Continuous-Variable Ramp Quantum Secret Sharing with Gaussian States and Operations

Habibi Davijani, Masoud

UNIVERSITY OF CALGARY

Continuous-Variable Ramp Quantum Secret Sharing with Gaussian States and Operations

by

Masoud Habibi Davijani

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

APRIL, 2019

Abstract

Our aim is to formulate continuous-variable quantum secret sharing as a continuous-variable ramp quantum secret sharing protocol, provide a certification procedure for it and explain the criteria for the certification. Here we introduce a technique for certifying continuous-variable ramp quantum secret-sharing schemes in the framework of quantum interactive-proof systems. We devise pseudocodes in order to represent the sequence of steps taken to solve the certification problem. Furthermore, we derive the expression for quantum mutual information between the quantum secret extracted by any multi-player structure and the share held by the referee corresponding to the Tyc-Rowe-Sanders continuous-variable quantum secret-sharing scheme. We solve by converting the Tyc-Rowe-Sanders position representation for the state into a Wigner function from which the covariance matrix can be found, then insert the covariance matrix into the standard formula for continuous-variable quantum mutual information to obtain quantum mutual information in terms of squeezing. Our quantum mutual information result quantifies the leakage of the ramp quantum secret-sharing schemes.

Preface

In this thesis, I employ ISO 4 standard for abbreviations and ISO 80000 standard for symbols.

Acknowledgements

I am indebted to my adviser Barry C. Sanders for his expert scientific guidance, patient writing advice and generous support. It was my pleasure to work under his supervision during the last two years. I am grateful to David Feder and Christoph Simon for wise professional advise. I thank Abdullah Khalid, Ya-Dong Wu, Archismita Dalal and Mohsen Falamarzi Askarani for helpful discussions.

Table of Contents

List of Figures and Illustrations

Chapter 1

Introduction

1.1 Background

This section provides the required context to tackle the problem that is solved in this thesis. The aim of Subsec. 1.1.1 is to present the key notions of quantum mutual information, which is the method for quantifying information security and defining quantum secret sharing, and plays a starring role in this thesis. I begin by presenting salient facts about Shannon and von Neumann entropies, which are the cornerstone of classical and quantum information theories, respectively. Then I present requisite knowledge concerning classical and quantum mutual information.

In Subsec. 1.1.2, I review the main results on the theory of classical secret sharing. In Subsec. 1.1.2.2, I discuss the theory of discrete and continuous-variable quantum secret sharing. In Subsec. 1.1.3, I explain ramp secret sharing protocol which has been proposed to overcome the limitation that is naturally imposed on secret sharing protocols. In Sebsec. 1.2 I explain the aim, claim, novelty and importance of the problem, that has been solved in this thesis. Finally, I discuss the organization of the thesis.

1.1.1 Classical and quantum mutual information

Here I review Shannon and von Neumann entropies as these notions of entropy underpin the formulation of classical and quantum mutual information. Then I present the key notions of mutual information, which is vital to evaluate security for secret sharing.

Shannon's theory of information provides a mathematical definition of information, and describes precisely how much information can be communicated between different elements of a system [1]. The Shannon entropy is a measure of the uncertainty associated with a

probablity distribution $\{p_i\}$. Shannon entropy quantifies the average information content gained when one learns the value of a random variable X described by the probability distribution $\{p_i\}$.

Shannon entropy demonstrates the smallest number of bits needed to represent a random variable [1]. The fundamental definition of entropy has been proposed based upon a set of axioms. Intuitively, entropy can be interpreted as the average amount of surprise associated with the set of events [2]. The amount of surprise of an event is a function of the probability of the event. The amount of surprise should be higher for low probability events and lower for high probability events. The amount of surprise of two independent events should be the sum of the amount of the surprise of each event. These three axioms imply that the amount of surprise should be proportional to $-\log p(x)$ where $p(x)$ is the probability of the event x. By taking the average over all events respective to their probabilities, a mathematical expression for entropy is given.

Various derived quantities can be defined in terms of the Shannon entropy. One such quantity is the classical mutual information. Classical mutual information quantifies the information shared between random variables X and Y: it quantifies how much information from one of these variables lowers the uncertainty about the other [2]. For instance, in the case where X and Y are independent, then knowing X does not provide any information about Y and vice versa, thus their mutual information is zero. If X is a deterministic function of Y, and Y is a deterministic function of X , it is concluded that the mutual information has its maximum value: knowing X determines the value of Y and vice versa.

Another useful quantity is the conditional entropy [2]. The classical conditional entropy of a random variable X relative to a random variable Y is interpreted as the amount of information needed to describe the outcome of the random variable X given that the random variable Y is known. Classical secrecy conditions of classical secret-sharing schemes are expressed in terms of conditional entropy but equivalently can be expressed in terms of

mutual information.

The von Neumann entropy [3] is the quantum generalization of the Shannon entropy. The relationship is strengthened by the fact that the von Neumann entropy reduces to the Shannon entropy of the probability distribution over measurement outcomes for the case of density matrices that are diagonal, i.e. the classical states. Unlike the Shannon entropy that only grasps the classical uncertainty, von Neumann entropy captures both classical and quantum uncertainty in a quantum state. Quantum information theory is largly concerned with the interpretation and uses of von Neumann entropy, much as classical information theory is largly concerned with the interpretation and uses of Shannon entropy.

The standard informational measure of correlations in the classical regime is the classical mutual information, which is translated as the quantum mutual information into the quantum regime [2]. Quantum mutual information is nonnegative because of the subadditivity of Von Neumann entropy, and zero only for a product state. Unlike classical mutual information that only accounts for the classical correlation, quantum mutual information measures both classical and quantum correlations [2].

The quantum conditional entropy is the quantum generalization of the classical conditional entropy. The interpretation of quantum conditional entropy is less straightforward because unlike classical conditional entropy, it can be negative. This property is understood based on the operational interpretation of the quantum conditional entropy [4]. Thus far, we have the necessary background to evaluate the security of classical and quantum secret-sharing schemes. In the next section I review the basic results on secret-sharing protocols.

1.1.2 Secret sharing

In this subsubsection, I explain classical and quantum secret-sharing protocols. I begin by establishing the agents of the protocol namely dealer and players and the structures corresponding to the set of players. Afterwards, I explain classical secret-sharing schemes. Then I define quantum secret sharing and provide the main results corresponding to it.

Secret sharing comprises $n+1$ agents, namely one dealer $\mathcal{D}$ and n players. The role of the dealer is to encode the secret message $S \in \{0,1\}^*$ classically [5] or $\rho_s \in \mathcal{S}(\mathscr{H})$ quantumly [6], into n shares and distribute them among players in such a way that specific subsets of players form the authorized structure to retrieve the secret message, whereas the remaining subsets are denied any information about the secret whatsoever.

The sets of players that are denied any information are known as the forbidden sets. The set of forbidden sets is called forbidden structure, denoted by $\mathcal{F}$. The subset of players who are able to fully reconstruct the secret are authorized sets. The set of authorized sets is called authorized structure, denoted by $\mathcal{A}$. Quantumly, the no-cloning theorem implies that the existence of two disjoint authorized sets is forbidden [7].

Based on the type of the secret and the channel over which the secret is distributed, there exist three kinds of secret-sharing protocols [8]. The secret might be either a bit string or a qubit string and the channel can be public or private. Unlike a public channel, which is susceptible to eavesdropping, a private channel is secured from it. All the existing secret-sharing protocols are classified into three categories: sharing classical information with classical cryptography [5, 9], or quantum cryptography [10, 11], and sharing quantum information using quantum cryptography [6]. The third category is called quantum secret sharing, and the two others are referred as to classical secret sharing.

The second category proposes public channels into secret-sharing protocols. Contrary to private channels, a public channel is vulnerable to eavesdropping. Therefore, to defeat the eavesdroppers, quantum cryptography can be employed. An example of this category, is a (2,2) threshold protocol in which Greenberger-Horne-Zeilinger states are used by the dealer in order to check whether an eavesdropper has been active during a process [10]. A generalized version of this protocol, which is a (n, n) threshold protocol has been proposed [12] and experimentally realized [13].

1.1.2.1 Classical secret sharing

The first classical secret-sharing scheme was proposed by Shamir and Blakley [5, 9], independently. Both of these schemes are in the special class of (k, n) threshold protocols for which any k out of n shares can decrypt the secret, whereas any $k-1$ or fewer shares cannot obtain any information about the secret whatsoever.

Classical secret-sharing protocols are designed based on monotone span programs [14, 15] in which the secret and shares are random variables chosen from a finite field (Galois field). These protocols take advantage of the properties of vector spaces and matrices over finite fields. Both the encoding and decoding of the secret is achieved using linear functions over a finite field $\mathbb{F}$ and requires relatively little computational power.

The simplest example of a DV classical secret-sharing protocol is a (2,2) threshold classical secret-sharing protocol in which the secret is a bit string s. The aim of the dealer is to encode the secret into two shares in such a way that each share contains no information about the secret, but both players can fully reconstruct the secret by collaboration. For example, the dealer can choose a random bit string with the same size as the secret as one of the shares, and determine the other share by adding the secret to the random bit string; i.e., s (secret) $\oplus$ r (random bit string) where $\oplus$ stands for adding bitwise module 2. In this way, each player can not obtain any information about the secret individually, but two players can retrieve the secret by adding their shares together.

1.1.2.2 Quantum secret sharing

Quantum secret sharing is a generalization of classical secret sharing to the framework of quantum information. The secret in a quantum secret-sharing protocol is an unknown quantum state which can be a pure or mixed state. Initially, the dealer, who holds the quantum secret in the form of a quantum state of a given system, encodes the quantum state into an n mode entangled state and distributes these shares among players. The encoding is such that for any authorized group of players there exists a unitary operation that the players

can apply to their shares and in this way the state of one of the shares become the same as the original secret. Also, the density matrix of the unauthorized group of players should be independent of the secret. Thus, they can not obtain any information about the quantum secret no matter what operations they apply on their shares.

The $((k, n))$ threshold QSS schemes (the use of double parentheses distinguishes it from a classical scheme) are a class of QSS in which any group of k or more players can together reconstruct the secret but no group of fewer than k players can. The $((k, n))$ quantum threshold schemes exist provided the no-cloning theorem is satisfied [7]. Any QSS scheme can be reduced to $((k, 2k-1))$ threshold schemes [7]. In QSS schemes, the size of shares allocated to each player must be at least as large as the size of the secret [7, 16].

QSS can be implemented by employing quantum systems described by both CV [17, 18] and DV [6, 7, 15]. DV quantum secret sharing employs qudits as the carriers of quantum secrets and shares. In DV QSS protocols, the encoding is designed using the properties of matrices over finite number fields. In the CV quantum secret-sharing protocols, the secret is realized as the quadrature of a quantized light field instead of binary quantities such as the polarization state of a single photon.

CV QSS was proposed by Tyc and Sanders [18]. In their protocol, the quantum information is to be shared locally and only sufficiently large (but arbitrary) subgroups of all the participants can have access to the secret quantum information. The multi-mode entangled states used in the protocol of Tyc and Sanders are producible with squeezed light and beam splitters. Tyc, Row and Sanders (TRS03) characterized the quality of secret extraction of the protocol by calculating the fidelity in terms of the squeezing parameter between the original and the extracted secret, for an arbitrary coherent state as the secret [17]. Their result shows that in the case of finite squeezing, the players in the access structure are not able to fully reconstruct the secret and the extracted secret will be degraded increasingly

with decreasing amount of squeezing used by the dealer.

Another way of looking at a quantum secret-sharing protocol is to view it as an error correcting code that corrects erasure errors. A code that corrects erasure errors reconstructs the original qubit even if certain number of qubits are lost from the encoding. Similarly, in a QSS protocol, the secret can be reconstructed by excluding a certain number of secret shares. For instance, a $[[2k-1,1,k]]$ stabilizer code is considered as a $((k,2k-1))$ threshold QSS protocol [6]. DV quantum error correction has been extended to CV the realm as a direct generalization of the qubit redundancy codes [19, 20].

1.1.3 Ramp secret sharing

As an extension of (k,n)–threshold SS schemes, ramp secret-sharing (RSS) schemes were proposed by Blakley-Meadows [9] and Yamamoto [21]. In RSS schemes, the dimension of each share is reduced than that of the original system by the sacrifice of security admitting the intermediate property for some sets of shares, which are denoted as intermediate sets.

The adversary structure of a RSS scheme is divided into a forbidden and an intermediate structure. The intermediate structure $\mathcal{I}$ is defined as the collection of unauthorized sets that can gain some information about the secret, but are not able to fully reconstruct it. The forbidden structure $\mathcal{F}$ is characterized as a collection of unauthorized sets that are denied any information of the secret whatsoever.

In a (k,L,n) threshold RSS scheme, any k or more players are able to fully reconstruct the secret s, whereas any $k-L$ or less players are denied to obtain any information about it. Furthermore, from arbitrary $k-j$ shares for $j=1,\ldots,L-1$, some information about the secret leaks out with the amount of $\frac{j}{L}$ in $H_{\mathrm{Sh}}(s)$.

As an extension of $((k,L,n))$–threshold RSS schemes, quantum ramp secret-sharing (QRSS) schemes have been proposed. In a $((k,L,n))$ RQSS scheme, the dealer encodes the secret message $\rho_s \in \mathcal{S}(\mathscr{H})$, into n shares and distributes them among players in such a way that any k or more players are able to fully reconstruct the secret ρ_s, whereas any $k-L$

or less players are denied to obtain any information about it. Furthermore, any arbitrary $k-j$ shares for $j=1,\ldots,L-1$, has some information about the quantum secret.

A measurement on an intermediate set of shares can affect the quantum state of another intermediate set through the property of the entanglement. For this reason, it is a challenging problem to classify intermediate sets in RQSS schemes [16]. In this thesis I describe my study of security conditions for RQSS schemes and the development of tools to quantify the information that an intermediate set of shares has.

1.2 CV ramp quantum secret-sharing protocol with Gaussian states and operations

Secret-sharing is an information theoretically secure cryptographic protocol that is applicable to online auctions, electronic voting, shared electronic banking and cooperative activation in the classical domain [22], and distributed quantum computing in the quantum regime [23]. Ramp classical [9,21] and quantum [16] secret-sharing protocols were proposed to reduce the communication complexity by the sacrifice of security conditions. CV QSS [17,18,24,25] has been formulated in the framework of DV QSS protocols [6], which does not accommodate the quantum-information leakage inherent in continuous representations of quantum information. My aim is to formulate CV QSS as a CV ramp quantum secret-sharing (CV RQSS) protocol and introduce a technique to certify the protocol.

In order to reach my aims, I introduce four advances in my work. I develop the quantum mutual information approach to the CV regime to evaluate the security of CV QSS protocols. I derive quantum mutual information between referee and any multi-player structure corresponding to the TRS03 [17]. Furthermore, I introduce a certification technique for CV QSS in the framework of quantum interactive proofs [26,27] and accounting for the necessity of it being the RQSS protocol. Also, I give an upper-bound for the failure probability in terms of the number of experimental runs from which the referee knows how many rounds

are required to have sufficient information.

I focus on the "quantum-quantum" (QQ) secret-sharing protocols [6] in which the secret is a quantum state and communication occurs over quantum channels. The QQ case was extended to CV regime by Tyc and Sanders [18] and has been realized experimentally for three players, any two of which are authorized to extract the secret state [24,28]. Importantly, TRS03 later showed that the CV quantum state sharing could be extended to a (k, n) threshold protocol (a class of QSS protocols in which the authorized structure consists of all groups of k or more players while there are n players in total [6]), without a corresponding scale up in quantum resources.

Whereas conditional entropy is employed to evaluate the security of CC protocols, quantum mutual information is needed for the quantum case [29]. Quantum mutual information has been used as a means to evaluate the secrecy condition of Cleve-Gottesman-Lo QSS in the $(2, 3)$ case [29]. TRS03 characterized the quality of secret extraction of their protocol by calculating the fidelity in terms of squeezing parameter between the original and the extracted secret for an arbitrary coherent state as the secret. Here I develop a quantum mutual information approach for evaluating the CV QSS security. Restricting to Gaussian states and operations allows all the calculations to be performed within the convenient framework of the semidirect product of the symplectic group $\mathrm{Sp}(2n, \mathbb{R})$ with the Heisenberg-Weyl group $\mathrm{HW}(2n, \mathbb{R})$ for n the number of modes [30], which makes the calculations tractable but ignores the potentially powerful tools of non-gaussian operations [31].

1.3 Overview of chapters

This thesis is written in five chapters. In this chapter I have presented an overview of the problem, the methods I used to tackle the problem, and my research achievements in investigating the problem. The problem of interest is to formulate CV quantum secret-sharing as a CV ramp quantum secret-sharing protocol, provide a certification procedure for

it and explain the criteria for the certification.

In Chapter 2 I provide the necessary background to understand the result of this thesis. I begin in Sec. 2.1, by introducing Gaussian states. In Subsec. 2.1.1.1, I explain Gaussian-preserving maps, which preserve the Gaussian property of quantum states. Finally, I discuss von Neumann entropy (quantum version of Shannon entropy), mutual information and the entropy of Gaussian states in Sec. 2.1.2.

In Chapter 3, I review the main results on secret-sharing protocols. In Sec. 3.1, I begin by establishing the agents of the protocol, namely dealer and players. Afterwards, I introduce the structures corresponding to the set of players. In Sec. 3.2, I introduce classical secret sharing. In Sec. 3.3, I discuss the information-theoretic description of classical secret-sharing protocols. In Sec. 3.4, I explain classical ramp secret sharing, which reduces the size of shares with the price of leakage of information to unauthorized players. In Sec. 3.6, I explain ramp quantum secret-sharing protocols. Then I discuss the information-theoretic description of quantum secret-sharing protocols, which has a crucial role in defining and evaluating secret-sharing protocols. In Sec. 3.10, I introduce the TRS03. Finally, in Sec. 3.11, I explain the quantum error correcting codes and their relationship with quantum secret-sharing protocols.

In Chapter 4, I begin by elaborating on the approach I use to introduce the CV ramp quantum secret sharing protocol and its corresponding certification test. In Sec. 4.1, I introduce a CV RQSS protocol and how to certify it. I discuss the success criterion of the certification protocol. Furthermore, I specify what the parties need to do to complete the certification. In Sec. 4.2 I present my main results. My first result is a CV version of quantum mutual information. This CV quantum mutual information is then used to quantify quantum-information leakage for Gaussian states and operations. Based on this leakage characterization, I introduce a certification test, in the framework of quantum-interactive proofs, and provide a practical test to implement it.

Chapter 5 concludes this thesis, where I provide a discussion of the results, and the

impact and consequences of this work. Finally, I summarize the research accomplished and provide suggestions for future work.

Chapter 2

Background on CV quantum information

The aim of this chapter is to provide the necessary background to understand the result of this thesis. I begin in Sec. 2.1, by introducing Gaussian states. In Sec. 2.1.1.1, I explain Gaussian-preserving maps, which preserve the Gaussian property of quantum states. Finally, I discuss von Neumann entropy (quantum version of Shannon entropy), mutual information and the entropy of Gaussian states in Sec. 2.1.2.

2.1 Continuous-variable quantum information with Gaussian states and Gaussian operations

In this subsection, we begin by introducing Gaussian states [32] and some of their important properties. Then we explain the Gaussian preserving maps, which preserve the Gaussian property of quantum states.

2.1.1 Gaussian states

A continuous-variable quantum state is an continuously parameterized element of Hilbert space described by observables with continuous eigenspectra. Typically, a continuous-variable quantum state is described by N bosonic modes, associated with a tensor-product Hilbert space

$$\mathscr{H}^{\otimes N} = \bigotimes_{k=1}^{k=N} \mathscr{H}_k \sim \mathcal{L}^2\left(\mathbb{R}^N\right), \tag{2.1}$$

i.e., square integrable complex-valued functions over $\mathbb{R}^N$ and a vector of quadrature operators

$$\hat{\boldsymbol{x}} \coloneqq (\hat{q}_1, \hat{p}_1, ..., \hat{q}_n, \hat{p}_n)^{\mathrm{T}}. \tag{2.2}$$

The vector $\hat{\boldsymbol{x}}$ satisfies the commutation relation

$$[\hat{\boldsymbol{x}}_i, \hat{\boldsymbol{x}}_j] = \Omega_{ij}, \quad \boldsymbol{\Omega} = \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{2.3}$$

known as the symplectic form.

An arbitrary continuous-variable quantum state is characterized by a density operator

$$\rho \in \mathcal{S}(\mathscr{H}), \tag{2.4}$$

where $\mathcal{S}(\mathscr{H})$ is the set of positive semidefinite trace-class operators, which can be represented by the Wigner function [33]

$$W(\boldsymbol{x}) = \frac{1}{(2\pi)^{2n}} \int_{\mathbb{R}^{2n}} \mathrm{d}^{2n}\boldsymbol{\xi} \exp\left(-\mathrm{i}\boldsymbol{x}^{\mathrm{T}}\boldsymbol{\xi}\right) \chi(\boldsymbol{\xi}) \tag{2.5}$$

for

$$\chi(\boldsymbol{\xi}) \coloneqq \mathrm{tr}\left[\rho \hat{D}(\boldsymbol{\xi})\right], \tag{2.6}$$

being the the Wigner characteristic function and

$$\hat{D}(\boldsymbol{\xi}) \coloneqq \exp\left(\mathrm{i}\boldsymbol{x}^{\mathrm{T}}\boldsymbol{\xi}\right), \qquad \boldsymbol{\xi} \in \mathbb{R}^{2n} \tag{2.7}$$

being the Weyl operator. Wigner functions are particularly useful for calculating expectation values of symmetrically ordered functions $\hat{q}$ and $\hat{p}$ denoted by $S(\hat{q}^n\hat{p}^m)$ with expectation value

$$\mathrm{tr}\left[\rho S(\hat{q}^n\hat{p}^m)\right] = \int \mathrm{d}q\mathrm{d}p\, W(\boldsymbol{x})\, q^n p^m. \tag{2.8}$$

Thus far, we have the Wigner representation for any state; now we restrict to Gaussian states.

A Gaussian state is defined to be a state whose Wigner representation is Gaussian. A Gaussian state can be completely characterized by its first moment $\bar{\boldsymbol{x}} = \mathrm{tr}\left(\hat{\boldsymbol{x}}\rho\right)$ and covariance matrix $\boldsymbol{V}$. The covariance matrix entries are

$$V_{ij} \coloneqq \frac{1}{2}\mathrm{tr}\left[\{\boldsymbol{\Delta}\hat{\boldsymbol{x}}_i, \boldsymbol{\Delta}\hat{\boldsymbol{x}}_j\}\right], \ \boldsymbol{\Delta}\hat{\boldsymbol{x}}_i \coloneqq \hat{\boldsymbol{x}}_i - \mathrm{tr}\left(\hat{\boldsymbol{x}}_i\rho\right) \tag{2.9}$$

with $\{,\}$ the anticommutator.

