UNIVERSITY OF CALGARY

ENTANGLEMENT SHARING PROTOCOL VIA QUANTUM ERROR CORRECTING CODE

by

RAN HEE CHOI

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF PHYSICS AND ASTRONOMY
INSTITUTE FOR QUANTUM INFORMATION SCIENCE

CALGARY, ALBERTA

September, 2012

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Entanglement sharing protocol via quantum error correcting code" submitted by RAN HEE CHOI in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Supervisor, Dr. Barry C. Sanders
Department of Physics and Astronomy

Co-Supervisor, Dr. Gilad Gour
Department of Mathematics and Statistics

Dr. David Feder
Department of Physics and Astronomy

Dr. Rei Safavi-Naini
Department of Computer Science

Dr. Renate Scheidler
Department of Mathematics and Statistics

Date

Abstract

Quantum secret sharing concerns secure and reliable distribution of classical or quantum information by a dealer to a set of "players" such that authorized subsets of players can access full information and unauthorized subsets are denied any information whatsoever. Exploiting quantum secret sharing concepts and techniques, I introduce a new protocol of "entanglement sharing" wherein half of maximally entangled bipartite states are encrypted into multipartite states in such a way that unauthorized players can only establish shared separable (not entangled) states with the dealer. Only authorized subsets of players obtain entangled states, which enable quantum information tasks such as quantum teleportation. Entanglement sharing can reduce the size of shares to individual players by half depending on the choice of encoding operation, as I show with the $[[4, 2, 2]]$ stabilizer code. In fact, the $[[4, 2, 2]]$ stabilizer code induces an optimal and threshold entanglement sharing scheme.

Furthermore, I propose a new secrecy condition of quantum ramp secret sharing based on the bipartite setting of entanglement sharing. Ramp secret sharing relieves the bandwidth requirement of a protocol by reducing the size of shares at a cost of information leakage. Although quantum ramp secret sharing has been studied, to date it has been a challenge to classify leaked information. In this thesis, I define classical and quantum information with respect to the channels through which information is transmitted, and determine whether the information leakage is classical or quantum.

Finally, I establish hybrid entanglement sharing by introducing classical shares in non-perfect entanglement sharing schemes. Hybrid entanglement sharing exploits a technique of locking entanglement with classical information, and can be devised from any quantum error correcting code.

Acknowledgements

I would like to thank my supervisor Barry Sanders for guiding and supporting me with patience, and also thank my co-supervisor Gilad Gour and co-worker Ben Fortescue for their guidance, encouragement and many valuable advices. It was my pleasure to have collaborated with them during the last two years.

I am so grateful to Vlad Gheorghiu and Yun-jiang Wang for many stimulating conversations and comments on my works, and to Lucia Wang, Nancy Jing Lu and Tracy Korsgaard for many administrative assistances. Also, I would like to thank Wolfgang Tittel and his group members for letting me attend their presentations and share ideas, and in particular my friends Khulud Almutairi and Jong Chan Lee for the time we shared. I acknowledge Alberta Innovates Technology Futures, CIFAR, iCORE, NSERC and University of Calgary for financial supports.

Special thanks go toward my parents and brother. Thanks to their sacrifices, encouragement and their praying, I can overcome the hard time and finish my program. Also, I would like to thank to my grandparents for always being on my sides. I love them so much. All the glory to my Lord God.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Entanglement sharing is a new cryptographic protocol that achieves secure entanglement-based tasks in a network where some collaborating subgroups of players are authorized to access maximal entanglement required for the tasks, and other subgroups must be denied any entanglement. Entanglement sharing is designed based on quantum secret sharing. I first motivate the study of entanglement sharing in Sec. 1.1, and review the main studies on secret sharing in Sec. 1.2.

In Sec. 1.3, I review the main results on quantum ramp secret sharing. Ramp secret sharing has been proposed to overcome the limitation that is naturally imposed on secret sharing, but in the quantum case there are some open problems [34]. In this section, I remark one of the most challenging problems of quantum ramp secret sharing. Finally, I briefly address my contribution to entanglement sharing with the outline of this thesis in Sec. 1.4.

