta,\beta>0$ and $0<\gamma\delta<2$. Let $\lambda(\gamma,\delta) \coloneqq 1+\frac{\gamma^2\delta^2}{4}$. Then, the momentum representations of the states* (5.34)*,* (5.35)*, and* (5.36) *are given as follows:*

- *(Approximation 1)*

$$\langle p|j^{(1)}_{\kappa,\Delta}\rangle = \left(\frac{2\sqrt{\pi\Delta^2}}{(1+\kappa^2\Delta^2)dN^{(1)}_{\kappa,\Delta,j}}\right)^{\frac{1}{2}} \tilde{E}_{\frac{1}{\Delta^2(1+\kappa^2\Delta^2)},\frac{\alpha_d}{1+\kappa^2\Delta^2},\frac{j}{d}} * G_{\frac{\kappa^2}{1+\kappa^2\Delta^2}}(p). \tag{5.51}$$

- *(Approximation 2)*

$$\langle p|j^{(2)}_{\gamma,\delta}\rangle = \left(\frac{\alpha_d}{\lambda(\gamma,\delta)N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} \tilde{E}_{\frac{\lambda(\gamma,\delta)}{\delta^2}\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^2,\alpha_d\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right),\frac{j}{d}} * G_{\frac{\gamma^2}{\lambda(\gamma,\delta)}}(p). \tag{5.52}$$

- *(Approximation 3)*

$$\langle p|j^{(3)}_{\beta}\rangle = \left(\frac{\alpha_d}{\cosh\beta\ N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} \tilde{E}_{\frac{1}{\sinh\beta\cosh\beta},\frac{\alpha_d}{\cosh\beta},\frac{j}{d}} * G_{\tanh\beta}(p). \tag{5.53}$$

Here, we only write the expressions in terms of $\tilde{E}_{\mu,\Gamma,a}$, but the expressions in terms of the theta function can also be obtained by applying Lemma 5.3.3 to these expressions.

Proof. We use the fact that the momentum representation of a state is a Fourier transform of its position representation, i.e., $\langle p|j\rangle = \frac{1}{\sqrt{2\pi}}\int dq\, e^{-ipq}\langle q|j\rangle$. We can thus derive Eqs. (5.51), (5.52), and (5.53) as Fourier transforms of Eqs. (5.44), (5.46), and (5.48), respectively, exploiting the fact that the Fourier transform of the product of two functions is given by the convolution of the Fourier transforms of the respective functions, and the Fourier transform of $\frac{1}{\sqrt{2\pi}}\vartheta\begin{bmatrix}0\\a\end{bmatrix}\left(-\frac{\Gamma}{2\pi}x, \frac{i\Gamma^2}{2\pi\mu}\right)$ is $\tilde{E}_{\mu,\Gamma,a}$ while the Fourier transform of G_ν is $\sqrt{1/\nu}\, G_{\frac{1}{\nu}}$. □

5.3.2 Explicit relations among the three approximations

The position and momentum representations of the three different approximate GKP logical basis states lead to conditions for equivalence of these approximations. Since $E_{\mu,\Gamma,a} * G_\nu(x)$ denotes the array of the Gaussian spikes $G_\nu(x)$ at intervals Γ, one can notice from Eqs. (5.45) and (5.47) that the intervals of the Gaussian spikes of the approximate code states are narrower than those of the ideal one, $\alpha_d d$, in the case of Approximations 2 and 3. Furthermore, from Eqs. (5.52) and (5.53), the intervals of the Gaussian spikes of each of these approximate code states in the momentum representations get narrower in the same proportion as that of their respective position representations. With this observation, Approximation 3, which has symmetric envelope functions in position and momentum representations, Eqs. (5.47) and (5.53), is expected to be a symmetric case ($\gamma = \delta$) of Approximation 2 in the sense of "symmetric" in Definition 5.2.1. This can be confirmed by the following.

Corollary 5.3.5 (The symmetric code)**.** *Let $R(\pi/2)$ be the Fourier operator defined in Eq. 3.83. Then, the following relation holds for the logical basis states of the Approximation 3:*

$$R(-\pi/2)\,|j^{(3)}_\beta\rangle = \sum_{j'=0}^{d-1}\sqrt{\frac{N^{(3)}_{\beta,j'}}{N^{(3)}_{\beta,j}}}\,|j'^{(3)}_\beta\rangle\,. \tag{5.54}$$

The same relation holds for Approximation 2 iff $\gamma = \delta$, i.e.,

$$R(-\pi/2)\,|j^{(2)}_{\gamma,\gamma}\rangle = \sum_{j'=0}^{d-1} \sqrt{\frac{N^{(2)}_{\gamma,\gamma,j'}}{N^{(2)}_{\gamma,\gamma,j}}}\,|j'^{(2)}_{\gamma,\gamma}\rangle\,. \tag{5.55}$$

Proof. It can be observed by combining $\langle x|_{\hat{q}}\,R(-\pi/2) = \langle x|_{\hat{p}}$ with Eqs. (5.45), (5.47), (5.46), and (5.53). □

In contrast with Approximations 2 and 3, the interval of Gaussian spikes in the position representation (5.43) of Approximation 1 is the same as that in the position representation of the ideal code state, and the interval in the momentum representation (5.51) of Approximation 1 is narrower than that in the momentum representation of the ideal code state. This means that Approximation 1 narrows the lattice spacing of the code space asymmetrically in position and momentum. This suggests that Approximation 1 may be related to Approximation 2 and Approximation 3 by a transformation that symmetrizes the interval of the lattice spacing in position and momentum.

We confirm this by applying the squeezing operation $S(\ln\sqrt{1+\kappa^2\Delta^2})$ for symmetrizing the intervals of the Gaussian spikes of the code state $|j^{(1)}_{\kappa,\Delta}\rangle$ in position and momentum coordinates:

$$\langle q|_{\hat{q}}\,S\left(\ln\sqrt{1+\kappa^2\Delta^2}\right)|j^{(1)}_{\kappa,\Delta}\rangle = (1+\kappa^2\Delta^2)^{\frac{1}{4}}\,\langle\sqrt{1+\kappa^2\Delta^2}q|j^{(1)}_{\kappa,\Delta}\rangle \tag{5.56}$$

$$= \sqrt{m}\;E_{\frac{1}{\kappa^2(1+\kappa^2\Delta^2)},\frac{\alpha_d d}{\sqrt{1+\kappa^2\Delta^2}},\frac{j}{d}} * G_{\frac{\Delta^2}{(1+\kappa^2\Delta^2)}}(q), \tag{5.57}$$

$$\langle p|_{\hat{p}}\,S\left(\ln\sqrt{1+\kappa^2\Delta^2}\right)|j^{(1)}_{\kappa,\Delta}\rangle = (1+\kappa^2\Delta^2)^{-\frac{1}{4}}\,\langle p/\sqrt{1+\kappa^2\Delta^2}|j^{(1)}_{\kappa,\Delta}\rangle \tag{5.58}$$

$$= \sqrt{\frac{m}{d}}\;\tilde{E}_{\frac{1}{\Delta^2},\frac{\alpha_d}{\sqrt{1+\kappa^2\Delta^2}},\frac{j}{d}} * G_{\kappa^2}(p), \tag{5.59}$$

where $m = \frac{2}{N^{(1)}_{\kappa,\Delta,j}}\sqrt{\frac{\pi\Delta^2}{1+\kappa^2\Delta^2}}$. In order to derive Eqs. (5.57) and (5.59), we used $E_{\mu,\Gamma,a} * G_\nu(bx) = \frac{1}{b}E_{\frac{\mu}{b^2},\frac{\Gamma}{b},a} * G_{\frac{\nu}{b^2}}(x)$ and $\tilde{E}_{\mu,\Gamma,a} * G_\nu(bx) = \frac{1}{b}\tilde{E}_{\frac{\mu}{b^2},\frac{\Gamma}{b},a} * G_{\frac{\nu}{b^2}}(x)$, which can be obtained from the definition of the functions $E_{\mu,\Gamma,a}(x)$, $\tilde{E}_{\mu,\Gamma,a}(x)$, and $G_\nu(x)$. Comparing the position representation (5.57) of the squeezed version of Approximation 1 with the position representation (5.45) of Approximation 2 and (5.47) of Approximation 3, we arrive at the following theorem.

Theorem 5.3.6 (Equivalence of the approximate GKP logical basis states)**.** *By choosing the parameters in Approximations 1 and 2 as*

$$\kappa^2 = \frac{\gamma^2}{\lambda(\gamma,\delta)} = \tanh\beta, \tag{5.60}$$

$$\Delta^2 = \frac{\delta^2}{\lambda(\gamma,\delta)}\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^{-2} = \sinh\beta\cosh\beta, \tag{5.61}$$

$$\gamma^2 = \delta^2 = 2\tanh\frac{\beta}{2}, \tag{5.62}$$

where $\lambda(\gamma,\delta) \coloneqq 1+\frac{\gamma^2\delta^2}{4}$, we have

$$S\left(\ln\sqrt{1+\kappa^2\Delta^2}\right)|j^{(1)}_{\kappa,\Delta}\rangle = |j^{(2)}_{\gamma,\delta}\rangle = |j^{(3)}_{\beta}\rangle\,. \tag{5.63}$$

Proof. It directly follows from Eqs. (5.45), (5.47), and (5.57). □

Theorem 5.3.6 together with Corollary 5.3.5 shows that up to a squeezing of the factor $\ln(\sqrt{1+\kappa^2\Delta^2})$ for Approximation 1 in order to make the code symmetric in the sense of Definition 5.2.1, the logical basis states of the symmetric code of Approximations 1, 2, and 3 are exactly the same quantum state. This squeezing becomes negligible in the limit of good approximation. In this sense, all these approximations are equivalent up to a squeezing that is ignorable in the limit of good approximation. This definition of equivalence is well-motivated since single-mode Gaussian unitary operations are easy to implement compared to non-Gaussian operations on continuous-variable systems such as optical systems, and among displacement, phase rotation, and squeezing for decomposing Gaussian unitaries [EP03], only squeezing can change the lattice spacing.

The converse of the theorem is also true; the choice of parameters in Theorem 5.3.6 is the only choice for the logical basis states of these approximations to be the same quantum states. This fact can be seen by the following remark.

Remark 5.3.7. So far, we followed the convention to fix the lattice spacing parameter as $\alpha = \alpha_d$, and derived equivalence relations among symmetric approximate codes. Such an exact correspondence between approximate codes can be generalized to asymmetric case. Let us remove the constraint of Eq. (5.14) and regard α as a free parameter in each approximation, and define states $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle$, $|j^{(2)}_{\gamma,\delta,\alpha}\rangle$, and $|j^{(3)}_{\beta,\alpha}\rangle$ (see Appendix B.1). We can observe from Eqs. (B.4) and (B.11) in Appendix B.1 that $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle = |j^{(2)}_{\gamma,\delta,\alpha'}\rangle$ with the following choice of parameters:

$$\kappa^2 = \frac{\gamma^2}{\lambda(\gamma,\delta)}\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^{-2}, \tag{5.64}$$

$$\alpha = \alpha'\left(1-\frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right), \tag{5.65}$$

$$\Delta^2 = \frac{\delta^2}{\lambda(\gamma,\delta)}. \tag{5.66}$$

Compared to $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle$ and $|j^{(2)}_{\gamma,\delta,\alpha}\rangle$, the third approximation $|j^{(3)}_{\beta,\alpha}\rangle$ has fewer parameters and cannot always be made equivalent to $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle$ and $|j^{(2)}_{\gamma,\delta,\alpha}\rangle$. It is because each Gaussian spike of the third approximation $|j^{(3)}_{\beta,\alpha}\rangle$ always has the same variance in position and momentum. If we apply the squeezing $S(\ln\zeta)$ to $|j^{(3)}_{\beta,\alpha}\rangle$ so that the variances of Gaussian spike in position and momentum can differ, we have $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle = |j^{(2)}_{\gamma,\delta,\alpha'}\rangle = S(\ln\zeta)\,|j^{(3)}_{\beta,\alpha''}\rangle$ with the following correspondence of the parameters in addition to Eqs. (5.64), (5.65), and (5.66):

$$\kappa^2 = \zeta^2 \sinh\beta\cosh\beta, \tag{5.67}$$

$$\alpha = \frac{\alpha''}{\zeta\cosh\beta}, \tag{5.68}$$

$$\Delta^2 = \frac{\tanh\beta}{\zeta^2}. \tag{5.69}$$

This can be confirmed from the fact that $\langle q| S(\ln\zeta)\,|j\rangle = \sqrt{\zeta}\,\langle \zeta q|j\rangle$, and $E_{\mu,\Gamma,a} * G_\nu(\zeta q) = \zeta^{-1} E_{\frac{\mu}{\zeta^2},\frac{\Gamma}{\zeta},a} * G_{\frac{\nu}{\zeta^2}}(q)$.

Remark 5.3.8. The equivalence of Approximation 2 with $\gamma = \delta$ and Approximation 3 can also be proved from Eqs. (1.4) and (7.12) in Ref. [AND+18] by setting $l = l' = 0$, while Ref. [AND+18] does not prove the equivalence. Our contribution here is to derive their position wave functions in Proposition 5.3.2 and to show the equivalence using these position wave functions.

5.3.3 The standard form

Now that we have shown the equivalence of Approximations 1, 2, and 3, we introduce a standard form of the approximate GKP logical basis state, which we will use in the rest of the paper.

Definition 5.3.9 (Standard form of the approximate GKP logical basis states)**.** Given three parameters σ_q^2, σ_p^2, and Γ with $0 < \sigma_q^2, \sigma_p^2 < 1/2$, the standard form of the approximate GKP code is defined as the code which is spanned by a logical qudit basis $\{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle : j = 0,\dots,d-1\}$ with its position representation given by

$$\langle q|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle \coloneqq \left(\frac{2\Gamma\left(\Lambda(\sigma_q^2,\sigma_p^2)\right)^{-\frac{1}{2}}}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\right)^{\frac{1}{2}} E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{2\sigma_p^2},\Gamma,\frac{j}{d}} * G_{2\sigma_q^2}(q), \tag{5.70}$$

where $\Lambda(\sigma_q^2,\sigma_p^2)$ is defined as

$$\Lambda(\sigma_q^2,\sigma_p^2) \coloneqq 1 - 4\sigma_q^2\sigma_p^2, \tag{5.71}$$

and $N_{\sigma_q^2,\sigma_p^2,\Gamma,j}$ is a normalization constant. For the symmetric code, the logical basis $\{|j_{\sigma^2}\rangle : j = 0,\dots,d-1\}$ is parametrized by only one parameter σ^2 $(0 < \sigma^2 < 1/2)$ as

$$\langle q|j_{\sigma^2}\rangle \coloneqq \left(\frac{2\alpha_d d}{N_{\sigma^2,j}}\right)^{\frac{1}{2}} E_{\frac{\Lambda(\sigma^2)}{2\sigma^2},\alpha_d d\sqrt{\Lambda(\sigma^2)},\frac{j}{d}} * G_{2\sigma^2}(q), \tag{5.72}$$

where

$$\Lambda(\sigma^2) \coloneqq 1 - 4\sigma^4. \tag{5.73}$$

Note that $|j_{\sigma^2}\rangle$ is equal to $|j_{\sigma^2,\sigma^2,\alpha_d d\sqrt{\Lambda(\sigma^2)}}\rangle$. The momentum representation of $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ is given by

$$\langle p|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle = \left(\frac{4\pi\sqrt{\Lambda(\sigma_q^2,\sigma_p^2)}}{\Gamma\, N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\right)^{\frac{1}{2}} \tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{2\sigma_q^2},\frac{2\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{j}{d}} * G_{2\sigma_p^2}(p), \tag{5.74}$$

and thus, for the symmetric code, it is given by

$$\langle p|j_{\sigma^2}\rangle = \left(\frac{2\alpha_d}{N_{\sigma^2,j}}\right)^{\frac{1}{2}} \tilde{E}_{\frac{\Lambda(\sigma^2)}{2\sigma^2},\alpha_d\sqrt{\Lambda(\sigma^2)},\frac{j}{d}} * G_{2\sigma^2}(p). \tag{5.75}$$

We can also write Eqs. (5.70), (5.72), (5.74), and (5.75) in terms of the theta function by using Lemma 5.3.3.

The physical meanings of the parameters σ_q^2, σ_p^2, and Γ of the state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ (and hence σ^2 of the state $|j_{\sigma^2}\rangle$) will be clarified in Section 5.3.4. Furthermore, an explicit form of the normalization constant $N_{\sigma_q^2,\sigma_p^2,\Gamma,j}$ (and hence $N_{\sigma^2,j}$) is given in Proposition 5.3.11. The expressions corresponding to Approximations 1–3 can be obtained simply by substituting the corresponding parameters:

$$|j_{\kappa,\Delta}^{(1)}\rangle = |j_{\sigma_q^2=\frac{\Delta^2}{2},\sigma_p^2=\frac{\kappa^2}{2(1+\Delta^2)},\Gamma=\alpha_d d}\rangle\,, \tag{5.76}$$

$$|j_{\gamma,\delta}^{(2)}\rangle = |j_{\sigma_q^2=\frac{\delta^2}{2\lambda(\gamma,\delta)},\sigma_p^2=\frac{\gamma^2}{2\lambda(\gamma,\delta)},\Gamma=\alpha_d d\left(1-\frac{\gamma^2\delta^2}{2\Lambda(\gamma,\delta)}\right)}\rangle\,, \tag{5.77}$$

$$|j_{\beta}^{(3)}\rangle = |j_{\sigma^2=\frac{\tanh\beta}{2}}\rangle\,, \tag{5.78}$$

where $\lambda(\gamma,\delta) = 1 + \frac{\gamma^2\delta^2}{4}$.

5.3.4 Explicit expressions of the Wigner function, inner products, and average photon number

In this section, we derive the expressions of the Wigner function, inner products, and the average photon number for the standard form of the approximate code state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ in Definition 5.3.9. Those for $|j_{\sigma^2}\rangle$ can also be obtained by substituting $\sigma_q^2 = \sigma_p^2 = \sigma^2$ and $\Gamma = \alpha_d d\sqrt{\Lambda(\sigma^2)}$. They also have expressions in terms of the Riemann theta function [MM07] (also known as the Siegel theta function), which is a multi-variable generalization of the theta function. These alternative expressions are relatively neat, but for the later analyses of the asymptotic behaviors (5.89) and (5.90), the expressions in terms of the theta function are more convenient. Thus we give the alternative expressions in terms of the Riemann theta function in Appendix C.

We will first derive the Wigner function of the operators $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|$. The Wigner function of the approximate GKP code can be used for the analyses of quantum error correction, as shown in Refs. [Men14, FTO17, FTOF18].

Proposition 5.3.10 (Wigner function)**.** *For the approximate code states $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ and $|j'_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ in Definition 5.3.9, the Wigner function $W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|}(q,p)$ of the operator $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|$ is given by*

$$\begin{aligned}
&W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|}(q,p)\\
&= \frac{1}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j} N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}} \left[\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}} * G_{\sigma_q^2}(q)\right)\left(\tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{j-j'}{2d}} * G_{\sigma_p^2}(p)\right)\right.\\
&\qquad \left. + \left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}+\frac{1}{2}} * G_{\sigma_q^2}(q)\right)\left(\tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{j-j'}{2d}+\frac{1}{2}} * G_{\sigma_p^2}(p)\right)\right],
\end{aligned} \tag{5.79}$$

where E and $\tilde{E}$ are defined in Definition 5.3.1, and $\Lambda(\sigma_q^2,\sigma_p^2)$ is defined in Eq. (5.71)*.*

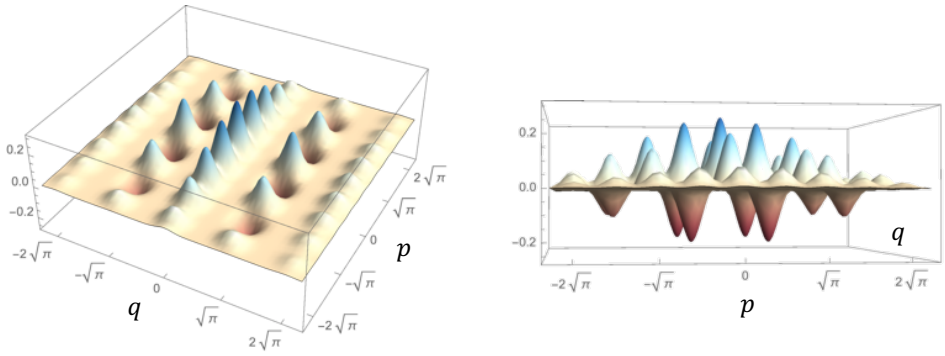

Figure 5.3: The Wigner function of the symmetric code state $|0_{\sigma^2}\rangle$ in the case $d = 2$ with $\sigma^2 = 0.05$, which is calculated from Eq. (5.79) along with the explicit form of the normalization constant given in Proposition 5.3.11.