The symplectic manipulation of a Gaussian state's covariance matrix can be used to express its fundamental properties. By definition, a matrix $\boldsymbol{S}$ is called *symplectic* if it preserves the symplectic form of Eq. (2.2); i.e.,

$$\boldsymbol{S}\boldsymbol{\Omega}\boldsymbol{S}^{\mathrm{T}} = \boldsymbol{\Omega}. \tag{2.10}$$

According to the Williamson theorem [34], each covariance matrix $\boldsymbol{V}$ has a corresponding symplectic transformation $\boldsymbol{S}$ satisfying

$$\boldsymbol{V} = \boldsymbol{S}\left[\bigoplus_{k=1}^{n} \nu_k \boldsymbol{I}_k\right]\boldsymbol{S}^{\mathrm{T}}, \tag{2.11}$$

with symplectic spectrum defined by the vector

$$\boldsymbol{\nu} \coloneqq (\nu_1, \ldots, \nu_n), \tag{2.12}$$

unique to each $\boldsymbol{V}$ and satisfying

$$\prod_{k=1}^{n} \nu_k^2 = \det \boldsymbol{V}. \tag{2.13}$$

As an example, a two-mode Gaussian state has covariance matrix

$$\boldsymbol{V} = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C}^{\mathrm{T}} & \boldsymbol{B} \end{pmatrix};\ \boldsymbol{A} = \boldsymbol{A}^{\mathrm{T}}, \boldsymbol{B} = \boldsymbol{B}^{\mathrm{T}}, \boldsymbol{C} \in \mathbb{R}^{2\times 2}. \tag{2.14}$$

The symplectic spectrum is [35]

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det \boldsymbol{V}}}{2}}, \tag{2.15}$$

where

$$\Delta \coloneqq \det \boldsymbol{A} + \det \boldsymbol{B} + 2\det \boldsymbol{C}. \tag{2.16}$$

As Gaussian states are easy to describe mathematically, a large class of transformations acting on such states are easy to characterize as well. In the next section, we discuss this class of transformations called Gaussian preserving maps.

2.1.1.1 Gaussian-preserving maps

Gaussian (linear) unitary Bogoliubov transformations are interactions that preserve the Gaussian character of a quantum state. In terms of the quadrature operators, a Gaussian map is described by the affine map

$$(\boldsymbol{S}, \boldsymbol{d}) : \boldsymbol{S}\hat{\boldsymbol{x}} + \boldsymbol{d}, \qquad \boldsymbol{d} \in \mathbb{R}^{2n}, \tag{2.17}$$

where $\boldsymbol{S}$ (2.9) is the matrix representation of the symplectic group. The most general form of a Gaussian map in terms of its action on the statistical moments $\bar{\boldsymbol{x}}$ and $\boldsymbol{V}$ is

$$\bar{\boldsymbol{x}} \mapsto \boldsymbol{S}\bar{\boldsymbol{x}} + \boldsymbol{d}, \ \boldsymbol{V} \mapsto \boldsymbol{S}\boldsymbol{V}\boldsymbol{S}^{\mathrm{T}}. \tag{2.18}$$

For single-mode squeezing we have the infinite-dimensional unitary representation [36]

$$S_1 = \mathrm{e}^{\frac{1}{2}\left(\zeta^{\star}\hat{a}^2 - \zeta\hat{a}^{\dagger 2}\right)}, \tag{2.19}$$

and for two-mode squeezing we have the infinite-dimensional unitary representation

$$S_2 = \mathrm{e}^{\frac{1}{2}\left(\zeta^{\star}\hat{a}_1\hat{a}_2 - \zeta\hat{a}_1^{\dagger}\hat{a}_2^{\dagger}\right)}, \tag{2.20}$$

where

$$\hat{a}_k = \frac{\hat{q}_k + \mathrm{i}\hat{p}_k}{\sqrt{2}}, \ \hat{a}_k^{\dagger} = \frac{\hat{q}_k - \mathrm{i}\hat{p}_k}{\sqrt{2}}, \ \zeta = s\mathrm{e}^{\mathrm{i}\theta}, \ s \in \mathbb{R}^{+}. \tag{2.21}$$

A two-mode squeezed vacuum (TMSV) state is mathematically represented as [36]

$$|\zeta\rangle_{\mathrm{TMSV}} := S_2\left(\zeta\right)|0\rangle, \ \zeta \in \mathbb{C}. \tag{2.22}$$

In the next section, I review Shannon and von Neumann entropy as these notions of entropy underpin the formulation of classical and quantum mutual information.

2.1.2 Mutual information

Here we review the key notions of mutual information, which is the method for quantifying information security and defining quantum secret sharing. We begin by presenting salient

facts about Shannon and von Neumann entropy followed by requisite knowledge concerning classical and quantum mutual information. Finally, in this subsection, we discuss the security for discrete quantum secret sharing as our aim is to analyze security for continuous-variable quantum secret sharing.

2.1.2.1 Shannon and von Neumann entropy

Here we review Shannon and von Neumann entropy as these notions of entropy underpin the formulation of classical and quantum mutual information. This subsubsection also helps to elucidate the compact notation we use throughout this paper.

Shannon entropy. Let Z be a statistical ensemble defined by a classical random variable z and its associated probability distribution $\{p_j\} = \{p_1, \ldots, p_n\}$, which can be expressed as a probability vector $\boldsymbol{p} = (p_1, \ldots, p_n)^\top$. The logarithm of this vector (always using base 2 here) is

$$\log \boldsymbol{p} := (\log \boldsymbol{p}_j). \tag{2.23}$$

Using the Hadamard (elementwise) product $\boldsymbol{a} \circ \boldsymbol{b} := (a_i b_i)$ [37] for vectors and the sum of such elements $\boldsymbol{a} \odot \boldsymbol{b} := \sum_i a_i b_i$, the Shannon entropy is

$$H_{\mathrm{Sh}}(\boldsymbol{p}) = -\boldsymbol{p} \odot \log \boldsymbol{p} = -\boldsymbol{p} \cdot \mathbf{log}\, \boldsymbol{p}. \tag{2.24}$$

Thus, H_{Sh} yields the number of bits per letter needed to completely specify Z in the asymptotic limit of infinitely long strings [1]. Shannon entropy is thus a measure for the uncertainty of z or it indicates how much information each letter in the string that uses the alphabet Z carries.

Von Neumann entropy In the same vein, the information content of a quantum state ρ (2.4) can be quantified by determining how many qubits are needed to represent state ρ in the asymptotic limit of an infinite ensemble of physical systems. This quantum-information content, known as the von Neumann entropy [3], amounts to computing a classical Shannon

entropy (2.24)

$$H_{\mathrm{vN}}(\rho) = -\operatorname{tr}(\rho \log_2 \rho) = H_{\mathrm{Sh}}(\operatorname{spec} \boldsymbol{\rho}), \tag{2.25}$$

for $\operatorname{spec} \boldsymbol{\rho}$ a vector comprising eigenvalues of the state ρ.

Continuous-variable quantum entropy. For continuous-variable Gaussian states, we define the vectors

$$\boldsymbol{\nu}^{\pm} := \frac{\boldsymbol{\nu} \pm \mathbb{1}}{2} \tag{2.26}$$

with $\boldsymbol{\nu}$ the symplectic spectrum (2.12) and $\mathbb{1}$ the vector with all entries being unity. Thus, the von Neumann entropy is [38]

$$H_{\mathrm{vN}}(\rho) = \boldsymbol{\nu}^{+} \odot \log \boldsymbol{\nu}^{+} + \boldsymbol{\nu}^{-} \odot \log \boldsymbol{\nu}^{-}. \tag{2.27}$$

These entropy expressions are used in the formulæ for mutual information.

Convenient notation for states in entropy formulæ A convenient notation for entropy, which is independent of being classical or quantum, uses a label for the classical or quantum state. Rather than specify the state as $\boldsymbol{p}$ classically or ρ quantumly, we label the state by a capital letter such as A and B, with these labels commensurate with the usual Alice-and-Bob nomenclature in cryptology [39].

Conditional entropy. Labelling the joint state held by A and B as AB, the conditional entropy is abstractly expressed as

$$H(\mathrm{A}|\mathrm{B}) \coloneqq H(\mathrm{AB}) - H(\mathrm{B}) \tag{2.28}$$

for any valid formula for entropy, whether classical (2.24) or quantum (2.25).

Classical conditional entropy. The classical conditional entropy [40] is obtained from Eq. (2.28) by replacing

$$H(\mathrm{A}) \mapsto H_{\mathrm{Sh}}(\boldsymbol{p}_{\mathrm{A}}) \tag{2.29}$$

for $\boldsymbol{p}_{\mathrm{A}}$ the distribution held by A. Similarly, we replace

$$H(\mathrm{B}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{B}}\right) \tag{2.30}$$

and

$$H(\mathrm{AB}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{AB}}\right). \tag{2.31}$$

$H\left(\mathrm{A}|\mathrm{B}\right)$ quantifies the correlation between A and B as the reduction of the number of bits per letter needed to specify A given B is known.

Quantum conditional entropy. The quantum conditional entropy [2] is obtained from Eq. (2.28) by replacing

$$H(\mathrm{A}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{A}}\right) \tag{2.32}$$

for ρ_{A} the quantum state held by A. Similarly, we replace

$$H(\mathrm{B}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{B}}\right) \tag{2.33}$$

and

$$H(\mathrm{AB}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{AB}}\right). \tag{2.34}$$

Although classical conditional entropy is always positive, for evaluatingquantum conditional entropy can be negative [4].

2.1.2.2 Classical and quantum mutual information

We explain classical mutual information [40] and quantum mutual information [2], first as an abstract concept regardless of whether classical or quantum information is chosen. Then we explain each of classical and quantum mutual information. Quantum mutual information is vital for evaluating security for secret sharing.

Mutual information. Labelling the joint state held by A and B as AB, mutual information is abstractly expressed as

$$I\left(\mathrm{A};\mathrm{B}\right) \coloneqq H\left(\mathrm{A}\right) + H\left(\mathrm{B}\right) - H\left(\mathrm{AB}\right) \tag{2.35}$$

for any valid formula for entropy, whether classical (2.24) or quantum (2.25). Classical mutual information [2] is obtained from Eq. (2.35) by replacing

$$H(\mathrm{X}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{X}}\right) \tag{2.36}$$

with $\mathrm{X} \in \{\mathrm{A}, \mathrm{B}\}$ for $\boldsymbol{p}_{\mathrm{X}}$ and

$$H(\mathrm{AB}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{AB}}\right) \tag{2.37}$$

as discussed in ¶2.1.2.1. Classical mutual information quantifies the correlation between two statistical ensembles A and B as the reduction of the number of bits per letter needed to specify one of the variables given the other variable is known.

Quantum mutual information. The quantum mutual information [2] is obtained from Eq. (2.35) by replacing

$$H(\mathrm{A}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{A}}\right) \tag{2.38}$$

for ρ_{A} the quantum state held by A. Similarly, we replace

$$H(\mathrm{B}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{B}}\right) \tag{2.39}$$

and

$$H(\mathrm{AB}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{AB}}\right). \tag{2.40}$$

Quantum mutual information is always positive and quantifies the total correlations contained in the bipartite state ρ_{AB}. Quantum mutual information is employed to define and evaluate the security of quantum secret-sharing schemes (QSS).

Relation between conditional entropy and mutual information. The relation between conditional entropy and mutual information is

$$I\left(\mathrm{A};\mathrm{B}\right) = H\left(\mathrm{A}\right) - H\left(\mathrm{A}|\mathrm{B}\right) = H\left(\mathrm{B}\right) - H\left(\mathrm{B}|\mathrm{A}\right) \tag{2.41}$$

for any valid formula for entropy, whether classical (2.24) or quantum (2.25). The relation between classical mutual information and classical conditional entropy is obtained from

Eq. (2.41) by replacing

$$H(\mathrm{X}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{X}}\right) \tag{2.42}$$

with $\mathrm{X} \in \{\mathrm{A}, \mathrm{B}\}$ and

$$H(\mathrm{X}|\mathrm{Y}) \mapsto H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{XY}}\right) - H_{\mathrm{Sh}}\left(\boldsymbol{p}_{\mathrm{Y}}\right) \tag{2.43}$$

with $(\mathrm{X}, \mathrm{Y}) \in \{(\mathrm{A}, \mathrm{B}), (\mathrm{B}, \mathrm{A})\}$ as discussed in ¶2.1.2.1.

The relation between quantum mutual information and quantum conditional entropy is obtained from Eq. (2.41) by replacing

$$H(\mathrm{X}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{X}}\right) \tag{2.44}$$

with $\mathrm{X} \in \{\mathrm{A}, \mathrm{B}\}$ and

$$H(\mathrm{X}|\mathrm{Y}) \mapsto H_{\mathrm{vN}}\left(\rho_{\mathrm{XY}}\right) - H_{\mathrm{vN}}\left(\rho_{\mathrm{Y}}\right) \tag{2.45}$$

with $(\mathrm{X}, \mathrm{Y}) \in \{(\mathrm{A}, \mathrm{B}), (\mathrm{B}, \mathrm{A})\}$ as discussed in ¶2.1.2.1.

In this chapter, I introduced the Gaussian states along with the Gaussian preserving maps, which preserve the Gaussian property of quantum states. Furthermore, I discussed the von Neumann entropy (quantum version of Shannon entropy), mutual information and the entropy of Gaussian states.

Chapter 3

Secret sharing

In this chapter, I review the main results on secret-sharing protocols. In Sec. 3.1, I begin by establishing the agents of the protocol namely dealer and players. Afterwards, I introduce the structures corresponding to the set of players. In Sec. 3.2, I introduce classical secret sharing. In Sec. 3.3, I describe the information-theoretic description of classical secret-sharing protocols. In Sec. 3.4, I outline classical ramp secret sharing, which reduces the size of shares at the cost of leaking information to unauthorized players. In Sec. 3.6, I introduce ramp quantum secret-sharing protocols, and discuss the information-theoretic description of quantum secret-sharing protocols, which is crucial in defining and evaluating secret-sharing protocols. In Sec. 3.10, I introduce the TRS03. Finally, in Sec. 3.11, I describe quantum error correcting codes, and their relationship to quantum secret-sharing protocols.

3.1 Secret-sharing protocol

In this section, I explain secret-sharing protocols. I begin by establishing the agents of the protocol namely dealer and players. Afterwards, I introduce the structures corresponding to the set of players namely authorized and forbidden structures.

Dealer and players. We establish the agents of the protocol and the structures corresponding to sets of players, who are one kind of agent. Specifically, secret sharing comprises $n+1$ agents namely one dealer $\mathcal{D}$ and n players labelled

$$\mathcal{P} = \{P_1, P_2, \ldots, P_n\}. \tag{3.1}$$

The power set of players is $2^{\mathcal{P}}$, which is the set of all subsets of the set of players (3.1). The role of the dealer is to encode the secret message $S \in \{0,1\}^*$ classically or $\rho_s \in \mathcal{S}(\mathscr{H})$

(2.4) quantumly, into n shares and distribute them among players in such a way that specific elements of $2^{\mathcal{P}}$ form the authorized structure denoted by $\mathcal{A}$ to retrieve the secret message, while other elements are denied any information about the secret whatsoever. The set of elements that are denied any information is known as the forbidden structure, and is denoted by $\mathcal{F}$.

Access structure. Let

$$\mathcal{F},\, \mathcal{A} \subseteq 2^{\mathcal{P}}, \qquad \mathcal{F}, \mathcal{A} \neq \emptyset, \qquad \mathcal{F} \cap \mathcal{A} = \emptyset, \tag{3.2}$$

where $\mathcal{F}$ is monotonically decreasing, and $\mathcal{A}$ is monotonically increasing. Formally, an authorized structure $\mathcal{A}$ is monotonically increasing if

$$(\gamma \in \mathcal{A} \text{ and } \gamma \subseteq \gamma') \Rightarrow \gamma' \in \mathcal{A}. \tag{3.3}$$

Furthermore, a forbidden structure $\mathcal{F}$ is monotonically decreasing if

$$(\gamma' \in \mathcal{F} \text{ and } \gamma \subseteq \gamma') \Rightarrow \gamma \in \mathcal{F}. \tag{3.4}$$

Then the set

$$\Gamma = \{\mathcal{F}, \mathcal{A}\}, \tag{3.5}$$

is called an access structure on $\mathcal{P}$. Quantumly, the no-cloning theorem implies that the existence of two disjoint authorized groups is forbidden [7].

3.2 Classical secret-sharing protocol

In this section we explain classical secret-sharing protocols. Let

$$V = \{\nu_1, \nu_2, \ldots, \nu_n\}, \tag{3.6}$$

be the shares of the secret s to be encoded. I suppose the secret and each share ν_i are elements of finite fields $\mathbb{F}_S$ and $\mathbb{F}_{V_i}$, respectively. A secret-sharing scheme Π is a randomized

mapping from $\mathbb{F}$ to n-tuples

$$\Pi : \mathbb{F} \times R \to \mathbb{F}_{V_1} \times \mathbb{F}_{V_2} \times \cdots \times \mathbb{F}_{V_n}, \tag{3.7}$$

where

$$R \in \{\{r_1, \ldots, r_{n-1}\} | r_i \in \mathbb{F}\}, \tag{3.8}$$

is a set of random inputs. The dealer encrypts $s \in \mathbb{F}$ into n shares according to Π by sampling a vector of shares $(v_1, v_2, \ldots, v_n)$ from $\Pi(s)$. Then the dealer privately sends each share ν_i to the party P_i (for simplicity, and without loss of generality, we assume that each player holds one share). Let

$$\mathcal{B} = \{P_{i_1}, P_{i_2}, \ldots, P_{i_{|\mathcal{B}|}}\} \in 2^{\mathcal{P}}, \tag{3.9}$$

be a subset of players. For each $\mathcal{B} \in 2^{\mathcal{P}}$, let $\langle \mathcal{B} \rangle$ be the finite set of shares given to $\mathcal{B}$. Then Π realizes an access structure Γ if there exists a reconstruction function denoted by Rec which satisfies the following requirements

1. $\forall \mathcal{B} \in \mathcal{A}$

$$\exists\, \mathrm{Rec}_{\mathcal{B}} : \mathbb{F}_{i_1} \times \mathbb{F}_{i_2} \times \cdots \times \mathbb{F}_{i_{|\mathcal{B}|}} \to \mathbb{F}, \tag{3.10}$$

such that $\forall s \in \mathbb{F}$

$$\mathrm{pr}\left[\mathrm{Rec}_{\mathcal{B}}\left(\Pi(s)\right)_{\mathcal{B}} = s\right] = 1. \tag{3.11}$$

2. $\forall \mathcal{B} \notin \mathcal{A}$, and $\forall a, b \in S$, and for every possible shares $\langle \mathcal{B} \rangle$

$$\mathrm{pr}\left[\Pi(a)_{\mathcal{B}} = \langle \mathcal{B} \rangle\right] = \mathrm{pr}\left[\Pi(b)_{\mathcal{B}} = \langle \mathcal{B} \rangle\right]. \tag{3.12}$$

The first protocol for classical secret sharing was created by Shamir [5] and Blakley [9] independently. Both of these protocols are in the class of (k, n) threshold protocols, which means any k out of n shares can decrypt the secret, but any $k-1$ or fewer shares can not obtain any information about the secret. Formally, in a (k, n) threshold secret-sharing protocol the authorized structure is

$$\mathcal{A} = \{\gamma \subseteq \mathcal{P} \mid |\gamma| \geq k\}, \tag{3.13}$$

and the adversary structure is

$$\mathcal{F} = \{\gamma \subseteq \mathcal{P} \mid |\gamma| \leq k-1\}. \tag{3.14}$$

Here we provide an example of classical threshold schemes [5]. Consider a finite field $\mathbb{F}_q$ where q is a prime number satisfying

$$0 < k \leq n < q. \tag{3.15}$$

Let the secret s be uniformly distributed on $\mathbb{F}_q$, i.e., $H(s) = \log|\mathbb{F}_q|$. Let $r_1, r_2, \ldots, r_{k-1}$ be independent uniform random numbers on $\mathbb{F}_q$. Then the i_{th} share ν_i is constructed by $\nu_i = f(i)$, where $f(x)$ is the following polynomial of degree $k-1$ on $\mathbb{F}_q$

$$f(x) = s + r_1 x + r_2 x^2 + \ldots + r_{k-1} x^{k-1} \mod q. \tag{3.16}$$

The dealer then distributes shares between players such that each player P_i receives $(i, f(i))$ as his/her share of the secret.

Reconstruct the secret. The goal for any set of players with k or more players is to retrieve the secret which is the leading coefficient of $f(x)$. According to Lagrange theorem, given m distinct points $(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)$, there is a unique polynomial p of degree less than m for which $p(x_i) = y_i$. Now to reconstruct the secret, a set of players who hold $(i_1, f(i_1)), (i_2, f(i_2)), \ldots, (i_m, f(i_m))$ as their shares for which $m \geq k$, can construct a polynomial $p(x)$ from any of their k secret shares

$$(i_{j_1}, f(i_{j_1})), (i_{j_2}, f(i_{j_2})), \ldots, (i_{j_k}, f(i_{j_k})) \qquad \{j_1, j_2, \ldots, j_k\} \subset \{1, 2, \ldots, m\}, \tag{3.17}$$

as

$$p(x) = \sum_{u=1}^{k} f(i_{j_u}) \prod_{\substack{t=1 \\ t \neq u}}^{k} \frac{x - i_{j_t}}{i_{j_u} - i_{j_t}}. \tag{3.18}$$

Hence s is obtained by $s = p(0)$, i.e.,

$$s = \sum_{u=1}^{k} f(i_{j_u}) \prod_{\substack{t=1 \\ t \neq u}}^{k} \frac{i_{j_t}}{i_{j_t} - i_{j_u}}. \tag{3.19}$$

On the other hand, for a set of players with fewer than k shares, the secret is totally random over $\mathbb{F}_q$, hence these players do not obtain any information about the secret whatsoever.