1.1 Motivation

In the modern world, information is processed on digital computers in the form of strings of bits: 0's and 1's. This type of information is called classical information. However, another type of information—namely, quantum information—has been introduced to understand fascinating works in quantum computation and communication: factorization of large integers in Shor's quantum algorithms [1] and information-theoretically secure communication of quantum key distribution (i.e., secure against adversaries who have unlimited computing power) [2] [3].

A *qubit* (quantum bit) is a basic concept of quantum information. The state of a qubit is described as a superposition of 0 and 1 states. Consider an electron in a two-level system of spin-up and spin-down states. The spin-up and spin-down states corresponds to 0 and 1 states, respectively, because they are distinguishable. According to a classical assumption of *realism*, the electron must be in either the spin-up or spin-down state without any ambiguity. However, the electron is actually able to be in a superposition of two spin states. Therefore, the spin information of an electron is encoded in a qubit but not in a classical bit. The qubit in a superposition of distinguishable states can be collapsed into one of the states with probabilities through a measurement. Before the measurement, however, it is not pre-determined which state the qubit will be collapsed into.

One of the most interesting quantum phenomena is *entanglement.* Entanglement is observed in composite systems consisting of two or more qubits (a string of qubits). If a composite state of qubits cannot be described as the product of individual states of qubits, it is said to be entangled. Interestingly, entangled qubits are intertwined across time and space. When one of two entangled qubits is measured, the result instantaneously determines the state of the other qubit, no matter how far they are separated. This violates Bell's inequalities [4] [5] that are based on *local realism.* Local realism assumes that the measurable properties of systems are independent of observation and no information can travel faster than the speed of light.

Entanglement can be used as an essential resource in various quantum information protocols [6] [7] [8] [9]. One of the best-known entanglement-based protocols is *quantum teleportation* [6]. Quantum teleportation enables two parties who initially share entanglement to transmit an arbitrary state of a qubit by communicating two classical bits. This is analogous to a fax machine. A fax machine scans a material and sends its copy to other machines. However, the process of quantum teleportation is totally different from the fax machine. In fact, quantum states are much harder to transmit than bit values, as they obey the laws of quantum mechanics. For example, measurements analogous to the precess of scanning in a fax machine can destroy the original quantum state by collapsing it to another state. Moreover, according to the no-cloning theorem, the original state cannot be copied. In spite of these obstacles, entanglement makes it possible to transmit an arbitrary quantum state in quantum teleportation.

Quantum teleportation can be applied to the fundamental components of quantum computation. For example, it can be used to implement Clifford gates for universal quantum computation [10], to enhance the success probability of quantum gates with linear optics [11], or as a quantum scissors that truncates the redundant terms of a quantum state [12] [13]. Also, it is extensively applied to entanglement swapping [14] and quantum key agreement protocols [15], which are for remote and secure quantum communications, respectively.

In this thesis, I investigate a secure way to distribute entangled states in networks consisting of a single sender called a dealer and multiple receivers called players. *Entanglement sharing* is a new cryptographic protocol which allows a dealer to share maximally entangled states with a set of players in a way that any authorized subset of players can recover the states and perform entangled-based protocols successfully, but any unauthorized subset acquires no entanglement whatsoever.

Suppose that a company has offices, each of which is occupied by employees. The offices are equipped by quantum computers, but each quantum computer cannot perform universal gates because each one is designed to be missing essential Clifford gates (the defeat can be accomplished by choosing the proper medium for quantum computers such as linear optical quantum computing for which quantum phase gates are extremely difficult to implement). This problem can be overcome by employing a Gottesman-Chuang gate (i.e., Clifford gates using quantum teleportation [10]), which requires an extra source of suitable entangled states. In this case, I can consider this supply of entanglement as being achieved through an entanglement sharing protocol because the employees are not trusted; thus, subsets of them must collaborate to make at least one of their computers to achieve universality.