Calculations for deriving the Wigner function are similar to those for deriving the position and momentum representations but are more complicated. The proof of Proposition 5.3.10 is in Appendix B.2. We can also write Eq. (5.79) in terms of the theta function by applying Lemma 5.3.3 to Eq. (B.35) in Appendix B.2.

The Wigner function in Proposition 5.3.10 shows the physical meanings of σ_q^2, σ_p^2, and Γ. The first term in the square bracket of Eq. (5.79) with $j = j'$ denotes an infinite sequence of Gaussian spikes each of which has variance σ_q^2 in position and σ_p^2 in momentum with periods Γ and $\pi\Lambda(\sigma_q^2, \sigma_p^2)\Gamma^{-1}$, respectively, and has overall Gaussian envelopes with variances $(4\sigma_p^2)^{-1}\Lambda(\sigma_q^2, \sigma_p^2)$ and $(4\sigma_q^2)^{-1}\Lambda(\sigma_q^2, \sigma_p^2)$, respectively. The second term shows that the same structure is also at the places shifted by half periods in position, but with positive and negative signs alternately in momentum. The Gaussian spikes in the first and second terms with different signs interfere destructively when projected onto position or momentum, while constructively with the same signs. Since $E_{\mu,\Gamma,a}(x) \to \sum_{s\in\mathbb{Z}} \delta(x - (s + a)\Gamma)$ and $\tilde{E}_{\mu,\Gamma,a}(x) \to \sum_{s\in\mathbb{Z}} e^{2\pi i a s}\delta(x + s\Gamma)$ as $\mu \to \infty$, and $G_\nu(x) \to \delta(x)$ as $\nu \to 0$, we can observe that Eq. (5.79) with $\Gamma = \alpha_d d$ approaches Eq. (5.33) as $\sigma_q^2, \sigma_p^2 \to 0$, as expected. Note that for the symmetric code state $|j_{\sigma^2}\rangle$, the intervals of the neighboring Gaussian peaks $\alpha_d d\sqrt{\Lambda(\sigma^2)}$ is smaller than $\alpha_d d$ of the ideal one. The change in the interval is $\mathcal{O}(\sigma^4)$, and thus may be negligible for small σ^2. However, in experiments, we cannot always make σ^2 small enough to keep the change in the intervals negligible. With our results, we can quantitatively analyze the code performance even for not necessarily small σ^2.

Using Eq. (5.79) with the explicit form of the normalization constant given in Proposition 5.3.11, we plot the Wigner function of the GKP logical basis state in Figure 5.3. Note that a similar expression has already been used in Ref. [Men14] with a more intuitive explanation. Our contribution here is to derive the Wigner function corresponding to the approximate code states explicitly, which we will use in the detailed analysis of the average photon number.

Next, using the Wigner function (5.79), we provide a closed-form expression for the normalization constant $N_{\sigma_q^2,\sigma_p^2,\Gamma}$. The normalization constants were calculated numerically in previous works [Men14, TW16, AND+18, SCC19], but here we can provide

their analytical expressions in terms of the theta functions. Furthermore, since the logical basis states of the approximate GKP codes are nonorthogonal, their inner products are nonzero in general, which we quantitatively analyze in the following. Since the theta functions used in the following proposition can be calculated with arbitrary precision by a method in, e.g., Ref. [DHB+04], the results are useful for evaluating the code performance reliably, as demonstrated in Section 5.4.

Proposition 5.3.11 (Normalization constant and inner product)**.** *The normalization factor $N_{\sigma_q^2,\sigma_p^2,\Gamma,j}$ of the approximate code state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ in Definition 5.3.9 is given in terms of the theta functions by*

$$\begin{aligned} N_{\sigma_q^2,\sigma_p^2,\Gamma,j} = \vartheta\begin{bmatrix}\frac{j}{d}\\0\end{bmatrix}\left(0,\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)\vartheta\begin{bmatrix}0\\0\end{bmatrix}\left(0,\frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}\right) \\ + \vartheta\begin{bmatrix}\frac{j}{d}+\frac{1}{2}\\0\end{bmatrix}\left(0,\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)\vartheta\begin{bmatrix}0\\\frac{1}{2}\end{bmatrix}\left(0,\frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}\right). \end{aligned} \tag{5.80}$$

Furthermore, the inner product between $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ and another approximate code state $|j'_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ is given by

$$\begin{aligned} &\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle \\ &= \frac{1}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\left\{\vartheta\begin{bmatrix}\frac{j+j'}{2d}\\0\end{bmatrix}\left(0,\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)\vartheta\begin{bmatrix}0\\\frac{j-j'}{2d}\end{bmatrix}\left(0,\frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}\right)\right. \\ &\qquad\left. + \vartheta\begin{bmatrix}\frac{j+j'}{2d}+\frac{1}{2}\\0\end{bmatrix}\left(0,\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)\vartheta\begin{bmatrix}0\\\frac{j-j'}{2d}+\frac{1}{2}\end{bmatrix}\left(0,\frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}\right)\right\}. \end{aligned} \tag{5.81}$$

Proof. We exploit the following facts:

$$\langle j'|j\rangle = \mathrm{Tr}\left[|j\rangle\langle j'|\right] = \iint dqdp\; W_{|j\rangle\langle j'|}(q,p), \tag{5.82}$$

$$\int dx\; f * g(x) = \int dx\; f(x)\int dy\; g(y), \tag{5.83}$$

$$\int dx\; E_{\mu,\Gamma,a}(x) = \sum_{s\in\mathbb{Z}}\exp[-(s+a)^2\Gamma^2/2\mu] = \vartheta\begin{bmatrix}a\\0\end{bmatrix}\left(0,\frac{i\Gamma^2}{2\pi\mu}\right), \tag{5.84}$$

$$\int dx\; \tilde{E}_{\mu',\Gamma',a'}(x) = \sum_{s\in\mathbb{Z}}\exp[-\Gamma'^2s^2/2\mu' + 2\pi i a's] = \vartheta\begin{bmatrix}0\\a'\end{bmatrix}\left(0,\frac{i\Gamma'^2}{2\pi\mu'}\right), \tag{5.85}$$

$$\int dx\; G_{\sigma^2}(x) = 1. \tag{5.86}$$

Combining the above with the Wigner function of $W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|}$ in Eq. (5.79), we obtain Eqs. (5.80) and (5.81). □

The expressions in Proposition 5.3.11 are exact and applicable to any σ^2, but at the same time complicated. Thus, we investigate their asymptotic behaviors in order to obtain intuitive relations with respect to the degree of approximation. As shown in

Ref. [BK11], the asymptotic behavior of the theta function in the form of $\vartheta\begin{bmatrix}a\\0\end{bmatrix}(0,it)$ as $t \to +0$ is given by

$$\vartheta\begin{bmatrix}a\\0\end{bmatrix}(0,it) = \sum_{s=0}^{\infty} e^{-\pi t(s+a)^2} + \sum_{s=0}^{\infty} e^{-\pi t(s+1-a)^2} = \frac{1}{\sqrt{t}} + \mathcal{O}\left(t^{\frac{1}{2}}\right). \tag{5.87}$$

Furthermore, the asymptotic behavior of $\vartheta\begin{bmatrix}0\\a\end{bmatrix}(0,it)$ as $t \to +0$ is given by

$$\vartheta\begin{bmatrix}0\\a\end{bmatrix}(0,it) = \frac{1}{\sqrt{t}}\vartheta\begin{bmatrix}a\\0\end{bmatrix}(0,it^{-1}) = \frac{1}{\sqrt{t}} \sum_{s=-\infty}^{\infty} e^{-\frac{\pi}{t}(s+a)^2} \simeq \frac{1}{\sqrt{t}} e^{-\frac{\pi}{t}a^2}, \tag{5.88}$$

where we used Eq. (B.25) in Appendix B.1 in the first equality. The last approximation takes the dominant term as $t \to +0$ up to a constant coefficient.

Now the asymptotic form of the logarithm of the normalization constant $N_{\sigma_q^2,\sigma_p^2,\Gamma,j}$ in Eq. (5.80) as $\sigma_q^2, \sigma_p^2 \to +0$ is given by

$$\ln N_{\sigma_q^2,\sigma_p^2,\Gamma,j} \to -\ln\sqrt{4\sigma_q^2\sigma_p^2}. \tag{5.89}$$

In the same way, the asymptotic behavior of the logarithm of $|\,\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\,|$ in Eq. (5.81) as $\sigma_q^2, \sigma_p^2 \to +0$ is given by

$$\ln|\,\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\,| \to -\frac{(j'-j)^2\Gamma^2}{8d^2\sigma_q^2}. \tag{5.90}$$

The overlap between logical basis states thus decreases exponentially with respect to σ_q^{-2}.

Along with the asymptotic behavior, we numerically calculate Eqs. (5.80) and (5.81) to see how the overlaps between code states change with respect to the degree of approximation. Figure 5.4 shows the logarithms of the absolute values of an inner product $\left|\langle 0_{\sigma^2}|1_{\sigma^2}\rangle\right|$ of the approximate code states (5.72) in Definition 5.3.9 with $d = 2, 3$, and 6, with respect to a squeezing level in decibels $-10\log_{10}(2\sigma^2)$, which is a quality measure of an approximate code state and explained later. One can observe that, in the region where the squeezing level is over 5 dB for $d = 3$ and 6, the minus of the logarithm of the inner product increases linearly with respect to the squeezing level in the log plot, that is, $-\ln\left|\langle 0_{\sigma^2}|1_{\sigma^2}\rangle\right| \propto \sigma^{-2}$, as expected in the asymptotic behavior (5.90). In the case of $d = 2$, the inclination of the plot is larger than those in the case of $d = 3$ and 6, which may be caused by a constant factor in Eq. (5.90) when $\frac{j+j'}{2d} \lesssim \frac{1}{2}$. Note that the squeezing levels of the GKP-encoded states when $d = 2$ in the recent experiments are 5.5–7.3 dB with the position and momentum degrees of freedom in trapped ion system [FNM+19], and 7.4–9.5 dB with the cavity mode of the superconducting system [CIET+20]. The required squeezing level for the fault-tolerant threshold of the universal QC is considered to be 8–16 dB [FTOF18, VAW+19, WMBM19, NC20, HHK20], depending on experimental setups and noise models.

"Squeezing level" of the (symmetric) GKP-encoded state was first considered in Ref. [Men14] in order to characterize the variance σ^2 of each convoluted Gaussian spike G_{σ^2} in the Wigner function of the approximate code state, which directly affects the performance of the error correction with approximate GKP codes. Since the

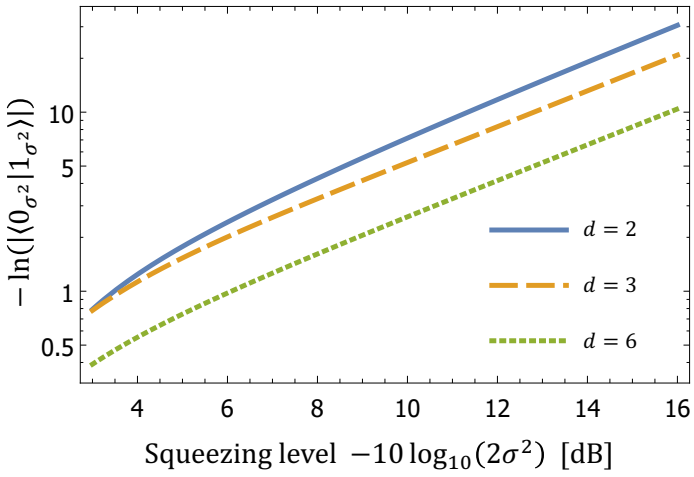

Figure 5.4: The logarithms of the absolute values of an inner product $-\ln\left(\left|\langle 0_{\sigma^2}|1_{\sigma^2}\rangle\right|\right)$ for the code state (5.72) in Definition 5.3.9 with $d = 2,\ 3$, and 6. The horizontal axis, $-10\log_{10}(2\sigma^2)$, is a squeezing level in decibels, which is a convention to express the degree of squeezing. The vertical axis is in the log scale. One can observe that, in the region where the squeezing level is over 5 dB for $d = 3$ and 6, the negative logarithm of the inner product increases linearly with respect to the squeezing level in the log plot, that is, $-\ln\left|\langle 0_{\sigma^2}|1_{\sigma^2}\rangle\right| \propto \sigma^{-2}$, as expected in the asymptotic behavior (5.90).

squeezing level of a squeezed state is the logarithm of the ratio of the variances of the position quadrature $(\Delta\hat{q})^2$ of that state and the vacuum state, Ref. [Men14] defines the squeezing level of the symmetric GKP logical basis state by $-10\log_{10}(2\sigma^2)$. In the case of an asymmetric code state, there are two parameters $-10\log_{10}(2\sigma_q^2)$ and $-10\log_{10}(2\sigma_p^2)$, where σ_q^2 and σ_p^2 denote the variance of Gaussian spike in position and momentum, respectively, in the Wigner function of the standard form (5.79). This definition leads us to identifying $-10\log_{10}\Delta^2$ ($\simeq -10\log_{10}\kappa^2$) as the squeezing parameter for Approximation 1 [FTO17, FTOF18, VAW+19, WMBM19, CIET+20] due to the relation (5.76). Note that there also exists another definition of "effective squeezing parameter", motivated by quantum metrology [DTW17, WT18, FNM+19]. In this paper, we adopt the former definition as a "squeezing level" in order to observe the relation between the performance of error correction and the average photon number of the approximate code states.

Finally, using the Wigner function (5.79) of the approximate code state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$, we can calculate the average photon number of the code state. Below we write $\langle A\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} := \langle j_{\sigma_q^2,\sigma_p^2,\Gamma}|\, A\, |j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ for an operator A.

Proposition 5.3.12 (Average photon number)**.** *The average photon number* $\langle\hat{n}\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ *of the approximate code state* $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ *in Definition 5.3.9 is given as follows:*

$$\langle\hat{n}\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} = \frac{\sigma_q^2+\sigma_p^2-1}{2} - \left(\frac{\partial}{\partial x}+\frac{\partial}{\partial y}\right)\ln \tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y)\Big|_{x=\frac{4\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)},\, y=\frac{4\sigma_q^2}{\Lambda(\sigma_q^2,\sigma_p^2)}}, \quad (5.91)$$

where $\tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y)$ *is defined as*

$$\begin{aligned}\tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y) \coloneqq \vartheta\begin{bmatrix}\frac{j}{d}\\0\end{bmatrix}\left(0,\frac{i\Gamma^2}{2\pi}x\right)\vartheta\begin{bmatrix}0\\0\end{bmatrix}\left(0,\frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\Gamma^2}y\right)\\ +\vartheta\begin{bmatrix}\frac{j}{d}+\frac{1}{2}\\0\end{bmatrix}\left(0,\frac{i\Gamma^2}{2\pi}x\right)\vartheta\begin{bmatrix}0\\\frac{1}{2}\end{bmatrix}\left(0,\frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\Gamma^2}y\right)\end{aligned} \tag{5.92}$$

Sketch of proof. Using the Wigner function (5.79), we can derive the expectation values of the square of the position and momentum quadrature, $\langle\hat{q}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ and $\langle\hat{p}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$. Then we can derive the explicit expression of $\langle\hat{n}\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ by exploiting the fact that $\langle\hat{q}^2+\hat{p}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} = \langle 2\hat{n}+1\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$. The full proof is in Appendix B.3. □

As an application of the results, we observe the relation between the squeezing level and the average photon number of approximate code states. The squeezing level has a direct connection to the performance of the quantum error correction using GKP codes [Men14, FTO17, FTOF18, VAW+19, WMBM19, HHK20]. On the other hand, the average photon number of the encoded state is relevant to the capacity of the continuous-variable quantum channel [NAJ18, HSH99, WQ18], which works as an effective dimension of the Hilbert space. Since it is found that the GKP code has high performance in the channel coding for bosonic Gaussian channels [AND+18, NAJ18], the connections between these two notions are important for further analyses of the Gaussian channel coding.

Previous literature estimates the average photon number of the encoded state as $\simeq \frac{1}{4\sigma^2}-\frac{1}{2}$ for the symmetric code for given squeezing level $-10\log_{10}(2\sigma^2) \gg 1$ [GKP01, GK06, Men14, TW16, NAJ18, AND+18]. This is because the variance of the envelope Gaussian in the Wigner function of the approximate code states is roughly equal to $\frac{1}{4\sigma^2}$, and the average photon number relates to the expectation values of the squares of the position and momentum quadratures by $\langle\hat{q}^2+\hat{p}^2\rangle_{|j_{\sigma^2}\rangle} = \langle 2\hat{n}+1\rangle_{|j_{\sigma^2}\rangle}$. It is also consistent with the expression of the average photon number given in Eq. (5.91) when the asymptotic form $\tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y) \propto \frac{1}{\sqrt{xy}}$ is considered. However, this estimation is no longer valid in the case of a low squeezing level. Here we are interested in the squeezing level at which this estimation deviates from the exact value.

We compute the average photon number of the code state $|j_{\sigma^2}\rangle$ defined in Eq. (5.72) in Definition 5.3.9 with $d = 2$, by using the formula (5.91). As mentioned above, the squeezing level of $|j_{\sigma^2}\rangle$ is given by $-10\log_{10}(2\sigma^2)$. Figure 5.5 shows the average photon number of $|0_{\sigma^2}\rangle$ and $|1_{\sigma^2}\rangle$ with respect to the squeezing level $-10\log_{10}(2\sigma^2)$. In Figure 5.5, we compare our result with a conventionally used estimate of the average photon number $\frac{1}{4\sigma^2}-\frac{1}{2}$. The figure reveals that when the squeezing level is less than 10 dB, the conventionally used estimate of the average photon number deviates from the exact values. Note that 10 dB squeezing is in a range of the expected thresholds for fault-tolerant continuous-variable QC [FTOF18, VAW+19, WMBM19, NC20, HHK20], which is a curious coincidence.

5.3.5 Discussion

In this section, we explicitly showed conditions under which the conventional approximations of the GKP code, Approximations 1, 2, and 3, defined in Eqs. (5.34),

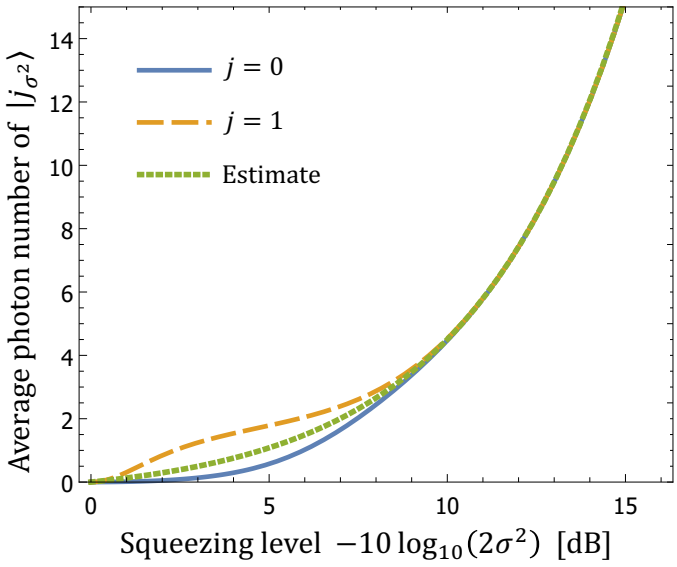

Figure 5.5: The average photon number of the code state (5.72) in Definition 5.3.9 with $d = 2$. "Estimate" denotes the function $\frac{1}{4\sigma^2} - \frac{1}{2}$. These three are in good accordance when the squeezing level is over 10 dB, but our rigorous calculations provide better estimates at the squeezing levels in the recent experiments, that is, 5.5–7.3 dB in the trapped ion system [FNM+19] and 7.4–9.5 dB in the superconducting system [CIET+20].

(5.35), and (5.36), are made equivalent. We observed that up to a slight squeezing for Approximation 1, Approximations 1, 2, and 3 are equivalent for the symmetric code, in which the logical basis states and their Fourier transforms span the same code space. Furthermore, we quantitatively showed that in all these approximations, the lattice spacing of the Gaussian spikes in phase space appearing in the description of the approximate code states is narrower than that of the corresponding ideal GKP code state. Although this effect may be negligible in the limit of large squeezing levels, it potentially affects the performance of the error correction. It is because the error correction strategy explicitly depends on the lattice spacing of the code states in the GKP code. Quantitatively, in the case of approximate code state of $d = 2$ with 8 dB squeezing, the lattice spacing is about 1% narrower than that of the ideal one. It is thus needed to investigate error correction schemes taking the change in lattice spacing into account, especially at a moderate squeezing level relevant to experimental realizations of GKP codes.

Exploiting the equivalence, we also gave the standard form of the approximate code states in terms of the position representation. Furthermore, we derived the explicit formulas of the Wigner function, normalization constant, inner product, and the average photon number of the logical basis states. These tools given in this section may accelerate further theoretical developments of continuous-variable quantum information processing based on quantum error correction and channel coding with the GKP error-correcting code.