Example 3.2.1. *Let us consider a* $(3,4)$*-threshold SS scheme over* $\mathbb{F}_{17}$ *with* $s = 10$*. If* $r_1 = 5$ *and* $r_2 = 7$*, the polynomial of degree 2 becomes*

$$f(x) = 10 + 5x + 7x^2. \tag{3.20}$$

Then the shares are $\nu_1 = 5, \nu_2 = 14, \nu_3 = 3$ *and,* $\nu_4 = 6$*. As an example, from* $\nu_1, \nu_2,$ *and,* ν_4*, we can calculate secret* s *as follows*

$$s = 5\frac{2}{2-1}\frac{4}{4-1} + 14\frac{1}{1-2}\frac{4}{4-2} + 6\frac{1}{1-4}\frac{2}{2-4} = 2 + 6 + 2 = 10. \tag{3.21}$$

In the next section, I discuss the information-theoretic description of classical secret sharing, which plays a crucial role in defining and evaluating classical secret-sharing protocols.

3.3 Classical secrecy and recoverability conditions

Classical secrecy is expressed in terms of conditional entropy, but can be equivalently expressed in terms of mutual information. Strictly speaking, conditional entropy is between shares. However, for simplicity, in the literature, there is a tendency to refer to conditional entropy between players. Π is a perfect SS scheme on Γ if [41]

- $\forall \mathcal{B} \in \mathcal{A}\ H(s|\mathcal{B}) = 0,$
- $\forall \mathcal{B} \notin \mathcal{A}\, H(s|\mathcal{B}) = H(s).$

Also the size of each share should be at least as the same as the secret, namely

$$H_{\mathrm{Sh}}(\nu_i) \geq H_{\mathrm{Sh}}(s), \tag{3.22}$$

where $1 \leq i \leq n$ [42] [43] [44]. It is desirable to reduce the size of the shares in a secret-sharing protocol because it reduces the communication complexity. In the next section I introduce ramp secret sharing in which the size of shares is reduced at the cost of leaking information to the intermediate structure.

3.4 Ramp secret sharing

As an extension of (k, n) threshold secret-sharing protocols, ramp secret-sharing (RSS) protocols were proposed by Blakley-Meadows [9] and Yamamoto [21]. In secret-sharing protocols, the size of shares allocated to each player must be at least as large as the size of the secret. In RSS protocols, the dimension of each share is reduced to less than that of the original system by the sacrifice of security admitting the intermediate property for some sets of shares, which are denoted as intermediate sets. In a (k, L, n) threshold RSS protocol, any k or more players are able to fully reconstruct the secret s, whereas any $k - L$ or less players are denied to obtain any information about it. Furthermore, from arbitrary $k - j$ shares for $j = 1, \ldots, L - 1$, some information of the secret will leak out with the amount of $\frac{j}{L}$ in $H_{\mathrm{Sh}}(s)$.

(k, L, n) ramp classical secret sharing. A (k, L, n) ramp scheme was first proposed as an extension of the Shamir's threshold scheme [9]. Consider a finite field $\mathbb{F}_q$ were q is a prime number. Let the secret be $s = (s_0, s_1, \ldots, s_{L-1})$ where $s_i \in \mathbb{F}_q$. The dealer picks $k - L$ elements $\beta_L, \beta_{L+1}, \ldots, \beta_{k-1}$ in $\mathbb{F}_q$ randomly, and hides the secret in the polynomial below as follows

$$f(x) = s_0 + s_1 x + \cdots + s_{L-1} x^{L-1} + \beta_L x^L + \ldots + \beta_{k-1} x^{k-1} \mod q. \tag{3.23}$$

Then the i_{th} share ν_i is constructed by $\nu_i = f(i)$. The function f can be reconstructed by any k or more shares via Lagrange theorem. Furthermore, for any set of shares with $k - L$ or fewer elements, the L elements of the secret are totally random over $\mathbb{F}_q$. However, a set of shares γ where $k - L < |\gamma| < k$ can narrow down the range of the secret which means that some information about the secret is leaked to γ.

In a ramp secret-sharing protocol, the subset of players that can obtain some information about the secret but are not able to fully reconstruct it are called the intermediate sets. The collection of all intermediate sets is defined as the intermediate structure. A classical ramp

secret-sharing protocol can be described by conditional entropy similar to classical threshold protocol. [44]. Let us define $\mathcal{I}$ as intermediate structure. A RSS protocol then satisfies the following requirements

1. $\forall\gamma \in \mathcal{A}$, $H(s|\gamma) = 0$,

2. $\forall\gamma \in \mathcal{I}$, $0 < H(s|\gamma) < H(s)$,

3. $\forall\gamma \in \mathcal{F}$, $H(s|\gamma) = H(s)$.

In this description, the leaked information is classical and the amount of it can be determined using conditional entropy $H(s|\gamma)$. In the next section, I discuss the notion of reversibility of quantum operations as these notions underpin the formulation of quantum secret sharing.

3.5 Reversibility of quantum operations

Before I discuss quantum secret-sharing schemes, I explain the notion of reversibility, from which my definition of quantum secret-sharing protocols and their secrecy requirements is based on.

Let $\mathscr{H}$ and $\mathscr{K}$ be Hilbert spaces, and let $\mathcal{S}(\mathscr{H})$ and $\mathcal{S}(\mathscr{K})$ be the set of density operators on $\mathscr{H}$ and $\mathscr{K}$, respectively. A quantum operation

$$W : \mathcal{S}(\mathscr{H}) \to \mathcal{S}(\mathscr{K}), \tag{3.24}$$

is reversible with respect to a subset $\mathcal{S} \subset \mathcal{S}(\mathscr{H})$ of density operators if there exists a quantum operation

$$\mathcal{R} : \mathcal{S}(\mathscr{K}) \to \mathcal{S}(\mathscr{H}), \tag{3.25}$$

such that $\forall\rho \in \mathcal{S}$, $\mathcal{R} \cdot W(\rho) = \rho$ [16]. W is vanishing with respect to $\mathcal{S}$ if there exists a density operator $\rho_0 \in \mathcal{S}(\mathscr{K})$ such that $\forall\rho \in \mathcal{S}$, $W(\rho) = \rho_0$ [16]. Next we define quantum secret sharing.

3.6 Quantum secret-sharing protocols

Let $\mathscr{H}$ be a Hilbert space and let $\mathcal{S}(\mathscr{H})$ be the set of all density operators on $\mathscr{H}$. In a quantum secret-sharing scheme, the dealer's task is to encrypt a quantum secret $\rho_{\mathrm{s}} \in \mathcal{S}(\mathscr{H})$ into a composite system of Hilbert spaces

$$\mathscr{H}_1, \mathscr{H}_2, \ldots, \mathscr{H}_n, \tag{3.26}$$

each of which is called a share labled by $S_1, S_2, \ldots, S_n$. Let

$$N \coloneqq \{S_1, S_2, \ldots, S_n\}, \tag{3.27}$$

be the entire set of shares and

$$\mathscr{H}_N \coloneqq \bigotimes_{S_i \in N} \mathscr{H}_{S_i}, \tag{3.28}$$

be the corresponding Hilbert space. For a subset $A \subseteq N$ of shares let

$$\mathscr{H}_{\mathrm{A}} \coloneqq \bigotimes_{S_i \in A} \mathscr{H}_{S_i}. \tag{3.29}$$

QSS encoding is

$$W_N : \mathcal{S}(\mathscr{H}) \to \mathcal{S}(\mathscr{H}_N), \tag{3.30}$$

which is a completely positive and trace preserving map [16].

The composition map of the encoder W_N for a subset $X \subseteq N$ and the partial trace of the complement $N \setminus X$ is

$$W_X \coloneqq \mathrm{Tr}_{N \setminus X} \cdot W_N. \tag{3.31}$$

A QSS scheme is then defined by the quantum operation W_N (3.30) that is reversible with respect to $\mathcal{S}(\mathscr{H})$. The set N is divided into two mutually disjoint subsets known as authorized (or qualified) and forbidden structures.

1. A set $X \subseteq N$ is called *authorized* if W_X is reversible with respect to $\mathcal{S}(\mathscr{H})$ [16].

2. A set $X \subseteq N$ is called *forbidden* if W_X is vanishing with respect to $\mathcal{S}(\mathscr{H})$ [16].

Before we provide an example for threshold quantum secret-sharing schemes, we introduce two theorems which are useful for our later discussions.

Theorem 3.6.1. *$((k;n))$ scheme implies $((k;n-1))$ scheme when $k < n$ (here the use of double parentheses distinguishes the quantum schemes from the classical schemes).*

Proof. For proof of the theorem, refer to Fig.3.1. For any $((k,n))$ threshold scheme, only k shares are needed at any time to reconstruct the secret. Erasing shares would not affect the scheme until total number of shares is at least k. □

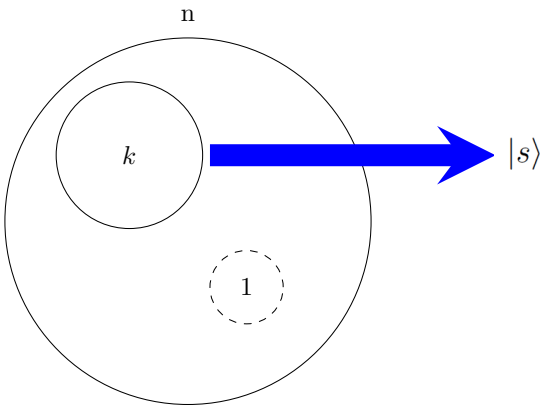

Figure 3.1: Existence of $((k,n-1))$ scheme if $((k,n))$ scheme exists.

Theorem 3.6.2. *If the secret is a quantum state, then no $((k,n))$ scheme exists for $n \geq 2k$. [7].*

Proof. The proof of the theorem is provided as Fig. 3.2. Cloning an arbitrary quantum state is impossible according to quantum no-cloning theorem. Let $n \geq 2k$. The independent sets of k shares can be used to reconstruct the secret. Two copies of the same secret means the no-cloning theorem is violated. hence, $n < 2k$. □

Next, I shall prove the existence of $((k,n))$ quantum threshold schemes where $n \leq 2k-1$.

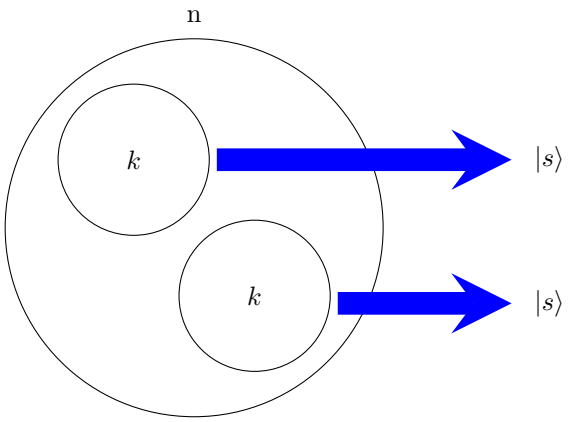

Figure 3.2: Violation of no-cloning if $n \geq 2k$.

3.7 Construction of threshold QSS schemes

A $((k, n))$ threshold scheme is constructed based on quantum polynomial codes [6]. Quantum polynomial codes are quantum version of classical Reed Solomon codes. Reed Solomon codes are used in error correction where k symbols are instructed to correct $n - k$ erasure errors. Let s be the dimension of the secret quantum state $|\psi\rangle$ to be encoded. The goal is to encode $|\psi\rangle$ into n shares such that the data that is encoded can always be recovered from any k shares.

3.7.0.1 Encoding

Here I explain the encoding procedure. A prime number q is chosen such that $q \geq \max(s, n)$. This is because, I would correspond each basis vector of the quantum state to a unique element of $\mathbb{F}_q$. For

$$\boldsymbol{c} = (c_0, \ldots, c_{k-1}) \in \mathbb{F}_q^k, \tag{3.32}$$

define the polynomial

$$p_{\boldsymbol{c}}(t) = c_0 + c_1 t + \ldots + c_{k-1} t^{k-1}. \tag{3.33}$$

The dealer then chooses $x_1, \ldots, x_n \in \mathbb{F}_q$ $(x_i \neq x_j)$ which are publicly revealed constants and encode a q-ary quantum state by the linear mapping which is defined on basis states $\{|i\rangle\}_{i \in \mathbb{F}_q}$

as

$$|i\rangle \mapsto \sum_{c\in\mathbb{F}_q^k,\ c_{k-1}=i} |p_{\boldsymbol{c}}(x_0)\, p_{\boldsymbol{c}}(x_1)\cdots p_{\boldsymbol{c}}(x_{n-1})\rangle\,. \tag{3.34}$$

The secret is thus encoded as the coefficient of the highest degree element in the polynomial. Hence, an arbitrary quantum state would be encoded as

$$|\psi\rangle = \sum_i \alpha_i |i\rangle \mapsto \sum_i \alpha_i \sum_{c\in\mathbb{F}_q^k,\ c_{k-1}=i} |p_{\boldsymbol{c}}(x_0)\, p_{\boldsymbol{c}}(x_1)\cdots p_{\boldsymbol{c}}(x_{n-1})\rangle\,. \tag{3.35}$$

Each component of the tensor is then a share of the secret.

3.7.0.2 Decoding

It now suffices to show that, given an encoding (3.35) of a quantum state, the state can be retrieved by any k coordinates. One way to show this is by employing theory of CSS codes. To make the treatment comprehensive, I provide an explicit decoding procedure for the special case of $n = 2k-1$ scheme.

The decoding procedure takes advantageous of the properties of the Vandermonde matrix V_d. The Vandermonde matrix V_d is a square matrix of dimension $d \times d$ defined as

$$V_d\left[x_0, x_1, x_2, \ldots, x_n\right]_{ij} = x_j^i, \qquad x_i \in \mathbb{F}. \tag{3.36}$$

V_d is invertible when $x_i = x_j$ iff $i = j$. Observe that

$$(c_0, c_1, \ldots, c_{k-1})\, V_k\,(x_0, x_1, \ldots, x_{k-1}) = (p_{\boldsymbol{c}}(x_0), p_{\boldsymbol{c}}(x_1), \ldots, p_{\boldsymbol{c}}(x_{k-1}))\,. \tag{3.37}$$

Therefore,

$$(c_0, c_1, \ldots, c_{k-1}) = (p_{\boldsymbol{c}}(x_0), p_{\boldsymbol{c}}(x_1), \ldots, p_{\boldsymbol{c}}(x_{k-1}))\, V_k\,(x_0, x_1, \ldots, x_{k-1})^{-1}\,. \tag{3.38}$$

This means, by picking k polynomial evaluations of $p_{\boldsymbol{c}}(x)$ and applying corresponding inverse Vandermonde matrix, one can construct the polynomial $p(x)$ again. However, in quantum secret sharing the secret state is encoded in a superposition of polynomials. Also, secret state itself can be a simple basis vector or a linear combination of basis vectors. The below are the steps to recover the secret from the encoded quantum state.

Given the first k registers as $(p_{\boldsymbol{c}}(x_0), p_{\boldsymbol{c}}(x_1), \ldots, p_{\boldsymbol{c}}(x_{k-1}))$, the tensor product of these shares is

$$|p_{\boldsymbol{c}}\rangle = |p_{\boldsymbol{c}}(x_0), p_{\boldsymbol{c}}(x_1) \ldots p_{\boldsymbol{c}}(x_{k-1})\rangle \,. \tag{3.39}$$

The steps to recover the secret are listed below.

1. Multiply $|p_{\boldsymbol{c}}\rangle$ by V_k^{-1}

$$|p_{\boldsymbol{c}}\rangle \bigotimes_{j=k+1}^{2k-1} |p_{\boldsymbol{c}}(x_j)\rangle \left(V_k^{-1} \otimes \mathbb{I}\right) = \bigotimes_{j=0}^{k-1} |c_j\rangle \bigotimes_{j=k+1}^{2k-2} |p_{\boldsymbol{c}}(x_j)\rangle \,. \tag{3.40}$$

2. Cyclically right shift the first k states of the resultant state (3.40) by one position. The resultant state is

$$|c_{k-1}\rangle \bigotimes_{j=0}^{k-2} |c_j\rangle \bigotimes_{i=k+1}^{2k-2} |p_{\boldsymbol{c}}(x_j)\rangle \,. \tag{3.41}$$

   If the secret $|\psi\rangle$ is a basis state $|i\rangle$, then the secret can be recovered from the first component of the tensor product state directly because $c_{k-1} = i$. However, if $|\psi\rangle$ is not a basis state, then steps 3 and 4 below must be performed to recover the secret. In such a case, the first component of the tensor product state will be entangled with the rest of the components.

3. Multiply the resultant state (3.41) from the previous step by $\mathbb{I}_1 \otimes V_{k-1}(x_k, x_{k+1}, \ldots, x_{2k-2}) \otimes \mathbb{I}_{k-1}$. The resultant state is

$$|\psi\rangle \otimes \sum_{c \in \mathbb{F}_k, c_{k-1}=i} \left[\bigotimes_{i=k+1}^{2k-2} |p_{\boldsymbol{c}}(x_j)\rangle \bigotimes_{i=k+1}^{2k-2} |p_{\boldsymbol{c}}(x_j)\rangle \right] . \tag{3.42}$$

4. $\forall i \in \{1, \ldots k-1\}$, add first component multiplied by $(x_{k+i-1})^{(k-1)}$ of the tensor product state to every i^{th} component.

In order to gain intuition about this QSS protocol, the encoding and reconstruction procedure for the special case of $(2, 3)$ QSS are discussed in the next section.

3.7.1 (2,3) QSS

Consider the case where secret is a state $|\psi\rangle = \alpha|1\rangle + \beta|1\rangle + \gamma|3\rangle$. Let $|\psi\rangle_{\mathrm{e}}$ be the n-ary encoded state of the secret. Let $n = 3,\ q = 3,\ k = 2,\ s = 3$. Then $\mathbb{F}_3 = \{0, 1, 2\}$. Let $x_0 = 0, x_1 = 1, x_2 = 2$. Then

$$\mathbb{F}_3^2 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)\}. \tag{3.43}$$

Construct the encoded state (3.34). Hence,

$$\begin{aligned} W_{2,3} : |\psi\rangle \mapsto |\psi\rangle_{\mathrm{e}} =& \alpha\left(|000\rangle + |111\rangle + |222\rangle\right) \\ &+ \beta\left(|012\rangle + |120\rangle + |201\rangle\right) \\ &+ \gamma\left(|021\rangle + |102\rangle + |210\rangle\right). \end{aligned} \tag{3.44}$$

The goal is to retrieve the secret from the first two shares. The reconstruction procedure is given below

$$V_2(x_0 = 0, x_1 = 1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \tag{3.45}$$

$$V_2^{-1}(x_0 = 0, x_1 = 1) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}. \tag{3.46}$$

Thus,

$$(0,0)\cdot V_2^{-1}(x_0=0,x_1=1)=(0,0)\,, \tag{3.47}$$

$$(1,1)\cdot V_2^{-1}(x_0=0,x_1=1)=(1,0)\,, \tag{3.48}$$

$$(2,2)\cdot V_2^{-1}(x_0=0,x_1=1)=(2,0)\,, \tag{3.49}$$

$$(0,1)\cdot V_2^{-1}(x_0=0,x_1=1)=(0,1)\,, \tag{3.50}$$

$$(1,2)\cdot V_2^{-1}(x_0=0,x_1=1)=(1,1)\,, \tag{3.51}$$

$$(2,0)\cdot V_2^{-1}(x_0=0,x_1=1)=(2,1)\,, \tag{3.52}$$

$$(0,2)\cdot V_2^{-1}(x_0=0,x_1=1)=(0,2)\,, \tag{3.53}$$

$$(1,0)\cdot V_2^{-1}(x_0=0,x_1=1)=(1,2)\,, \tag{3.54}$$

$$(2,1)\cdot V_2^{-1}(x_0=0,x_1=1)=(2,2)\,. \tag{3.55}$$

Therefore,

$$\begin{aligned}\left(V_2^{-1}\otimes\mathbb{I}\right)|\psi\rangle =&\alpha\left(|000\rangle+|101\rangle+|202\rangle\right)\\ &+\beta\left(|012\rangle+|110\rangle+|211\rangle\right)\\ &+\gamma\left(|021\rangle+|122\rangle+|220\rangle\right).\end{aligned} \tag{3.56}$$

Now, I cyclically shift the first two registers by one to the right. The resultant state is

$$\alpha\left(|000\rangle+|011\rangle+|022\rangle\right)+\beta\left(|102\rangle+|110\rangle+|121\rangle\right)+\gamma\left(|201\rangle+|212\rangle+|220\rangle\right).$$

Then I apply $V_0(x_1)=1$ to first register. The resultant state is

$$\alpha\left(|000\rangle+|011\rangle+|022\rangle\right)+\beta\left(|102\rangle+|110\rangle+|121\rangle\right)+\gamma\left(|201\rangle+|212\rangle+|220\rangle\right).$$

After performing the last step, the secret state is recovered as follows

$$\begin{aligned}&\alpha\left(|000\rangle+|011\rangle+|022\rangle\right)+\beta\left(|122\rangle+|100\rangle+|111\rangle\right)\\ &+\gamma\left(|201\rangle+|222\rangle+|210\rangle\right)=\left(\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle\right)\left(|00\rangle+|11\rangle+|22\rangle\right).\end{aligned} \tag{3.57}$$

In the next section I discuss information-theoretic description of QSS protocols which is used to define and evaluate QSS protocols.

3.8 Information-theoretic description of quantum secret-sharing protocols

The information-theoretic description of secret sharing has played a crucial role in defining and evaluating secret-sharing protocols [16, 42, 44, 45]. In this section, I give the information theoretical description of QSS protocols [45].

Quantum mutual information is employed to define and evaluate the security of QSS protocols [29]. In a QSS protocol, a dealer $\mathcal{D}$ shares a quantum state $\rho^{\mathrm{S}} \in \mathcal{S}(\mathscr{H}_{\mathrm{S}})$ between a set of players $\mathcal{P}$, such that specific subsets of players form the authorized structure (denoted by $\mathcal{A}$) to retrieve the message, whereas the other subsets (i.e., the adversarial structure denoted by $\mathcal{F}$), are denied any information about the secret whatsoever. I might imagine, however, that the system ρ^{S} is part of a larger system and that this compound system, is initially in a pure state $|\psi^{\mathrm{RS}}\rangle$. Therefore

$$\rho^{\mathrm{S}} = \mathrm{tr}_{\mathrm{R}} \left(|\psi^{\mathrm{RS}}\rangle \langle \psi^{\mathrm{RS}}| \right). \tag{3.58}$$

In a QSS, if a subset $X \subseteq \Gamma$ satisfies

$$I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{X}}\right) = 0 \quad \text{(secrecy condition)}, \tag{3.59}$$

then ρ^{X} does not contain any information about ρ^{S}, which means that X is an element of forbidden structure [29]. On the other hand, if a subset X satisfies

$$I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{X}}\right) = I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{S}}\right) \quad \text{(recoverability condition)}, \tag{3.60}$$

then ρ^{X} contains full information about ρ^{S} [29]. In the next subsection, I discuss the relation between recoverability and secrecy requirements, and the reversibility of quantum operations.