Entanglement sharing is useful not only for quantum computation using quantum teleportation, but also for *device-independent quantum key distribution* [8] [9]. In most cryptosystems, information is encrypted and transformed back into its original form by a secret key. Quantum key distribution enables a receiver to generate identical secret keys with a sender for secure communication through insecure channels. Device-independent quantum key distribution is more powerful in practical realization of quantum key distribution because its security does not depend on the physical details of quantum devices that are used to generate a secret key. It is achieved when the sender and the receiver possess a correlation that violates Bell inequalities [4] [5] [9]. In this sense, entanglement sharing protocols can be applied to distribute secret keys between a dealer and an authorized set of players with the shared entanglement, no matter what quantum devices are available to generate the keys.

Entanglement sharing protocols exploit *quantum secret sharing* (QSS) concepts and techniques in that maximally entangled states are encoded into shares by means of *quantum error correcting codes* and then these shares are distributed among the multiple players [16]. Thus, I will review the basic results of classical and quantum secret sharing in the next section.

1.2 Quantum Secret Sharing

Secret sharing is an information-theoretically secure protocol for managing secret information over multiple parties or systems. It can be extensively applied to joint checking account, electronic votes, online auctions and missile launching codes.

Consider military confidential files that are locked by a security password. A defense minister wants to share the password with three aides for reliable access to the files, but unfortunately one of the aides might be a betrayer. Thus, he wants to distribute the password in such a way that any single aide has no information on the password but any two of them can get the password together. In 1979, Shamir [17] and Blakley [18] addressed this problem generally and devised the first (k, n) threshold secret sharing scheme.

Secret sharing deals a secret to players in a way that some subsets of players can collaborate to recover the secret fully, but all other subsets gain no information on the secret even with unlimited computing power. The subsets of players that are able to reconstruct the secret are called authorized sets, and the subsets of players that are totally denied the secret are called unauthorized sets. An access structure is the collection of all authorized sets and an adversary structure is the collection of all unauthorized sets. A (k, n) threshold scheme is defined as secret sharing with an access structure

$$\mathcal{A} = \{\Gamma \subseteq P \mid |\Gamma| \geq k\} \tag{1.1}$$

and an adversary structure

$$\mathcal{U} = \{\Gamma \subseteq P \mid |\Gamma| \leq k - 1\}. \tag{1.2}$$

where $P = \{P_1, P_2, \cdots, P_n\}$ is the entire set of n players. If secret sharing is described by a certain threshold number k, its access structure will be called a *general access structure.*

Every access structure must be monotone [16] [19] [20]. An access structure $\mathcal{A}$ is called monotone if

$$(\Gamma \in \mathcal{A} \text{ and } \Gamma \subseteq \Gamma') \Rightarrow \Gamma' \in \mathcal{A} \tag{1.3}$$

That is, if a subset Γ is authorized to recover the secret, all subsets containing Γ must recover the secret as well.

Secret sharing schemes can be largely classified into three cases according to whether a secret is a bit string or an arbitrary quantum state, or whether a secret is distributed over private or public channels. A private channel is safe from eavesdropping, but a public channel is vulnerable to it. All existing secret sharing schemes fall into one of these cases [21]:

Case 1. sharing classical information with classical cryptography [17] [18]

Case 2. sharing classical information with quantum cryptography [22] [23]

Case 3. sharing quantum information with quantum cryptography [16]

In the first case, secret sharing schemes are designed to distribute bit strings over private channels between a dealer and each player [17] [18]. Consider a classical secret encoded in a bit string 010011. If a dealer simply splits it into two shares 010 and 011, each share will contain some information about the secret. However, simple cryptography enables him to hide all information from each share. For instance, the dealer can take a random bit string of the same length as one share, and compute the other share by adding the secret to the random bit string, e.g., 010011 (secret) + 111011 (random bit string) modulo 2 i.e., bitwise. Then, each share contains no information about the secret, but the secret can be recovered by adding up two shares. Shamir's threshold scheme is an example of this case.