5.4 Cost-reduced all-Gaussian universality with the GKP code

In the QC with qubits (or more generally qudits), the Clifford operations, i.e., the operations realized by the combinations of the Pauli-eigenstate preparations, the Clifford gates, and the Pauli measurements, cannot realize the universal QC [Got98, AG04]. This no-go statement is known as the Gottesman-Knill theorem. In order to perform the universal QC, one needs to implement a non-Clifford gate [NC10] such as the T-gate defined as

$$T = \begin{pmatrix} \mathrm{e}^{-\frac{\pi}{8}i} & 0 \\ 0 & \mathrm{e}^{\frac{\pi}{8}i} \end{pmatrix}. \tag{5.93}$$

The same is true for the GKP code. For the GKP code, the GKP-logic Clifford gates, i.e., the logical Clifford gates on qubits encoded in the continuous-variable system by the GKP code, can be realized only by Gaussian operations (defined in Section 3.1.4) as stated in the previous section. In order to realize the universality, a GKP-logic non-Clifford gate is necessary. In the original paper [GKP01], the GKP-logic non-Clifford gate is shown to be implementable either by using the optical non-Gaussian operation or by using the GKP-encoded magic states such as $|H\rangle$ and $|\frac{\pi}{8}\rangle$, where these magic states are defined as

$$|H\rangle \coloneqq \cos(\pi/8)\,|0\rangle + \sin(\pi/8)\,|1\rangle\,, \tag{5.94}$$

$$|\tfrac{\pi}{8}\rangle \coloneqq (\mathrm{e}^{-\frac{\pi}{8}i}\,|0\rangle + \mathrm{e}^{\frac{\pi}{8}i}\,|1\rangle)/\sqrt{2}. \tag{5.95}$$

Here we remark that Gaussian operations and logical Clifford operations on the GKP qubits are different in that Pauli eigenstates of the GKP code, such as $|0\rangle$ and $|1\rangle$, are non-Gaussian; i.e., initialization of GKP qubits requires non-Gaussian operations.

Ref. [BPA+19] has recently shown that the noisy GKP-encoded magic state can be probabilistically generated if one has the ability to prepare the GKP $|0\rangle$ states and to perform Gaussian operations. It is known that a higher-fidelity magic state can be distilled from many low-fidelity ones if the fidelity of lower ones is above a certain threshold. Therefore, the proposed method of probabilistically preparing noisy $|H\rangle$ means that we need only one type of a GKP-encoded state $|0\rangle$ with Gaussian operations to realize the universal QC. It is no longer required to develop technologies for preparing both $|0\rangle$ and $|H\rangle$ of the GKP code. However, in contrast to the majority of qubit-based codes in which the preparation of the magic state is much more costly than the preparation of the Pauli eigenstate, both $|0\rangle$ and $|H\rangle$ of the GKP code are non-Gaussian, and hence the preparation of them is equally costly compared to the realization of Gaussian operations in the quantum optical system. Thus, the overhead of consuming many expensive $|0\rangle$s for the distillation of $|H\rangle$ may become a bottleneck for the optical quantum computer.

In order to overcome the obstacle arising from the magic state distillation and achieve a fundamental cost reduction in implementing optical QC, we propose an idea of preparing only the GKP-logic magic state $|H\rangle$. We show a scheme that realizes the universal QC by combining Gaussian operations only with $|H\rangle$ instead of $|0\rangle$. Compared to the previous scheme, our scheme does not suffer from the overhead of the magic state distillation because $|0\rangle$ can be deterministically prepared from only two $|H\rangle$s by

the state-injection protocol [BK05]. While the scheme itself is pretty simple, our contribution is a fundamental cost reduction of non-Gaussian resources for implementing the optical quantum computer. Furthermore, we introduce a simple method for obtaining a fundamental limit on the transformation between $|H\rangle$ and $|0\rangle$ of the GKP code by any Gaussian operations, utilizing the resource theory of non-Gaussianity [TZ18, AGPF18], one of quantum resource theories [CG19] for continuous-variable QC. We also show the feasibility of the direct preparation of $|H\rangle$ of the GKP code. The existing proposals [PMVT04, VSG10, EBKTB14, ABI$^+$18, FMA$^+$20, TM02, MBGM17, WT18, ENP19, TBMS20, PMVT06a, PMVT06b, BKP13, TW16, FNMH18, LSW20, CIET$^+$20, SCC19, WT20, FNM$^+$19, LGMS19, HPB$^+$21, HA21, FTE$^+$21, FEA$^+$21] for the preparation of the GKP-encoded state mostly focus on the preparation of $|0\rangle$ state, but we discuss possibilities to generalize these proposals to the preparation of $|H\rangle$ state with a comparable technological cost.

5.4.1 Deterministic all-Gaussian universality using the GKP magic states

In the following, the logical qubit encoded in a physical continuous-variable system by the GKP code is referred to as *a GKP qubit*, and a physical state of a GKP qubit as *a GKP state*. Towards realizing fault-tolerant QC with quantum optical systems, it is promising to combine Gaussian operations with the GKP qubits [Men14, FTOF18, NC20, VAW$^+$19]. It is because Gaussian errors on the continuous-variable systems, which frequently occur in quantum optical systems, cannot be corrected solely by Gaussian operations [NFcvC09] but can be by combining Gaussian operations with an approximate GKP code concatenated with a multi-qubit quantum error-correcting code [Men14].

The GKP code can be used not only for correcting errors on the continuous-variable system but also for realizing the universal QC with its non-Gaussianity. The protocol developed in Ref. [BPA$^+$19] that realizes the universal QC utilizing the non-Gaussianity of the GKP-encoded state is based on the magic state distillation [BK05, Rei05] that probabilistically and approximately transforms GKP qubits prepared in $|0\rangle \otimes |0\rangle \otimes \cdots$ into a magic state $|H\rangle$ only using Gaussian operations. This protocol suggests that when Gaussian operations are available, the ability to prepare *only one type* of the GKP-encoded state $|0\rangle$ suffices to implement universal QC. However, this protocol has the significant overhead arising from the magic state distillation; whenever we need to obtain one GKP magic state $|H\rangle$ with a sufficiently high fidelity, many $|0\rangle$s will be consumed. More precisely, the required number of $|0\rangle$s to prepare a GKP magic state $|H\rangle$ up to an infidelity ϵ with the scheme in Ref. [BPA$^+$19] amounts to [BH12, Jon13, HHPW17]

$$\mathcal{O}\left(\mathrm{polylog}\left(\frac{1}{\epsilon}\right)\right) \quad \text{as } \epsilon \to 0. \tag{5.96}$$

This overhead per the preparation of $|H\rangle$ pushes up the implementation cost of the fault-tolerant logical non-Clifford gate on a qubit-based quantum error-correcting code concatenated with the GKP code and thus raise the total cost of the fault-tolerant QC.

In order to reduce the mass consumption of GKP qubits, here we propose choosing $|H\rangle$ instead of $|0\rangle$ as the single GKP state along with Gaussian operations for realizing

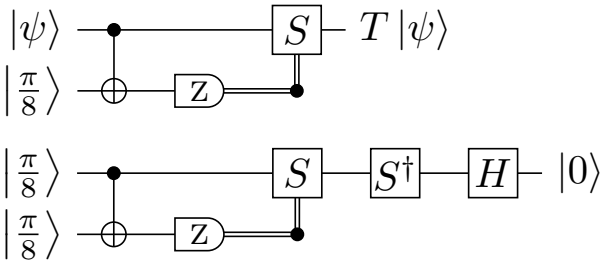

Figure 5.6: A quantum circuit of state injection for applying the T gate to any one-qubit input state $|\psi\rangle$ by Clifford operations assisted by an auxiliary input qubit prepared in $|\frac{\pi}{8}\rangle$ at the top, and that for converting a two-qubit input state $|\frac{\pi}{8}\rangle^{\otimes 2}$ to $|0\rangle$ at the bottom. The latter conversion circuit can be implemented only by adaptive Gaussian operations on the GKP qubits, namely, performing the Clifford gates (CNOT, S, $S^\dagger$, and H) that are implemented with Gaussian unitary operations, and conditioning on an outcome of the Z-basis measurement that is implemented with a homodyne detection.

the universal QC. Note that $|H\rangle$ and $|\frac{\pi}{8}\rangle$ defined in Eqs. (5.94) and (5.95) are Clifford equivalent, i.e., related by $|H\rangle = SH\,|\frac{\pi}{8}\rangle$ with the Clifford gates H and S given in Eqs. (5.2) and (5.3), which can thus be interchanged by Gaussian operations in the GKP code. Therefore, in the following we use these states interchangeably. Our cost-reduced scheme use a well-known quantum circuit for the T-gate teleportation [GKP01, BK05, NC10] given at the top of Figure 5.6. This circuit can apply the T gate to an arbitrary input state $|\psi\rangle$ by the combination of an ancillary magic state $|\frac{\pi}{8}\rangle$ and Clifford operations. When we set $|\psi\rangle = |\frac{\pi}{8}\rangle$, we have

$$T\,|\tfrac{\pi}{8}\rangle = e^{-\pi i/4}(|0\rangle + i\,|1\rangle)/\sqrt{2} = e^{-\pi i/4}SH\,|0\rangle\,, \tag{5.97}$$

and can thus prepare the GKP $|0\rangle$ with additional Gaussian operations as shown at the bottom of Figure 5.6. We can thus deterministically transform two GKP qubits prepared in $|\frac{\pi}{8}\rangle^{\otimes 2}$ into $|0\rangle$ only by Gaussian operations. Our deterministic protocol transforming two $|H\rangle$ states to a $|0\rangle$ state can be advantageous over the probabilistic protocol developed in Ref. [BPA$^+$19] transforming many $|0\rangle$ states to a $|H\rangle$ state; given the target infidelity ϵ, the number of the consumed GKP-encoded states in our protocol is bounded by a constant in contrast to (5.96), which essentially reduces the overhead. In fact, in the ideal case, $|0\rangle$ state can be exactly ($\epsilon = 0$) prepared in our protocol while it cannot be in Ref. [BPA$^+$19].

Notice that this cost reduction may be unique to quantum optical architectures in which preparing non-Gaussian states such as the GKP-encoded states is more costly than performing Gaussian operations. It does not necessarily hold for other continuous-variable systems than the quantum optical system, such as superconducting cavities [CIET$^+$20] and trapped-ion mechanical oscillators [FNM$^+$19], where Gaussian operations are not necessarily reliable to implement compared to non-Gaussian operations.

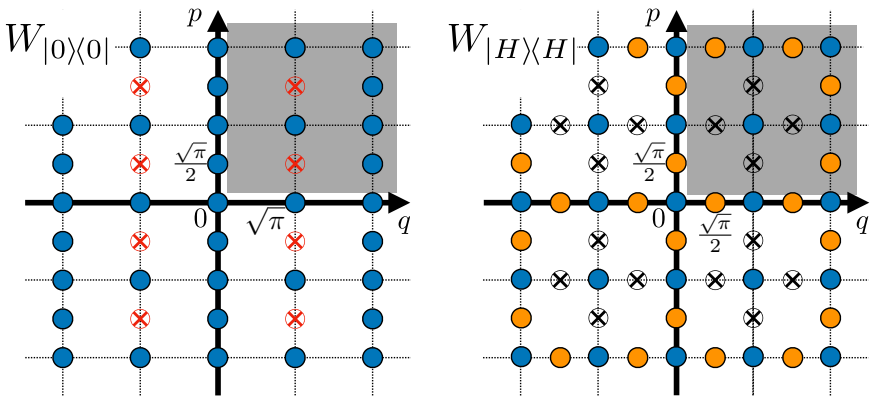

Figure 5.7: The schematics of the Wigner functions of the ideal GKP states $|0\rangle$ on the left and $|H\rangle$ on the right, where each blue filled circle represents a positive delta function $\delta(\boldsymbol{r})$ with $\boldsymbol{r} \coloneqq (q, p)$, each red circled X represents a negative delta function $-\delta(\boldsymbol{r})$, each yellow filled circle represents a weighted positive delta function $\frac{1}{\sqrt{2}}\delta(\boldsymbol{r})$, and each black circled X represents a weighted negative delta function $-\frac{1}{\sqrt{2}}\delta(\boldsymbol{r})$. These can be derived from Eq. (5.79) with the limit $\sigma_q^2, \sigma_p^2 \to 0$. The gray region shows the periodicity of these Wigner functions.

5.4.2 A resource-theoretical analyses for fundamental limitations on GKP state conversion

Since the convertibility between the GKP states $|H\rangle$ and $|0\rangle$ under Gaussian operations is crucial for the argument so far, we here develop a simple method for obtaining fundamental bounds on the convertibility between the GKP states. For this analysis, we use the resource theory of non-Gaussianity in which Gaussian operations are considered to be free and non-Gaussian states, unitaries, and measurements are regarded as resources for assisting Gaussian operations [TZ18, AGPF18, LRW$^+$18, ZSS18]. Following the rule of the convex resource theories [TZ18, AGPF18], we include adaptive Gaussian operations conditioned on the outcomes of Gaussian measurements in the free operations. Note that the resource theories of magic [VMGE14, HC17], where Clifford operations are considered to be free, are inapplicable to our case because Pauli eigenstates of the GKP qubits, e.g., $|0\rangle$, are the resourceful states while they are free in the resource theories of magic.

Resource theories of non-Gaussianity introduce a measure that quantifies the non-Gaussianity of a state on the continuous-variable system. We may be able to convert a state with high non-Gaussianity into that with low non-Gaussianity but cannot in the reverse direction. One way to quantify the non-Gaussianity of a given state ψ is to use the logarithmic negativity [TZ18, AGPF18] of the Wigner function W_ψ of ψ defined as $\mathcal{N}_L(\psi) \coloneqq \ln\left(\iint_{-\infty}^{\infty} dqdp\ |W_\psi(q,p)|\right)$. For the pure Gaussian state ρ, for example, we have $\mathcal{N}_L(\rho) = 0$ since the Wigner function W_ρ of the pure Gaussian state ρ is always nonnegative [Hud74, SC83]. The logarithmic negativity $\mathcal{N}_L$ does not increase under any Gaussian operations (monotonicity).

Although the logarithmic negativity is well-defined for the Wigner functions of

approximate GKP states, it is not for the Wigner functions of the ideal GKP states, where infinitely many Dirac delta functions are arranged according to a square lattice in concept, as depicted in Figure 5.7. We can compute the logarithmic negativity for the Wigner functions of approximate GKP states in principle, but we would like more intuitive ways of comparing the non-Gaussianity and analyzing the convertibility between ideal GKP states. For this, we develop an alternative measure to quantify the non-Gaussianity of the ideal GKP states exploiting the periodicity of the Wigner functions as shown in Figure 5.7 and replacing the improper integral of $\mathcal{N}_L$ from $-\infty$ to ∞ with an integral over a period. More precisely, in place of $\mathcal{N}_L$, we define

$$\widetilde{\mathcal{N}}_L(\psi) \coloneqq \ln\left(\frac{\iint_{\mathcal{I}} dqdp\ |W_\psi(q,p)|}{\iint_{\mathcal{I}} dqdp\, W_\psi(q,p)}\right), \tag{5.98}$$

where $\mathcal{I} \coloneqq [0+\epsilon, 2\sqrt{\pi}+\epsilon]$ for any fixed $\epsilon \in (0, \sqrt{\pi}/2)$ represents the period shown in Figure 5.7. It is defined so that $\widetilde{\mathcal{N}}_L(\psi) = 0$ for a state ψ whose Wigner function is nonnegative. Then, by counting delta functions in Figure 5.7, we have

$$\widetilde{\mathcal{N}}_L(|0\rangle\langle 0|) = \ln\frac{8}{4} = \ln 2, \tag{5.99}$$

$$\widetilde{\mathcal{N}}_L(|H\rangle\langle H|) = \ln\frac{4+8\times\left(1/\sqrt{2}\right)}{4} = \ln(1+\sqrt{2}). \tag{5.100}$$

Thus, we quantitatively compare the non-Gaussianity of $|H\rangle$ and $|0\rangle$ by

$$\widetilde{\mathcal{N}}_L(|H\rangle\langle H|) - \widetilde{\mathcal{N}}_L(|0\rangle\langle 0|) = \ln\frac{1+\sqrt{2}}{2} > 0, \tag{5.101}$$

which implies that $|H\rangle$ has more non-Gaussianity than $|0\rangle$, and hence no Gaussian operation can deterministically transform $|0\rangle$ into $|H\rangle$.

In order to justify the use of $\widetilde{\mathcal{N}}_L$ instead of $\mathcal{N}_L$ for the ideal GKP states, we carried out a numerical simulation of the negativity $\mathcal{N}_L$ of approximate GKP states. More precisely, we performed the numerical integration using Mathematica 11.2.0 for the absolute values of the Wigner functions of $|0_{\sigma^2}\rangle$ and $|H_{\sigma^2}\rangle \propto (\cos(\pi/8)\,|0_{\sigma^2}\rangle + \sin(\pi/8)\,|1_{\sigma^2}\rangle)$ with the approximate GKP states $|j_{\sigma^2}\rangle$ defined in Eq. (5.72). Figure 5.8 plots the logarithmic negativities of the Wigner functions of $|0_{\sigma^2}\rangle$ and $|H_{\sigma^2}\rangle$ against the squeezing level $-10\log_{10}(2\sigma^2)$. The figure indicates that the logarithmic negativity of $|0_{\sigma^2}\rangle$ approaches to $\widetilde{\mathcal{N}}_L(|0\rangle\langle 0|) = \ln(2) = 0.69\cdots$ as $-10\log_{10}(2\sigma^2) \to \infty$ and that of $|H_{\sigma^2}\rangle$ to $\widetilde{\mathcal{N}}_L(|H\rangle\langle H|) = \ln(1+\sqrt{2}) = 0.88\cdots$, as expected from our arguments.

With $\widetilde{\mathcal{N}}_L$ defined, we can provide an upper bound on the conversions from the GKP $|0\rangle$s to the GKP $|H\rangle$s or the conversions in the reverse direction. In the same way as the additivity of the logarithmic negativity $\mathcal{N}_L$ [TZ18, AGPF18], $\widetilde{\mathcal{N}}_L$ is additive, i.e., $\widetilde{\mathcal{N}}_L(\psi^{\otimes n}) = n\widetilde{\mathcal{N}}_L(\psi)$. Although we have developed the protocol converting $|H\rangle^{\otimes 2}$ into $|0\rangle$ under Gaussian operations, the additivity of $\widetilde{\mathcal{N}}_L$ shows that $|H\rangle^{\otimes 2}$ cannot be transformed into $|0\rangle^{\otimes 3}$ under any Gaussian operations because of the inequality

$$\widetilde{\mathcal{N}}_L(|H\rangle\langle H|^{\otimes 2}) - \widetilde{\mathcal{N}}_L(|0\rangle\langle 0|^{\otimes 3}) = \ln\frac{\left(1+\sqrt{2}\right)^2}{2^3} < 0. \tag{5.102}$$

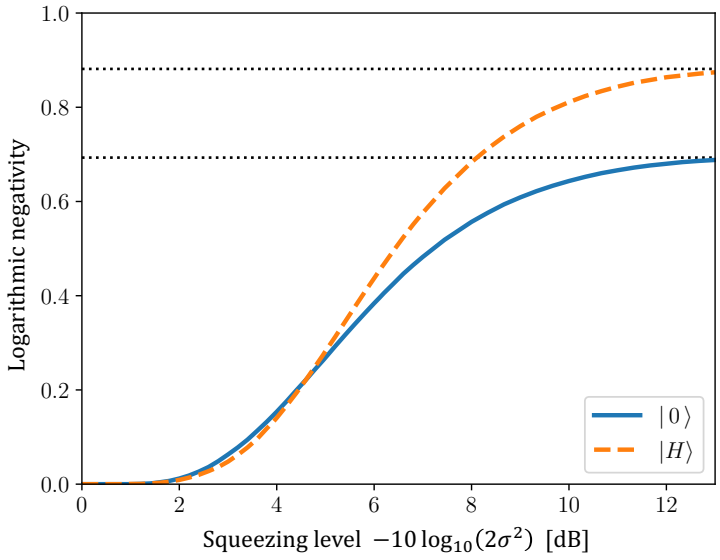

Figure 5.8: The logarithmic negativities of the Wigner functions of $|0_{\sigma^2}\rangle$ (blue solid line) and $|H_{\sigma^2}\rangle \propto (\cos(\pi/8)\,|0_{\sigma^2}\rangle + \sin(\pi/8)\,|1_{\sigma^2}\rangle)$ (orange dashed line) with respect to the squeezing level $-10\log_{10}(2\sigma^2)$. The logarithmic negativity of $|0_{\sigma^2}\rangle$ approaches to $\ln(2) = 0.69\cdots$, and that of $|H_{\sigma^2}\rangle$ to $\ln(1+\sqrt{2}) = 0.88\cdots$, as expected from the calculations (5.99) and (5.100).