3.8.1 Relation between the reversibility of quantum operations and secrecy requirements

In this subsection, I state a theorem that show the recoverability requirement discussed in §3.8 implies the existence of a reversible quantum operation [29], as discussed in §3.6.

Theorem 3.8.1. *Let W_N be a QSS with authorized structure $\mathcal{A}$. Then the recoverability condition (3.60) holds iff a quantum operator $\mathcal{R}$ exists such that*

$$\mathcal{R}\left(\rho^X\right) = \rho^S. \tag{3.61}$$

Furthermore, for quantum secret sharing schemes where the unauthorized sets are the complements of the authorized sets, the recoverability requirement implies the secrecy requirement.

To give an example, I show that the scheme $W_{2,3}$ (3.44) satisfies the recoverability and secrecy requirements [29]. Suppose the quantum secret is

$$\rho^{\mathrm{S}} = \frac{1}{3}\sum_{i=1}^{3} |i\rangle\langle i|\,; \tag{3.62}$$

therefore, the purification of ρ^{S} is

$$|\mathrm{RS}\rangle := \frac{1}{\sqrt{3}}\left(|00\rangle + |11\rangle + |22\rangle\right). \tag{3.63}$$

The system corresponding to the shares and the reference system can then be described as

$$\begin{aligned}\left(\mathbb{I}\otimes W_{2,3}\right)\rho^{\mathrm{RS}} =& \frac{1}{3}\Big(|0000\rangle + |0111\rangle + |0222\rangle + |1012\rangle + |1120\rangle \\ &+ |1201\rangle + |2021\rangle + |2102\rangle + |2210\rangle \Big).\end{aligned} \tag{3.64}$$

Then $I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{S}}\right) = 2\log 3$. In the case of $X = \{1, 2\}$,

$$H_{\mathrm{vN}}\left(\mathrm{RX}\right) = \log 3, \tag{3.65}$$

$$H_{\mathrm{vN}}\left(\mathrm{X}\right) = 2\log 3, \tag{3.66}$$

hold; hence,

$$I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{X}}\right) = 2\log 3. \tag{3.67}$$

Therefore the recoverability requirement is satisfied. On the other hand, if $X = \{1\}$, then $I\left(\rho^{\mathrm{R}} : \rho^{\mathrm{X}}\right) = 0$. Hence, the secrecy requirement is satisfied. Next I discuss ramp quantum secret-sharing protocols.

3.9 Ramp quantum secret-sharing scheme

As an extension of (k, n)–threshold SS schemes discussed in ¶3.4, ramp secret-sharing (RSS) schemes were proposed by Blakley-Meadows [9] and Yamamoto [21]. In RSS schemes, the dimension of each share is reduced to less than that of the original system by sacrificing security, admitting the intermediate property for some sets of shares, which are called intermediate sets.

A QSS scheme W_N is called perfect if any set $X \subseteq N$ is either authorized or forbidden. Otherwise, W_N is a RQSS scheme. The access structure of a RQSS scheme is the list of the forbidden, intermediate, and authorized sets. A set $X \subseteq N$ is called *intermediate* if W_X is neither vanishing nor reversible with respect to $\mathcal{S}(\mathscr{H})$ [16]. Formally, the access structure of the set N is defined by a map

$$f : 2^{\mathcal{P}} \to \{0, 1, 2\}, \tag{3.68}$$

where $0, 1$ and 2 represent $\mathcal{F}, \mathcal{I}$ and $\mathcal{A}$, respectively. Next I discuss a particular scheme for constructing threshold RQSS protocols.

3.9.1 Construction of RQSS schemes

In this subsection, I introduce a method to construct $((k, L, n))$-threshold RQSS schemes [16]. The encoding and decoding used here are extensions of the scheme discussed in §3.7.

Let $\mathbb{F}_q$ be a finite field where $q \geq n$. Furthermore, let

$$\mathscr{K}_j \, (j = 1, \ldots, L) \text{ and } \mathscr{H}_i \qquad i \in N = \{1, \ldots, n\} \tag{3.69}$$

be Hilbert spaces with dimension $\dim \mathscr{H}_j = \dim \mathscr{K}_i = q$ and an orthonormal basis $\{|s\rangle\}_{s \in \mathbb{F}}$. Here I construct a pure state RQSS scheme W_N, which maps the state on $\mathscr{H} \coloneqq \otimes_{j=1}^{L} \mathscr{K}_j$ into the system of shares $\mathscr{H}_N \coloneqq \otimes_{i \in N} \mathscr{H}_i$. The basis

$$|s^L\rangle = |s_1\rangle \otimes \cdots \otimes |s_L\rangle \,, \;\; s^L = (s_1, \ldots, s_L) \in \mathbb{F}^L, \tag{3.70}$$

on $\mathscr{H}$ is then encoded by utilizing the linear mapping

$$|s_L\rangle \mapsto \frac{1}{\sqrt{C}} \sum_{c \in D(s^L)} |p_{\boldsymbol{c}}(x_1), \ldots, p_{\boldsymbol{c}}(x_n)\rangle, \tag{3.71}$$

where $x_1, \ldots, x_n \in \mathbb{F}$ $(x_i \neq x_j)$ are publicly revealed constants and $D\left(s^L\right)$ is

$$D\left(s^L\right) \coloneqq \{(c_1, \ldots c_k) \in \mathbb{F}^k | c_i = s_i \, (i = 1, \ldots, L)\}, \tag{3.72}$$

for which $p_{\boldsymbol{c}}$ is defined in Eq. (3.33). For future convenience, let us introduce the following notations for $X \in \{i_1, \ldots, i_m\} \subseteq N$

$$M_b^a(X) \coloneqq \begin{bmatrix} x_{i_1}^a & \ldots & x_{i_m}^a \\ x_{i_1}^{a+1} & \ldots & x_{i_m}^{a+1} \\ \vdots & & \vdots \\ x_{i_1}^b & \ldots & x_{i_m}^b \end{bmatrix},$$

$$p_{\boldsymbol{c}}(X) \coloneqq (p_{\boldsymbol{c}}(x_{i_1}), \ldots, p_{\boldsymbol{c}}(x_{i_m})). \tag{3.73}$$

It follows that $p_{\boldsymbol{c}}(X) = (c_1, \ldots, c_k) M_{k-1}^0(X)$, and the following proposition is useful for our later discussion.

Proposition 1. *For each $s_L \in \mathbb{F}^L$, the map $\boldsymbol{c} \in D\left(s^L\right) \mapsto p_{\boldsymbol{c}}(X)$ is injective if $|X| \geq k - L$. Importantly, it is one to one if $|X| = k - L$. In the same vein, the map $c \in \mathbb{F}^k \mapsto p_{\boldsymbol{c}}(X)$ is injective if $|X| \geq k$ and it is one-to-one if $|X| = k$.*

From Proposition 1, the terms in the right hand side of Eq. (3.71) are orthogonal to each other; therefore, the normalization constant C is q^{k-L}. Next I prove that the linear mapping (3.71) realizes a (k, L, n)-threshold RQSS scheme [16].

Authorized sets. In order to prove that X is authorized in the case of $|X| \geq k$, it is enough to prove that X is authorized for $X = \{1, \ldots, k\}$. This is because of the symmetric way to construct W_N, and the monotonicity of quantum access structure. Here I give an explicit decoding for the case of interest, where $X = \{1, \ldots, k\}$. Suppose that the first k

registers are given. Perform the unitary transformation on the first k registers corresponding to $p_{\boldsymbol{c}}(X) M_{k-1}^{0}(X)^{-1}$, which maps the summation (3.71) into

$$\sum_{c \in D(s^L)} |c_1, \ldots, c_k, p_{\boldsymbol{c}}(x_{k+1}), \ldots, p_{\boldsymbol{c}}(x_n)\rangle . \tag{3.74}$$

Then perform the unitary transformation on first k registers corresponding to the linear transformation

$$(c_1, \ldots, c_k) \begin{bmatrix} I & M_{L-1}^{0}(N \backslash X) \\ 0 & M_{k-1}^{L}(N \backslash X) \end{bmatrix} .$$

Equation. (3.74) then turns into

$$|s^L\rangle \sum_{c \in D(s^L)} |p_{\boldsymbol{c}}(N \backslash X)\rangle \, |p_{\boldsymbol{c}}(N \backslash X)\rangle , \tag{3.75}$$

which, according to Prop. 1, can be equivalently expressed as

$$|s^L\rangle \sum_{y^{k-L} \in \mathbb{F}^{k-L}} |y^{k-L}\rangle \, |y^{k-L}\rangle . \tag{3.76}$$

Thus, $|s^L\rangle$ is recovered from the first k registers via local operations.

Forbidden sets. In the case of $|X| \leq k - L$, $N \backslash X$ is authorized as $|N \backslash X| \geq k$. Therefore, because of the no-clonning theorem, any set of players X where $|X| \leq k - L$ is a forbidden set.

Intermediate sets. In the case of $|X| = k - l$ $(0 < l < L)$, I prove that X is an intermediate set [16]. In order to do so, I follow the approach introduced in §3.8 and prove that W_X is neither vanishing nor reversible in the case of $|X| = k - l$ $(0 < l < L)$. Suppose the quantum secret is

$$\rho^{\mathrm{S}} = \sum_{s^L \in \mathbb{F}^L} p_{s^L} |s^L\rangle \langle s^L| . \tag{3.77}$$

For simplicity and without loss of generality I consider the case where $\{p_{s^L}\}$ is uniformly random, hence

$$\rho^{\mathrm{S}} = \sum_{s^L \in \mathbb{F}^L} \frac{1}{q^L} |s^L\rangle \langle s^L| . \tag{3.78}$$

Let $\mathscr{S}$ be a Hilbert space with orthonormal basis $\{|j\rangle\}$ $j \in \{1, \ldots, q^L\}$. Then the purification of ρ^{S} is

$$|\mathrm{RS}\rangle \coloneqq \sum_{s^L \in \mathbb{F}^L, j \in \mathbb{F}_{q^L}} \sqrt{\frac{1}{q^L}} \, |j\rangle \, |s^L\rangle \in \mathscr{S} \otimes \mathscr{H}. \tag{3.79}$$

$|\mathrm{RS}\rangle$ is pure; hence,

$$H_{\mathrm{vN}}\left(\rho^{\mathrm{S}}\right) = H_{\mathrm{vN}}\left(\rho^{\mathrm{R}}\right) = \sum_{s^L \in \mathbb{F}^L} \frac{1}{q^L} \log\left(\frac{1}{q^L}\right) = L \log q. \tag{3.80}$$

Therefore,

$$I\left(\mathrm{R}; \mathrm{X}\right) = 2L \log q. \tag{3.81}$$

Next we calculate

$$\begin{aligned} W_X\left(\rho^{\mathrm{S}}\right) &= \sum_{s^L \in \mathbb{F}^L} \frac{1}{q^L} W_X\left(|s^L\rangle \langle s^L|\right) \\ &= \frac{1}{C} \sum_{s^L \in \mathbb{F}^L} \frac{1}{q^L} \sum_{c,d \in D(s^L)} \langle p_d\left(N \backslash X\right) | p_{\boldsymbol{c}}\left(N \backslash X\right)\rangle \, |p_{\boldsymbol{c}}\left(X\right)\rangle \langle p_d\left(X\right)| \\ &= \frac{1}{C} \sum_{s^L \in \mathbb{F}^L} \frac{1}{q^L} \sum_{c \in D(s^L)} |p_{\boldsymbol{c}}\left(X\right)\rangle \langle p_{\boldsymbol{c}}\left(X\right)| \, . \end{aligned} \tag{3.82}$$

As $|X| = k - l > k - L$ and because of Prop. (1), the set $\{|p_{\boldsymbol{c}}\left(X\right)\rangle\}$ in Eq. (3.82) comprises orthogonal states. Hence,

$$H_{\mathrm{vN}}\left(W_X\left(\rho^{\mathrm{S}}\right)\right) = H_{\mathrm{vN}}\left(\frac{\mathbb{I}}{q^{k-l}}\right) = (k-l) \log q. \tag{3.83}$$

In order to calculate $H_{\mathrm{vN}}\left(\left(I \otimes W_X\right)\left(|\mathrm{RS}\rangle \langle \mathrm{RS}|\right)\right)$, note that the von Neuman entropy is 0 for a pure state. Also, if a pure state is divided in two subsystems, the von Neuman entropies of the subsystems are equal. Therefore

$$H_{\mathrm{vN}}\left(\left(I \otimes W_X\right)\left(|\mathrm{RS}\rangle \langle \mathrm{RS}|\right)\right) = H_{\mathrm{vN}}\left(W_{N \backslash X}\left(\rho^{\mathrm{S}}\right)\right) = (n - k + l) \log q. \tag{3.84}$$

Consequently,

$$\begin{aligned} I\left(R; W_X\left(\rho^{\mathrm{S}}\right)\right) =& H_{\mathrm{vN}}\left(W_X\left(\rho^{\mathrm{S}}\right)\right) + H_{\mathrm{vN}}\left(\rho^{\mathrm{R}}\right) - H_{\mathrm{vN}}\left(\left(I \otimes W_X\right)\left(|\mathrm{RS}\rangle \langle \mathrm{RS}|\right)\right) \\ &= (k-l) \log q + L \log q - (n - k + l) \log q \\ &= (2k + L - n - 2l) \log q = 2\left(L - l\right) \log q, \end{aligned} \tag{3.85}$$

holds; therefore,

$$0 < I\left(\mathrm{R}; W_X\left(\rho^{\mathrm{S}}\right)\right) < I\left(\mathrm{R}; \mathrm{X}\right). \tag{3.86}$$

In the next section I review the main results for CV QSS protocols.

3.10 CV QSS protocol

In this section, I explain the TRS03 protocol. In a $((k, n))$ threshold scheme, Theorem 3.6.2 states the maximum value possible for n is $2k-1$. In addition, Theorem 3.6.1 states that any $((k, n))$ scheme can be constructed by removing shares from a $((k, 2k-1))$ scheme. Furthermore, any quantum secret sharing scheme can be reduced to $((k, 2k-1))$ threshold schemes [7]. Therefore, without loss of generality, in this section I restrict my discussion to $((k, 2k-1))$-threshold schemes

In a $((k, 2k-1))$-threshold scheme, the dealer holds a pure secret state $|\psi\rangle \in \mathscr{H}$ and encode the quantum secret into an entangled state of $2k-1$ modes of the electromagnetic field by combining it with $2k-2$ ancillary states. The dealer then distributes them among the n players, each of which receive one share, and at least k players must combine their shares in an active interferometer to extract the secret state.

Let $\mathscr{H}^{(2k-1)}$ be the tensor product of $2k-1$ copies of $\mathscr{H}^{(1)}$, and suppose each player owns one of these copies. Let me define $\mathbb{F}^{2k-1}$ as the real linear space of coordinate functions for $\mathbb{R}^{2k-1}$. Then a system of Euclidean coordinates

$$\boldsymbol{x} = \left(x_1, x_2, \ldots, x_{2k-1}\right)^{\mathrm{T}} \in \mathbb{R}^{2k-1} \tag{3.87}$$

is equivalent to picking an orthonormal basis $(f_1, f_2, \ldots, f_{2k-1})$ for $\mathbb{F}^{2k-1}$ such that

$$f_i\left(\boldsymbol{x}\right) = x_i, \tag{3.88}$$

where

$$f_i \cdot f_j = \delta_{ij}, \tag{3.89}$$

for coordinate $\boldsymbol{x}$ given by Eq. (3.87).

Initially, the dealer starts with a tensor product

$$|\Psi\rangle = |\psi\rangle \otimes \underbrace{|\phi_a\rangle \cdots |\phi_a\rangle}_{k-1} \otimes \underbrace{|\phi_{1/a}\rangle \cdots |\phi_{1/a}\rangle}_{k-1}, \tag{3.90}$$

where $|\psi\rangle$ is the secret state and

$$\phi_a(x) = \langle x|\phi_a\rangle = \left(\pi a^2\right)^{-1/4} \mathrm{e}^{-x^2/2a^2}. \tag{3.91}$$

This state (3.121) can be written as

$$\begin{aligned} |\Psi\rangle &= \int \mathrm{d}^n \boldsymbol{x}\, \Psi(\boldsymbol{x})\, |x_1\rangle \otimes \cdots \otimes |x_n\rangle \\ &= \int \mathrm{d}^n \boldsymbol{x}\ \Psi(\boldsymbol{x})\, |f_1(\boldsymbol{x})\rangle \otimes \cdots \otimes |f_n(\boldsymbol{x})\rangle\,, \end{aligned} \tag{3.92}$$

where

$$\Psi(\boldsymbol{x}) = \psi(x_1) \prod_{i=2}^{k} \phi_a(x_i) \prod_{i=k+1}^{n} \phi_{1/a}(x_i)\,. \tag{3.93}$$

Encoding. The dealer then performs the encoding using a linear canonical point transformation

$$f_j \mapsto g_i = \sum_j g_{ij} f_j. \tag{3.94}$$

The corresponding unitary transformation then maps the state $|\Psi\rangle$ to

$$|\det g|^{1/2} \int \mathrm{d}x^n \Psi(\boldsymbol{x})\, |g_1(\boldsymbol{x})\rangle \otimes \cdots \otimes |g_n(\boldsymbol{x})\rangle\,. \tag{3.95}$$

The dealer, however, has to choose $\{g_i\}$ such that any k players are able to disentangle the secret state but that any lesser number is unable to do so. Let ι_i be the orthogonal projection of each vector g_i into the space spanned by the vectors $\{f_1, \ldots, f_n\}$. The vectors $\{g_i\}$ then must be chosen such that any k vectors from the set $\{f_1, \iota_1, \ldots, \iota_n\}$ are linearly independent. This linearly independence condition guarantees that any k players are able to extract the secret in the case of infinitely large amount of a.

For convenience, let us express $\mathbb{F}^{2k-1} \in \mathbb{R}^{2k-1}$ as a direct sum of three mutually orthogonal subspaces

$$\mathbb{F}^n = \mathbb{X} \oplus \mathbb{Y} \oplus \mathbb{Z}, \tag{3.96}$$

where $\mathbb{X}$ is the one-dimensional space spanned by f_1 and, $\mathbb{Y}$ and $\mathbb{Z}$ are $k-1$-dimensional spaces spanned by $\{f_2, \ldots, f_k\}$ and $\{f_{k+1}, \ldots, f_n\}$ respectively. Now, let us relabel $\{x_i\}$ coordinates as (x, y_i, z_i) coordinates with

$$x = x_1, \quad y_i = x_{i+1}, \quad z_i = x_{k+i}, \tag{3.97}$$

where $i = 1, \ldots, k-1$. The wave-function Ψ is then

$$\Psi(\boldsymbol{x}) = \psi(x) \prod_{i=1}^{k-1} \phi_a(y_i)\, \phi_{1/a}(z_i). \tag{3.98}$$

Without loss of generality, let us assume the first k players collaborate to retrieve the quantum secret. The players perform the linear coordinate transformation

$$g_i \mapsto \xi_i = \sum_j \xi_{ij} f_j, \tag{3.99}$$

assuming $\xi_i = g_i$ for all $i > k$.

For convenience, let us define a decomposition for every vector ξ_i as a sum of three mutually orthogonal vectors, each of which belongs to subspaces $\mathbb{X}$, $\mathbb{Y}$ and $\mathbb{Z}$

$$\xi_i = \alpha_i + \beta_i + \gamma_i. \tag{3.100}$$

Equivalently, I write Eq. (3.100) as

$$\xi_i(\boldsymbol{x}) = \alpha_i x + \sum_j \beta_{ij} y_j + \sum_j \gamma_{ij} z_j. \tag{3.101}$$

In the case that the vectors g_i are chosen in such a way that any k vectors from the set $\{f_1, \iota_1, \ldots, \iota_n\}$ are linearly independent, the players can design the transformation $g_i \mapsto \xi_i$ such that

$$\begin{aligned} \alpha_1 &= 1, \qquad \beta_1 = 0, \\ \alpha_{i+1} &= \alpha_{k+i}, \quad \beta_{i+1} = \beta_{k+i}, \end{aligned} \tag{3.102}$$

where $i = 1, \ldots, k-1$. The transformation (3.102) extracts the secret for sufficiently large values of parameter a. Another way of looking at a quantum secret-sharing protocol is to view it as an error correcting code that corrects erasure errors. In the next section, I provide the basic results of quantum error correction codes.

3.10.1 Example: the (2,3) threshold scheme

In this section I explain TRS03 protocol using an example of the $((2,3))$ threshold scheme in which there are three players in total and any two of them can fully reconstruct the quantum secret.

The initial state of dealer $|\phi\rangle_0$ contains the quantum secret and two quadrature states, one infinitely squeezed in quadrature $\hat{p}$ and the other one infinitely squeezed in quadrature $\hat{q}$; hence

$$|\phi\rangle_0 = \int_{\mathbb{R}^2} \mathrm{d}x_1 \mathrm{d}x_2 \psi(x_1) |x_1\rangle_1 |x_2\rangle_2 |0\rangle_3 . \tag{3.103}$$

Then the dealer chooses a linear transformation g that satisfies the condition discussed in ¶3.10 as

$$g = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{\sqrt{2}} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} . \tag{3.104}$$

By performing the linear transformation g on $|\phi\rangle_0$, the dealer encodes $|\phi\rangle_0$ into

$$|\phi\rangle = \int_{\mathbb{R}^2} \mathrm{d}x_1 \mathrm{d}x_2 \psi(x_1) |\frac{x_1}{\sqrt{2}} + \frac{x_2}{2}\rangle_1 |\frac{x_1}{\sqrt{2}} - \frac{x_2}{2}\rangle_2 |\frac{x_2}{\sqrt{2}}\rangle_3 . \tag{3.105}$$

After encoding, the dealer distribute the shares to the players, each of whom receives one share.

If the first and second players collaborate to extract the secret, they can use a 1:1 beam splitter in order to combine their shares and extract the quantum secret. Particularly, players

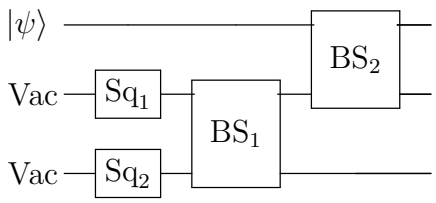

Figure 3.3: The encoding transformation corresponding to $(2, 3)$ CV QSS.