Case 2 introduces public channels into secret sharing schemes. When each share of a secret is transmitted over a public channel, it can be easily attacked by eavesdroppers. Thus, quantum cryptography is used to defeat the eavesdroppers [22] [23]. In a

$(2, 2)$ threshold scheme, maximally entangled three-dimensional states (i.e., Greenberger-Horne-Zeilinger states) enable a dealer to determine whether an eavesdropper has been active during a process [22]. This scheme is generalized to a (n, n) threshold scheme [24], and experimentally realized [25].

In contrast to the first two cases, Case 3 considers quantum secrets encoded in arbitrary quantum states. Hereafter, Case 3 is referred as to quantum secret sharing, and the others are classical secret sharing. Classical secret sharing schemes exist for any access structure that is monotone [19]. However, this does not hold in quantum case, due to the no-cloning theorem. According to the no-cloning theorem, an arbitrary quantum state cannot be copied. This prohibits an access structure from having two disjoint sets of players [16] [20]. If the access structure has two disjoint sets, each set can recover a quantum secret independently, which implies that the secret can be copied. For the same reason, no (k, n) quantum threshold scheme exists if $n > 2k$. Thus, every (k, n) quantum threshold scheme must satisfy $n/2 < k \leq n$ [16].

It is possible to impose a more strict condition on some quantum secret sharing schemes. In general, quantum secret sharing schemes can be divided into two kinds, a pure-state quantum secret scheme and a mixed-state quantum secret scheme [16] [20]. A pure state is a quantum state that can be described as a normalized vector in some vector space, and a mixed state is a probabilistic mixture of pure states. A pure-state quantum secret sharing scheme encodes a pure state into pure states, and a mixed-state quantum secret sharing scheme encodes a pure state into mixed states. In a pure-state scheme, any authorized set is the complement of an unauthorized set and vice versa [20]. Thus, any (k, n) pure-state quantum threshold scheme satisfies $n = 2k - 1$ [16] [20].

So far, I have reviewed the basic results on secret sharing. Secret sharing was described with an access structure and an adversary structure, and threshold secret sharing was considered as a special case. Also, I showed that there are three cases of secret sharing.

In particular, quantum secret sharing was restricted on the laws of quantum mechanics, e.g., the no-cloning theorem. Quantum secret sharing schemes have been demonstrated by an experiment [26] [27]. I will deal with more results on classical and quantum secret sharing in Chapter 2.

Finally, I remark on the relationship between quantum secret sharing and quantum error correction [16]. In quantum secret sharing schemes, an authorized set of players recovers a quantum secret by correcting the shares of excluded players, and an unauthorized set cannot learn any information on the secret. These conditions of quantum secret sharing are exactly regarded as those of quantum error correcting codes. Quantum error correcting codes can correct some erroneous qubits and recover an original quantum state. Also, correctible errors never leak any information about which codeword the errors occur on [28]. This is equivalent to saying that the environment does not gain any information about the original state. In [16], it was proven that any quantum secret sharing scheme is constructed by exploiting the secrecy and recovery of quantum error correcting codes. I obtained a cental idea for constructing entanglement sharing from the relationship between quantum secret sharing and quantum error correcting codes. I will discuss this relationship more in Chapter 2, and show how to use quantum error correcting codes to share maximally entangled states between a dealer and collaborating sets of players (i.e., how to construct entanglement sharing by exploiting a quantum error correcting code) in Chapter 3.

In the next section, I review the basic results on quantum ramp secret sharing (QRSS). Secret sharing satisfies perfect secrecy in that an adversary structure is perfectly denied any access to a secret. However, it gives rise to a critical limitation on the size of shares allocated to each player. In secret sharing, the size of shares must be at least the same as the size of a secret (for the classical case, see [29] [30] [31] and for the quantum case, see [16] [20]). For example, at least 1000 qubits are required to share the arbitrary state of a single qubit with 1000 players. This limitation imposes a large potential bandwidth for communication. In order to overcome it, ramp secret sharing has been devised [32] [33] [34].