Whether the one-to-one transformation from $|H\rangle$ to $|0\rangle$ is possible or not is unknown. On the other hand, the conversion from $|0\rangle^{\otimes 2}$ to $|H\rangle$ is not prohibited in terms of the logarithmic negativity since

$$\widetilde{\mathcal{N}}_L(|0\rangle\langle 0|^{\otimes 2}) - \widetilde{\mathcal{N}}_L(|H\rangle\langle H|) = \ln\frac{2^2}{1+\sqrt{2}} > 0, \tag{5.103}$$

whereas it is still open whether a deterministic or exact Gaussian transformation from a constant number of $|0\rangle$s to $|H\rangle$ is possible or not. We here remark that the estimation on the required resource for the state conversion made by the logarithmic negativity is in general very loose; the state with larger logarithmic negativity does not necessarily mean the convertibility to the state with smaller logarithmic negativity [TZ18, AGPF18].

Note that the measure $\widetilde{\mathcal{N}}_L$ was also introduced in Ref. [GÁFF21], which is done independently. In contrast to Ref. [GÁFF21], we justified the use of $\widetilde{\mathcal{N}}_L$ by numerically calculating the original logarithmic negativity $\mathcal{N}_L$ for the approximate GKP states and then taking the limit of the infinite squeezing level as shown in Figure 5.8. Furthermore, we explicitly show an example for the transformation under Gaussian operations in Figure 5.6, which supports the usefulness of the resource theory.

To obtain further insight on the convertibility between GKP states, more sophisticated resource-theoretic analyses may be needed. For example, an interesting possibility is that Gaussian operations combined with post-selection may increase the negativity of a GKP state with nonzero probability. Such a possibility is not covered by the analysis using the logarithmic negativity. Our resource-theoretical arguments and methods are thus starting points for tackling questions on the GKP-state conversion.

5.4.3 Feasibility of preparing a GKP magic state

Since Gaussian operations combined with a GKP magic state $|H\rangle$ can be advantageous in implementing QC over those with $|0\rangle$ of GKP qubits, we here discuss possible protocols for directly preparing $|H\rangle$. Note that choosing $|H\rangle$ among GKP-encoded magic states may not just be a matter of convention; the $|H\rangle$ state has the symmetry of $\frac{\pi}{2}$-rotation in the phase space as seen in Figure 5.7 and thus lies in an eigenspace of the photon number operator modulo four. Some proposals exploit this symmetry for the preparation [GKP01]. Our following discussion is based on the proposals for the quantum optical implementation of approximate GKP qubits [TM02, PMVT04, VSG10, EBKTB14, MBGM17, ABI$^+$18, WT18, ENP19, FMA$^+$20, TBMS20, HA21, FTE$^+$21, FEA$^+$21], while there also exist other proposals and experimental demonstrations of generating approximate GKP states in various systems [PMVT06a, PMVT06b, BKP13, TW16, FNMH18, LSW20, CIET$^+$20, SCC19, WT20, FNM$^+$19, LGMS19, HPB$^+$21]. Note that architectures such as superconducting cavities [CIET$^+$20] and trapped-ion mechanical oscillators [FNM$^+$19] are also promising candidates to realize the GKP code, but we here focus on quantum optical implementations since Gaussian operations are not necessarily easier to implement than non-Gaussian operations on the superconducting cavities and the trapped-ion mechanical oscillators. We remark that these existing proposals mostly focus on preparing $|0\rangle$ or $|1\rangle$ of the GKP code.

Some of the proposals, such as those in Refs. [PMVT04, FEA$^+$21, HA21], may not be suitable for the direct preparation of $|H\rangle$. References [PMVT04, FEA$^+$21] considers using the cross-Kerr non-linearity to couple two optical modes initially prepared in a coherent state and a squeezed coherent state, respectively, followed by performing homodyne measurement of the mode initialized as the coherent state, which results in generating approximate GKP-Pauli eigenstate $|0\rangle$ or $|1\rangle$. In this scheme, $|H\rangle$ cannot be directly prepared as long as Gaussian states are fed into the cross-Kerr interaction followed by the homodyne detection. Reference [HA21] considers using the optical displacement and the controlled-π rotation controlled by the state of the two-level atom. This setup cannot directly prepare the $|H\rangle$ state since the controlled-π rotation cannot add relative phases between superposed peaks. As for other proposals, Ref. [ABI$^+$18] analyzes optimization of parametrized non-Gaussian optical circuits by machine learning, and Ref. [FMA$^+$20] uses time-frequency degrees of freedom. These proposals do not fit our current settings for preparing the quantum optical GKP qubits where Gaussian operations are easy compared to non-Gaussian operations, while they are also interesting research directions.

There are, however, some existing proposals that can be used for preparing $|H\rangle$. One approach is to breed the peaks of the approximate GKP states by the controlled-displacement operation using the interaction with the discrete-variable system in the cavity QED setups [TM02, MBGM17, HPB$^+$21] or by the interference between two premature approximate GKP states in the all-optical setups [VSG10, EBKTB14, WT18]. Another approach is to use linear optical circuits followed by photon-number-resolving (PNR) detectors and post-select certain outcome patterns [ENP19, TBMS20, FTE$^+$21].

For the former approach, $|H\rangle$ can be prepared if the circuit given in Figure 5.9 can be implemented by the same experimentally allowed operations that prepare $|0\rangle$. Reference [WT18] develops a refinement of the proposals in Refs. [VSG10, EBKTB14] of the

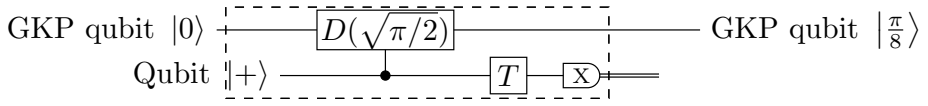

Figure 5.9: A quantum circuit for preparing a GKP $\frac{\pi}{8}$-phase state $|\frac{\pi}{8}\rangle$ from an input GKP $|0\rangle$ state using the breeding-like (phase-estimation-like) circuit.

all-optical interference-based breeding protocol. The method proposed in Ref. [WT18] can realize the circuit equivalent to that in Figure 5.9 by post-selecting the homodyne outcome and adjusting the relative phase between $|0\rangle$ and $|1\rangle$. (In principle, an arbitrary superposition of $|0\rangle$ and $|1\rangle$ can be prepared with the method in Ref. [WT18].) Reference [HPB$^+$21], which uses the recursive interaction between a discrete-variable system and a continuous-variable system, can also realize the circuit equivalent to that in Figure 5.9 by adjusting the interaction terms. (The explicit methodology is given in the literature.) Thus in these protocols, the technological requirements for preparing $|0\rangle$ and $|H\rangle$ are at the same level. Note that if we are allowed to use an interaction between a qubit and a continuous-variable system beyond the controlled-displacement gate, an additional controlled-Fourier operation between the qubit and the continuous-variable system can also prepare $|H\rangle$ from $|0\rangle$ as already shown in Ref. [GKP01].

For the latter approach, generating the non-Gaussian states with linear optical circuits followed by the PNR detectors as proposed in Refs. [ENP19, TBMS20, FTE$^+$21] can implement $|0\rangle$ and $|H\rangle$ on an equal footing with almost the same resource requirements, as pointed out in Ref. [TBMS20]. Furthermore, preparing only one type of GKP state in this protocol may be desired since optical circuits and PNR detectors to generate the GKP state need to be finely tuned to keep the fidelity high. These protocols indicate that it is feasible to prepare $|H\rangle$ of the GKP qubits with a technological requirement comparable to preparing $|0\rangle$ in some cases.

5.4.4 Discussion

We have proposed the implementation of the universal continuous-variable QC based on the preparation of $|H\rangle$ rather than $|0\rangle$ of the GKP code combined with the Gaussian operations. Our main contribution is the fundamental cost reduction of the non-Gaussian resources compared to the existing proposal [BPA$^+$19] by the direct preparation of $|H\rangle$. This can avoid the costly distillation in [BPA$^+$19] for converting $|0\rangle$ states into a $|H\rangle$ state, and achieve a constant overhead in converting $|H\rangle$ states into a $|0\rangle$ state. This cost reduction holds under the condition that the preparation of the non-Gaussian states such as the GKP $|0\rangle$ and $|H\rangle$ states are equally costly compared to Gaussian operations, which is true in the quantum optical system. It holds neither for qubit error-correcting codes in which the preparation of the magic state is much more costly than that of the Pauli eigenstate nor for the continuous-variable systems other than the quantum optical system in which Gaussian operations are not necessarily easy compared to the non-Gaussian operations.

In addition to the development of the cost-reduced protocol, we have introduced the measure $\widetilde{\mathcal{N}}_L$ to quantify the non-Gaussianity of the ideal GKP states and addressed the fundamental limitation on the convertibility between GKP $|H\rangle$ and $|0\rangle$

under Gaussian operations. Our findings of the usefulness of the resource theory of non-Gaussianity in the continuous-variable QC may open up new directions for the applications of the resource theory in continuous-variable systems. We have also discussed two promising protocols for the direct preparation of $|H\rangle$ in the quantum optical system; one is based on the breeding of peaks of approximate GKP states (Refs. [WT18, HPB$^+$21]), and the other is on the photon-number-resolving measurement (Refs. [ENP19, TBMS20, FTE$^+$21]). We point out that not much attention has been paid to the direct preparations of the GKP magic state $|H\rangle$. Our results thus put forward an argument on which of the GKP-encoded state should be used for the initialization to implement the fault-tolerant optical QC, while more concrete comparisons for the implementation cost may require further assumptions on advances in quantum optical technologies and hence are left for future work.

5.5 Conclusion for this chapter

In this chapter, we focus on the GKP code, which encodes a digitized degree of freedom into a continuous-variable system. The GKP code can correct displacement errors in the continuous-variable system up to half the lattice spacing of the GKP-encoded state. The ideal GKP code, however, assumes the use of an unphysical state and should thus be regarded as the limit of its approximations. There are several conventional approximations of the GKP states, which are thought to be equivalent at least in the limit of good approximation, but the lack of explicit correspondence prevents the accurate comparison between researches based on the different conventions. In Section 5.3, we showed that these conventional (symmetric) approximations of the GKP states are equivalent by showing the exact correspondence between approximation parameters. This result motivates us to introduce the standard form of approximate GKP codes, and for the standard form, we derived their Wigner functions, the inner products, and the average photon numbers. Our results bridge the gap for the past studies based on different approximations and may be useful to analyze the recent and near-future experimental realizations of the approximate GKP-encoded states.

There are several reasons why the GKP code is suitable for the optical fault-tolerant continuous-variable QC. The foremost reason is that Gaussian operations, which can be reliably implemented in quantum optical systems, are sufficient, in addition to the preparation of the GKP-encoded states, to achieve the fault-tolerant universal QC. In Section 5.4, we showed that, in addition to Gaussian operations, the ability to prepare only one type of the GKP-encoded magic state is sufficient to realize the fault-tolerant universality in a cost-efficient way. The cost-efficiency is achieved by the deterministic state conversion from the GKP magic states to the GKP Pauli state with Gaussian operations, while the known state conversion from the GKP Pauli states to the GKP magic state is probabilistic. To analyze the state convertibility between the GKP-encoded states under Gaussian operations, we apply the resource theory of non-Gaussianity. Our argument of cost efficiency is implicitly based on the fact that the required cost for generating the GKP magic state is comparable to that for generating the GKP Pauli state, which is not true for the majority of the qubit-based quantum error-correcting codes. To justify this, we proposed possible ways to directly prepare the GKP magic state with slight modifications to the existing proposals for the experimental GKP Pauli state realization.

With the results in Sections 5.3 and 5.4 combined, the (approximate) GKP code is shown to be a powerful tool to realize the optical fault-tolerant continuous-variable QC [BAV$^+$21, TMA$^+$21]. Our results thus show rich potentials of the continuous-variable system for realizing the fault-tolerant universal QC by encoding the digitized quantum information into the continuous-variable system such as the GKP code.

Chapter 6

Conclusion

For experimental implementations of quantum information processing, a promising candidate for the hardware is a continuous-variable system, a quantum optical system as a prominent example. In this thesis, we studied digital quantum information processing with continuous-variable systems. More specifically, we studied continuous-variable quantum key distribution (QKD) and continuous-variable quantum computation (QC) based on digitized information processing.

For continuous-variable QKD, we developed a binary-modulation protocol that is adapted to digital signal processing and proved its composable security against general attacks in the case of a finite number of communication rounds. This complete security proof was obtained by the newly developed fidelity estimation to an arbitrary coherent state using the heterodyne measurement and the classical post-processing. Using the fidelity as the measure of disturbance, we obtained an upper bound on the number of phase errors that reflect the information leakage to the eavesdropper by the heuristic operator inequality. The finite-size security against general attacks for discrete-modulation continuous-variable QKD protocols had been an open problem; our result partially solves the problem and can be a milestone for the ultimate goal. The obtained key rate with our security proof did not, however, achieve the asymptotically optimal scaling rate estimated in previous studies. Therefore, we further refined the proof based on the reverse reconciliation, the frequently used technique in the field of the continuous-variable QKD, with a slight modification to the classical post-processing in the original protocol while keeping the original experimental setups unchanged. As a result, under the pure-loss channel, the protocol asymptotically achieves an almost optimal key-rate scaling against the transmissivity. Thus, the developed protocol turns out to have fairly good performance for quantum channels that are close to the pure loss. Based on the results in this thesis, the next step is to generalize the security proof to more general discrete-modulation continuous-variable QKD protocols and obtain higher tolerance against excess noises, which has practical as well as theoretical importance.

For continuous-variable QC, we gave several results on the GKP code, which encodes a qudit into a continuous-variable system and has many desirable properties for optical QC. The GKP code can be implemented in a physical system only approximately, and thus several approximations of the GKP code have been widely used. We showed that these conventional approximations are equivalent by showing the ex-

plicit correspondence between the approximation parameters. This result bridges the gap of previous studies that were based on different approximations. Furthermore, we constructed a resource-efficient protocol to realize the universal QC, requiring the preparation of only one type of the GKP-encoded magic state and Gaussian operations. We showed the deterministic GKP state conversion from the two GKP-encoded magic states to the GKP-encoded Pauli state while only the probabilistic conversion is known for the converse direction. We deepened the analysis for the convertibility of the GKP-encoded states using the resource theory of non-Gaussianity. Our resource estimation implicitly assumed that the preparation of the GKP magic states was as costly as the preparation of the GKP Pauli states. We justified this by showing that the slight modifications to some of the existing proposals for implementing GKP Pauli states can realize the GKP magic state preparation. Notably, for the proposals of using parametrized linear optical circuits followed by photon-number-resolving detectors to implement the GKP-encoded states, it is already known that the GKP magic state can be implemented on equal footing with the GKP Pauli state. Our results thus show the rich potentials of the GKP code for realizing fault-tolerant continuous-variable QC and may lead to mitigating the implementation cost of the optical fault-tolerant continuous-variable QC.

Throughout the thesis, we have developed information processing of quantum and classical digital information encoded in continuous-variable quantum systems. Thus, the contributions of this thesis are to elaborate the theory and enhance the experimental feasibility for digital information processing with the continuous-variable system, which opens up new possibilities for this field.

Appendix A

The grid representation

The grid representation appeared in the paper by Zak [Zak68], and was later elaborated upon [Jan82, GM96] and used in the context of quantum information theory [KKW+16, TW16, DTW17, WT18]. Here we make a brief review. Let $(u,v) \in [0,1)\times[0,1)$, and $\mathcal{V}(u,v) \coloneqq V\left((2\pi v/(\alpha_d d), \alpha_d d u)^\top\right)$. Then, $e^{-\pi i t}\mathcal{V}$ forms a Heisenberg group $e^{-\pi i t}\mathcal{V}(u,v)\cdot e^{-\pi i t'}\mathcal{V}(u',v') = e^{-\pi i(t+t'+uv'-u'v)}\mathcal{V}(u+u',v+v')$. Define $|u,v\rangle_{\text{grid}}$ as

$$|u,v\rangle_{\text{grid}} \coloneqq \mathcal{V}(u,v)\,|0^{(\text{ideal})}\rangle \tag{A.1}$$

$$= e^{-\pi i u v} Z(2\pi v/(\alpha_d d)) X(\alpha_d d u)\,|0^{(\text{ideal})}\rangle\,. \tag{A.2}$$

In Refs. [TW16, DTW17, WT18], $|u,v\rangle_{\text{grid}}$ with $d=1$ is called the "shifted grid state". The generalized "shifted grid state" $|u,v\rangle_{\text{grid}}$ with arbitrary d satisfies an orthogonality and completeness relation in the following sense [KKW+16, WT18]:

$$\langle u,v|u',v'\rangle_{\text{grid}} = \delta(u-u')\delta(v-v'),$$
$$\int_0^1 du \int_0^1 dv\ \ |u,v\rangle\langle u,v|_{\text{grid}} = I.$$

The "wave function" $\phi_f(u,v)$ of a state $|f\rangle$ with respect to the "shifted grid states", i.e., the grid representation of $|f\rangle$, is defined as $\phi_f(u,v) \coloneqq \langle u,v|f\rangle$, which satisfies

$$\int_0^1 du \int_0^1 dv \left|\phi_f(u,v)\right|^2 = 1. \tag{A.3}$$

The "wave function" of the ideal GKP logical basis state $|j^{(\text{ideal})}\rangle$ can be regarded as a Dirac delta function centered at $(j/d,0)$, which does not satisfy Eq. (A.3) and therefore, cannot be regarded as a physical state. However, functions satisfying Eq. (A.3) and localized at $(j/d,0)$ are well-defined approximate logical basis states.

Given the position representation $\psi_f(q) \coloneqq \langle q|f\rangle$ of a (pure) state $|f\rangle$, its grid representation $\phi_f(u,v)$ can be given by

$$\phi_f(u,v) \coloneqq \langle u,v|f\rangle \tag{A.4}$$

$$= \int dq\ \ \langle u,v|_{\text{grid}}\,|q\rangle\langle q|_{\hat{q}}\,|f\rangle \tag{A.5}$$

$$= \sqrt{\alpha_d d}\sum_{s\in\mathbb{Z}} e^{-2\pi i v\left(s+\frac{u}{2}\right)}\psi_f\left(\alpha_d d(u+s)\right). \tag{A.6}$$

Using the last equality, we can expand the domain $[0,1)\times[0,1)$ of the "wave function" of the grid representation ϕ to $\mathbb{R}^2$. This redefined "wave function" $\phi:\mathbb{R}^2\to\mathbb{C}$ satisfies Eq. (A.3) and the following:

$$\forall(n_1,n_2)^\top\in\mathbb{Z}^2,\qquad \phi(u+n_1,v+n_2)=e^{-\pi i(n_1n_2+un_2-vn_1)}\phi(u,v), \tag{A.7}$$

which can be confirmed from Eq. (A.6). The functions $\phi:\mathbb{R}^2\to\mathbb{C}$ that satisfy Eqs. (A.3) and (A.7) form a representation space of the Heisenberg group called $L^2(\mathbb{R}^2/\mathbb{Z}^2)$ [MNN07], where the action of the group element $\mathrm{Op}(\cdot)$ on ϕ is given by

$$\mathrm{Op}(e^{-\pi i}\mathcal{V}(u,v))\phi_f(x,y) \coloneqq \langle x,y|_{\mathrm{grid}}\, e^{-\pi it}\mathcal{V}(u,v)\,|f\rangle \tag{A.8}$$

$$= e^{-\pi i(t+xv-yu)}\phi_f(x-u,y-v). \tag{A.9}$$

The formulation can easily be generalized to the g-mode case by considering the representation space $L^2(\mathbb{R}^{2g}/\mathbb{Z}^{2g})$ [MNN07].

Appendix B

Proofs of the propositions and lemmas in Section 5.3

B.1 Proof of Proposition 5.3.2 and Lemma 5.3.3

First, we derive Eqs. (5.43), (5.45), and (5.47) in Proposition 5.3.2. In the main text, α is fixed to α_d for $|j^{(\mathrm{ideal})}\rangle$ and all the approximations, but here, for later use, we perform calculation for a general α; that is, we derive the position representation of $|j^{(1)}_{\kappa,\Delta,\alpha}\rangle$, $|j^{(2)}_{\gamma,\delta,\alpha}\rangle$, and $|j^{(3)}_{\beta,\alpha}\rangle$. We start with the derivation of Eq. (5.43). We have

$$\langle q|j^{(1)}_{\kappa,\Delta,\alpha}\rangle = \frac{1}{\sqrt{N^{(1)}_{\kappa,\Delta,j}}} \sum_{s\in\mathbb{Z}} e^{-\frac{1}{2}\kappa^2\alpha^2(ds+j)^2} \langle q|_{\hat{q}}\, X(\alpha(ds+j)) S\left(-\ln\Delta\right)|0\rangle_f \tag{B.1}$$

$$= \sum_{s\in\mathbb{Z}} \frac{e^{-\frac{1}{2}\kappa^2\alpha^2(ds+j)^2}}{\sqrt{\Delta N^{(1)}_{\kappa,\Delta,j}}} \langle (q-\alpha(ds+j))/\Delta|0\rangle_f \tag{B.2}$$

$$= \left(\sqrt{\pi\Delta^2} N^{(1)}_{\kappa,\Delta,j}\right)^{-\frac{1}{2}} \sum_{s\in\mathbb{Z}} e^{-\frac{1}{2}\kappa^2\alpha^2 d^2\left(s+\frac{j}{d}\right)^2 - \frac{1}{2\Delta^2}\left(q-\alpha d\left(s+\frac{j}{d}\right)\right)^2} \tag{B.3}$$

$$= \left(\frac{2\sqrt{\pi\Delta^2}}{N^{(1)}_{\kappa,\Delta,j}}\right)^{\frac{1}{2}} E_{\frac{1}{\kappa^2},\alpha d,\frac{j}{d}} * G_{\Delta^2}(q), \tag{B.4}$$

where we used $\langle q|_{\hat{q}}\, X(a) = \langle q-a|_{\hat{q}}$ and $\langle q|_{\hat{q}}\, S(r) = \langle e^r q|_{\hat{q}}\, e^{r/2}$ in the second equality, and $\langle q|0\rangle_f = \pi^{-\frac{1}{4}} \exp(-q^2/2)$ in the third equality. Substituting α with α_d in Eq. (B.4), we obtain Eq. (5.43).