1 and 2 perform the passive transformation

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.106}$$

After performing the transformation (3.106), the resultant state $|\phi_{12}\rangle$ contains the quantum secret in mode 1, namely

$$|\phi_{12}\rangle = \int_{\mathbb{R}^2} \mathrm{d}x_1 \mathrm{d}x_2 \psi(x_1) |x_1\rangle_1 |\frac{x_2}{\sqrt{2}}\rangle_2 |\frac{x_2}{\sqrt{2}}\rangle_3 . \tag{3.107}$$

Players 1 and 3 employ the active transformation

$$\begin{pmatrix} \sqrt{2} & -1 \\ 1 & -\sqrt{2} \end{pmatrix} \tag{3.108}$$

in order to extract the quantum secret. The resultant state after performing the transformation (3.108) is

$$|\phi_{13}\rangle = \int_{\mathbb{R}^2} \mathrm{d}x_1 \mathrm{d}x_2 \psi(x_1) |x_1\rangle_1 |\frac{x_1}{\sqrt{2}} - \frac{x_2}{2}\rangle_2 |\frac{x_1}{\sqrt{2}} - \frac{x_2}{2}\rangle_3 . \tag{3.109}$$

Therefore, the quantum secret is reconstructed in mode 1. The reconstruction of quantum secret using players 2 and 3 is similar to the extraction of quantum secret by players 1 and 3. In the next section I describe quantum error correcting codes, and their relationship to quantum secret-sharing protocols.

3.11 Quantum error correcting codes

In this section, I provide the basic results of quantum error correction [46–48]. The aim of error correction is to protect information that is sent over unreliable communication channels.

Quantum information is susceptible to errors due to interaction with an environment or eavesdropper, as well as imperfect physical devices. In error correction, the information is encoded into a codeword, which is used to detect and correct errors. The set of codewords is defined as a code.

The simplest example of a noisy classical channel is a bit flip channel [2]. This channel flips the data with probability p and transfer it correctly with probability $1-p$. Suppose Alice wants to send 1 bit at a time through this noisy channel, but Alice does not want Bob receive the wrong message due to errors. In this case, Bob and Alice can use an error correcting code to decrease the probability of error. The simplest example of an error correcting code is the 3 bit repetition code. The encoding is simply to repeat the bit three times; i.e.,

$$0 \mapsto 000, 1 \mapsto 111, \tag{3.110}$$

and decoding is by taking the most frequent bit, which is the same as computing the majority function. If 0 or 1 of the bits are flipped during transmission, Bob is able to recover the original bit sent by Alice. The probability of error changes from p to $3p^2 - 2p^3$. This is a reduction in error when $p < 1/2$. If $p = 1/2$ then the channel is useless for transmitting the information and if $p > 1/2$ Bob can flip every bit before decoding that converts p to $1-p$ [2]. This method however, can not be applied for quantum error correction as the no-cloning [49] theorem prevents the copy of an arbitrary quantum state.

A quantum error correcting code can be designed by utilizing an unitary operation that maps a quantum state into a subspace, which is called coding space denoted by C, of a larger-dimensional Hilbert space. For instance, consider the following unitary operation that encodes an arbitrary qubit with two ancillary states in the codeword of three qubits

$$\mathrm{U_{enc}} : (\alpha |0\rangle + \beta |1\rangle) |0\rangle |0\rangle \mapsto \alpha |000\rangle + \beta |111\rangle . \tag{3.111}$$

This unitary operation implements a three-qubit code. The coding space corresponding to this encoding operation is the two-dimensional subspace of a larger 2^3-dimensional Hilbert

space. This encoding operation does not have any conflict with no cloning theorem as there is no m such that $(\alpha|0\rangle + \beta|1\rangle)^{\otimes m} = \alpha|000\rangle + \beta|111\rangle$.

This code can correct a bit flip error if it takes place on a single qubit. If one of the qubits flip, I am able to know on which qubit the error takes place by comparing the state of the first qubit by second qubit and the state of second qubit by third qubit via measurements. I measure the differences between two states in order to not collapse the superpositions.

Another possible error is the phase-flip error. The phase flip acts the same as a bit-flip error but in the $\{|+\rangle, |-\rangle\}$ basis. The three-qubit code can correct a phase-flip error if I apply the encoding operation in the $|+\rangle$ and $|-\rangle$ basis; i.e.,

$$U_{\text{enc}} : (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \mapsto \alpha|+++\rangle + \beta|---\rangle. \tag{3.112}$$

In this basis, the effect of phase-flip error is the same as bit-flip error in the $|0\rangle$ and $|1\rangle$ basis; therefore, it can be corrected using the same method.

To correct both bit-flip and phase-flip errors, I can use both encoding procedures (3.111) and (3.112) at once, which is called Shor's 9-qubit code. The state of a qubit can be encoded by

$$|0\rangle \mapsto |\bar{0}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle), \tag{3.113}$$

$$|1\rangle \mapsto |\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \tag{3.114}$$

In the next section, I discuss the necessary and sufficient condition that a QECC should satisfy in order to be able to correct errors successfully.

3.11.1 Necessary and sufficient condition for QECC

A code that encodes k qubits into n qubits has 2^k basis codewords. Each of these basis codewords corresponds to one of the bases of original states. Because of linearity (if a quantum code can correct errors F and E, it can also correct any linear combination of

them) feature of quantum error correcting codes, I only need to check whether a code can correct a basis of errors. One appropriate basis is the set of tensor products of $\sigma_x,\ \sigma_y,\ \sigma_z,\ I$.

In this section, I explain the necessary and sufficient conditions for successful error correction of a coding space C [46–48]. Consider two errors E_a and E_b act on two different basis codewords $|\psi_i\rangle$ and $|\psi_j\rangle$, respectively. I should always be able to distinguish $E_a |\psi_i\rangle$ from $E_b |\psi_j\rangle$, as otherwise, I might confuse them. Therefore

$$\langle\psi_i| E_a^\dagger E_b |\psi_j\rangle = 0, \tag{3.115}$$

when $i \neq j$ for correctable errors E_a.

However, the condition (3.115) is necessary but not sufficient. The measurement that is performed to learn about the error should not exhibit any information about the actual state of the code as such a measurement will disturb superpositions of the basis states. I learn about the error by measuring $\langle\psi_i| E_a^\dagger E_b |\psi_i\rangle$ for all possible errors E_a and E_b. Therefore, this quantity should be the same for all the basis codewords. Hence

$$\langle\psi_i| E_a^\dagger E_b |\psi_i\rangle = \langle\psi_j| E_a^\dagger E_b |\psi_j\rangle . \tag{3.116}$$

Eqs. (3.115) and (3.116) can be combined into a single equation as

$$\langle\psi_i| E_a^\dagger E_b |\psi_j\rangle = C_{ab}\delta_{ij}, \tag{3.117}$$

where $|\psi_i\rangle$ and $|\psi_j\rangle$ are all possible basis codewords. Also, E_a and E_b are all possible errors. The *distance* d of a QECC is the minimum weight of pauli operator E such that Eq. (3.117) does not hold. A quantum code with distance equal to $2t+1$ can correct maximum t errors no matter where the location of errors are. A code that encodes k qubits in n qubits is depicted by $[[n, k, d]]$.

Sometimes I know where the location of errors are, perhaps I know some qubits are more likely to be damaged by errors. An erasure error is a general error on a known coordinate. Let $\mathcal{C}$ be a subspace of a Hilbert space $\mathscr{H}$. Then $\mathcal{C}$ corrects erasure errors on a set K of

coordinates iff

$$\langle\psi|\, E\, |\psi\rangle = c\,(E)\,, \tag{3.118}$$

for all E acting on K. A code with distance d can correct $d-1$ erasure errors.

Quantum secret sharing as a quantum error correcting code. Another way of looking at a quantum secret-sharing protocol is to view it as an error correcting code that corrects erasure errors. A code that corrects erasure errors reconstructs the original qubit even if certain number of qubits are lost from the encoding. Similarly, in a quantum secret-sharing protocol, the secret can be reconstructed by excluding certain number of secret shares. For instance, a $[[2k-1, 1, k]]$ stabilizer code is considered as a $((k, 2k-1))$ threshold quantum secret-sharing protocol. In the next section, I explain continuous-variable quantum error correcting codes.

3.12 Continuous-variable quantum error correction with linear optics

In the final section of this chapter, I consider the extension of DV quantum error correction to the CV realm as a direct generalization of the qubit redundancy codes [19, 20, 50]. Particularly, I describe a CV error correction code that protect a quantum state from arbitrary displacements in phase space. Remarkably, this code is realizable using ony linear-optical elements, such as squeezing.

I consider a 9-wave-packet code introduced by Braunstein [19,20], which is the continuous-variable extension of Shore's original 9-qubit code. This code is a concatenation of majority codes for position errors and momentum errors. These codes rely on the fact that a single non-zero mode x can be distributed over three modes according to

$$|x, 0, 0\rangle \to |\frac{x}{\sqrt{3}}, \frac{x}{\sqrt{3}}, \frac{x}{\sqrt{3}}\rangle\,. \tag{3.119}$$

The distribution (3.119) can be implemented with a three-mode beam splitter, called a

tritter $\mathcal{T}$. The $\mathcal{T}$ acts on the three quadrature operators according to

$$\mathcal{T} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}} & \mathrm{e}^{\frac{4\mathrm{i}\pi}{3}} \\ 1 & \mathrm{e}^{\frac{4\mathrm{i}\pi}{3}} & \mathrm{e}^{\frac{8\mathrm{i}\pi}{3}} \end{pmatrix}. \tag{3.120}$$

In order to obtain an intuition about the 9-wavepacket code, let us show how this 3-

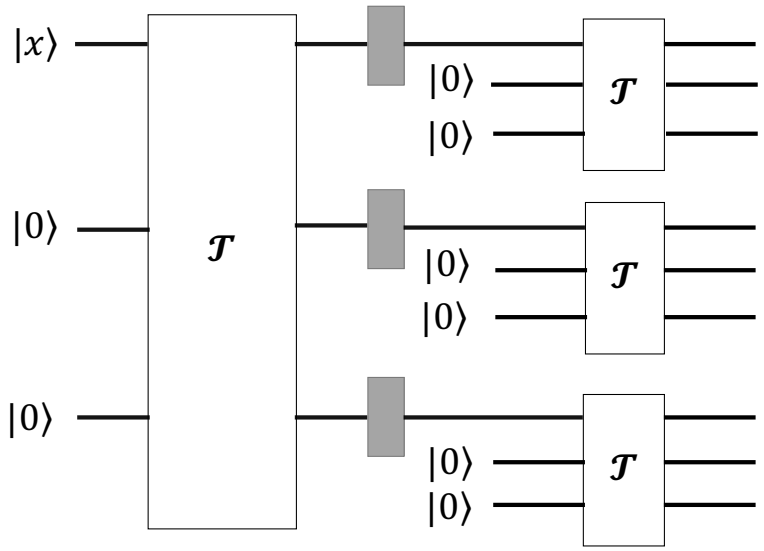

Figure 3.4: The optical implementation of a nine-wavepacket encoder.

wavepacket code can correct displacement errors. Consider an encoded state

$$|\frac{x}{\sqrt{3}}, \frac{x}{\sqrt{3}}, \frac{x}{\sqrt{3}}\rangle\,. \tag{3.121}$$

As

$$1 + \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}} + \mathrm{e}^{\frac{4\mathrm{i}\pi}{3}} = 1 + \mathrm{e}^{\frac{4\mathrm{i}\pi}{3}} + \mathrm{e}^{\frac{8\mathrm{i}\pi}{3}} = 0, \tag{3.122}$$

performing the inverse tritter $\mathcal{T}^\dagger$ to the encoded state (3.121) reconstruct the input state $|x, 0, 0\rangle$. Now, assume one of the modes in the encoded state (3.121) undergoes a displacement error $\frac{\delta}{\sqrt{3}}$ in the position quadrature. Without loss of generality, let us consider the case where

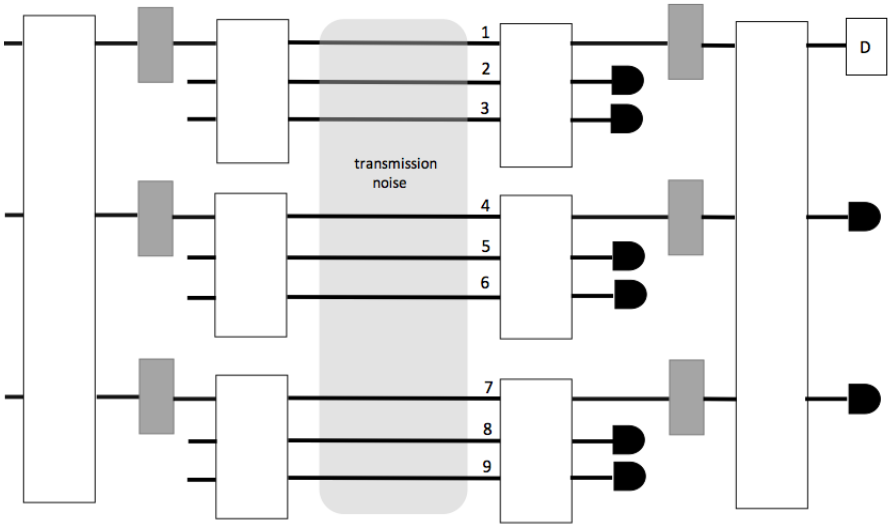

Figure 3.5: The complete realization of the 9-wavepacket code. The corrective displacement operator depends on the syndrome provided by the measurement outcomes of the eight homodyne detections.

second mode experiences the error. Then the state after decoding is

$$\mathcal{T}\,|\frac{x}{\sqrt{3}},\frac{x+\delta}{\sqrt{3}},\frac{x}{\sqrt{3}}\rangle = \begin{pmatrix} x+\frac{\delta}{3} \\ \mathrm{e}^{\frac{2\mathrm{i}\pi\delta}{3}}\frac{\delta}{3} \\ \mathrm{e}^{\frac{4\mathrm{i}\pi\delta}{3}}\frac{\delta}{3} \end{pmatrix}. \tag{3.123}$$

As $\mathrm{e}^{\frac{2\mathrm{i}\pi\delta}{3}}$ and $\mathrm{e}^{\frac{4\mathrm{i}\pi\delta}{3}}$ are pure phases, the ideal measurement outcomes in second and third modes are $\frac{\delta}{3}$. According to these outcomes, I then displace the position quadrature of the undetected mode by an amount of $\frac{-\delta}{\sqrt{3}}$.

This code does not protect the encoded state against displacements in the momentum quadrature; therefore, I concatenate this code with a similar code for momentum. In order to do so, I apply the Fourier transform

$$\mathcal{F}\,|x\rangle = \frac{1}{\sqrt{2\pi\hbar}}\int_{-\infty}^{+\infty}\mathrm{d}q\,\mathrm{e}^{\frac{\mathrm{i}}{\hbar}xq}\,|q\rangle\,, \tag{3.124}$$

on the three output of the tritter. I then couple each mode to two modes in the position eigenstates with eigenvalue zero, again using the tritter (3.120). The total encoding operation

is

$$\mathcal{T}_{789}\mathcal{T}_{456}\mathcal{T}_{123}\mathcal{F}_7\mathcal{F}_4\mathcal{F}_1\mathcal{T}_{147}, \tag{3.125}$$

and the decoding operation is the adjoint. The state after encoding procedure is

$$|x_{\rm enc}\rangle = \frac{1}{\sqrt{(2\pi\hbar)^3}} \int {\rm d}x_1 {\rm d}x_2 {\rm d}x_3 {\rm e}^{\frac{\rm i}{\hbar}(x_1+x_2+x_3)x} \, |\frac{x_1}{3}, \frac{x_1}{3}, \frac{x_1}{3}, \frac{x_2}{3}, \frac{x_2}{3}, \frac{x_2}{3}, \frac{x_3}{3}, \frac{x_3}{3}, \frac{x_3}{3}\rangle \, . \tag{3.126}$$

In the 9-wavepacket code, I perform eight position-quadrature measurements on the eight auxiliary modes from which I obtain a list of real numbers that constitute the syndrome. The entire quantum error correction code is shown in Fig. 3.5 . As the Fourier transform can be implemented with a simple phase shift, the entire encoder can be implemented using passive linear optics acting on highly squeezed states in the position quadrature. Similarly, the decoding can be implemented with passive linear optics and homodyne detection.

I have to take into account the fact that any optical implementation can achieve only finite squeezing in the auxiliary modes. Clearly, the amount of squeezing in the auxiliary modes must be such that the error in the undetected output mode is smaller than the error that would have been accumulated without error correction. In the next chapter I develop a method for quantifying quantum information leakage due to the limitation of squeezing. The method can be used to analyze the effect of finite squeezing in the auxiliary modes on the performance of CV QSS and CV QECC that rely on linear optics.

3.13 Summary

In chapter three, I reviewed the main results of secret-sharing protocols. I began by introducing classical secret sharing. I then discussed the information theoretic description of classical secret-sharing protocols along with classical ramp secret sharing, which reduces the size of the shares at the cost of leakage of information to unauthorized players. Then I explained ramp quantum secret-sharing protocols. Subsequently, I introduced discrete-variable quantum secret sharing. Then I discussed the information-theoretic description of quantum

secret-sharing protocols, which has a crucial role in defining and evaluating secret-sharing protocols. Then I explained the TRS03 protocol. Afterwards, I described the aforementioned protocol in the Heisenberg picture, which is useful for analysing the effect of finite squeezing in the dealers encoding process. Finally, I explained the quantum error correcting codes and their relationship with quantum secret-sharing protocols.

Chapter 4

Continuous-variable ramp quantum secret sharing

In this chapter, I begin by elaborating on the approach I use to introduce CV ramp quantum secret sharing protocol and its corresponding certification test. In Sec. 4.1, I introduce a CV RQSS protocol and how to certify. I discuss the success criterion of the certification protocol. Furthermore, we specify what the parties need to do to complete the certification. In Sec. 4.2 I present our main results. Our first result is a CV version of quantum mutual information. This CV quantum mutual information is then used to quantify quantum-information leakage for Gaussian states and operations. Based on this leakage characterization, we introduce a certification test, in the framework of quantum-interactive proofs, and provide a practical test to implement this test.

4.1 Approach

In this section, we introduce a CV RQSS protocol and how to certify. We discuss the success criterion of the certification protocol. Furthermore, we specify what the parties need to do to complete the certification.

4.1.1 Continuous-variable ramp quantum secret-sharing protocol with Gaussian states and operations

Here we modify the discrete-variable RQSS protocol discussed in §3.9 into a continuous-variable counterpart. We choose Gaussian states and operations, which are convenient mathematically due to the elegance of techniques based on the semidirect product of the symplectic group and the Heisenberg-Weyl group [30]. However, the price paid for this convenient is discarding potentially powerful universal operations [31]. Whereas in the dis-

crete case specification of number of players and threshold condition L suffices to determine the cardinality of the three structures, the CV case is more complicated due to squeezing limitations.

4.1.1.1 Quantum-optical resources

The optical realization comprises displacers that generate Heisenberg-Weyl group elements and single-mode squeezers, passive beam-splitters and phase-shifters that generate the semidirect product of the symplectic group [30]. The inputs are vacuum states of light. For the closed disk

$$D_s := \left\{\zeta \in \mathbb{C} : |\zeta| \leq s^2\right\},\ s \in \mathbb{R}^+, \tag{4.1}$$

the dealer's and players' single-mode squeezers (2.19) have limited squeezing capability corresponding to $\zeta \in D_s$, with $s = s^{\mathrm{D}}_{\max}$ for the dealer and $s = s^{\mathrm{P}}_{\max}$ for the player.

4.1.1.2 Dealer's task

Here we specify the dealer's task in the RQSS protocol. Dealer's tasks include preparing a quantum secret, choosing an access structure, encoding the quantum secret and distributing shares.

Two-mode squeezed-vacuum source. The dealer prepares a TMSV state (2.22) drawn randomly from

$$Q_{\mathrm{D}} := \left\{|\zeta\rangle_{\mathrm{TMSV}}\,;\zeta \in D_{s^{\mathrm{D}}_{\max}}\right\}. \tag{4.2}$$

The dealer's task is to encode one mode of this quantum state into an n-mode entangled state by mixing it with $n-1$ ancillary states in an n-mode active interferometer. The dealer then sends one share to each of the players in such a way that the elements of power set of players are divided into three predetermined mutually disjoint sets known as authorized, intermediate and forbidden structures.

In order for dealer to prepare the TMSV randomly, first, he needs to decide the complex two-mode squeezing parameter $\zeta = s\mathrm{e}^{\mathrm{i}\theta}$ (2.21), where s is bounded by $s^{\mathrm{D}}_{\max}$. The dealer

generates two random numbers $a, b \in [0, 1]$. Then the dealer assigns

$$s \leftarrow \sqrt{2as^{\mathrm{D}}_{\max}},\ \theta \leftarrow 2\pi b. \tag{4.3}$$

Choosing a useful, feasible access structure. The dealer chooses an access structure Γ based on the desired application. The dealer then runs an algorithm that accepts Γ, covariance matrix of TMSV state $\boldsymbol{V}$, $s^{\mathrm{D}}_{\max}$ and $s^{\mathrm{P}}_{\max}$ as input and yields the encoding transformation or null as output. The dealer then performs the encoding transformation and distributes the shares among players.

4.1.1.3 Players' task

The players' task in any authorized set is to reconstruct the quantum secret. One player is assigned to hold the secret after reconstruction. The aforementioned player forms a structure with other players in the authorized set and perform a Gaussian unitary operation on their shares such that the state of the share belongs to assigned player become the same as the original secret state. The players in any intermediate set are allowed to partially reconstruct the secret state. Furthermore, the players in a forbidden structure should not gain any information about the quantum secret whatsoever.

4.1.2 Certification protocol

In this subsection we introduce a certification protocol that ascertains whether the RQSS protocol succeeds. The success criterion is discussed in this subsection. We specify what the parties need to do to complete the certification.

4.1.2.1 Agents and resources

In this subsection, we establish the agents of the certification protocol, namely, the dealer, the players and the referee who is a skeptical certifier. Furthermore, we specify available resources for each party.

The dealer and players share trusted error-free classical and quantum communication channels between each other, and the referee also shares trusted error-free classical and quantum communication channels with each player and with the dealer. In our continuous-variable setting, the referee possesses single-mode homodyne detectors [32]. Henceforth, we only refer explicitly to homodyne measurement, without loss of generality.

The dealer holds a classical computer to choose the access structure Γ discussed in ¶4.1.1.2, and the referee possesses a classical computer to run the certification algorithm.