1.3 Quantum Ramp Secret Sharing

In secret sharing, every share must have the same size as a secret [20]. However, ramp secret sharing can reduce the size of shares at a cost of some information leakage. In a ramp secret sharing scheme, its adversary structure is divided into *an intermediate structure* and *a forbidden structure*. The intermediate structure is the collection of unauthorized sets that can obtain some information about a secret, and the forbidden structure is the collection of unauthorized sets that are completely denied any information. For a (k, L, n) threshold ramp scheme, an access structure $\mathcal{A}$, an intermediate structure $\mathcal{I}$ and an forbidden structure $\mathcal{F}$ are given by

1. $\mathcal{A} = \{\Gamma \subseteq P \mid |\Gamma| \geq k\}$
2. $\mathcal{I} = \{\Gamma \subseteq P \mid k - L < |\Gamma| < k\}$
3. $\mathcal{F} = \{\Gamma \subseteq P \mid |\Gamma| \leq k - L\}$

where P is a set of n players [32] [33] [34].

In a (k, L, n) ramp scheme, the size of shares can be reduced by $1/L$ [34] [35]. Suppose that a dealer wants to share a password with seven aides in a way that any five aides can recover the password perfectly in collaboration. However, there are three unknown betrayers among the aides. In this situation, how can he share the password? At first, he might use a $(5, 7)$ threshold secret sharing scheme. Then, every group of fewer than five aides is completely denied any information about the password, but each share must be at least the same as the size of the password. However, if he uses a $(5, 3, 7)$ threshold ramp scheme, each share can be reduced to one-third the size of the password. Instead, any four aides might learn some information about the password. In Chapter 2, I show how to construct a (k, L, n) classical ramp secret sharing scheme, and discuss the size of shares in detail for both secret sharing and ramp secret sharing.

To date, several studies on classical ramp schemes have been conducted [32] [33], but very little work has been done in the quantum domain [34]. In 2005, a (k, L, n) quantum ramp scheme was first introduced using a quantum polynomial code by Ogawa, Sasaki, Iwamoto, and Yamamoto [34]. As in quantum secret sharing, the (k, L, n) quantum ramp scheme must satisfy $n \leq 2k - L$ due to the no-cloning theorem [34]. Equality holds for any (k, L, n) pure-state quantum ramp scheme.

One of the most important issues for quantum ramp secret sharing is determining a security condition. The security of a scheme depends on the importance of the information leaked to an intermediate set, but it is hard to characterize the leaked information. In this thesis, I focus on the problem of determining whether the leaked information is classical or quantum. If any quantum information about a secret is not leaked to an intermediate structure, the corresponding quantum ramp scheme can be said to be secure against any quantum leakage. I will discuss the relevant results that appeared in [38] [39] and propose a new way to solve this problem based on entanglement sharing.

1.4 Outlines of this Thesis

This thesis is organized as follows. In Chapter 2, the basic backgrounds about quantum information theory and useful mathematical tools that are used throughout the rest of this thesis are explained. Also, this chapter includes some interesting results on classical, quantum secret sharing and quantum error correcting codes. In particular, I discuss the relationship between quantum secret sharing and quantum error correction.

The main aim of Chapter 3 is introducing entanglement sharing and its properties. Entanglement sharing is a new cryptographic protocol allowing a dealer to share entanglement with multiple players in such a way that some collaborating groups of players are authorized to obtain the initial entanglement, but the other groups are totally denied any entanglement with the dealer. I guess entanglement sharing based on the existing stabilizer codes and assess its secrecy. The assess is primarily analytical with lengthy algebraic computation by hand or sometimes by means of Mathematica$^{\text{TM}}$. Along the way, I show two examples of entanglement sharing. Next, I prove the amount of initial entanglement cannot be larger than double the size of shares, using the work of [37], and I present the case of optimal entanglement sharing that has the minimum size of shares with respect to the initial amount of entanglement.