The derivation of Eq. (5.45) is similar. We have

$$\langle q|j^{(2)}_{\gamma,\delta,\alpha}\rangle = \frac{1}{\sqrt{N^{(2)}_{\gamma,\delta,j}}} \iint \frac{dr_1 dr_2}{2\pi\gamma\delta}\, e^{-\frac{r_1^2}{2\gamma^2}-\frac{r_2^2}{2\delta^2}} \langle q|_{\hat{q}}\, V(\boldsymbol{r})\, |j^{(\mathrm{ideal})}\rangle \tag{B.5}$$

$$= \frac{1}{\sqrt{N^{(2)}_{\gamma,\delta,j}}} \iint \frac{dr_1 dr_2}{2\pi\gamma\delta}\, e^{-\frac{r_1^2}{2\gamma^2}-\frac{r_2^2}{2\delta^2}-\frac{ir_1r_2}{2}+ir_1 q} \langle q-r_2|j^{(\mathrm{ideal})}\rangle\,, \tag{B.6}$$

where we used $V(\boldsymbol{r}) \coloneqq \exp(-ir_p r_q/2) Z(r_p) X(r_q)$, $\langle q|_{\hat{q}}\, Z(r_p) = \langle q|_{\hat{q}}\, e^{-ir_p q}$, and $\langle q|_{\hat{q}}\, X(r_q) =$

$\langle q - r_q|_{\hat{q}}$. Using $\langle q - r_2|j^{(\text{ideal})}\rangle = \sum_{s\in\mathbb{Z}} \delta\left(\alpha(ds+j) - q + r_2\right)$, we have

$$(\text{B.6}) = \left(\frac{\alpha d}{N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} \iint \frac{dr_1 dr_2}{2\pi\gamma\delta}\, e^{-\frac{r_1^2}{2\gamma^2} - \frac{r_2^2}{2\delta^2} - \frac{ir_1r_2}{2} + ir_1 q} \sum_{s\in\mathbb{Z}} \delta\left(r_2 - q + \alpha(ds+j)\right) \tag{B.7}$$

$$= \left(\frac{\alpha d}{N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} \int \frac{dr_1}{2\pi\gamma\delta}\, e^{-\frac{1}{2\gamma^2}\left[r_1 - \frac{i\gamma^2}{2}(q+\alpha(ds+j))\right]^2 - \frac{\gamma^2}{8}(q+\alpha(ds+j))^2 - \frac{1}{2\delta^2}(q-\alpha(ds+j))^2} \tag{B.8}$$

$$= \left(\frac{\alpha d}{2\pi\delta^2 N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} e^{-\frac{\lambda(\gamma,\delta)q^2}{2\delta^2}} \sum_{s\in\mathbb{Z}} e^{-\frac{\alpha^2 d^2 \lambda(\gamma,\delta)}{2\delta^2}\left(s+\frac{j}{d}\right)^2 + \frac{\alpha d q}{\delta^2}\left(\lambda(\gamma,\delta) - \frac{\gamma^2\delta^2}{2}\right)\left(s+\frac{j}{d}\right)} \tag{B.9}$$

$$= \left(\frac{\alpha d}{2\pi\delta^2 N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} e^{-\frac{\lambda(\gamma,\delta)}{2\delta^2}\left[q - \alpha d\left(1 - \frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)\left(s+\frac{j}{d}\right)\right]^2 - \frac{\alpha^2 d^2 \lambda(\gamma,\delta)}{2\delta^2}\left[1 - \left(1 - \frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^2\right]\left(s+\frac{j}{d}\right)^2} \tag{B.10}$$

$$= \left(\frac{\alpha d}{\lambda(\gamma,\delta) N^{(2)}_{\gamma,\delta,j}}\right)^{\frac{1}{2}} E_{\frac{\lambda(\gamma,\delta)}{\gamma^2}\left(1 - \frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^2, \alpha d\left(1 - \frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right), \frac{j}{d}} * G_{\frac{\delta^2}{\lambda(\gamma,\delta)}}(q), \tag{B.11}$$

where we used a Gaussian integral in the third equality, and used

$$1 - \left(1 - \frac{\gamma^2\delta^2}{2\lambda(\gamma,\delta)}\right)^2 = \left(\frac{\gamma\delta}{\lambda(\gamma,\delta)}\right)^2 \tag{B.12}$$

in the last equality. Substituting α with α_d in Eq. (B.11) leads to Eq. (5.45).

The derivation of Eq. (5.47) needs a trick. We have

$$\langle q|j^{(3)}_{\beta,\alpha}\rangle = \frac{1}{\sqrt{N^{(3)}_{\beta,j}}} \langle q|_{\hat{q}} \sum_{n\in\mathbb{N}} |n\rangle\langle n|_f\, e^{-\beta\left(n+\frac{1}{2}\right)} |j^{(\text{ideal})}\rangle \tag{B.13}$$

$$= \left(\frac{\alpha d}{N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} \sum_{n\in\mathbb{N}} e^{-\beta\left(n+\frac{1}{2}\right)} \psi_n(q)\psi_n^*(\alpha(ds+j)), \tag{B.14}$$

where $\psi_n(x) \coloneqq (2^n n!\sqrt{\pi})^{-1/2} e^{-x^2/2} H_n(x)$ denotes the wave function of the Fock state. Using Mehler's Hermite polynomial formula [Wei]

$$\sum_{n\in\mathbb{N}} \frac{(u/2)^n}{n!} H_n(x) H_n(y) \exp\left(-\frac{x^2+y^2}{2}\right) = \frac{1}{\sqrt{1-u^2}} \exp\left[-\frac{(1+u^2)(x^2+y^2) - 4uxy}{2(1-u^2)}\right], \tag{B.15}$$

we obtain

$$\langle q|j^{(3)}_{\beta}\rangle = \left(\frac{\pi^{-1} e^{-\beta}\alpha d}{(1-e^{-2\beta}) N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} e^{-\frac{(1+e^{-2\beta})\left(q^2 + \alpha^2(ds+j)^2\right)}{2(1-e^{-2\beta})} - \frac{4e^{-\beta}\alpha(ds+j)q}{2(1-e^{-2\beta})}} \tag{B.16}$$

$$= \left(\frac{(2\pi)^{-1}\alpha d}{\sinh\beta N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} e^{-\frac{\alpha^2 d^2}{2\tanh\beta}\left(s+\frac{j}{d}\right)^2 + \frac{\alpha d q}{\sinh\beta}\left(s+\frac{j}{d}\right) - \frac{q^2}{2\tanh\beta}} \tag{B.17}$$

$$= \left(\frac{(2\pi)^{-1}\alpha d}{\sinh\beta N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} \sum_{s\in\mathbb{Z}} e^{-\frac{1}{2\tanh\beta}\left(q-\frac{\alpha d}{\cosh\beta}\left(s+\frac{j}{d}\right)\right)^2-\frac{\alpha^2 d^2\tanh\beta}{2}\left(s+\frac{j}{d}\right)^2} \tag{B.18}$$

$$= \left(\frac{\alpha d}{\cosh\beta\ N^{(3)}_{\beta,j}}\right)^{\frac{1}{2}} E_{\frac{1}{\sinh\beta\cosh\beta},\frac{\alpha d}{\cosh\beta},\frac{j}{d}} * G_{\tanh\beta}(q). \tag{B.19}$$

Substituting α with α_d in Eq. (B.19) leads to Eq. (5.47).

Next, we prove Lemma 5.3.3 to derive Eqs. (5.44), (5.46), and (5.48) from Eqs. (5.43), (5.45), and (5.47), respectively. From the definition of $E_{\mu,\Gamma,a}$ and $\tilde{E}_{\mu,\Gamma,a}$ in Definition 5.3.1 as well as the definition of G_ν in Eq. (5.40), we have

$$E_{\mu,\Gamma,a} * G_\nu(q) = \frac{1}{\sqrt{2\pi\nu}} \sum_{s\in\mathbb{Z}} \exp\left[-\frac{(s+a)^2\Gamma^2}{2\mu} - \frac{\left(q-(s+a)\Gamma\right)^2}{2\nu}\right] \tag{B.20}$$

$$= \frac{e^{-\frac{1}{2\nu}q^2}}{\sqrt{2\pi\nu}}\,\vartheta\begin{bmatrix}a\\0\end{bmatrix}\left(\frac{\Gamma q}{2\pi i\nu}, \frac{i(1+\nu/\mu)\Gamma^2}{2\pi\nu}\right), \tag{B.21}$$

$$\tilde{E}_{\mu,\Gamma,a} * G_\nu(q) = \frac{1}{\sqrt{2\pi\nu}} \sum_{s\in\mathbb{Z}} \exp\left[-\frac{s^2\Gamma^2}{2\mu} - \frac{(q+s\Gamma)^2}{2\nu} + 2\pi i a s\right] \tag{B.22}$$

$$= \frac{e^{-\frac{1}{2\nu}q^2}}{\sqrt{2\pi\nu}}\,\vartheta\begin{bmatrix}0\\a\end{bmatrix}\left(\frac{i\Gamma q}{2\pi\nu}, \frac{i(1+\nu/\mu)\Gamma^2}{2\pi\nu}\right). \tag{B.23}$$

The theta function has the following identity [MM07]

$$\vartheta(z/\tau, -1/\tau) = (-i\tau)^{\frac{1}{2}} \exp(\pi i z^2/\tau)\,\vartheta(z,\tau), \tag{B.24}$$

which leads to

$$\vartheta\begin{bmatrix}0\\a\end{bmatrix}(z/\tau, -1/\tau) = (-i\tau)^{\frac{1}{2}} \exp(\pi i z^2/\tau)\,\vartheta\begin{bmatrix}a\\0\end{bmatrix}(z,\tau). \tag{B.25}$$

Applying this to Eqs. (B.21) and (B.23), we have

$$\text{(B.21)} = \frac{e^{\left(-\frac{1}{2\nu}+\frac{1}{2\nu(1+\nu/\mu)}\right)q^2}}{\sqrt{(1+\nu/\mu)\Gamma^2}}\vartheta\begin{bmatrix}0\\a\end{bmatrix}\left(-\frac{q}{(1+\nu/\mu)\Gamma}, \frac{2\pi i\nu}{(1+\nu/\mu)\Gamma^2}\right) \tag{B.26}$$

$$= \sqrt{\frac{2\pi\mu}{\Gamma^2}}\ G_{\mu+\nu}(q)\ \vartheta\begin{bmatrix}0\\a\end{bmatrix}\left(-\frac{q}{(1+\nu/\mu)\Gamma}, \frac{2\pi i\nu}{(1+\nu/\mu)\Gamma^2}\right), \tag{B.27}$$

$$\text{(B.23)} = \sqrt{\frac{2\pi\mu}{\Gamma^2}}\ G_{\mu+\nu}(q)\ \vartheta\begin{bmatrix}a\\0\end{bmatrix}\left(-\frac{q}{(1+\nu/\mu)\Gamma}, \frac{2\pi i\nu}{(1+\nu/\mu)\Gamma^2}\right), \tag{B.28}$$

which proves Lemma 5.3.3. Then, as mentioned above, we obtain Eqs. (5.44), (5.46), and (5.48) by applying Lemma 5.3.3 to Eqs. (5.43), (5.45), and (5.47), respectively. □

B.2 Proof of Proposition 5.3.10

We compute $W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|}$ as follows:

$$
\begin{aligned}
&W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|} \\
&= \frac{1}{\pi}\int dx\, e^{2ipx}\,\langle q-x|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\,\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|q+x\rangle \qquad \text{(B.29)}\\
&= \frac{2\Gamma\left(\Lambda(\sigma_q^2,\sigma_p^2)\right)^{-\frac{1}{2}}}{\pi\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\int dx\, e^{2ipx}\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{2\sigma_p^2},\Gamma,\frac{j}{d}} * G_{2\sigma_q^2}(q-x)\right) \\
&\qquad\qquad \times\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{2\sigma_p^2},\Gamma,\frac{j'}{d}} * G_{2\sigma_q^2}(q+x)\right) \qquad \text{(B.30)}\\
&= \frac{\left(2\pi^2\sigma_q^2\sqrt{\Lambda(\sigma_q^2,\sigma_p^2)}\right)^{-1}\Gamma}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\int dx\, e^{2ipx}\sum_s \exp\left[-\frac{\left(s+\frac{j}{d}\right)^2\Gamma^2\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)}-\frac{1}{4\sigma_q^2}\left(q-x-\left(s+\frac{j}{d}\right)\Gamma\right)^2\right] \\
&\qquad\qquad \times\sum_{s'}\exp\left[-\frac{\left(s'+\frac{j'}{d}\right)^2\Gamma^2\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)}-\frac{1}{4\sigma_q^2}\left(q+x-\left(s'+\frac{j'}{d}\right)\Gamma\right)^2\right] \qquad \text{(B.31)}\\
&= \frac{\left(2\pi^2\sigma_q^2\sqrt{\Lambda(\sigma_q^2,\sigma_p^2)}\right)^{-1}\Gamma}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\int dx\,\sum_{s,s'}\exp\left(-\frac{1}{2\sigma_q^2}\left\{x-i\left[2\sigma_q^2p+\frac{i\Gamma}{2}\left(s+\frac{j}{d}-s'-\frac{j'}{d}\right)\right]\right\}^2\right) \\
&\quad\times\exp\left\{-\frac{1}{2\sigma_q^2}\left[2\sigma_q^2p+\frac{i\Gamma}{2}\left(s+\frac{j}{d}-s'-\frac{j'}{d}\right)\right]^2-\frac{1}{2\sigma_q^2}\left[q^2-\Gamma q\left(s+\frac{j}{d}+s'+\frac{j'}{d}\right)\right]\right\} \\
&\quad\times\exp\left\{-\frac{\Gamma^2}{2}\left(\frac{\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)}+\frac{1}{4\sigma_q^2}\right)\left[\left(s+\frac{j}{d}+s'+\frac{j'}{d}\right)^2+\left(s+\frac{j}{d}-s'-\frac{j'}{d}\right)^2\right]\right\} \qquad \text{(B.32)}\\
&= \frac{\left(2\pi^3\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)\right)^{-\frac{1}{2}}\Gamma}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\sum_{s,s'}\exp\left\{-\frac{\Gamma^2\sigma_p^2}{2\Lambda(\sigma_q^2,\sigma_p^2)}\left[\left(s+\frac{j}{d}+s'+\frac{j'}{d}\right)^2+\left(s+\frac{j}{d}-s'-\frac{j'}{d}\right)^2\right]\right\} \\
&\quad\times\exp\left\{-\frac{1}{2\sigma_q^2}\left[q-\frac{\Gamma}{2}\left(s+\frac{j}{d}+s'+\frac{j'}{d}\right)\right]^2-2\sigma_q^2p^2-i\Gamma p\left(s+\frac{j}{d}-s'-\frac{j'}{d}\right)\right\} \qquad \text{(B.33)}
\end{aligned}
$$

where we used the standard form (5.70) in the second equality. At this stage, we will change the variables for the summation from s and s' to $s+s'$ and $s-s'$. Since $s+s'$ and $s-s'$ have the same parity, the summation splits into two parts: one with $s+s'=2t,\ s-s'=2t'$, $(t,t'\in\mathbb{Z})$ and the other with $s+s'=2t+1,\ s-s'=2t'+1$. Thus, we have

$$= \frac{\left(2\pi^3\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)\right)^{-\frac{1}{2}}\Gamma}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\sum_{t,t'}\Bigg(\exp\Bigg\{-\frac{1}{2\sigma_q^2}\left[q-\Gamma\left(t+\frac{j+j'}{2d}\right)\right]^2-2\sigma_q^2p^2-2i\Gamma p\left(t'+\frac{j-j'}{2d}\right)\Bigg\}$$
$$\times\exp\Bigg\{-\frac{2\Gamma^2\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)}\left[\left(t+\frac{j+j'}{2d}\right)^2+\left(t'+\frac{j-j'}{2d}\right)^2\right]\Bigg\}$$
$$+\exp\Bigg\{-\frac{1}{2\sigma_q^2}\left[q-\Gamma\left(t+\frac{j+j'}{2d}+\frac{1}{2}\right)\right]^2-2\sigma_q^2p^2-2i\Gamma p\left(t'+\frac{j-j'}{2d}+\frac{1}{2}\right)\Bigg\}$$
$$\times\exp\Bigg\{-\frac{2\Gamma^2\sigma_p^2}{\Lambda(\sigma_q^2,\sigma_p^2)}\left[\left(t+\frac{j+j'}{2d}+\frac{1}{2}\right)^2+\left(t'+\frac{j-j'}{2d}+\frac{1}{2}\right)^2\right]\Bigg\}\Bigg) \tag{B.34}$$

$$= \frac{\left(\pi^2\Lambda(\sigma_q^2,\sigma_p^2)\right)^{-\frac{1}{2}}\Gamma}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\Bigg\{\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}}*G_{\sigma_q^2}(q)\right)e^{-2\sigma_q^2p^2}\vartheta\begin{bmatrix}\frac{j-j'}{2d}\\0\end{bmatrix}\left(-\frac{\Gamma p}{\pi},\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)$$
$$+\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}+\frac{1}{2}}*G_{\sigma_q^2}(q)\right)e^{-2\sigma_q^2p^2}\vartheta\begin{bmatrix}\frac{j-j'}{2d}+\frac{1}{2}\\0\end{bmatrix}\left(-\frac{\Gamma p}{\pi},\frac{2i\Gamma^2\sigma_p^2}{\pi\Lambda(\sigma_q^2,\sigma_p^2)}\right)\Bigg\} \tag{B.35}$$

$$= \frac{(2\pi\sigma_p^2)^{-\frac{1}{2}}}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\Bigg\{\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}}*G_{\sigma_q^2}(q)\right)e^{-\frac{p^2}{2\sigma_p^2}}\vartheta\begin{bmatrix}0\\\frac{j-j'}{2d}\end{bmatrix}\left(\frac{ip\Lambda(\sigma_q^2,\sigma_p^2)}{2\Gamma\sigma_p^2},\frac{\pi i\Lambda(\sigma_q^2,\sigma_p^2)}{2\Gamma^2\sigma_p^2}\right)$$
$$+\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}+\frac{1}{2}}*G_{\sigma_q^2}(q)\right)e^{-\frac{p^2}{2\sigma_p^2}}\vartheta\begin{bmatrix}0\\\frac{j-j'}{2d}+\frac{1}{2}\end{bmatrix}\left(\frac{ip\Lambda(\sigma_q^2,\sigma_p^2)}{2\Gamma\sigma_q^2},\frac{\pi i\Lambda(\sigma_q^2,\sigma_p^2)}{2\Gamma^2\sigma_p^2}\right)\Bigg\} \tag{B.36}$$

$$= \frac{(2\pi\sigma_p^2)^{-\frac{1}{2}}}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}$$
$$\times\sum_t\Bigg\{\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}}*G_{\sigma_q^2}(q)\right)e^{2\pi it\frac{j-j'}{2d}}e^{-\frac{1}{2\sigma_p^2}\left(p+\frac{\pi t\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma}\right)^2-\frac{2\pi^2t^2\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}}$$
$$+\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}+\frac{1}{2}}*G_{\sigma_q^2}(q)\right)e^{2\pi it\left(\frac{j-j'}{2d}+\frac{1}{2}\right)}e^{-\frac{1}{2\sigma_p^2}\left(p+\frac{\pi t\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma}\right)^2-\frac{2\pi^2t^2\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2}}\Bigg\} \tag{B.37}$$

$$= \frac{1}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}}\Bigg[\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}}*G_{\sigma_q^2}(q)\right)\left(\tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{j-j'}{2d}}*G_{\sigma_p^2}(p)\right)$$
$$+\left(E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j+j'}{2d}+\frac{1}{2}}*G_{\sigma_q^2}(q)\right)\left(\tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{j-j'}{2d}+\frac{1}{2}}*G_{\sigma_p^2}(p)\right)\Bigg], \tag{B.38}$$

where we used Eq. (B.25) in the third equality. □

B.3 The proof of Proposition 5.3.12

In order to derive the average photon number of the approximate code state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ in Definition 5.3.9, we first calculate the expectation values $\langle\hat{q}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ and $\langle\hat{p}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ of the squares $\hat{q}^2$ and $\hat{p}^2$ of the quadrature operators with respect to $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$, using its Wigner function (5.79). Then, one can obtain the average photon number $\langle\hat{n}\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ of the state $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ by exploiting the fact that $\langle\hat{q}^2+\hat{p}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} = \langle 2\hat{n}+1\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$. We frequently use Eqs. (5.83), (5.84), (5.85), and (5.86) in the following calculation. Let $\mathrm{pr}(q)$ and $\widetilde{\mathrm{pr}}(p)$ be the probability density functions to obtain the values q and p in the $\hat{q}$- and $\hat{p}$-quadrature measurements, respectively. Then, they can be given by

$$\mathrm{pr}(q) = \int dp\, W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j_{\sigma_q^2,\sigma_p^2,\Gamma}|}(q,p) \tag{B.39}$$

$$= \frac{1}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\left[c_1 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}} + c_2 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}+\frac{1}{2}}\right] * G_{\sigma_q^2}(q), \tag{B.40}$$

$$\widetilde{\mathrm{pr}}(p) = \int dq\, W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j_{\sigma_q^2,\sigma_p^2,\Gamma}|}(q,p) \tag{B.41}$$

$$= \frac{1}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\left[c_3 \tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},0} + c_4 \tilde{E}_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2},\frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma},\frac{1}{2}}\right] * G_{\sigma_p^2}(p), \tag{B.42}$$

where c_1, c_2, c_3, and c_4 are defined as

$$c_1 \coloneqq \vartheta\begin{bmatrix}0\\0\end{bmatrix}\left(0, 2\pi i\Gamma^{-2}\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)\right), \tag{B.43}$$

$$c_2 \coloneqq \vartheta\begin{bmatrix}0\\\frac{1}{2}\end{bmatrix}\left(0, 2\pi i\Gamma^{-2}\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)\right), \tag{B.44}$$

$$c_3 \coloneqq \vartheta\begin{bmatrix}\frac{j}{d}\\0\end{bmatrix}\left(0, 2\pi^{-1} i\Gamma^2\sigma_p^2\left[\Lambda(\sigma_q^2,\sigma_p^2)\right]^{-1}\right), \tag{B.45}$$

$$c_4 \coloneqq \vartheta\begin{bmatrix}\frac{j}{d}+\frac{1}{2}\\0\end{bmatrix}\left(0, 2\pi^{-1} i\Gamma^2\sigma_p^2\left[\Lambda(\sigma_q^2,\sigma_p^2)\right]^{-1}\right). \tag{B.46}$$