4.1.2.2 Dealer's encoding and announcement

The dealer chooses an access structure Γ discussed in ¶4.1.1.2 and announces Γ to the players and to the referee. The dealer encodes shares based on the choice of Γ and the quantum secret, such as a randomly chosen state in the parameter disk (4.2) and announces this encoding to the players.

4.1.2.3 Rounds

In this subsubsection, we define 'rounds', which are repetitions of the protocol between the dealer, player and referees. First the dealer prepare a suitable two-mode Gaussian state, which is the same two-mode Gaussian state for all rounds, and sends one mode to the referee and the other mode into an encoder, which is also unchanging over all rounds. This encoder creates shares that are sent to each player.

After the shares are received by players, the referee requests a subset of players, which can be authorized, forbidden or intermediate, to try to reconstruct the quantum secret and then send their shares to the referee. The referee then performs single-mode homodyne measurements and save the measurement results. Rounds continue until the referee lets the dealer and players stop.

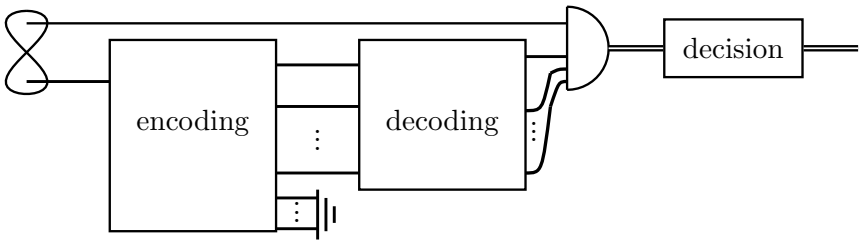

Figure 4.1: Two-mode entangled state with one share, or mode, sent directly to the referee and the other share encoded for the players. The referee requests a subset of players to decode their shares and send this result to the referee who decides whether they have succeeded or not.

4.1.2.4 Referee's certification strategy

The referee's task is to certify the protocol by ascertaining the dealer's announcement that the access structure is the announced Γ. The referee conducts the test by requiring many rounds per instance, with each instance corresponding to testing whether a fixed subset of players is in the authorized, intermediate or forbidden structures determined by Γ. Due to the statistical nature of the test, the referee cannot be 100% sure that the inference is correct; rather the referee makes a decision if the probability of being correct is above some threshold value, itself strictly greater than $1/2$.

Sufficiency condition. When a sufficiency condition is met to ascertain whether the subset of players are determined to be in a structure compatible with the dealer's announced Γ, the referee tells the players to stop. If that instance passes the test, the referee announces a new subset of players to test and the rounds repeat until the referee has enough data to pass the sufficiency test. If the instance results in the dealer and players failing, the procedure stops as the team of dealer and players has failed the test. The dealer and players pass only if every instance passes.

4.1.3 Summary of approach

Here we modified the discrete-variable RQSS protocol as the CV counterpart in the case of Gaussian states and operations. Furthermore, we introduced a certification protocol that ascertains whether the RQSS protocol succeeds. Also we discussed the success criterion and we specified what the parties need to do to complete the certification.

4.2 Results

In this section we present our main results. Our first result is a CV version of quantum mutual information. This CV quantum mutual information is then used to quantify quantum-information leakage for Gaussian states and operations. Based on this leakage characterization, we introduce a certification test, in the framework of quantum-interactive proofs, and provide a practical test to implement this test.

4.2.1 CV quantum mutual information

In this subsection, we develop the quantum mutual information for the CV RQSS quantum access structures and employ it to quantify quantum-information leakage for Gaussian states and operations. We define the intermediate structure corresponding to CV RQSS protocols based on quantum mutual information.

Let $|\psi\rangle^{\mathrm{RS}}$ be a pure two-mode Gaussian state and let the quantum secret be ρ_{s} (3.58). Then the intermediate structure is

$$\mathcal{I} \coloneqq \{X \ ; \ 0 < I\left(\mathrm{R};\mathrm{X}\right) < I\left(\mathrm{R};\mathrm{S}\right)\}, \tag{4.4}$$

and the authorized and forbidden structures are obtained by

$$\mathcal{A} \coloneqq \left\{Y \in 2^{\mathcal{P}}; I(\mathrm{R};\mathrm{S}) = I(\mathrm{R};\mathrm{X})\right\}, \tag{4.5}$$

and

$$\mathcal{F} \coloneqq \left\{X \in 2^{\mathcal{P}}; I(\mathrm{R};\mathrm{X}) = 0\right\}. \tag{4.6}$$

We now calculate mutual information between the referee and any multiplayer structure for TRS03. We consider a two-mode entangled state (4.1) such that one mode is used for the secret and the other mode is used for the reference system. We choose this system because that way the referee can do a sensitive entanglement check to verify that the reconstructed state is entangled with a reference system as it should be. To keep matters simple, while maintaining the generality of the method, we investigate in particular a TMSV with one mode being the quantum secret and the other mode being the reference system.

We solve the quantum mutual information between an extracted secret obtained by any player structure with k elements and the reference system. In order to do so, by using Eq. (2.4), we transform the density function of the reference system and the extracted secret (A.4) into a Gaussian Wigner function represented by a mean vector and a covariance matrix from which the symplectic eigenvalues (2.12) are calculated.

The symplectic eigenvalues (2.12) are inserted into Eq. (2.27) in order to calculate the local and global von Neumann entropy of the extracted secret and reference system from which the quantum mutual information is solved (2.35). Figure 4.2 shows the resultant quantum mutual information versus squeezing parameter in the case of $|\zeta| = 2$. In §4.2.2 we employ the CV quantum mutual-information approach to introduce a certification technique for CV RQSS schemes.

4.2.2 Certification test for RQSS protocols

In this subsection, we establish our model for certification tests. Specifically, we introduce certification tests for $\mathcal{A}$, $\mathcal{F}$ and $\mathcal{I}$, respectively.

RQSS certification for authorized structure. Let $I_{\mathrm{T}}^{\mathcal{A}}$ be a threshold quantum mutual information chosen by the referee. This quantum mutual information quantifies the minimum knowledge that players in an access structure are able to obtain about the secret. Also let $\beta > 0$ be a maximal failure probability. A test, which receives as input copies of some X,

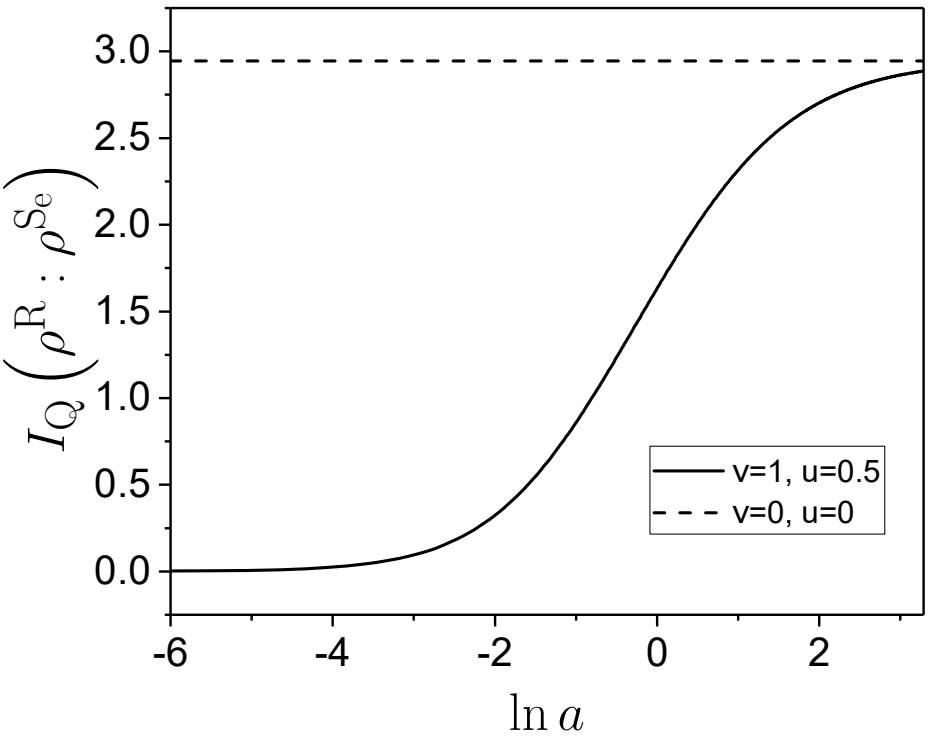

Figure 4.2: Mutual information versus the squeezing parameter $\ln a$ for one mode of a two mode squeezed vacuum state.

and yields accept or reject, is a test for certifying whether $X \in \mathcal{A}$, if, with probability at least $1-\beta$, it both rejects every ρ^{X} for which

$$I\left(\mathrm{X};\mathrm{R}\right) < I_{\mathrm{T}}^{\mathcal{A}} \tag{4.7}$$

and accepts if

$$I\left(\mathrm{X};\mathrm{R}\right) \geq I_{\mathrm{T}}^{\mathcal{A}} + \delta. \tag{4.8}$$

These conditions correspond to soundness (4.7) and completeness (4.8)

RQSS certification for forbidden structure. Let $I_{\mathrm{T}}^{\mathcal{F}}$ be a threshold quantum mutual information chosen by the referee, which quantifies the maximum knowledge that players in the forbidden structure can obtain about the secret. A test, which receives as input copies of some ρ^{X}, and yields accept or reject, is a certification test for certifying whether $X \in \mathcal{F}$, if,

with probability at least $1-\beta$, it both accepts every X for which

$$I\left(\mathrm{X};\mathrm{R}\right) \leq I_{\mathrm{T}}^{\mathcal{F}} - \delta, \tag{4.9}$$

and rejects a different ρ^{X} for

$$I\left(\mathrm{X};\mathrm{R}\right) > I_{\mathrm{T}}^{\mathcal{F}}. \tag{4.10}$$

These conditions are completeness (4.9) and soundness (4.10).

RQSS certification for intermediate structure. A test that receives as input copies of some X and yields accept or reject is a test for certifying whether $X \in \mathcal{I}$ if for a least probability given by $1-\beta$, it both rejects every X for

$$I\left(\mathrm{X};\mathrm{R}\right) \leq I_{\mathrm{T}}^{\mathcal{F}} - \delta, \tag{4.11}$$

or

$$I\left(\mathrm{X};\mathrm{R}\right) \geq I_{\mathrm{T}}^{\mathcal{A}} + \delta. \tag{4.12}$$

and accepts if

$$I_{\mathrm{T}}^{\mathcal{F}} < I\left(\mathrm{X};\mathrm{R}\right) < I_{\mathrm{T}}^{\mathcal{A}}. \tag{4.13}$$

Conditions (4.11) and (4.12) are soundness and condition (4.13) is completeness. In the next subsection we employ our certification model to propose a practical test to ascertain RQSS protocols.

4.2.3 Practical realization of the certification test

In this subsection, we propose a practical algorithm, for determining if X is in $\mathcal{A}$, $\mathcal{I}$ or $\mathcal{F}$. We prove propositions that the algorithm is both sound and complete. Furthermore, we provide a sufficiency test for the referee to know how many runs are required for her to have sufficient information to check if a particular element is in $\mathcal{A}$, $\mathcal{I}$ or $\mathcal{F}$.

4.2.3.1 Steps for certification

Below we provide the steps for certifying RQSS. Before commencing certification, the referee numerically labels each element of the power set and proceeds to test each labelled element of the power set in order according to this labelling. For simplicity, and without loss of generality, we assume that each player holds one share; thus, the number n of modes equals one more than the number of players, hence shares, in the given subset. This extra mode allows a single-mode reference field in addition to the modes held by the players.

The referee conducts a test that requires many rounds (4.1.2.3) for each power-set element. The test evaluates whether a fixed subset of players is in $\mathcal{A}$, $\mathcal{I}$ or $\mathcal{F}$. In order to do so, the referee estimates the quantum mutual information $I_{\mathrm{e}}(\mathrm{R},\mathrm{S_e})$ between the reference state ρ^{R} and the extracted secret state $\rho^{\mathrm{S_e}}$ such that

$$I_{\mathrm{e}}(\mathrm{R};\mathrm{S_e}) \in [I(\mathrm{R};\mathrm{S_e}) - \epsilon, I(\mathrm{R};\mathrm{S_e}) + \epsilon], \tag{4.14}$$

with a failure probability $\beta < 1/2$. Algorithm 4 accepts $I_{\mathrm{e}}(\mathrm{R},\mathrm{S_e})$ as input and determines the structure of the power-set element. If the test result is consistent with the dealer's announcement that the access structure is the announced Γ, the referee announces a new subset of players to test; otherwise the procedure halts as the team of dealer and players has failed the certification test.

To estimate $I_{\mathrm{e}}(\mathrm{R};\mathrm{S_e})$, the referee estimates the expectation values corresponding to each element of the matrices

$$\boldsymbol{G} = \begin{pmatrix} 2\hat{\boldsymbol{x}}_1^2 & \frac{(\hat{\boldsymbol{x}}_1+\hat{\boldsymbol{x}}_2)^2}{2} & \hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_3 + \hat{\boldsymbol{x}}_3\hat{\boldsymbol{x}}_1 & \hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_4 + \hat{\boldsymbol{x}}_4\hat{\boldsymbol{x}}_1 \\ \frac{(\hat{\boldsymbol{x}}_1+\hat{\boldsymbol{x}}_2)^2}{2} & 2\hat{\boldsymbol{x}}_2^2 & \hat{\boldsymbol{x}}_2\hat{\boldsymbol{x}}_3 + \hat{\boldsymbol{x}}_3\hat{\boldsymbol{x}}_2 & \hat{\boldsymbol{x}}_2\hat{\boldsymbol{x}}_4 + \hat{\boldsymbol{x}}_4\hat{\boldsymbol{x}}_2 \\ \hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_3 + \hat{\boldsymbol{x}}_3\hat{\boldsymbol{x}}_1 & \hat{\boldsymbol{x}}_2\hat{\boldsymbol{x}}_3 + \hat{\boldsymbol{x}}_3\hat{\boldsymbol{x}}_2 & 2\hat{\boldsymbol{x}}_3^2 & \frac{(\hat{\boldsymbol{x}}_3+\hat{\boldsymbol{x}}_4)^2}{2} \\ \hat{\boldsymbol{x}}_1\hat{\boldsymbol{x}}_4 + \hat{\boldsymbol{x}}_4\hat{\boldsymbol{x}}_1 & \hat{\boldsymbol{x}}_3\hat{\boldsymbol{x}}_4 + \hat{\boldsymbol{x}}_4\hat{\boldsymbol{x}}_3 & \frac{(\hat{\boldsymbol{x}}_3+\hat{\boldsymbol{x}}_4)^2}{2} & 2\hat{\boldsymbol{x}}_4^2 \end{pmatrix}, \tag{4.15}$$

and

$$\boldsymbol{C} = \begin{pmatrix} \hat{\boldsymbol{x}}_1 & \hat{\boldsymbol{x}}_2 & \hat{\boldsymbol{x}}_3 & \hat{\boldsymbol{x}}_4 \end{pmatrix}, \tag{4.16}$$

with $\hat{\boldsymbol{x}}$ defined in Eq. (2.2). The first and second modes hold reference and reconstructed secret states, respectively. The referee's result is then used to estimate the covariance matrix (2.9) of $\rho^{\mathrm{RS_e}}$ according to [51]

$$V_{ij}^{\mathrm{RS_e}} = \langle \boldsymbol{G}_{ij} \rangle - \langle \boldsymbol{C}_i \rangle \langle \boldsymbol{C}_j \rangle, \qquad ij \notin \{12, 21, 34, 43\}, \tag{4.17}$$

$$V_{ij}^{\mathrm{RS_e}} = 2\langle \boldsymbol{G}_{ij} \rangle - \langle \boldsymbol{G}_{ii} \rangle/2 - \langle \boldsymbol{G}_{jj} \rangle/2 - \langle \boldsymbol{C}_i \rangle \langle \boldsymbol{C}_j \rangle, \qquad ij \in \{12, 21, 34, 43\}. \tag{4.18}$$

This covariance matrix is used to calculate the entropies of $\rho^{\mathrm{S_e}}$, ρ^{R} and $\rho^{\mathrm{RS_e}}$ using Algorithm 1. The resultant entropies are then inserted into the standard formula for quantum mutual information (2.41).

The expectation value of each element of (4.15) and (4.16) is calculated by performing multiple homodyne measurements on identical and independent copies of $\rho^{\mathrm{RS_e}}$ and taking the average of the measurement results. Using Chebyshev's inequality [51], the referee calculates an upper-bound for the estimation error of each expectation value as a function of number of rounds and β. Subsequently, this estimation error is then used to calculate the maximum expectation values' estimation error $\epsilon_{\max}$ of covariance-matrix entries via the standard formula for error propagation. Afterwards she calculates the bound on the estimation error of entropies following Algorithm 2. The estimation error of $I_{\mathrm{e}}(\mathrm{R};\mathrm{S_e})$ is bounded by summation of the entropies estimation errors. The rounds continue until the estimation error of $I_{\mathrm{e}}(\mathrm{R};\mathrm{S_e})$ is below a prespecified acceptable ϵ error. acceptable ϵ error.

Algorithm 1 Continuous-variable quantum entropy (H_{vN}).

Input:

$n \in \mathbb{N}$ ▷ Number of modes

$\boldsymbol{V} \in \mathbb{R}^{2n} \times \mathbb{R}^{2n}$ ▷ Covariance matrix

$\boldsymbol{\Omega} \in \mathbb{Z}^{2n} \times \mathbb{Z}^{2n}$ (2.3)

Output:

$H_{\mathrm{vN}} \in \mathbb{R}^{+}$ ▷ von Neumann entropy

function VONNEUMANNH($\boldsymbol{V}$)

$\boldsymbol{\nu} \leftarrow$ Eigenvalues$_{+}$ ($\mathrm{i}\Omega\boldsymbol{V}$). ▷ Calculates positive eigenvalues.

$\boldsymbol{\nu}^{\pm} \leftarrow \frac{\boldsymbol{\nu} \pm \mathbb{1}}{2}$.

return $H_{\mathrm{vN}} \leftarrow \boldsymbol{\nu}^{+} \cdot \log \boldsymbol{\nu}^{+} + \boldsymbol{\nu}^{-} \cdot \log \boldsymbol{\nu}^{-}$.

end function

Algorithm 2 Upper bound of H_{vN} estimation error.

Input:

$n \in \mathbb{N}$ ▷ Number of modes

$\boldsymbol{V} \in \mathbb{R}^{2n} \times \mathbb{R}^{2n}$ ▷ Covariance matrix

$\epsilon_{\max}$ ▷ Maximum estimation error of covariance matrix elements

Output:

$H^{\mathrm{upper}}_{\mathrm{vN,error}} \in \mathbb{R}^{+}$ ▷ Upper bound of QMI estimation error

function $H^{\mathrm{UPPER}}_{\mathrm{vN,ERROR}}(\boldsymbol{V}, \epsilon_{\max})$

$\sigma_{\max} \leftarrow$ maximal singular value of $\boldsymbol{V}$.

$\sigma_{\min} \leftarrow$ minimal singular value of $\boldsymbol{V}$.

return $H^{\mathrm{upper}}_{\mathrm{vN,error}} \leftarrow \kappa \left(1 + \log\left(2n\sigma_{\max}\right)\right) 2n\epsilon_{\max}$. ▷ $\kappa = \frac{\sigma_{\max}}{\sigma_{\min}}$ is always finite.

end function

Algorithm 3 Estimation of QMI.