Chapter 4 concerns characterization of leaked information in quantum ramp secret sharing. As leaked information can damage the secrecy of schemes, it is important to characterize the leaked information and define secrecy conditions for quantum ramp secret sharing schemes. In this chapter, I review previous works concerning the leaked information. Then, I propose a new approach to characterize information leakage. First, I define classical and quantum information in the context of channels through which information is transmitted. Then, I show that entanglement sharing can be applied to characterize the leaked information in quantum ramp secret sharing. Finally, I propose a new secrecy condition of quantum ramp secret sharing. This approach has an advantage of being applicable to any quantum ramp secret sharing scheme.

In Chapter 5, I hybridize non-perfect entanglement sharing with a support of classical secret sharing. Hybrid entanglement sharing can effectively lock leaked entanglement of non-perfect entanglement sharing using a classical key. In fact, it is difficult to construct entanglement sharing and verify its secrecy. However, hybrid entanglement sharing makes its construction and verification easier alternatively; it can be constructed from any quantum error correcting code and its secrecy depends on whether or not unauthorized sets obtain any information about the classical key.

The main results of this thesis are summarized in Chapter 6. Also, further work on this topic is briefly discussed. Finally, the investigation of Shor's code is completed in Appendix A, and a property of the relative entropy of entanglement is derived in Appendix B, which is importantly used to prove the relationship between the size of shares and entanglement in Chapter 3.

Chapter 2

Preliminaries

The aim of this chapter is to provide the necessary backgrounds to understand this thesis. I explain basic elements of quantum information theory in Sec. 2.1, and von Neumann entropies that are quantum versions of Shannon entropies in Sec. 2.2. In Sec. 2.3, I provide entanglement measures that will be importantly used to define entanglement sharing. In particular, I deal with one of the entanglement measures, the relative entropy of entanglement, and its basic properties. Also, quantum teleportation is explained in Sec. 2.4.

Before explaining quantum cryptographic protocols, it is helpful to understand their classical counterparts. In Sec. 2.5, I construct Shor's threshold scheme and explain the size of shares in classical secret sharing. Then, I present classical ramp secret sharing in Sec. 2.6. In Sec. 2.10, the size of shares for quantum secret sharing is compared with that for quantum ramp secret sharing. Next, the main results on quantum error correction is reviewed in Sec. 2.8 and an important class of quantum error correcting codes, so-called stabilizer codes, is explained in Sec. 2.9. A more detailed discussion on stabilizer codes can be found in [28]. Finally, I discuss the relationship between quantum secret sharing schemes and quantum error correcting code in Sec. 2.10.

2.1 Basics of Quantum Information Theory

This section provides an overview of quantum information theory. A bit is the basic unit of classical information, which is an element of $\mathbb{F}_2$. Similarly, quantum information contained in two-level systems is described as a string of qubits (quantum bits). In this section, I express the state of a qubit as a state vectore in Subsec. 2.1.1 and as a density matrix in Subsec. 2.1.3. The density matrix is useful for describing a probabilistic distribution of quantum states. In Subsec. 2.1.2, I explain the manipulation of a quantum state in terms of operators. Finally, I discuss a composite states of two or more qubits in Subsec. 2.1.4. See [40] for a more detailed account of the following subjects.

2.1.1 State Vector Representation

The state of a qubit can be completely described as a unit vector in the two-dimensional complex vector space $\mathbb{C}^2$. The unit vector is called a *state vector*.

A *Dirac* notation is commonly used to express the state vector. In the Dirac notation, a state vector is denoted by $|\psi\rangle$ and its dual vector by $|\psi\rangle^\dagger = \langle\psi|$. The inner product between two vectors $|\psi\rangle$ and $|\phi\rangle$ is then written as $\langle\phi|\psi\rangle$.

Consider two orthonormal basis vectors, $|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix}$. The state of a qubit is represented by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \quad \text{where} \quad \alpha, \beta \in \mathbb{C} \tag{2.1}$$

which satisfies the normalization condition given by

$$\langle\psi|\psi\rangle = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = |\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

The complex vector $|\psi\rangle$ is said to be a superposition of the basis vectors.