Note that the normalization constant $N_{\sigma_q^2,\sigma_p^2,\Gamma,j}$ satisfies $N_{\sigma_q^2,\sigma_p^2,\Gamma,j} = c_1c_3 + c_2c_4$ as shown in Eq. (5.80). Using $\mathrm{pr}(q)$, we calculate the expectation value of $\hat{q}^2$ as follows:

$$\langle\hat{q}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$$

$$= \int dq\, q^2\, \mathrm{pr}(q) \tag{B.47}$$

$$= \int dq \int dr\, \frac{q^2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\left[c_1 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}}(r) + c_2 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}+\frac{1}{2}}(r)\right] G_{\sigma_q^2}(q-r) \tag{B.48}$$

$$= \int dq \int dr\, \frac{r^2+2r(q-r)+(q-r)^2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\left[c_1 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}}(r) + c_2 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}+\frac{1}{2}}(r)\right] G_{\sigma_q^2}(q-r) \tag{B.49}$$

$$= \int dq'\, q'^2 G_{\sigma_q^2}(q') + \int dr\, \frac{r^2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}}\left[c_1 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}}(r) + c_2 E_{\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2},\Gamma,\frac{j}{d}+\frac{1}{2}}(r)\right] \tag{B.50}$$

$$= \sigma_q^2 + \int \frac{dr}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}} \Bigg\{ c_1 \left[\sum_{s\in\mathbb{Z}} \Gamma^2 \left(s + \frac{j}{d} \right)^2 e^{-\frac{\Gamma^2}{2\mu}\left(s+\frac{j}{d}\right)^2} \delta\Big(r - \Gamma\left(s + \frac{j}{d} \right) \Big) \right] + c_2 \left[\sum_{s\in\mathbb{Z}} \Gamma^2 \left(s + \frac{j}{d} + \frac{1}{2} \right)^2 e^{-\frac{\Gamma^2}{2\mu}\left(s+\frac{j}{d}+\frac{1}{2}\right)^2} \delta\Big(r - \Gamma\left(s + \frac{j}{d} + \frac{1}{2} \right) \Big) \right] \Bigg\} \Bigg|_{\mu=\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2}} \tag{B.51}$$

$$= \sigma_q^2 - \frac{2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}} \frac{\partial}{\partial(\mu^{-1})} \left[c_1 \vartheta \begin{bmatrix} \frac{j}{d} \\ 0 \end{bmatrix} \left(0, \frac{i\Gamma^2}{2\pi\mu} \right) + c_2 \vartheta \begin{bmatrix} \frac{j}{d}+\frac{1}{2} \\ 0 \end{bmatrix} \left(0, \frac{i\Gamma^2}{2\pi\mu} \right) \right] \Bigg|_{\mu=\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_p^2}}, \tag{B.52}$$

where we used the fact that $G_{\sigma_q^2}(x)$ has zero mean in the fourth and the fifth equality. In the same way, for the expectation value of $\hat{p}^2$, we have

$$\langle \hat{p}^2 \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} \tag{B.53}$$

$$= \sigma_p^2 - \frac{2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}} \frac{\partial}{\partial(\mu'^{-1})} \left[c_3 \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} \left(0, \frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\mu'\Gamma^2} \right) + c_4 \vartheta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} \left(0, \frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\mu'\Gamma^2} \right) \right] \Bigg|_{\mu'=\frac{\Lambda(\sigma_q^2,\sigma_p^2)}{4\sigma_q^2}}. \tag{B.54}$$

Now we define $\tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y)$ as

$$\begin{aligned} \tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y) \coloneqq\ & \vartheta \begin{bmatrix} \frac{j}{d} \\ 0 \end{bmatrix} \left(0, \frac{i\Gamma^2}{2\pi} x \right) \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} \left(0, \frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\Gamma^2} y \right) \\ & + \vartheta \begin{bmatrix} \frac{j}{d}+\frac{1}{2} \\ 0 \end{bmatrix} \left(0, \frac{i\Gamma^2}{2\pi} x \right) \vartheta \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} \left(0, \frac{\pi i[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{2\Gamma^2} y \right), \end{aligned} \tag{B.55}$$

where $N_{\sigma_q^2,\sigma_p^2,\Gamma,j} = \tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}\left(4\sigma_p^2[\Lambda(\sigma_q^2,\sigma_p^2)]^{-1}, 4\sigma_q^2[\Lambda(\sigma_q^2,\sigma_p^2)]^{-1} \right)$. Then, the average photon number is given by

$$\begin{aligned} \langle n \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} &= \frac{\langle \hat{q}^2 + \hat{p}^2 \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} - 1}{2} \\ &= \frac{\sigma_q^2 + \sigma_p^2 - 1}{2} - \left(\frac{\partial}{\partial x} + \frac{\partial}{\partial y} \right) \ln \tilde{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(x,y) \Bigg|_{x=4\sigma_p^2[\Lambda(\sigma_q^2,\sigma_p^2)]^{-1}, y=4\sigma_q^2[\Lambda(\sigma_q^2,\sigma_p^2)]^{-1}}, \end{aligned} \tag{B.56}$$

which proves Eq. (5.91). □

Appendix C

Alternative expressions for the Wigner function, inner products, and average photon number of the approximate GKP code

In this appendix, we derive alternative expressions for the Wigner function, inner products, and the average photon number of the standard form $|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle$ in terms of multi-variable generalization of the theta function, the Riemann theta function (also called Siegel theta function) [MM07]. For a row vector $\boldsymbol{z} \in \mathbb{C}^n$ and a matrix $\boldsymbol{\tau} \in \mathbb{C}^n \times \mathbb{C}^n$ with $\boldsymbol{\tau} = \boldsymbol{\tau}^\top$ and $\mathrm{Im}(\boldsymbol{\tau}) > 0$, the Riemann theta function $\Theta\begin{bmatrix}\boldsymbol{a}\\ \boldsymbol{b}\end{bmatrix}(\boldsymbol{z}, \boldsymbol{\tau})$, is defined as

$$\Theta\begin{bmatrix}\boldsymbol{a}\\ \boldsymbol{b}\end{bmatrix}(\boldsymbol{z}, \boldsymbol{\tau}) \coloneqq \sum_{\boldsymbol{s}\in\mathbb{Z}^n} \exp\Big[\pi i(\boldsymbol{s}+\boldsymbol{a})\boldsymbol{\tau}(\boldsymbol{s}+\boldsymbol{a})^\top + 2\pi i(\boldsymbol{z}+\boldsymbol{b})(\boldsymbol{s}+\boldsymbol{a})^\top\Big]. \tag{C.1}$$

We also define multivariate normal distribution $\bar{G}[\boldsymbol{\nu}](\boldsymbol{x})$ as

$$\bar{G}[\boldsymbol{\nu}](\boldsymbol{x}) \coloneqq \frac{1}{\sqrt{2\pi\det(\boldsymbol{\nu})}} \exp\Big(-\frac{1}{2}\boldsymbol{x}\boldsymbol{\nu}^{-1}\boldsymbol{x}^\top\Big). \tag{C.2}$$

Now we define a multi-variable function combining $E_{\mu,\Gamma,a}(x)$ and $\tilde{E}_{\mu,\Gamma,a}(x)$ as follows.

Definition C.0.1. For a symmetric 2×2 matrix $\boldsymbol{\mu}$ satisfying $\mathrm{Re}(\boldsymbol{\mu}) > 0$ and 2-dimensional row vectors $\boldsymbol{\Gamma}, \boldsymbol{a}$, and $\boldsymbol{b}$, let $\bar{E}\Big[\boldsymbol{\mu}, \boldsymbol{\Gamma}, \boldsymbol{a}, \boldsymbol{b}\Big](\boldsymbol{x})$ be defined as

$$\bar{E}\Big[\boldsymbol{\mu}, \boldsymbol{\Gamma}, \boldsymbol{a}, \boldsymbol{b}\Big](\boldsymbol{x}) \coloneqq \exp\Big(-\frac{1}{2}\boldsymbol{x}\boldsymbol{\mu}^{-1}\boldsymbol{x}^\top\Big) \sum_{\boldsymbol{s}\in\mathbb{Z}^2} e^{2\pi i\boldsymbol{b}(\boldsymbol{s}+\boldsymbol{a})^\top}\, \delta(\boldsymbol{x} - (\boldsymbol{s}+\boldsymbol{a}) \circ \boldsymbol{\Gamma}), \tag{C.3}$$

where $\circ$ denotes an Hadamard product $(A \circ B)_{ij} = (A)_{ij}(B)_{ij}$.

C.1 An alternative expression of the Wigner function

Under Definition C.0.1, we have an alternative expression of the Wigner function (5.79), which is relatively concise.

Corollary C.1.1 (Alternative expression of the Wigner function)**.** *The Wigner function given in Eq.* (5.79) *is alternatively represented as*

$$\begin{aligned} &W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma}|}(q,p) \\ &= \frac{1}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j} N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}} \bar{E}\left[\Lambda(\sigma_q^2,\sigma_p^2)\begin{pmatrix} 4\sigma_p^2 & 2i \\ 2i & 4\sigma_q^2 \end{pmatrix}^{-1}, \left(\tfrac{\Gamma}{2}, \tfrac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma}\right), \left(\tfrac{j+j'}{d}, 0\right), \left(0, \tfrac{j'}{d}\right)\right] \\ &\qquad \vec{*}\, \bar{G}\left[\begin{pmatrix} \sigma_q^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}\right](q,p), \end{aligned} \tag{C.4}$$

where $\bar{E}$ is defined in Definition C.0.1, and $\vec{*}$ denotes a convolution in a multivariate sense.

Proof. Comparing Eqs. (5.79) and (C.4), it is sufficient to show the following equality.

$$\begin{aligned} &\Big(E_{\mu,\Gamma,a} * G_{\sigma_q^2}(q)\Big)\Big(\tilde{E}_{\mu',\Gamma',a'} * G_{\sigma_p^2}(p)\Big) + \Big(E_{\mu,\Gamma,a+\frac{1}{2}} * G_{\sigma_q^2}(q)\Big)\Big(\tilde{E}_{\mu',\Gamma',a'+\frac{1}{2}} * G_{\sigma_p^2}(p)\Big) \\ &= \bar{E}\left[\begin{pmatrix} \mu^{-1} & \frac{2\pi i}{\Gamma\Gamma'} \\ \frac{2\pi i}{\Gamma\Gamma'} & \mu'^{-1} \end{pmatrix}^{-1}, \Big(\tfrac{\Gamma}{2}, \Gamma'\Big), \Big(2a, 0\Big), \Big(0, a-a'\Big)\right] \vec{*}\, \bar{G}\left[\begin{pmatrix} \sigma_q^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}\right](q,p). \end{aligned} \tag{C.5}$$

This follows from the following rearrangement of the summation.

$$\begin{aligned} &\Big(E_{\mu,\Gamma,a} * G_{\sigma_q^2}(q)\Big)\Big(\tilde{E}_{\mu',\Gamma',a'} * G_{\sigma_p^2}(p)\Big) + \Big(E_{\mu,\Gamma,a+\frac{1}{2}} * G_{\sigma_q^2}(q)\Big)\Big(\tilde{E}_{\mu',\Gamma',a'+\frac{1}{2}} * G_{\sigma_p^2}(p)\Big) \\ &= \iint dxdy \sum_{s,s'}\Bigg[\exp\Big(-\frac{x^2}{2\mu}\Big)\delta\Big(x-(s+a)\Gamma\Big)G_{\sigma_q^2}(q-x) \\ &\qquad\qquad \times \exp\Big(-\frac{y^2}{2\mu'} + 2\pi i a' s'\Big)\delta(y+s'\Gamma')G_{\sigma_p^2}(p-y) \\ &\qquad + \exp\Big(-\frac{x^2}{2\mu}\Big)\delta\Big(x-\Big(s+a+\frac{1}{2}\Big)\Gamma\Big)G_{\sigma_q^2}(q-x) \\ &\qquad\qquad \times \exp\Big(-\frac{y^2}{2\mu'} + 2\pi i\Big(a'+\frac{1}{2}\Big)s'\Big)\delta(y+s'\Gamma')G_{\sigma_p^2}(p-y)\Bigg] \\ &= \iint dxdy \sum_{s,s'}\Bigg[\exp\Big(-\frac{x^2}{2\mu}\Big)\delta\Big(x-(2s+2a)\frac{\Gamma}{2}\Big)G_{\sigma_q^2}(q-x) \\ &\qquad\qquad \times \exp\Big(-\frac{y^2}{2\mu'} - 2\pi i a' s' - \pi i(2s)s'\Big)\delta(y-s'\Gamma')G_{\sigma_p^2}(p-y) \\ &\qquad + \exp\Big(-\frac{x^2}{2\mu}\Big)\delta\Big(x-\Big(2s+1+2a\Big)\frac{\Gamma}{2}\Big)G_{\sigma_q^2}(q-x) \\ &\qquad\qquad \times \exp\Big(-\frac{y^2}{2\mu'} - 2\pi i a' s' - \pi i(2s+1)s'\Big)\delta(y-s'\Gamma')G_{\sigma_p^2}(p-y)\Bigg] \end{aligned} \tag{C.6, C.7}$$

$$= \iint dxdy \sum_{s',s''} \exp\Big[-\frac{x^2}{2\mu} - \frac{y^2}{2\mu'} - \pi i s'' s' - 2\pi i a' s'\Big] \times \delta\Big(x - (s'' + 2a)\frac{\Gamma}{2}\Big)\delta(y - s'\Gamma')\, \bar{G}\Big[\begin{pmatrix} \sigma_q^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}\Big](q - x, p - y) \tag{C.8}$$

$$= \iint dxdy \sum_{s',s''} \exp\Big[-\frac{1}{2}(x,y)\begin{pmatrix} \mu^{-1} & \frac{2\pi i}{\Gamma\Gamma'} \\ \frac{2\pi i}{\Gamma\Gamma'} & \mu'^{-1} \end{pmatrix}(x,y)^\top + 2\pi i(a - a')s'\Big] \times \delta\Big(x - (s'' + 2a)\frac{\Gamma}{2}\Big)\delta(y - s'\Gamma')\, \bar{G}\Big[\begin{pmatrix} \sigma_q^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}\Big](q - x, p - y) \tag{C.9}$$

$$= \bar{E}\left[\begin{pmatrix} \mu^{-1} & \frac{2\pi i}{\Gamma\Gamma'} \\ \frac{2\pi i}{\Gamma\Gamma'} & \mu'^{-1} \end{pmatrix}^{-1}, \Big(\frac{\Gamma}{2}, \Gamma'\Big), \Big(2a, 0\Big), \Big(0, a - a'\Big)\right] \vec{*}\, \bar{G}\Big[\begin{pmatrix} \sigma_q^2 & 0 \\ 0 & \sigma_p^2 \end{pmatrix}\Big](q,p). \tag{C.10}$$

□

Note that the right-hand side of Eq. (C.4) approaches the right-hand side of Eq. (5.32) as $\sigma_q^2, \sigma_p^2 \to 0$. Equation (C.4) fits a viewpoint that a state corresponding to the Wigner function $\bar{E}(q,p)$ is subject to Gaussian random displacement channel [CGH06], since random displacement can be represented as a convolution in the Wigner function picture. This viewpoint is utilized in numerical simulations of error analyses using approximate GKP codes [Men14, FTOF18, VAW+19, NC20, Wan19]. It should be noted that an operator corresponding to $\bar{E}(q,p)$ with parameters chosen as in Eq. (C.4) is neither a density operator nor a limit of density operators. There is thus no contradiction with the observation that an approximate GKP state differs from an ideal code state subject to random displacement noise, as stated in the explanation below the definition of Approximation 2.

C.2 Alternative expressions of normalization constant and inner product

The alternative expression of the Wigner function in Corollary C.1.1 leads to the following alternative concise expressions of the normalization constant and inner product with the Riemann theta function.

Corollary C.2.1 (Alternative expressions of normalization constant and inner product)**.** *The normalization factor given in Eq.* (5.80) *is alternatively represented as*

$$N_{\sigma_q^2,\sigma_p^2,\Gamma,j} = \Theta\begin{bmatrix} \Big(\frac{2j}{d}, 0\Big) \\ \Big(0, \frac{j}{d}\Big) \end{bmatrix}\left(\mathbf{0}, \begin{pmatrix} \frac{i\sigma_p^2\Gamma^2}{2\pi\Lambda(\sigma_q^2,\sigma_p^2)} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2} \end{pmatrix}\right). \tag{C.11}$$

Furthermore, the inner product given in Eq. (5.81) *is alternatively represented as*

$$\langle j'_{\sigma_q^2,\sigma_p^2,\Gamma} | j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle = \frac{1}{\sqrt{N_{\sigma_q^2,\sigma_p^2,\Gamma,j} N_{\sigma_q^2,\sigma_p^2,\Gamma,j'}}} \Theta\begin{bmatrix} \Big(\frac{j+j'}{d}, 0\Big) \\ \Big(0, \frac{j'}{d}\Big) \end{bmatrix}\left(\mathbf{0}, \begin{pmatrix} \frac{i\sigma_p^2\Gamma^2}{2\pi\Lambda(\sigma_q^2,\sigma_p^2)} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{2\pi i\sigma_q^2\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma^2} \end{pmatrix}\right). \tag{C.12}$$

Proof. We combine Eq. (5.82) with the followings:

$$\int d\boldsymbol{x}\, f(\boldsymbol{x}) \vec{*} g(\boldsymbol{x}) = \int d\boldsymbol{x}\, f(\boldsymbol{x}) \int d\boldsymbol{y}\, g(\boldsymbol{y}), \tag{C.13}$$

$$\begin{aligned}\int d\boldsymbol{x}\, \bar{E}[\boldsymbol{\mu}, \boldsymbol{\Gamma}, \boldsymbol{a}, \boldsymbol{b}](\boldsymbol{x}) &= \sum_{\boldsymbol{s}\in\mathbb{Z}^2} \exp\Big[-\tfrac{1}{2}\Big((\boldsymbol{s}+\boldsymbol{a})\circ\boldsymbol{\Gamma}\Big)^\top \boldsymbol{\mu}^{-1}\Big((\boldsymbol{s}+\boldsymbol{a})\circ\boldsymbol{\Gamma}\Big) + 2\pi i \boldsymbol{b}(\boldsymbol{s}+\boldsymbol{a})^\top\Big] \\ &= \Theta\begin{bmatrix}\boldsymbol{a}\\ \boldsymbol{b}\end{bmatrix}\left(\boldsymbol{0}, \frac{i}{2\pi}\boldsymbol{\mu}^{-1} \circ \begin{pmatrix} \Gamma_1^2 & \Gamma_1\Gamma_2 \\ \Gamma_1\Gamma_2 & \Gamma_2^2 \end{pmatrix}\right),\end{aligned} \tag{C.14}$$

$$\int d\boldsymbol{x}\, \bar{G}[\boldsymbol{\nu}](\boldsymbol{x}) = 1. \tag{C.15}$$

□

C.3 Alternative expression of average photon number

The alternative expression of the normalization constant leads to the following alternative expression of the average photon number with the Riemann theta function.