Input:

$T \in \mathbb{N}$ ▷ Number of trials

$\rho^{\otimes T} \in \mathcal{B}\left(L^2(\mathbb{R}^{2T})\right)$ ▷ T copies of the joint state ρ for the reference and players' reconstructed state

$\epsilon \in \mathbb{R}^+$ ▷ Error tolerance for estimated QMI

$\textsc{Tol} \in (0,1/2)$ ▷ Failure probability tolerance

$\sigma \in \mathbb{R}^+$ ▷ A uniform upper bound on the standard deviations of measurement results

$\textsc{HomMeas}[\rho, x, \textsc{Mode}, \theta]$ ▷ Homodyne measurement on mode $\textsc{Mode} \in \{0,1\}$ with respect to local-oscillator phase θ; replaces ρ by some $|x\rangle\langle x|$ with probability $\langle x|\rho|x\rangle$

Output:

$\textsc{EstQMI} \in \mathbb{R}^+$ ▷ Estimated QMI

procedure $\textsc{EstimateQMI}(\epsilon, \textsc{Tol}, T, \rho^{\otimes T}, \sigma, \textsc{HomMeas}[\rho, x, \textsc{Mode}, \theta])$

for i from 1 to 2 **do**

for j from 1 to 2 **do**

$\textsc{CovRecon}[ij] \leftarrow 0$ ▷ Initialize covariance matrix for the players' reconstructed state including position-position, position-momentum, momentum-position and momentum-momentum

$\textsc{CovRef}[ij] \leftarrow 0$ ▷ Initialize covariance matrix for the reference state including position-position, position-momentum, momentum-position and momentum-momentum

end for

end for

for i from 1 to 4 **do**

$\textsc{HomResult}[i] \leftarrow 0$ ▷ Initialize vector comprising sums of in-phase and out-of-phase homodyne measurements of modes 0 and 1

for j from 1 to 4 **do**

$\textsc{CovRecRef}[ij] \leftarrow 0$ ▷ Initialize joint reconstructed-reference covariance matrix including position-position, position-momentum, momentum-position and momentum-momentum

$\textsc{SecondMom}[ij] \leftarrow 0$ ▷ Second-moment matrix defined in Eq. (4.15)

end for

end for

$\varepsilon \leftarrow \left\lceil \sigma \sqrt{\frac{1}{l\left(1-(1-\textsc{Tol})^{1/14}\right)}} \right\rceil$ ▷ Maximum estimation error of measurement results expectation values with a least probability $\textsc{Tol}$

$l \leftarrow 0$ ▷ Number of times that the referee performs the sufficiency test
$\textsc{Rho} \leftarrow \rho$ ▷ Initialize Rho to the first of input $\rho^{\otimes T}$
$\epsilon_{\text{QMI}} \leftarrow 2\epsilon$ ▷ Initialize to any value greater than ϵ
for r from 1 to T **do**
while $\epsilon_{\text{QMI}} > \epsilon$ **do**
$l \leftarrow l + 1$ ▷ Increment the sufficiency-test counter
if $14l > T$ **then** ▷ Referee measures 14 copies before ascertaining sufficiency
return Fail
Exit ▷ Abort procedure if fewer than 14 copies remain
end if
if $r - 1 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 0, 0)$ ▷ In-phase homodyne measurement of the reconstructed state
$\textsc{HomResult}[1] \leftarrow \textsc{HomResult}[1] + x$ ▷ Sum detection outcomes
else if $r - 2 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 0, \frac{\pi}{2})$ ▷ Out-of-phase homodyne measurement of the reconstructed state
$\textsc{HomResult}[2] \leftarrow \textsc{HomResult}[2] + x$ ▷ Sum detection outcomes
else if $r - 3 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 1, 0)$ ▷ In-phase homodyne measurement of the reference state
$\textsc{HomResult}[3] \leftarrow \textsc{HomResult}[3] + x$ ▷ Sum detection outcomes
else if $r - 4 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 1, \frac{\pi}{2})$ ▷ Out-of-phase homodyne measurement of the reference state
$\textsc{HomResult}[4] \leftarrow \textsc{HomResult}[4] + x$ ▷ Sum detection outcomes
else if $r - 5 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 0, 0)$ ▷ In-phase homodyne measurement of the reconstructed state
$\textsc{SecondMom}[11] \leftarrow \textsc{SecondMom}[11] + 2x^2$
else if $r - 6 \bmod 14{=}0$ **then** ▷ Measure one of T copies of ρ
Call $\textsc{HomMeas}(\textsc{Rho}, x, 0, 0)$ ▷ In-phase homodyne measurement of the reconstructed state
$y \leftarrow x$
Call $\textsc{HomMeas}(\textsc{Rho}, x, 1, 0)$ ▷ In-phase homodyne measurement of the reference state

SecondMom[13] $\leftarrow$ SecondMom[13] $+ 2xy$
SecondMom[31] $\leftarrow$ SecondMom[13]
else if $r - 7$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 0, 0$) ▷ In-phase homodyne measurement of the reconstructed state
$y \leftarrow x$
Call HomMeas(Rho, $x, 1, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reference state
SecondMom[14] $\leftarrow$ SecondMom[14] $+ 2xy$
SecondMom[41] $\leftarrow$ SecondMom[14]
else if $r - 8$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 0, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reconstructed state
SecondMom[22] $\leftarrow$ SecondMom[22] $+ 2x^2$
else if $r - 9$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 0, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reconstructed state
$y \leftarrow x$
Call HomMeas(Rho, $x, 1, 0$) ▷ In-phase homodyne measurement of the reference state
SecondMom[23] $\leftarrow$ SecondMom[23] $+ 2xy$
SecondMom[32] $\leftarrow$ SecondMom[23]
else if $r - 10$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 0, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reconstructed state
$y \leftarrow x$
Call HomMeas(Rho, $x, 1, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reference state
SecondMom[24] $\leftarrow$ SecondMom[24] $+ 2xy$
SecondMom[42] $\leftarrow$ SecondMom[24]
else if $r - 11$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 1, 0$) ▷ In-phase homodyne measurement of the reference state
SecondMom[33] $\leftarrow$ SecondMom[33] $+ 2x^2$
else if $r - 12$ mod 14=0 **then** ▷ Measure one of T copies of ρ
Call HomMeas(Rho, $x, 1, \frac{\pi}{2}$) ▷ Out-of-phase homodyne measurement of the reference state
SecondMom[44] $\leftarrow$ SecondMom[44] $+ 2x^2$
else if $r - 13$ mod 14=0 **then** ▷ Measure one of T copies of ρ

Call HomMeas(Rho, $x, 0, \frac{\pi}{4}$) ▷ Homodyne measurement of the reconstructed state with respect to local-oscillator phase $\frac{\pi}{4}$

SecondMom[12] $= 2x^2 -$ SecondMom[11]$^2 -$ SecondMom[22]^2

SecondMom[21] $\leftarrow$ SecondMom[12]

else$r - 14 \bmod 14 = 0$ ▷ Measure one of T copies of ρ

Call HomMeas(Rho, $x, 1, \frac{\pi}{4}$) ▷ Homodyne measurement of the reference state with respect to local-oscillator phase $\frac{\pi}{4}$

SecondMom[34] $= 2x^2 -$ SecondMom[33]$^2 -$ SecondMom[44]^2

SecondMom[43] $\leftarrow$ SecondMom[34]

end if

for i from 1 to 4 **do**

for j from i to 4 **do**

CovRecRef $[ij] \leftarrow \frac{1}{l}$ (SecondMom$[ij]$ − HomResult$[i]$HomResult$[j]$)

CovRecRef $[ij] \leftarrow$ CovRecRef $[ji]$

end for

end for

for i from 1 to 2 **do**

for j from 1 to 2 **do**

CovRecon $[ij] \leftarrow$ CovRecon $[ij]$

CovRef $[ij] \leftarrow$ CovRecon $[i + 2j + 2]$

end for

end for

$$\varepsilon_{\max} \leftarrow \frac{\varepsilon}{l} \max_{ij} \sqrt{1 + (\text{HomResult}\,[i])^2 + (\text{HomResult}\,[j])^2} \tag{4.19}$$

$$\varepsilon_{\max} \leftarrow \max\left\{ \varepsilon_{\max}, \frac{\varepsilon}{l} \sqrt{4 + (\text{HomResult}\,[1])^2 + (\text{HomResult}\,[2])^2}, \right. \tag{4.20}$$

$$\left. \frac{\varepsilon}{l} \sqrt{4 + (\text{HomResult}\,[3])^2 + (\text{HomResult}\,[4])^2} \right\} \tag{4.21}$$

▷ Via standard error propagation method

$\epsilon_{\text{QMI}} \leftarrow \sum_{\text{Q=Rp,p,R}} \text{H}^{\text{upper}}_{\text{vN,error}}\left(\text{V}^{\text{e,Q}}, \varepsilon_{\max}\right)$ ▷ See Algorithm 2

end while

end forreturn EstQMI $\leftarrow \sum_{\text{Q=R,p}}$ vonNeumannH$(\text{V}^{\text{e,Q}})$ − vonNeumannH$(\text{V}^{\text{e,Rp}})$ ▷ see Algorithm 1

end procedure

Algorithm 4 Certification of RQSS protocols.

Input:

$T \in \mathbb{N}$ ▷ Number of trials for each instance

$I_{\mathrm{T}}^{\mathcal{F}} \in \mathbb{R}^{+}$ ▷ Threshold quantum mutual information for the forbidden structure

$I_{\mathrm{T}}^{\mathcal{A}} \in \mathbb{R}^{+}$ ▷ Threshold quantum mutual information for all authorized structures

$\epsilon \in \mathbb{R}^{+}$ ▷ Estimation error bound of estimated QMI

$\textsc{Tol} \in (0,1/2)$ ▷ Maximum failure probability

$P \in \mathbb{N}$ ▷ Cardinality of the set of players

$\mathrm{F}[J] \in \{0,1,2\}$ ▷ Returns J^{th} power set of players structure claimed by the dealer (3.68)

$\bigotimes_{J=1}^{2^P-1} \rho_J^{\otimes T} \in \mathcal{B}\left(L^2(\mathbb{R}^{2^P T})\right)$ ▷ ρ_J is the joint state for the reference and players' reconstructed state for J^{th} subset of players

$\sigma \in \mathbb{R}^{+}$ ▷ A uniform upper bound on the standard deviations of measurement results

$\textsc{HomMeas}[\rho, x, \textsc{Mode}, \theta]$ ▷ Homodyne measurement on mode $\textsc{Mode} \in \{0,1\}$ with respect to local-oscillator phase θ; replaces ρ by some $|x\rangle\langle x|$ with probability $\langle x|\rho|x\rangle$

Output:

$b \in \{0,1\}$ ▷ Certify $(b=1)$ or not certify $(b=0)$

procedure $\textsc{Certification}(I_{\mathrm{T}}^{\mathcal{F}}, I_{\mathrm{T}}^{\mathcal{A}}, \epsilon, P, \bigotimes_{J=1}^{2^P-1} \rho_J^{\otimes T}, \mathrm{F}[J], \sigma, \textsc{Tol}, \textsc{HomMeas}[\rho, x, \textsc{Mode}, \theta])$

$c \leftarrow \mathrm{F}[1]$ ▷ initialize the structure of power-set elements based on referees' test to $\mathrm{F}[1]$

$\textsc{pass} \leftarrow 0$ ▷ initialize the number of power-set elements that pass the test

for J from 1 to $2^P - 1$ **do**

$\textsc{EstQMI} \leftarrow \textsc{EstimateQMI}\left(\epsilon, \textsc{Tol}, T, \rho_J^{\otimes T}, \sigma, \textsc{HomMeas}[\rho, x, \textsc{Mode}, \theta]\right)$ ▷ see Algorithm 3.

if

$$\textsc{EstQMI} > I_{\mathrm{T}}^{\mathcal{A}} + \epsilon, \tag{4.22}$$

then

$c \leftarrow 2$
else if

$$I_{\mathrm{T}}^{\mathcal{F}} - \epsilon < \textsc{EstQMI} < I_{\mathrm{T}}^{\mathcal{A}} + \epsilon, \tag{4.23}$$

then
$c \leftarrow 1$
else
$c \leftarrow 0$
end if
if $c = \textsc{f}[J]$ **then** $\textsc{pass} \leftarrow \textsc{pass} + 1$
else
Exit ▷ Halt
end if
end for
if $\textsc{pass} = 2^P$ **then**
$b \leftarrow 1.$
else
$b \leftarrow 0.$
end if
return b
end procedure

Proposition 2. *Algorithm 3 ensures*

$$pr\left[\left|I_e\left(X;R\right) - I\left(X;R\right)\right| \leq \epsilon_{QMI}\right] \geq 1 - \beta, \tag{4.24}$$

and

$$\epsilon_{QMI} \in O\left(\frac{1}{\sqrt{N}}\right) \tag{4.25}$$

for N the number of rounds.

Proof. Using Chebyshev's inequality [51],

$$\mathrm{pr}\left[\left|\bar{\boldsymbol{G}}_{ij} - \mathbb{E}\left(\boldsymbol{G}_{ij}\right)\right| \geq \epsilon\right] \leq \frac{\sigma^2}{\epsilon^2 l}, \tag{4.26}$$

$$\mathrm{pr}\left[\left|\bar{\boldsymbol{C}}_{i} - \mathbb{E}\left(\boldsymbol{C}_{i}\right)\right| \geq \epsilon\right] \leq \frac{\sigma^2}{\epsilon^2 l}. \tag{4.27}$$

Equations (4.26) and (4.27) equivalently are

$$\mathrm{pr}\left[\left|\bar{\boldsymbol{G}}_{ij} - \mathbb{E}\left(\boldsymbol{G}_{ij}\right)\right| \leq \epsilon\right] \geq 1 - \frac{\sigma^2}{\epsilon^2 l}, \tag{4.28}$$

$$\mathrm{pr}\left[\left|\bar{\boldsymbol{C}}_{i} - \mathbb{E}\left(\boldsymbol{C}_{i}\right)\right| \leq \epsilon\right] \geq 1 - \frac{\sigma^2}{\epsilon^2 l}. \tag{4.29}$$

Assigning

$$\epsilon \leftarrow \left\lceil \frac{\sigma}{\sqrt{l\left(1-(1-\beta)^{\frac{1}{14}}\right)}} \right\rceil \tag{4.30}$$

and assuming an independent identically distributed (iid) protocol delivers

$$\mathrm{pr}\left[\forall i,j : \left|\bar{\boldsymbol{C}}_i - \mathbb{E}\left(\boldsymbol{C}_i\right)\right| \wedge \left|\bar{\boldsymbol{G}}_{ij} - \mathbb{E}\left(\boldsymbol{G}_{ij}\right)\right| \leq \epsilon\right] \geq 1-\beta. \tag{4.31}$$

Let $\epsilon_{\max}$ be the maximum estimation error of estimated covariance matrix, which is calculated in terms of ϵ (4.30) via standard error propagation methods. In the following we give an upper bound on the estimation error of quantum mutual information in terms of $\epsilon_{\max}$. In order to do so, we introduce some helpful notation and theorems used in our proofs.

For any two Gaussian states with corresponding covariance matrices $\boldsymbol{V}_{\mathrm{A}}$ and $\boldsymbol{V}_{\mathrm{B}}$, the entropy difference is bounded by [52]

$$\left|H_{\mathrm{vN}}\left(\boldsymbol{V}_{\mathrm{A}}\right) - H_{\mathrm{vN}}\left(\boldsymbol{V}_{\mathrm{B}}\right)\right| \leq \kappa\left(\boldsymbol{V}_{\mathrm{A}}\right) K \|\boldsymbol{V}_{\mathrm{A}} - \boldsymbol{V}_{\mathrm{B}}\|_1, \tag{4.32}$$

for

$$K := 1 + \log\left[\max\left(\|\boldsymbol{V}_{\mathrm{A}}\|_\infty, \frac{1}{2}\left(\|\boldsymbol{V}_{\mathrm{A}}^{-1}\|_\infty^{-1} - 1\right)\right)\right]. \tag{4.33}$$

Also

$$\left\|\boldsymbol{A}^{-1}\right\|_\infty^{-1} \leq \|\boldsymbol{A}\|_\infty, \tag{4.34}$$

holds for any covariance matrix $\boldsymbol{A}$ [53]. Hence,

$$\frac{1}{2}\left(\left\|\boldsymbol{A}^{-1}\right\|_\infty^{-1} - 1\right) \leq \|\boldsymbol{A}\|_\infty. \tag{4.35}$$

By substituting Eq. (4.35) into Eq. (4.33), we obtain the perturbation bound

$$\left|H_{\mathrm{vN}}\left(\boldsymbol{V}_{\mathrm{A}}\right) - H_{\mathrm{vN}}\left(\boldsymbol{V}_{\mathrm{B}}\right)\right| \leq \kappa\left(\boldsymbol{V}_{\mathrm{A}}\right) \|\boldsymbol{V}_{\mathrm{A}} - \boldsymbol{V}_{\mathrm{B}}\|_1 \left(1 + \log\left(\|\boldsymbol{V}_{\mathrm{A}}\|_\infty\right)\right). \tag{4.36}$$

For any $\mathrm{Q} \in \{\mathrm{R}, \mathrm{P}, \mathrm{RP}\}$, let $\boldsymbol{V}^{\mathrm{e,Q}}$ and $\boldsymbol{V}^{\mathrm{Q}}$ be the estimated and real covariance matrices, respectively. Then

$$\left\|\boldsymbol{V}^{\mathrm{e,Q}}\right\|_\infty \leq \|\boldsymbol{U}\|_\infty \|\boldsymbol{\Sigma}\|_\infty \|\boldsymbol{V}\|_\infty \leq \sigma_{\max,\mathrm{e,Q}} \dim \boldsymbol{V}^{\mathrm{e,Q}}. \tag{4.37}$$

Also

$$\left\|\boldsymbol{V}^{\mathrm{Q}}-\boldsymbol{V}^{\mathrm{e,Q}}\right\|_1 \leq \varepsilon_{\max} \dim \boldsymbol{V}^{\mathrm{e,Q}}. \tag{4.38}$$

Furthermore, let us define

$$\Delta H_{\mathrm{vN}}(\mathrm{Q}) := H_{\mathrm{vN}}\left(\boldsymbol{V}^{\mathrm{Q}}\right) - H_{\mathrm{vN}}\left(\boldsymbol{V}^{\mathrm{e,Q}}\right), \tag{4.39}$$

and

$$\Delta I(X) = I(X;R) - I_{\mathrm{e}}(X;R). \tag{4.40}$$

Thus,

$$\Delta I(X) = \Delta H_{\mathrm{vN}}(\mathrm{X}) + \Delta H_{\mathrm{vN}}(\mathrm{R}) - \Delta H_{\mathrm{vN}}(\mathrm{RX}) \tag{4.41}$$

Due to the triangle inequality,

$$|\Delta I(X)| \leq |\Delta H_{\mathrm{vN}}(\mathrm{X})| + |\Delta H_{\mathrm{vN}}(\mathrm{R})| + |\Delta H_{\mathrm{vN}}(\mathrm{RX})|. \tag{4.42}$$

Each of the terms in the right-hand side of Eq. (4.42) is suitably achieved by using Eq. (4.36). Substituting Eqs. (4.38) and (4.39) into the resultant equation delivers Eq. (4.24).

Now we show that ϵ_{QMI} scales properly with respect to number of rounds. Using the Weyl [54] perturbation bound for singular value decomposition, we conclude

$$\kappa\left(\boldsymbol{V}^{\mathrm{e,Q}}\right), \sigma_{\mathrm{max,e,Q}} \in O(1),\ \varepsilon_{\max} \in O\left(\frac{1}{\sqrt{N}}\right). \tag{4.43}$$

Therefore, the error bound scales inversely with square root of the number of rounds. Next we prove the algorithm 4 is both sound and complete. □

Proposition 3.

- *If $X \in \mathcal{A}$, then Algorithm 4 passes with probability at least $1-\beta$ and*
- *if $X \notin \mathcal{A}$ then the algorithm fails with probability at least $1-\beta$.*

Proof. We show cases (i) and (ii) in sequence.

Case (i): We first recall that

$$X \in \mathcal{A} \implies I(X;R) \geq I_{\mathrm{T}}^{\mathcal{A}} + \delta. \tag{4.44}$$

Also

$$\mathrm{pr}\left[\left|I\left(X;R\right)-I_{\mathrm{e}}\left(X;R\right)\right|\leq\epsilon\right]\geq1-\beta. \tag{4.45}$$

Therefore,

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{A}}+\delta-\epsilon\leq I_{\mathrm{e}}\left(X;R\right)\right]\geq1-\beta. \tag{4.46}$$

As $\delta-\epsilon\geq\epsilon$, we conclude

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{A}}+\epsilon\leq I_{\mathrm{e}}\left(X;R\right)\right]\geq1-\beta. \tag{4.47}$$

Thus, Algorithm 4 accepts with probability at least $1-\beta$ if $X\in\mathcal{A}$.

Case (ii): We note that

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right)-\epsilon\leq I\left(X;R\right)\right]\geq1-\beta \tag{4.48}$$

Therefore, substituting Eq. (4.7) into Eq. (4.48) delivers

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right)<I_{\mathrm{T}}^{\mathcal{A}}+\epsilon\right]\geq1-\beta. \tag{4.49}$$

Thus, Algorithm 4 rejects with probability at least $1-\beta$ if $X\notin\mathcal{A}$. □

Proposition 4.

- *If $X\in\mathcal{F}$, then Algorithm 4 accepts with probability at least $1-\beta$ and*
- *if $X\notin\mathcal{F}$ then Algorithm 4 rejects with probability at least $1-\beta$.*

Proof. We show cases (i) and (ii) in sequence.

Case (i):

$$X\in\mathcal{F}\implies I\left(X;R\right)\leq I_{\mathrm{T}}^{\mathcal{F}}-\delta. \tag{4.50}$$

Also

$$\mathrm{pr}\left[\left|I\left(X;R\right)-I_{\mathrm{e}}\left(X;R\right)\right|\leq\epsilon\right]\geq1-\beta. \tag{4.51}$$

Therefore,

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right)\leq I\left(X;R\right)+\epsilon\right]\geq1-\beta. \tag{4.52}$$

Substituting Eq. (4.50) in Eq. (4.52) delivers

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right) \leq I_{\mathrm{T}}^{\mathcal{F}} - \delta + \epsilon\right] \geq 1 - \beta. \tag{4.53}$$

As $\delta - \epsilon \geq \epsilon$, we conclude

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right) \leq I_{\mathrm{T}}^{\mathcal{F}} - \epsilon\right] \geq 1 - \beta. \tag{4.54}$$

Thus, Algorithm 4 accepts with probability at least $1 - \beta$ if $X \in \mathcal{F}$.

Case (ii):

$$\mathrm{pr}\left[I\left(X;R\right) - \epsilon \leq I_{\mathrm{e}}\left(X;R\right)\right] \geq 1 - \beta. \tag{4.55}$$

Substituting Eq. (4.10) into Eq. (4.52) delivers

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{F}} - \epsilon \leq I_{\mathrm{e}}\left(X;R\right)\right] \geq 1 - \beta. \tag{4.56}$$

Thus, Algorithm 4 rejects with probability at least $1 - \beta$ if $X \notin \mathcal{F}$. □

Proposition 5.

- *If $X \in \mathcal{I}$, then Algorithm 4 accepts with probability at least $1 - \beta$ and*
- *$X \notin \mathcal{I}$ then Algorithm 4 rejects with probability at least $1 - \beta$.*

Proof. We show cases (i) and (ii) in sequence.

Case (i):

$$X \in \mathcal{I} \implies I_{\mathrm{T}}^{\mathcal{F}} < I\left(X;R\right) < I_{\mathrm{T}}^{\mathcal{A}}. \tag{4.57}$$

Also

$$\mathrm{pr}\left[\left|I\left(X;R\right) - I_{\mathrm{e}}\left(X;R\right)\right| \leq \epsilon\right] \geq 1 - \beta. \tag{4.58}$$

Therefore,

$$\mathrm{pr}\left[I\left(\mathrm{X};\mathrm{R}\right) - \epsilon \leq I_{\mathrm{e}}\left(\mathrm{X};\mathrm{R}\right) \leq I\left(\mathrm{X};\mathrm{R}\right) + \epsilon\right] \geq 1 - \beta. \tag{4.59}$$

Substituting Eq. (4.57) into Eq. (4.59) delivers

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{F}} - \epsilon \leq I_{\mathrm{e}}\left(X;R\right) \leq I_{\mathrm{T}}^{\mathcal{A}} + \epsilon\right] \geq 1 - \beta. \tag{4.60}$$

Thus, Algorithm 4 accepts with probability at least $1-\beta$ if $X \in \mathcal{I}$.