The single qubit space spanned by $\{|0\rangle, |1\rangle\}$ is called a two-dimensional *Hilbert space* $\mathscr{H}$. The two-dimensional Hilbert space geometrically corresponds to the projective space with respect to the two-dimensional compex vector space $\mathbb{C}^2$ (i.e., the set of lines through the origin of $\mathbb{C}^2$).

Extending to higher dimensions, a more general expression of the qubit can be referred to as a *qudit* (i.e., a quantum d-ary digit), which corresponds to a d-dimensional Hilbert space. However, in this thesis, I focus on qubit cases because they can be generalized to qudit cases.

2.1.2 Operators

The evolution of a quantum state in a closed system is described by a unitary transformation. Note that a matrix U is unitary if $U^\dagger U = I$ where $U^\dagger$ is the Hermitian conjugate of U and I is the identity matrix. A unitary transformation conserves the inner product of a state. When an initial state $|\psi\rangle$ is evolved to $U|\psi\rangle$, its inner product after evolution is $\langle\psi|\psi\rangle = \langle\psi|U^\dagger U|\psi\rangle$.

On the other hand, the evolution of a state caused by measurements is not unitary because the system is not closed any more by interacting with measurement apparatuses. Note that a projection operator or a *projector* P is Hermitian (i.e., $P^\dagger = P$) and satisfies $P^2 = P$. A projective measurement is defined as a set of projectors $\{P_i\}$ that represent a decomposition of the identity,

$$I = \sum_i P_i. \tag{2.3}$$

After the projective measurement, the outcome i is obtained with the probability $p_i = \langle\phi|P_i|\phi\rangle$ and the state of a system $|\phi\rangle$ is collapsed to $P_i|\phi\rangle/\sqrt{p_i}$. The projective measurement is often described as an *observable* $A = \sum_i \lambda_i P_i$ where λ_i is an eigenvalue corresponding to the eigenvector $|\psi_i\rangle$ for $P_i = |\psi_i\rangle\langle\psi_i|$.

Now, consider a set of four important operations on a single qubit—*Pauli operators* and the identity matrix I. The Pauli operators are defined by the following complex matrices:

$$\hat{\sigma}_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X \qquad \hat{\sigma}_y \equiv \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} = Y = iXZ \qquad \hat{\sigma}_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z \tag{2.4}$$

The Pauli operators are Hermitian and unitary, and satisfy the following commutation relation.

$$[\hat{\sigma}_j, \hat{\sigma}_k] = 2i\epsilon_{jkl}\hat{\sigma}_l \tag{2.5}$$

where ϵ_{jkl} is the permutation symbol. Note that two operators A and B are said to commute if $[A, B] = AB - BA = 0$ and anti-commute if $\{A, B\} = AB + BA = 0$.

The Pauli operators are sometimes used to describe errors on a qubit. The errors can occur due to the imperfect manipulation or interaction with an environment, which make the state of a qubit evolve to a different state. The Pauli operators X and Z are called a bit flip error and a phase flip error, respectively, and the Pauli operator Y performs both bit flip and phase flip errors.

2.1.3 Density Matrix

Until now, the state of a qubit was described by a definite state vector in a Hilbert space. Such a state is referred to as a *pure* state. The state of a qubit is sometimes given by a statistical ensemble of several state vectors:

$$\{(|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \cdots, (|\psi_k\rangle, p_k)\} \tag{2.6}$$

where $\{p_i\}$ is a probability distribution with $p_i \geq 0$ for every i and $\sum_i p_i = 1$. Such an ensemble of the states is called a *mixed state*, i.e., a mixture of pure states.