Corollary C.3.1 (Alternative expression of average photon number)**.** *The average photon number given in Eq.* (5.91) *is alternatively represented as*

$$\begin{aligned}\langle \hat{n} \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} = \frac{\sigma_q^2+\sigma_p^2-1}{2} \\ - \left(\frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{11}} + \frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{22}}\right) \ln \check{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(\boldsymbol{\mu}^{-1})\Big|_{\boldsymbol{\mu}^{-1}=\frac{1}{\Lambda(\sigma_q^2,\sigma_p^2)}\begin{pmatrix}4\sigma_p^2 & 2i\\ 2i & 4\sigma_q^2\end{pmatrix}},\end{aligned} \tag{C.16}$$

where $\check{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(\boldsymbol{\mu}^{-1})$ *is given by*

$$\check{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(\boldsymbol{\mu}^{-1}) := \Theta\begin{bmatrix}\left(\frac{2j}{d},0\right)\\ \left(0,\frac{j}{d}\right)\end{bmatrix}\left(\boldsymbol{0}, \frac{i}{2\pi}\boldsymbol{\mu}^{-1} \circ \begin{pmatrix} \frac{\Gamma^2}{4} & \frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{2} \\ \frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{2} & \frac{\pi^2[\Lambda(\sigma_q^2,\sigma_p^2)]^2}{\Gamma^2} \end{pmatrix}\right). \tag{C.17}$$

Proof. We give a more intuitive proof rather than direct calculation given in Sec. B.3. We see that $\langle \hat{q}^2+\hat{p}^2\rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ denotes a second moment of the (quasi)probability distribution $W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j_{\sigma_q^2,\sigma_p^2,\Gamma}|}$, which is a convolution of "normalized" $\bar{E}$ and $\bar{G}[\boldsymbol{\nu}]$. Since $\bar{G}[\boldsymbol{\nu}](\boldsymbol{x})$ has zero mean, the second moment of $W_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle\langle j_{\sigma_q^2,\sigma_p^2,\Gamma}|}$ is a summation of the second moment of "normalized" $\bar{E}$ and that of $\bar{G}[\boldsymbol{\nu}]$. (Eq. (B.50) also shows this fact.) The second moment of $\bar{G}[\boldsymbol{\nu}]$ is simply given by $\sigma_q^2+\sigma_p^2$. On the other hand, the second

moment of normalization times $\bar{E}$ is given by

$$\frac{1}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}} \int d\boldsymbol{x}\, \|\boldsymbol{x}\|^2 \bar{E}\left[\Lambda(\sigma_q^2,\sigma_p^2)\begin{pmatrix} 4\sigma_p^2 & 2i \\ 2i & 4\sigma_q^2 \end{pmatrix}^{-1}, \left(\frac{\Gamma}{2}, \frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma}\right), \left(\frac{2j}{d}, 0\right), \left(0, \frac{j}{d}\right)\right](\boldsymbol{x}) \tag{C.18}$$

$$= -\frac{2}{N_{\sigma_q^2,\sigma_p^2,\Gamma,j}} \int d\boldsymbol{x}$$

$$\left(\frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{11}} + \frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{22}}\right) \bar{E}\left[\boldsymbol{\mu}, \left(\frac{\Gamma}{2}, \frac{\pi\Lambda(\sigma_q^2,\sigma_p^2)}{\Gamma}\right), \left(\frac{2j}{d}, 0\right), \left(0, \frac{j}{d}\right)\right](\boldsymbol{x})\Bigg|_{\boldsymbol{\mu}=\Lambda(\sigma_q^2,\sigma_p^2)\begin{pmatrix} 4\sigma_p^2 & 2i \\ 2i & 4\sigma_q^2 \end{pmatrix}^{-1}} \tag{C.19}$$

$$= -2\left(\frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{11}} + \frac{\partial}{\partial(\boldsymbol{\mu}^{-1})_{22}}\right) \ln \check{N}_{\sigma_q^2,\sigma_p^2,\Gamma,j}(\boldsymbol{\mu}^{-1})\Big|_{\boldsymbol{\mu}^{-1}=\frac{1}{\Lambda(\sigma_q^2,\sigma_p^2)}\begin{pmatrix} 4\sigma_p^2 & 2i \\ 2i & 4\sigma_q^2 \end{pmatrix}}, \tag{C.20}$$

where we used Eq. (C.14) in the last equality. Combining these with the relation $\langle \hat{q}^2 + \hat{p}^2 \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle} = \langle 2\hat{n} + 1 \rangle_{|j_{\sigma_q^2,\sigma_p^2,\Gamma}\rangle}$ proves the statement. □

Bibliography

[AAB+19] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, Oct 2019.

[ABI+18] Juan M. Arrazola, Thomas R. Bromley, Josh Izaac, Casey R. Myers, Kamil Brádler, and Nathan Killoran. Machine learning method for state preparation and gate synthesis on photonic quantum computers. *Quantum Sci. Tech.*, 2018.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982.

[AG04] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004.

[AGPF18] Francesco Albarelli, Marco G. Genoni, Matteo G. A. Paris, and Alessandro Ferraro. Resource theory of quantum non-Gaussianity and Wigner negativity. *Phys. Rev. A*, 98:052350, Nov 2018.

[AND+18] Victor V. Albert, Kyungjoo Noh, Kasper Duivenvoorden, Dylan J. Young, RT Brierley, Philip Reinhold, Christophe Vuillot, Linshu Li, Chao Shen, and SM Girvin. Performance and structure of single-mode bosonic codes. *Physical Review A*, 97(3):032346, 2018.

[AS48] Milton Abramowitz and Irene A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55. US Government printing office, 1948.

[AVDB18] Akshay Agrawal, Robin Verschueren, Steven Diamond, and Stephen Boyd. A rewriting system for convex optimization problems. *Journal of Control and Decision*, 5(1):42–60, 2018.

[Azu67] Kazuoki Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal, Second Series*, 19(3):357–367, 1967.

[BAV+21] J. Eli Bourassa, Rafael N. Alexander, Michael Vasmer, Ashlesha Patil, Ilan Tzitrin, Takaya Matsuura, Daiqin Su, Ben Q. Baragiola, Saikat Guha, Guillaume Dauphinais, Krishna K. Sabapathy, Nicolas C. Menicucci, and Ish Dhand. Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer. *Quantum*, 5:392, February 2021.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[BCMS19] Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage. Trapped-ion quantum computing: Progress and challenges. *Applied Physics Reviews*, 6(2):021314, 2019.

[BCRV16] Detlev Buchholz, Fabio Ciolli, Giuseppe Ruzzi, and Ezio Vasselli. The Universal C*-Algebra of the Electromagnetic Field. *Letters in Mathematical Physics*, 106(2):269–285, Feb 2016.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[Ben80] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, May 1980.

[Ben92] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal Blind Quantum Computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526, Oct 2009.

[BFK10] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Measurement-based and universal blind quantum computation. In *International School on Formal Methods for the Design of Computer, Communication and Software Systems*, pages 43–86. Springer, 2010.

[BGK18] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[BH12] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012.

[BK05] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, Feb 2005.

[BK11] Bruce Berndt and Byungchan Kim. Asymptotic expansions of certain partial theta functions. *Proceedings of the American Mathematical Society*, 139(11):3779–3788, 2011.

[BKP13] Peter Brooks, Alexei Kitaev, and John Preskill. Protected gates for superconducting qubits. *Phys. Rev. A*, 87(5):052306, 2013.

[BPA+19] Ben Q. Baragiola, Giacomo Pantaleoni, Rafael N. Alexander, Angela Karanjai, and Nicolas C. Menicucci. All-Gaussian universality and fault tolerance with the Gottesman-Kitaev-Preskill code. *Physical Review Letters*, 123(20):200502, 2019.

[BPLL20] J. Eli Bourassa, Ignatius William Primaatmaja, Charles Ci Wen Lim, and Hoi-Kwong Lo. Loss-tolerant quantum key distribution with mixed signal states. *Phys. Rev. A*, 102:062607, Dec 2020.

[Bra98] Samuel L. Braunstein. *Error correction for continuous quantum variables*, pages 19–29. Quantum Information with Continuous Variables. Springer, 1998.

[BvL05] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, Jun 2005.

[BvL16] Marcel Bergmann and Peter van Loock. Quantum error correction against photon loss using NOON states. *Physical Review A*, 94(1):012311, 2016.

[BW18] Kamil Brádler and Christian Weedbrook. Security proof of continuous-variable quantum key distribution using three coherent states. *Physical Review A*, 97(2):022310, 2018.

[CD94] Carlton M. Caves and P. D. Drummond. Quantum limits on bosonic communication rates. *Rev. Mod. Phys.*, 66:481–537, Apr 1994.

[CDG+19] Ulysse Chabaud, Tom Douce, Frédéric Grosshans, Elham Kashefi, and Damian Markham. Building trust for continuous variable quantum states, 2019. 1905.12700.

[CEGH08] F Caruso, J Eisert, V Giovannetti, and A S Holevo. Multi-mode bosonic Gaussian channels. *New Journal of Physics*, 10(8):083030, aug 2008.

[CEGH11] Filippo Caruso, Jens Eisert, Vittorio Giovannetti, and Alexander S. Holevo. Optimal unitary dilation for bosonic Gaussian channels. *Phys. Rev. A*, 84:022306, Aug 2011.

[CG69] K. E. Cahill and R. J. Glauber. Density Operators and Quasiprobability Distributions. *Phys. Rev.*, 177:1882–1902, Jan 1969.

[CG06] Filippo Caruso and Vittorio Giovannetti. Degradability of Bosonic Gaussian channels. *Phys. Rev. A*, 74:062307, Dec 2006.

[CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. *Rev. Mod. Phys.*, 91:025001, Apr 2019.

[CGH06] F Caruso, V Giovannetti, and A S Holevo. One-mode bosonic Gaussian channels: a full weak-degradability classification. *New Journal of Physics*, 8(12):310–310, dec 2006.

[CGKM21] Ulysse Chabaud, Frédéric Grosshans, Elham Kashefi, and Damian Markham. Efficient verification of Boson Sampling. *Quantum*, 5:578, November 2021.

[Che52] Herman Chernoff. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *The Annals of Mathematical Statistics*, 23(4):493 – 507, 1952.

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975.

[Chv79] V. Chvátal. The tail of the hypergeometric distribution. *Discrete Mathematics*, 25(3):285–287, 1979.

[CIET+20] P Campagne-Ibarcq, A Eickbusch, S Touzard, E Zalys-Geller, NE Frattini, VV Sivak, P Reinhold, S Puri, S Shankar, RJ Schoelkopf, et al. Quantum error correction of a qubit encoded in grid states of an oscillator. *Nature*, 584(7821):368–372, 2020.

[CLA01] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, Apr 2001.

[CLP07] Nicolas J Cerf, Gerd Leuchs, and Eugene S Polzik. *Quantum information with continuous variables of atoms and light*. World Scientific, 2007.

[CLY97] Isaac L. Chuang, Debbie W. Leung, and Yoshihisa Yamamoto. Bosonic quantum codes for amplitude damping. *Physical Review A*, 56(2):1114, 1997.

[CMM99] Paul T. Cochrane, Gerard J. Milburn, and William J. Munro. Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping. *Physical Review A*, 59(4):2631, 1999.

[CT12] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[CW79] J. L. Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of computer and system sciences*, 18(2):143–154, 1979.

[DB16] Steven Diamond and Stephen Boyd. Cvxpy: A Python-embedded modeling language for convex optimization. *Journal of Machine Learning Research*, 17(83):1–5, 2016.

[DBL21] Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, September 2021.

[DHB+04] Bernard Deconinck, Matthias Heil, Alexander Bobenko, Mark Van Hoeij, and Marcus Schmies. Computing Riemann theta functions. *Mathematics of Computation*, 73(247):1417–1442, 2004.

[DL70] E. B. Davies and J. T. Lewis. An operational approach to quantum probability. *Communications in Mathematical Physics*, 17(3):239–260, Sep 1970.

[DL15] Eleni Diamanti and Anthony Leverrier. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy*, 17(9):6072–6092, 2015.

[DMK+17] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock, and G. Ferrini. Continuous-Variable Instantaneous Quantum Computing is Hard to Sample. *Phys. Rev. Lett.*, 118:070503, Feb 2017.

[DN05] Christopher M Dawson and Michael A Nielsen. The solovay-kitaev algorithm, 2005.

[DP85] David Deutsch and Roger Penrose. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[DPTG16] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Passive States Optimize the Output of Bosonic Gaussian Quantum Channels. *IEEE Transactions on Information Theory*, 62(5):2895–2906, 2016.

[DPTG17] Giacomo De Palma, Dario Trevisan, and Vittorio Giovannetti. Gaussian States Minimize the Output Entropy of the One-Mode Quantum Attenuator. *IEEE Transactions on Information Theory*, 63(1):728–737, 2017.

[DTW17] Kasper Duivenvoorden, Barbara M. Terhal, and Daniel Weigand. Single-mode displacement sensor. *Physical Review A*, 95(1):012305, 2017.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, 461(2053):207–235, 2005.

[EBKTB14] Jean Etesse, Rémi Blandino, Bhaskar Kanseri, and Rosa Tualle-Brouri. Proposal for a loophole-free violation of Bell's inequalities with a set of single photons and homodyne measurements. *New J. Phys.*, 16(5):053001, 2014.

[EHO+18] Tobias A. Eriksson, Takuya Hirano, Motoharu Ono, Mikio Fujiwara, Ryo Namiki, Ken-ichiro Yoshino, Akio Tajima, Masahiro Takeoka, and Masahide Sasaki. Coexistence of continuous variable quantum key distribution and 7×12.5 Gbit/s classical channels. In *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pages 71–72. IEEE, 2018.

[EHP+19] Tobias A. Eriksson, Takuya Hirano, Benjamin J. Puttnam, Georg Rademacher, Ruben S. Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, and Naoya Wada. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. *Communications Physics*, 2(1):1–8, 2019.

[ELP+20] Tobias A. Eriksson, Ruben S. Luís, Benjamin J. Puttnam, Georg Rademacher, Mikio Fujiwara, Yoshinari Awaji, Hideaki Furukawa, Naoya Wada, Masahiro Takeoka, and Masahide Sasaki. Wavelength Division Multiplexing of 194 Continuous Variable Quantum Key Distribution Channels. *Journal of Lightwave Technology*, 38(8):2214–2218, 2020.

[ENP19] Miller Eaton, Rajveer Nehra, and Olivier Pfister. Non-Gaussian and Gottesman–Kitaev–Preskill state preparation by photon catalysis. *New Journal of Physics*, 21(11):113034, 2019.

[EP03] J. EISERT and M. B. PLENIO. Introduction to the basics of entanglement theory in continuous-variable systems. *International Journal of Quantum Information*, 01(04):479–506, 2003.

[FC72] Stuart J. Freedman and John F. Clauser. Experimental Test of Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 28:938–941, Apr 1972.

[FEA+21] Kosuke Fukui, Mamoru Endo, Warit Asavanant, Atsushi Sakaguchi, Jun ichi Yoshikawa, and Akira Furusawa. Generating Gottesman-Kitaev-Preskill qubit using a cross-Kerr interaction between a squeezed light and Fock states in optics, 2021.

[Fey82] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, Jun 1982.

[FMA+20] N. Fabre, G. Maltese, F. Appas, S. Felicetti, A. Ketterer, A. Keller, T. Coudreau, F. Baboux, M. I. Amanti, S. Ducci, and P. Milman. Generation of a time-frequency grid state with integrated biphoton frequency combs. *Phys. Rev. A*, 102:012607, Jul 2020.

[FNM+19] Christa Flühmann, Thanh L. Nguyen, Matteo Marinelli, Vlad Negnevitsky, Karan Mehta, and JP Home. Encoding a qubit in a trapped-ion mechanical oscillator. *Nature*, 566(7745):513, 2019.

[FNMH18] Christa Flühmann, Vlad Negnevitsky, Matteo Marinelli, and Jonathan P. Home. Sequential modular position and momentum measurements of a trapped ion mechanical oscillator. *Phys. Rev. X*, 8(2):021001, 2018.

[FTE+21] Kosuke Fukui, Shuntaro Takeda, Mamoru Endo, Warit Asavanant, Jun ichi Yoshikawa, Peter van Loock, and Akira Furusawa. Efficient backcasting search for optical quantum state synthesis, 2021.

[FTO17] Kosuke Fukui, Akihisa Tomita, and Atsushi Okamoto. Analog quantum error correction with encoding a qubit into an oscillator. *Physical Review Letters*, 119(18):180507, 2017.

[FTOF18] Kosuke Fukui, Akihisa Tomita, Atsushi Okamoto, and Keisuke Fujii. High-Threshold Fault-Tolerant Quantum Computation with Analog Quantum Error Correction. *Phys. Rev. X*, 8:021054, May 2018.

[GÁFF21] L. García-Álvarez, A. Ferraro, and G. Ferrini. From the Bloch Sphere to Phase-Space Representations with the Gottesman–Kitaev–Preskill Encoding. In Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, and Yasuhiko Ikematsu, editors, *International Symposium on Mathematics, Quantum Theory, and Cryptography*, pages 79–92, Singapore, 2021. Springer Singapore.

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, 2002.

[GGDL19] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Physical Review X*, 9(2):021059, 2019.

[GGPCH14] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo. Ultimate classical communication rates of quantum optical channels. *Nature Photonics*, 8(10):796–800, Oct 2014.

[GHGP15] V. Giovannetti, A. S. Holevo, and R. García-Patrón. A Solution of Gaussian Optimizer Conjecture for Quantum Channels. *Communications in Mathematical Physics*, 334(3):1553–1571, Mar 2015.

[GK06] S. Glancy and E. Knill. Error analysis for encoding a qubit in an oscillator. *Physical Review A*, 73(1):012325, 2006.

[GKP01] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64(1):012310, 2001.

[GM96] D. Galetti and MA Marchiolli. Discrete coherent states and probability distributions in finite-dimensional spaces. *annals of physics*, 249(2):454–480, 1996.

[Got98] Daniel Gottesman. The Heisenberg representation of quantum computers, 1998.

[GPNBL+12] Raúl García-Patrón, Carlos Navarrete-Benlloch, Seth Lloyd, Jeffrey H. Shapiro, and Nicolas J. Cerf. Majorization Theory Approach to the Gaussian Channel Minimum Entropy Conjecture. *Phys. Rev. Lett.*, 108:110505, Mar 2012.

[GVAW+03] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.

[HA21] Jacob Hastrup and Ulrik L. Andersen. Generation of optical Gottesman-Kitaev-Preskill states with cavity QED, 2021.

[HC17] Mark Howard and Earl Campbell. Application of a Resource Theory for Magic States to Fault-Tolerant Quantum Computing. *Phys. Rev. Lett.*, 118:090501, Mar 2017.

[HHH+08] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Unconditional Privacy over Channels which Cannot Convey Quantum Information. *Phys. Rev. Lett.*, 100:110502, Mar 2008.

[HHHO09] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General Paradigm for Distilling Classical Key From Quantum States. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009.

[HHK20] Lisa Hänggli, Margret Heinze, and Robert König. Enhanced noise resilience of the surface–Gottesman-Kitaev-Preskill code via designed bias. *Phys. Rev. A*, 102:052408, Nov 2020.

[HHL+16] Duan Huang, Peng Huang, Huasheng Li, Tao Wang, Yingming Zhou, and Guihua Zeng. Field demonstration of a continuous-variable quantum key distribution network. *Optics Letters*, 41(15):3511–3514, 2016.

[HHPW17] Jeongwan Haah, Matthew B. Hastings, D. Poulin, and D. Wecker. Magic state distillation with low space overhead and optimal asymptotic input count. *Quantum*, 1:31, October 2017.

[Hil00] Mark Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):022309, 2000.

[HIM+17] Takuya Hirano, Tsubasa Ichikawa, Takuto Matsubara, Motoharu Ono, Yusuke Oguri, Ryo Namiki, Kenta Kasai, Ryutaroh Matsumoto, and Toyohiro Tsurumaru. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, 2(2):024010, 2017.

[HLLO06] Karol Horodecki, Debbie Leung, Hoi-Kwong Lo, and Jonathan Oppenheim. Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States. *Phys. Rev. Lett.*, 96:070501, Feb 2006.

[HLW+15] Duan Huang, Dakai Lin, Chao Wang, Weiqi Liu, Shuanghong Fang, Jinye Peng, Peng Huang, and Guihua Zeng. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Optics express*, 23(13):17511–17519, 2015.