Case (ii):

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right)-\epsilon \leq I\left(X;R\right)\right] \geq 1-\beta, \tag{4.61}$$

and

$$\mathrm{pr}\left[I\left(X;R\right) \leq I_{\mathrm{e}}\left(X;R\right)+\epsilon\right] \geq 1-\beta. \tag{4.62}$$

Substituting Eq. (4.11) and Eq. (4.12) into Eq. (4.61) and Eq. (4.62), respectively, delivers

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right) \leq I_{\mathrm{T}}^{\mathcal{F}}-\delta+\epsilon\right] \geq 1-\beta, \tag{4.63}$$

and

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{A}} \leq I_{\mathrm{e}}\left(X;R\right)-\delta+\epsilon\right] \geq 1-\beta. \tag{4.64}$$

As $\delta-\epsilon \geq \epsilon$, we conclude

$$\mathrm{pr}\left[I_{\mathrm{e}}\left(X;R\right) \leq I_{\mathrm{T}}^{\mathcal{F}}-\epsilon\right] \geq 1-\beta, \tag{4.65}$$

and

$$\mathrm{pr}\left[I_{\mathrm{T}}^{\mathcal{A}}+\epsilon \leq I_{\mathrm{e}}\left(X;R\right)\right] \geq 1-\beta. \tag{4.66}$$

Thus, Algorithm 4 rejects with probability at least $1-\beta$ if $X \notin \mathcal{I}$. □

4.3 Summary

In this section I elaborated on the approach I used to introduce the CV ramp quantum secret-sharing protocol and its corresponding certification test. Furthermore, I introduced the certification protocol. Subsequently, I developed the discrete-variable quantum mutual information to the CV regime and utilize this approach to quantify the leakage of quantum information in the case of Gaussian states and operations. Furthermore, I introduced a certification test in the framework of quantum interactive proofs and I provided a practical test to implement it.

Chapter 5

Discussion and Conclusions

5.1 Discussion

In this section we discuss our results. We have two main results. The first result is a security analysis, which assigns subsets of players to each of the three structures, namely, authorized, intermediate, and forbidden structures. The second result is certification, which is performed by a referee. In our security analysis, we not only determine structures for subset of players, but we also quantify information leakage. For certification we introduce a referee who has limited resources such as finite local oscillator field. We now discuss these two results.

We base our approach on TRS03, which divides subsets of players into authorized and forbidden structures. TRS03 do not consider the intermediate structure because their security analysis is based on assuming infinite squeezing, but finite squeezing is responsible for information leakage, which leads us to introduce the intermediate structure based on ramp secret sharing concepts. Ramp quantum secret sharing has been considered before in two cases: discrete-variable threshold ramp quantum secret sharing [16] and entanglement sharing [55]. These analysis did not treat the continuous-variable case, however. In our case, for any amount of finite squeezing, we construct encoding and decoding procedures and thereby assign each subset to the correct structure.

Now we describe our result for certification. In our protocol, the dealer supplies the players with the encoded state, and in fact the state would be entangled with another share that goes directly to the referee. The referee identifies which subset of players are to transmit the decoded state to the referee, and the referee can combine this state with any shares that did not go through the players and then performs homodyne detection [51, 56]. The referee performs homodyne measurement, and, if the local oscillator strength is infinite,

then standard homodyne theory suffices to describe the statistics. We study the particular case of the referee performing tests based on Gaussian states and repeated measurements to allow the referee to estimate accurately the mean and covariance of the resultant state. The referee's procedure is valid even in the case of limited local-oscillator strength.

As our procedure is rather complicated and involves multiple parties, we have augmented our analysis by including pseudocode to explain step-by-step instructions on how to complete the procedure. Our pseudocode analysis makes clear exactly what is required of each party in the procedure. This pseudocode description could be a useful approach for describing future continuous-variable quantum-information protocols.

5.2 Conclusion

We have developed continuous-variable quantum mutual information with an external reference system in order to quantify the leakage of information and evaluate the security of continuous-variable quantum secret sharing protocols. Furthermore, we prove that information leakage arising in the TRS03 scheme monotonically decreases with reduced squeezing. In addition, we introduce a certification process for continuous-variable quantum secret sharing in the framework of quantum-interactive proofs and ramp quantum secret sharing schemes.

Pseudocodes have been introduced in order to represent clearly the sequence of steps taken to solve the certification problem. Subsequently, we provide a practical realization of the certification test using homodyne detection, including a sufficiency condition on the number of experimental runs the referee has to perform. We prove that the statistical error in the referee's estimated quantum mutual information scales with the inverse square root of number of rounds.

Our certification procedure assumes the extracted secret states are iid. In reality, this iid property does not hold due to the environmental noises. Furthermore, in quantum secret sharing schemes, malicious parties might generate highly complicated entanglement among

samples to fool the referee. As a future line of research, it is important to extend our certification procedure to the case of samples that are not independent and identically distributed.

Another useful avenue of research would be to analyze the effect of systematic errors in the referee's measurement procedure. As a final remark, we emphasize that our certification approach is applicable to certifying other quantum-information protocols such as summoning of quantum information in space time, quantum error correcting codes and quantum teleportation in the framework of quantum-interactive proof systems.

Appendix A

Calculation of quantum mutual information

The total density operator $\hat{\rho}_T$ of all shares and the reference system after the extraction procedure is

$$\begin{aligned}\hat{\rho}_{\mathrm{T}} =& \frac{1}{\pi}\int_{\mathbb{R}^{2n+2}} \mathrm{d}^n\boldsymbol{x}\mathrm{d}^n\boldsymbol{x}'\,\mathrm{d}y\mathrm{d}y'\,\rho\left(y,x_1,y',x_1'\right)|y\rangle\langle y'|\otimes\bigotimes_{i=1}^{n}|\xi_i\rangle\langle\xi_i'| \\ &\times\exp\left\{-\sum_{i=1}^{k-1}\left[\frac{y_i^2+y_i'^2}{2a^2}+\frac{a^2\left(z_i^2+z_i'^2\right)}{2}\right]\right\},\end{aligned} \tag{A.1}$$

where

$$\begin{aligned}\rho\left(y,x_1,y',x_1'\right) =& \exp\left[-\frac{\mathrm{e}^{-2|\zeta|}\left(x_1+y\right)^2}{4}-\frac{\mathrm{e}^{2|\zeta|}\left(y-x_1\right)^2}{4}-\frac{\mathrm{e}^{-2|\zeta|}\left(x_1'+y'\right)^2}{4}\right. \\ &\left.-\frac{\mathrm{e}^{2|\zeta|}\left(y'-x_1'\right)^2}{4}\right].\end{aligned} \tag{A.2}$$

The joint density operator

$$\rho' = \langle\omega'\eta'|\,\hat{\rho}\,|\omega\eta\rangle\,, \tag{A.3}$$

of the extracted secret and the reference system is obtained by tracing $\hat{\rho}_T$ over shares $\{2, 3, \ldots n\}$. The resultant density matrix is

$$\begin{aligned}
\rho'(\omega, \eta, \omega', \eta') =& \frac{a}{\pi}\sqrt{\frac{1}{a^2 + \frac{1}{2}\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2}} \\
& \times \exp\left\{ \left(-\frac{\mathrm{e}^{-2|\zeta|}}{4} - \frac{\mathrm{e}^{2|\zeta|}}{4} + \frac{\left(-4\mathrm{e}^{-2|\zeta|} + 4\mathrm{e}^{2|\zeta|}\right)^2}{4a^2 + \frac{\mathrm{e}^{2|\zeta|}}{2} + \frac{\mathrm{e}^{-2|\zeta|}}{2}v^2} \right)\left(\omega^2 + \omega'^2\right) \right. \\
& + \left(\frac{\mathrm{e}^{-4|\zeta|} + \mathrm{e}^{4|\zeta|} + 2}{16a^2 + 8\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2} - \frac{\mathrm{e}^{-2|\zeta|}}{4} - \frac{\mathrm{e}^{2|\zeta|}}{4} \right)\left(\eta^2 + \eta'^2\right) \\
& + \left(\frac{\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)}{2a^2 + 2\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2} - \frac{\mathrm{e}^{-2|\zeta|}}{2} - \frac{\mathrm{e}^{2|\zeta|}}{2} \right)(\omega\eta + \omega'\eta') \\
& + \left(\frac{\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)}{2a^2 + 2\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2} \right)(\eta\omega' + \eta'\omega) \\
& + \left(\frac{\mathrm{e}^{-4|\zeta|}\left(\mathrm{e}^{4|\zeta|} - 1\right)^2}{8a^2 + 4\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2} \right)\omega\omega' \\
& \left. + \left(\frac{\mathrm{e}^{-4|\zeta|} + \mathrm{e}^{4|\zeta|} + 2}{16a^2 + 8\left(\mathrm{e}^{2|\zeta|} + \mathrm{e}^{-2|\zeta|}\right)v^2} \right)\eta\eta' \right\},
\end{aligned} \tag{A.4}$$

where $v^2 = \boldsymbol{\gamma}_1 \odot \boldsymbol{\gamma}_1$ for which $\boldsymbol{\gamma}_1 = (\gamma_{11}, \gamma_{12}, \ldots, \gamma_{1k-1})$ (3.101). Also, $u^2 = \boldsymbol{u} \odot \boldsymbol{u}$ where $\{\boldsymbol{u}_i\}$ are the coefficients of the expansion $\alpha_j = \sum_{i=2}^{k-1} \boldsymbol{u}_i \beta_{ij}$ for which $j = 2, ..., k-1$. Then, by employing Eqs. (2.5),(2.6), and (2.7), we transform this density matrix into a Wigner

function representation (2.5), namely

$$
\begin{aligned}
W\left(q_1,p_1,q_2,p_2\right) = & \underbrace{\frac{2a}{\pi^2}\sqrt{\frac{\mathrm{e}^{2|\zeta|}}{2a^2\mathrm{e}^{2|\zeta|}+\mathrm{e}^{4|\zeta|}+1}}\sqrt{\frac{a^2\mathrm{e}^{2|\zeta|}}{2a^2\mathrm{e}^{2|\zeta|}+u^2\left(\mathrm{e}^{4|\zeta|}+1\right)}}}_{N} \\
& \times \exp\left\{ \underbrace{\left(-\frac{a^2\left(\mathrm{e}^{4|\zeta|}+1\right)+2\mathrm{e}^{2|\zeta|}}{2a^2\mathrm{e}^{2|\zeta|}+\mathrm{e}^{4|\zeta|}+1}\right)}_{\beta_1} q_1^2 \right. \\
& + \underbrace{\left(-\frac{a^2\left(\mathrm{e}^{4|\zeta|}+1\right)}{2a^2\mathrm{e}^{2|\zeta|}+\mathrm{e}^{4|\zeta|}+1}\right)}_{\beta_2} q_2^2 + \underbrace{\left(\frac{2a^2\left(\mathrm{e}^{4|\zeta|}-1\right)}{2a^2\mathrm{e}^{2|\zeta|}+\mathrm{e}^{4|\zeta|}+1}\right)}_{\beta_3} q_1 q_2 \\
& + \underbrace{\left(-\frac{a^2\left(\mathrm{e}^{4|\zeta|}+1\right)+2u^2\mathrm{e}^{2|\zeta|}}{2a^2\mathrm{e}^{2|\zeta|}+u^2\left(\mathrm{e}^{4|\zeta|}+1\right)}\right)}_{\gamma_1} p_1^2 \\
& + \underbrace{\left(-\frac{a^2\left(\mathrm{e}^{4|\zeta|}+1\right)}{2a^2\mathrm{e}^{2|\zeta|}+u^2\left(\mathrm{e}^{4|\zeta|}+1\right)}\right)}_{\gamma_2} p_2^2 \\
& \left. + \underbrace{\left(-\frac{2a^2\left(\mathrm{e}^{4|\zeta|}-1\right)}{2a^2\mathrm{e}^{2|\zeta|}+u^2\left(\mathrm{e}^{4|\zeta|}+1\right)}\right)}_{\gamma_3} p_1 p_2 \right\}. \qquad \text{(A.5)}
\end{aligned}
$$

By using Eq. (2.8), this Wigner function is employed to derive the generic elements of the covariance matrix $\boldsymbol{V}$ corresponding to the joint reference and extracted-secret state. The

elements of $\boldsymbol{V}$ are

$$V_{12} = V_{21} = V_{14} = V_{41} = V_{23} = V_{32} = V_{34} = V_{43} = 0, \tag{A.6a}$$

$$V_{11} = N\frac{2\pi^2}{\beta_2^{1/2}\left(\beta_1 - \frac{\beta_3^2}{4\beta_2}\right)^{3/2}\left(\gamma_1\gamma_2 - \frac{\gamma_3^2}{4}\right)^{1/2}}, \tag{A.6b}$$

$$V_{13} = N\frac{\pi^2\beta_3}{2\left(\beta_1\beta_2 - \frac{\beta_3^2}{4}\right)^{3/2}\left(\gamma_1\gamma_2 - \frac{\gamma_3^2}{4}\right)^{1/2}} = V_{31}, \tag{A.6c}$$

$$V_{22} = N\frac{2\pi^2}{\gamma_2^{1/2}\left(\gamma_1 - \frac{\gamma_3^2}{4\gamma_2}\right)^{3/2}\left(\beta_1\beta_2 - \frac{\beta_3^2}{4}\right)^{1/2}}, \tag{A.6d}$$

$$V_{24} = N\frac{\pi^2\gamma_3}{2\left(\gamma_1\gamma_2 - \frac{\gamma_3^2}{4}\right)^{3/2}\left(\beta_1\beta_2 - \frac{\beta_3^2}{4}\right)^{1/2}} = V_{42}, \tag{A.6e}$$

$$V_{33} = N\frac{2\pi^2}{\beta_1^{1/2}\left(\beta_2 - \frac{\beta_3^2}{4\beta_1}\right)^{3/2}\left(\gamma_1\gamma_2 - \frac{\gamma_3^2}{4}\right)^{1/2}}, \tag{A.6f}$$

$$V_{44} = N\frac{2\pi^2}{\gamma_1^{1/2}\left(\gamma_2 - \frac{\gamma_3^2}{4\gamma_1}\right)^{3/2}\left(\beta_1\beta_2 - \frac{\beta_3^2}{4}\right)^{1/2}}. \tag{A.6g}$$

$$\tag{A.6h}$$

The covariance matrix of the extracted secret and reference system denoted by V_{S} and V_{R} are

$$\boldsymbol{V}_{\mathrm{S}} = \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{pmatrix}, \qquad \boldsymbol{V}_{\mathrm{R}} = \begin{pmatrix} V_{33} & V_{34} \\ V_{43} & V_{44} \end{pmatrix}. \tag{A.7}$$

Also the joint covariance matrix of the extracted secret and reference system is

$$\boldsymbol{V}_{\rho^{\mathrm{RS}}} = \begin{pmatrix} V_{ij} \end{pmatrix}. \tag{A.8}$$

For convenience, let us also define

$$\boldsymbol{C} := \begin{pmatrix} V_{13} & V_{14} \\ V_{23} & V_{24} \end{pmatrix}. \tag{A.9}$$

Using Eq. (2.13), symplectic eigenvalues of $\boldsymbol{V}_{\mathrm{S}}$ and $\boldsymbol{V}_{\mathrm{R}}$ denoted by ν_{S} and ν_{R} are

$$\nu_{\mathrm{R}} = \sqrt{\det \boldsymbol{V}_{\mathrm{R}}}, \qquad \nu_{\mathrm{S}} = \sqrt{\det \boldsymbol{V}_{\mathrm{S}}}, \tag{A.10}$$

for which $\boldsymbol{V}_{\mathrm{S}}$ and $\boldsymbol{V}_{\mathrm{R}}$ are defined in Eq. (A.7). Symplectic eigenvalues of $\boldsymbol{V}_{\rho^{\mathrm{RS}}}$ denoted by $\nu_{\pm}$ is calculated using Eq. (2.15), therefore,

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det \boldsymbol{V}_{\rho^{\mathrm{RS}}}}}{2}}, \tag{A.11}$$

where $\Delta = \det \boldsymbol{V}_{\mathrm{S}} + \det \boldsymbol{V}_{\mathrm{R}} + 2 \det \boldsymbol{C}$.

Bibliography

[1] C. E. Shannon. A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(1):3–55, January 2001.

[2] Mark M Wilde. *Quantum Information Theory*, page 203. Cambridge:Cambridge University Press, 2013.

[3] John Von Neumann. *Mathematical Foundations of Quantum Mechanics*. Number 2. Princeton university press;New Jersey, 1955.

[4] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Partial quantum information. *Nature*, 436(7051):673–676, 2005.

[5] Adi Shamir. How to share a secret. volume 22, pages 612–613, New York, NY, USA, November 1979. ACM.

[6] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999.

[7] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[8] Damian Markham and B C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78:042309, Oct 2008.

[9] G. R. Blakley and Catherine Meadows. Security of ramp schemes. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pages 242–268, Berlin, 1985. Springer.

[10] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[11] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162–168, Jan 1999.

[12] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A*, 69:052307, May 2004.

[13] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys*, 74(1):145, 2002.

[14] Aleksej Dmitrievich Korshunov. Monotone boolean functions. *Russian Math. Surveys*, 58(5):929–1001, 2003.

[15] Adam D Smith. Quantum secret sharing for general access structures. *arXiv preprint quant-ph/0001087*, 2000.

[16] Tomohiro Ogawa, Akira Sasaki, Mitsugu Iwamoto, and Hirosuke Yamamoto. Quantum secret sharing schemes and reversibility of quantum operations. *Phys. Rev. A*, 72:032318, Sep 2005.

[17] Tomas Tyc, David J Rowe, and Barry C. Sanders. Efficient sharing of a continuous-variable quantum secret. *J. Phys. A: Math. Gen.*, 36(27):7625–7637, jun 2003.

[18] Tomas Tyc and Barry C. Sanders. How to share a continuous-variable quantum secret by optical interferometry. *Phys. Rev. A*, 65:042310, Apr 2002.

[19] Samuel L Braunstein. Quantum error correction for communication with linear optics. *Nature*, 394(6688):47–49, 1998.

[20] Samuel L Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.*, 80(18):4084, 1998.

[21] Hirosuke Yamamoto. Secret sharing system using (k, l, n) threshold scheme. *Electr. Eng. Jpn.*, 69(9):46–54, 1986.

[22] Sorin Iftene. Secret sharing schemes with applications in security protocols. *Sci. Ann. Cuza Univ.*, 16:63–96, 2006.

[23] Leuchs Gerd et al. *Quantum Information with Continuous Variables of Atoms and Light*. London:Imperial College Press, 2007.

[24] Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, and Ping Koy Lam. Tripartite quantum state sharing. *Phys. Rev. Lett.*, 92:177903, Apr 2004.

[25] Andrew M Lance, Thomas Symul, Warwick P Bowen, Tomás Tyc, Barry C Sanders, and Ping Koy Lam. Continuous variable (2, 3) threshold quantum secret sharing schemes. *New J. Phys*, 5:4–4, jan 2003.

[26] Theodoros Kapourniotis, Elham Kashefi, and Animesh Datta. Blindness and verification of quantum computation with one pure qubit. In *the 9th Conference on the Theory of Quantum Computation, Communication and Cryptography*, pages 176–204, Singapore:National University of Singapore, May 21–23, 2014.

[27] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiv preprint arXiv:1704.04487*, 2017.

[28] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, Tomas Tyc, T. C. Ralph, and Ping Koy Lam. Continuous-variable quantum-state sharing via quantum disentanglement. *Phys. Rev. A*, 71:033814, Mar 2005.

[29] Hideki Imai, Jörn Müller-Quade, Anderson C. A. Nascimento, Pim Tuyls, and Andreas Winter. An information theoretical model for quantum secret sharing. *Quantum Info. Comput.*, 5(1):69–80, January 2005.

[30] Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein, and Kae Nemoto. Efficient classical simulation of continuous variable quantum information processes. *Phys. Rev. Lett.*, 88:097904, Feb 2002.

[31] Seth Lloyd and Samuel L. Braunstein. *Quantum Computation Over Continuous Variables*, pages 9–17. Springer Netherlands, Dordrecht, 2003.

[32] 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.

[33] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, Jun 1932.

[34] R Simon, S Chaturvedi, and V Srinivasan. Congruences and canonical forms for a positive matrix: Application to the Schweinler–Wigner extremum principle. *J. Math. Phys.*, 40(7):3632–3642, 1999.

[35] Alessio Serafini, Fabrizio Illuminati, and Silvio De Siena. Symplectic invariants, entropic measures and correlations of Gaussian states. *J. Phys. B: At. Mol. Phys.*, 37(2):L21, 2004.

[36] A. I. Lvovsky. Squeezed light. *arXiv preprint quant-ph/1401.4118*, 2016.

[37] Chandler Davis. The norm of the Schur product operation. *Numerische Mathematik*, 4(1):343–344, Dec 1962.

[38] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum Gaussian channels. *Phys. Rev. A*, 59:1820–1828, Mar 1999.

[39] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[40] Thomas M Cover and Joy A Thomas. *Elements of Information Theory*. New Jersey; Wiley, 2012.

[41] Wentao Huang, Michael Langberg, Joerg Kliewer, and Jehoshua Bruck. Communication efficient secret sharing. *IEEE Trans. Inf. Theory*, 62(12):7195–7206, 2016.

[42] Ehud Karnin, Jonathan Greene, and Martin Hellman. On secret sharing systems. *IEEE Trans. Inf. Theory*, 29(1):35–41, 1983.

[43] Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptol*, 6(3):157–167, 1993.

[44] Kaoru Kurosawa, Koji Okada, Keiichi Sakano, Wakaha Ogata, and Shigeo Tsujii. Nonperfect secret sharing schemes and matroids. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 126–141. Springer, 1993.

[45] Hideki Imai, Jörn Müller-Quade, Anderson CA Nascimento, Pim Tuyls, and Andreas Winter. A quantum information theoretical model for quantum secret sharing schemes. *arXiv preprint quant-ph/0311136*, 2003.

[46] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900, 1997.

[47] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824, 1996.

[48] D. Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. *arXiv preprint quant-ph/0904.2557*, 2009.

[49] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[50] Takao Aoki, Go Takahashi, Tadashi Kajiya, Jun-ichi Yoshikawa, Samuel L Braunstein, Peter Van Loock, and Akira Furusawa. Quantum error correction beyond qubits. *Nat. Phys*, 5(8):541, 2009.

[51] Leandro Aolita, Christian Gogolin, Martin Kliesch, and Jens Eisert. Reliable quantum certification of photonic state preparations. *Nat. Commun*, 6:8498, 2015.

[52] Martin Idel, Sebastián Soto Gaona, and Michael M. Wolf. Perturbation bounds for williamson's symplectic normal form. *Linear Algebra Its Appl*, 525:45–58, 2017.

[53] Joseph F. Grcar. A matrix lower bound. *Linear Algebra Its Appl*, 433(1):203–220, 2010.

[54] G. W. Stewart. Perturbation theory for the singular value decomposition. Technical report, MD, USA, 1990.

[55] Ran Hee Choi, Ben Fortescue, Gilad Gour, and Barry C. Sanders. Entanglement sharing protocol via quantum error-correcting codes. *Phys. Rev. A*, 87:032319, Mar 2013.

[56] Tomas Tyc and Barry C Sanders. Operational formulation of homodyne detection. *J. Phys. A: Math.Gen.*, 37(29):7341–7357, Jul 2004.