[HM17] Aram W. Harrow and Ashley Montanaro. Quantum computational supremacy. *Nature*, 549:203–209, Sep 2017.

[Hoe63] Wassily Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, 58(301):13–30, 2021/12/08/ 1963. Full publication date: Mar., 1963.

[Hoe94] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. In *The collected works of Wassily Hoeffding*, pages 409–426. Springer, 1994.

[Hol73] A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973.

[Hol07] A. S. Holevo. One-mode quantum Gaussian channels: Structure and quantum capacity. *Problems of Information Transmission*, 43(1):1–11, Mar 2007.

[Hol11] Alexander S Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1. Springer Science & Business Media, 2011.

[Hol19] Alexander S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter, 2019.

[Hol21] A. S. Holevo. Structure of a General Quantum Gaussian Observable. *Proceedings of the Steklov Institute of Mathematics*, 313(1):70–77, Jul 2021.

[HP01] Jim Harrington and John Preskill. Achievable rates for the Gaussian quantum channel. *Physical Review A*, 64(6):062301, 2001.

[HPB+21] Jacob Hastrup, Kimin Park, Jonatan Bohr Brask, Radim Filip, and Ulrik Lund Andersen. Measurement-free preparation of grid states. *npj Quantum Information*, 7(1):17, Jan 2021.

[HQ11] Jinchuan Hou and Xiaofei Qi. Fidelity of states in infinite dimensional quantum systems, 2011.

[HRB08] H. Häffner, C.F. Roos, and R. Blatt. Quantum computing with trapped ions. *Phys. Rep.*, 469(4):155 – 203, 2008.

[HSH99] Alexander S. Holevo, Masaki Sohma, and Osamu Hirota. Capacity of quantum Gaussian channels. *Physical Review A*, 59(3):1820, 1999.

[HT12] Masahito Hayashi and Toyohiro Tsurumaru. Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9):093014, 2012.

[Hud74] R.L. Hudson. When is the wigner quasi-probability density non-negative? *Reports on Mathematical Physics*, 6(2):249–252, 1974.

[HW01] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Phys. Rev. A*, 63:032312, Feb 2001.

[HYA+03] Takuya Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki. Quantum cryptography using pulsed homodyne detection. *Physical Review A*, 68(4):042331, 2003.

[IH05] Kent D Irwin and Gene C Hilton. Transition-edge sensors. *Cryogenic particle detection*, pages 63–150, 2005.

[ISS11] J. Solomon Ivan, Krishna Kumar Sabapathy, and R. Simon. Operator-sum representation for bosonic Gaussian channels. *Phys. Rev. A*, 84:042311, Oct 2011.

[Jan82] Augustus Josephus Elizabeth Maria Janssen. Bargmann transform, Zak transform, and coherent states. *Journal of Mathematical Physics*, 23(5):720–731, 1982.

[JEKJ14] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, 90:042329, Oct 2014.

[JKJDL12] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Physical Review A*, 86(3):032309, 2012.

[JKJL+13] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature photonics*, 7(5):378–381, 2013.

[Jon13] Cody Jones. Multilevel distillation of magic states for quantum computing. *Phys. Rev. A*, 87:042305, Apr 2013.

[Kat20] Go Kato. Concentration inequality using unconfirmed knowledge, 2020.

[KBF+18] Fotini Karinou, Hans H. Brunner, Chi-Hang F. Fung, Lucian C. Comandar, Stefano Bettelli, David Hillerkuss, Maxim Kuschnerov, Spiros Mikroulis, Dawei Wang, and Changsong Xie. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photonics Technology Letters*, 30(7):650–653, 2018.

[KCB+17] F. Karinou, L. Comandar, HH Brunner, D. Hillerkuss, F. Fung, S. Bettelli, S. Mikroulis, D. Wang, Q. Yi, and M. Kuschnerov. Experimental evaluation of the impairments on a QKD system in a 20-channel WDM co-existence scheme. In *2017 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, pages 145–146. IEEE, 2017.

[KGW21] Eneet Kaur, Saikat Guha, and Mark M. Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Phys. Rev. A*, 103:012412, Jan 2021.

[Kir06] K. A. Kirkpatrick. The Schrödinger-HJW theorem. *Foundations of Physics Letters*, 19(1):95–102, Feb 2006.

[KKW+16] A. Ketterer, A. Keller, SP Walborn, T. Coudreau, and P. Milman. Quantum information processing in phase space: A modular variables approach. *Physical Review A*, 94(2):022325, 2016.

[KKY+19] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver. A quantum engineer's guide to superconducting qubits. *Applied Physics Reviews*, 6(2):021318, 2019.

[KL10] Pieter Kok and Brendon W Lovett. *Introduction to optical quantum information processing*. Cambridge university press, 2010.

[KLM01] Emanuel Knill, Raymond Laflamme, and Gerald J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46, 2001.

[Koa04] Masato Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters*, 93(12):120501, 2004.

[Koa09] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009.

[KQA15] Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics*, 17(4):043027, 2015.

[KRS09] Robert Konig, Renato Renner, and Christian Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009.

[KSVV02] Alexei Yu Kitaev, Alexander Shen, Mikhail N Vyalyi, and Mikhail N Vyalyi. *Classical and quantum computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[LBGP+07] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76:042305, Oct 2007.

[LC99] H. K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, Mar 26 1999.

[Lev15] Anthony Leverrier. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.*, 114:070501, Feb 2015.

[Lev17a] Anthony Leverrier. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Physical Review Letters*, 118(20):200501, 2017.

[Lev17b] Anthony Leverrier. $SU(q, p)$ coherent states and a Gaussian de Finetti theorem, 2017.

[LG09] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102(18):180504, 2009.

[LG11] Anthony Leverrier and Philippe Grangier. Erratum: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation [Phys. Rev. Lett. 102, 180504 (2009)]. *Phys. Rev. Lett.*, 106:259902, Jun 2011.

[LGMS19] Dat Thanh Le, Arne Grimsmo, Clemens Müller, and T. M. Stace. Doubly nonlinear superconducting qubit. *Phys. Rev. A*, 100:062321, Dec 2019.

[LGPRC13] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. *Phys. Rev. Lett.*, 110:030502, Jan 2013.

[LKGC09] A Leverrier, E Karpov, P Grangier, and N J Cerf. Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space. *New Journal of Physics*, 11(11):115009, nov 2009.

[LKV+13] Zaki Leghtas, Gerhard Kirchmair, Brian Vlastakis, Robert J. Schoelkopf, Michel H. Devoret, and Mazyar Mirrahimi. Hardware-efficient autonomous quantum memory protection. *Physical Review Letters*, 111(12):120501, 2013.

[LLX+21] Wen-Bo Liu, Chen-Long Li, Yuan-Mei Xie, Chen-Xun Weng, Jie Gu, Xiao-Yu Cao, Yu-Shuo Lu, Bing-Hong Li, Hua-Lei Yin, and Zeng-Bing Chen. Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum key Distribution with High Excess Noise Tolerance. *PRX Quantum*, 2:040334, Nov 2021.

[LO21] Cosmo Lupo and Yingkai Ouyang. Quantum key distribution with non-ideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols, 2021.

[LPF+18] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[LRS16] Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz. Coherent state constellations for Bosonic Gaussian channels. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2499–2503. IEEE, 2016.

[LRS17] Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz. Coherent-state constellations and polar codes for thermal Gaussian channels. *Physical Review A*, 95(6):062343, 2017.

[LRW+18] Ludovico Lami, Bartosz Regula, Xin Wang, Rosanna Nichols, Andreas Winter, and Gerardo Adesso. Gaussian quantum resource theories. *Phys. Rev. A*, 98:022335, Aug 2018.

[LS98] Seth Lloyd and Jean-Jacques E. Slotine. Analog quantum error correction. *Physical Review Letters*, 80(18):4088, 1998.

[LSW20] Chai-Yu Lin, Wang-Chang Su, and Shin-Tza Wu. Encoding qubits into harmonic-oscillator modes via quantum walks in phase space. *Quantum Information Processing*, 19(8):272, Jul 2020.

[LUL19] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 9(4):041064, 2019.

[Lup20] Cosmo Lupo. Towards practical security of continuous-variable quantum key distribution. *Phys. Rev. A*, 102:022623, Aug 2020.

[MBGM17] Keith R. Motes, Ben Q. Baragiola, Alexei Gilchrist, and Nicolas C. Menicucci. Encoding qubits into oscillators with atomic ensembles and squeezed light. *Physical Review A*, 95(5):053819, 2017.

[McD98] Colin McDiarmid. *Concentration*, pages 195–248. Probabilistic methods for algorithmic discrete mathematics. Springer, 1998.

[Men14] Nicolas C. Menicucci. Fault-tolerant measurement-based quantum computing with continuous-variable cluster states. *Physical Review Letters*, 112(12):120504, 2014.

[MGH14] A. Mari, V. Giovannetti, and A. S. Holevo. Quantum state majorization at the output of bosonic Gaussian channels. *Nature Communications*, 5(1):3826, May 2014.

[MM07] David Mumford and C. Musili. *Tata Lectures on Theta. I (Modern Birkhäuser classics)*. Birkhäuser Boston Incorporated, 2007.

[MMSK21] Takaya Matsuura, Kento Maeda, Toshihiko Sasaki, and Masato Koashi. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nature Communications*, 12(1):252, Jan 2021.

[MNN07] David Mumford, Madhav Nori, and Peter Norman. *Tata lectures on theta III*, volume 43. Springer, 2007.

[MQR09] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006, 2009.

[MSB+16] Marios H. Michael, Matti Silveri, RT Brierley, Victor V. Albert, Juha Salmilehto, Liang Jiang, and Steven M. Girvin. New class of quantum error-correcting codes for a bosonic mode. *Physical Review X*, 6(3):031006, 2016.

[MSK19] Takaya Matsuura, Toshihiko Sasaki, and Masato Koashi. Refined security proof of the round-robin differential-phase-shift quantum key distribution and its improved performance in the finite-sized case. *Physical Review A*, 99(4):042303, 2019.

[MVL+20] Dinka Milovančev, Nemanja Vokić, Fabian Laudenbach, Christoph Pacher, Hannes Hübel, and Bernhard Schrenk. Spectrally-Shaped Continuous-Variable QKD Operating at 500 MHz over an Optical Pipe Lit by 11 DWDM channels. In *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, 2020.

[MW95] Leonard Mandel and Emil Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995.

[MYK20] Takaya Matsuura, Hayata Yamasaki, and Masato Koashi. Equivalence of approximate Gottesman-Kitaev-Preskill codes. *Phys. Rev. A*, 102:032408, Sep 2020.

[NAC08] Julien Niset, Ulrik L. Andersen, and NJ Cerf. Experimentally feasible quantum erasure-correcting code for continuous variables. *Physical Review Letters*, 101(13):130503, 2008.

[NAJ18] Kyungjoo Noh, Victor V. Albert, and Liang Jiang. Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes. *IEEE Transactions on Information Theory*, 65(4):2563–2582, 2018.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[NC20] Kyungjoo Noh and Christopher Chamberland. Fault-tolerant bosonic quantum error correction with the surface–Gottesman-Kitaev-Preskill code. *Physical Review A*, 101(1):012316, 2020.

[NCS18] Murphy Y. Niu, Isaac L. Chuang, and Jeffrey H. Shapiro. Hardware-efficient bosonic quantum error-correcting codes based on symmetry operators. *Physical Review A*, 97(3):032323, 2018.

[NFcvC09] Julien Niset, Jaromír Fiurášek, and Nicolas J. Cerf. No-Go Theorem for Gaussian Quantum Error Correction. *Phys. Rev. Lett.*, 102:120501, Mar 2009.

[NH04] Ryo Namiki and Takuya Hirano. Practical limitation for continuous-variable quantum cryptography using coherent states. *Physical review letters*, 92(11):117901, 2004.

[NTH12] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor science and technology*, 25(6):063001, 2012.

[PAB+20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[PBM20] Giacomo Pantaleoni, Ben Q. Baragiola, and Nicolas C. Menicucci. Modular Bosonic Subsystem Codes. *Phys. Rev. Lett.*, 125:040501, Jul 2020.

[PGPBL09] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth Lloyd. Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.*, 102:050503, Feb 2009.

[PLOB17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, Apr 2017.

[PMVT04] Stefano Pirandola, Stefano Mancini, David Vitali, and P. Tombesi. Constructing finite-dimensional codes with optical continuous variables. *EPL (Europhysics Letters)*, 68(3):323, 2004.

[PMVT06a] Stefano Pirandola, Stefano Mancini, David Vitali, and Paolo Tombesi. Continuous variable encoding by ponderomotive interaction. *The European Phys. J. D*, 37(2):283–290, 2006.

[PMVT06b] Stefano Pirandola, Stefano Mancini, David Vitali, and Paolo Tombesi. Generating continuous variable quantum codewords in the near-field atomic lithography. *J. Phys. B*, 39(4):997, 2006.

[POP21] Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola. Security of continuous-variable quantum key distribution against canonical attacks. In *2021 International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6, 2021.

[PP21] Panagiotis Papanastasiou and Stefano Pirandola. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. *Phys. Rev. Research*, 3:013047, Jan 2021.

[QW17] Haoyu Qi and Mark M. Wilde. Capacities of quantum amplifier channels. *Phys. Rev. A*, 95:012339, Jan 2017.

[Ral99] Timothy C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1):010303, 1999.

[Rei05] Ben W. Reichardt. Quantum Universality from Magic States Distillation Applied to CSS Codes. *Quantum Information Processing*, 4(3):251–264, Aug 2005.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[RHG05] Timothy C. Ralph, AJF Hayes, and Alexei Gilchrist. Loss-tolerant optical qubits. *Physical Review Letters*, 95(10):100501, 2005.

[RK05] Renato Renner and Robert König. Universally Composable Privacy Amplification Against Quantum Adversaries. In Joe Kilian, editor, *Theory of Cryptography*, pages 407–425, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[RMG18] Matteo Rosati, Andrea Mari, and Vittorio Giovannetti. Narrow bounds for the quantum capacity of thermal attenuators. *Nature Communications*, 9(1):4339, Oct 2018.

[RS07] Joseph M. Renes and Graeme Smith. Noisy Processing and Distillation of Private Quantum States. *Phys. Rev. Lett.*, 98:020502, Jan 2007.

[RS13] Maxim Raginsky and Igal Sason. Concentration of Measure Inequalities in Information Theory, Communications, and Coding. *Foundations and Trends in Communications and Information Theory*, 10(1-2):1–246, 2013.

[RZBB94] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[SC83] Francisco Soto and Pierre Claverie. When is the Wigner function of multidimensional systems nonnegative? *Journal of Mathematical Physics*, 24(1):97–100, 1983.

[SCC19] Yunong Shi, Christopher Chamberland, and Andrew Cross. Fault-tolerant preparation of approximate GKP states. *New Journal of Physics*, 21(9):093007, 2019.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[SMD94] R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Phys. Rev. A*, 49:1567–1583, Mar 1994.

[SP00a] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[SP00b] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[SRLL02] Ch Silberhorn, Timothy C. Ralph, Norbert Lütkenhaus, and Gerd Leuchs. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review Letters*, 89(16):167901, 2002.

[Sti55] W Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[SWAT18] Kunal Sharma, Mark M Wilde, Sushovit Adhikari, and Masahiro Takeoka. Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels. *New Journal of Physics*, 20(6):063025, 2018.

[TBMS20] Ilan Tzitrin, J. Eli Bourassa, Nicolas C. Menicucci, and Krishna Kumar Sabapathy. Progress towards practical qubit computation using approximate Gottesman-Kitaev-Preskill codes. *Phys. Rev. A*, 101:032315, Mar 2020.

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, 2009.

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5(1):5235, Oct 2014.

[TH13] Toyohiro Tsurumaru and Masahito Hayashi. Dual Universality of Hash Functions and Its Applications to Quantum Cryptography. *IEEE Transactions on Information Theory*, 59(7):4700–4717, 2013.

[TKI03] Kiyoshi Tamaki, Masato Koashi, and Nobuyuki Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical Review Letters*, 90(16):167904, 2003.

[TM02] BC Travaglione and Gerard J. Milburn. Preparing encoded states in an oscillator. *Physical Review A*, 66(5):052322, 2002.

[TMA+21] Ilan Tzitrin, Takaya Matsuura, Rafael N. Alexander, Guillaume Dauphinais, J. Eli Bourassa, Krishna K. Sabapathy, Nicolas C. Menicucci, and Ish Dhand. Fault-Tolerant Quantum Computation with Static Linear Optics. *PRX Quantum*, 2:040353, Dec 2021.

[Tom12] Marco Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zurich, 2012.

[Tsu20a] Toyohiro Tsurumaru. Equivalence of three quantum algorithms: Privacy amplification, error correction, and data compression, 2020.

[Tsu20b] Toyohiro Tsurumaru. Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution. *IEEE Transactions on Information Theory*, 66(6):3465–3484, 2020.

[TW16] BM Terhal and Daniel Weigand. Encoding a qubit into a cavity mode in circuit QED using phase estimation. *Physical Review A*, 93(1):012315, 2016.

[TZ18] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-Gaussianity. *Phys. Rev. A*, 97:062337, Jun 2018.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[VAW+19] Christophe Vuillot, Hamed Asasi, Yang Wang, Leonid P. Pryadko, and Barbara M. Terhal. Quantum error correction with the toric Gottesman-Kitaev-Preskill code. *Physical Review A*, 99(3):032344, 2019.

[VMGE14] Victor Veitch, S A Hamed Mousavian, Daniel Gottesman, and Joseph Emerson. The resource theory of stabilizer quantum computation. *New J. Phys.*, 16(1):013009, jan 2014.

[VSG10] Hilma M. Vasconcelos, Liliana Sanz, and Scott Glancy. All-optical generation of states for "Encoding a qubit in an oscillator". *Optics Letters*, 35(19):3261–3263, 2010.

[Wan19] Yang Wang. Quantum Error Correction with the GKP Code and Concatenation with Stabilizer Codes, 2019.

[Wat18] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.

[WB07] Wojciech Wasilewski and Konrad Banaszek. Protecting an optical qubit against photon loss. *Physical Review A*, 75(4):042316, 2007.

[Wei] Eric W. Weisstein. Mehler's hermite polynomial formula. Visited on 28/06/2019.

[Wen17] G Wendin. Quantum information processing with superconducting circuits: a review. *Rep. Prog. Phys.*, 80(10):106001, Sep 2017.

[WHG12] Mark M. Wilde, Patrick Hayden, and Saikat Guha. Quantum trade-off coding for bosonic communication. *Phys. Rev. A*, 86:062306, Dec 2012.

[Wil13] Mark M. Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[WLB+04] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping K. Lam. Quantum cryptography without switching. *Physical Review Letters*, 93(17):170504, 2004.

[WLM+21] Xuan Wen, Qiong Li, Haokun Mao, Xiaojun Wen, and Nan Chen. Rotation Based Slice Error Correction Protocol for Continuous-variable Quantum Key Distribution and its Implementation with Polar Codes, 2021.

[WMBM19] Blayney W. Walshe, Lucas J. Mensen, Ben Q. Baragiola, and Nicolas C. Menicucci. Robust fault tolerance for continuous-variable cluster states with excess antisqueezing. *Phys. Rev. A*, 100:010301, Jul 2019.

[WPGG07] Michael M. Wolf, David Pérez-García, and Geza Giedke. Quantum Capacities of Bosonic Channels. *Phys. Rev. Lett.*, 98:130501, Mar 2007.

[WPGP+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[WQ18] Mark M. Wilde and Haoyu Qi. Energy-Constrained Private and Quantum Capacities of Quantum Channels. *IEEE Transactions on Information Theory*, 64(12):7802–7827, 2018.

[WT18] Daniel J. Weigand and Barbara M. Terhal. Generating grid states from Schrödinger-cat states without postselection. *Physical Review A*, 97(2):022341, 2018.

[WT20] Daniel J. Weigand and Barbara M. Terhal. Realizing modular quadrature measurements via a tunable photon-pressure coupling in circuit QED. *Phys. Rev. A*, 101:053840, May 2020.

[XMZ+20] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[YMK20] Hayata Yamasaki, Takaya Matsuura, and Masato Koashi. Cost-reduced all-Gaussian universality with the Gottesman-Kitaev-Preskill code: Resource-theoretic approach to cost analysis. *Phys. Rev. Research*, 2:023270, Jun 2020.

[YYK+16] Jun-ichi Yoshikawa, Shota Yokoyama, Toshiyuki Kaji, Chanond Sornphiphatphong, Yu Shiozawa, Kenzo Makino, and Akira Furusawa. Invited Article: Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing. *APL Photonics*, 1(6):060801, 2016.

[Zak68] J Zak. Dynamics of electrons in solids in external fields. *Physical Review*, 168(3):686, 1968.

[ZHRL09] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307, 2009.

[ZSS18] Quntao Zhuang, Peter W. Shor, and Jeffrey H. Shapiro. Resource theory of non-Gaussian operations. *Phys. Rev. A*, 97:052317, May 2018.