A density matrix provides a convenient and compact way to describe the mixed state, which is given by

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i| \tag{2.7}$$

The density matrix is a Hermitian, positive operator of trace one; that is, $\mathrm{tr}(\rho) = 1$ and its expectation value with respect to a state $|\phi\rangle$ (i.e., $\langle\phi|\rho|\phi\rangle$) is a non-negative real value. Obviously, a density matrix corresponding to a pure state $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$. If an operator U is applied to a density matrix ρ, ρ will be evolve to $\rho' = U\rho U^\dagger$.

The Pauli operators and the identity matrix form basis for the 2×2 Hermitian matrices. Therefore, any density matrix of a single qubit can be expressed as

$$\rho = \frac{I + \boldsymbol{r} \cdot \boldsymbol{\sigma}}{2} \tag{2.8}$$

where $\boldsymbol{r}$ is a three-component vector such that $|\boldsymbol{r}| \leq 1$ and $\boldsymbol{\sigma}$ is a vector of three Pauli matrices [40]. The density matrix ρ is a pure state if $|\boldsymbol{r}| = 1$.

2.1.4 A Composite System

This section considers a composite system of two or more qubits. Given n qubits, the Hilbert space of a composite system is given by the tensor product (in some contexts, it is also referred to as *outer product*)

$$\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_n \tag{2.9}$$

where $\mathscr{H}_i$ is a Hilbert space of the i-th qubit for $1 \leq i \leq n$. If each qubit is independently prepared in the state $|\psi_i\rangle$, the composite state is

$$|\psi_1\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1\psi_2 \cdots \psi_n\rangle. \tag{2.10}$$

This is analogous to a bit string (e.g., 01011110...). A composite state represented by the tensor product of the individual states of qubits is called a *separable state* [41]. However, not all the composite states can be written as such a separable form.

In general, a composite state in $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_n$ is given by

$$|\Psi\rangle = \sum_{j_1, j_2, \cdots, j_n} c_{j_1, j_2, \cdots, j_n} |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle \tag{2.11}$$

where $\{|j_i\rangle\}$ is basis vectors in $\mathscr{H}_i$ and $c_{j_1, j_2, \cdots, j_n}$ are coefficients. If qubits interact with each other, Eq. 2.11 cannot be reduced to the separable form

$$|\Psi\rangle \neq \sum_{j_1} c_{j_1} |j_1\rangle \otimes \sum_{j_2} c_{j_2} |j_2\rangle \otimes \cdots \otimes \sum_{j_n} c_{j_n} |j_n\rangle \tag{2.12}$$

In this case, the qubits are said to be entangled and their composite state is called *an entangled state*. Particularly, when all coefficients $c_{j_1,j_2,\cdots,j_n}$ are equal, the state is called a maximally entangled state. There is a useful set of four maximally entangled states that are called *Bell states* or *Einstein-Podolsky-Rosen pairs* [42].

$$|\beta_0\rangle = |\phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.13}$$

$$|\beta_1\rangle = |\phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2.14}$$

$$|\beta_2\rangle = |\psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{2.15}$$

$$|\beta_3\rangle = |\psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.16}$$

Note that the tensor product between the states can be dropped or superscribed (i.e., $|0\rangle \otimes |0\rangle = |00\rangle = |0\rangle^{\otimes 2}$).

The mixed state of a composite system is an ensemble of composite states with a probability distribution. Consider a bipartite system $\mathscr{H}_A \otimes \mathscr{H}_B$ of qubit A and B. The mixed state ρ^{AB} of the system is called a product state if it is simply written as a tensor product of individual states,

$$\rho^{AB} = \rho^A \otimes \rho^B \tag{2.17}$$

where ρ^A and ρ^B are the density matrices of qubit A and B, respectively. In this case, the state of qubit A is totally independent of the one of qubit B.

The mixed state is called a separable state if it can be written as a convex sum of product states,

$$\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B \tag{2.18}$$

where all $p_i \geq 0$ satifying $\sum_i p_i = 1$, and ρ_i^A and ρ_i^B are the density matrices of qubit A and B for all i [41]. The separable state can be prepared by LOCC (Local Operations and Classical Communication, Fig. 2.1) [41].

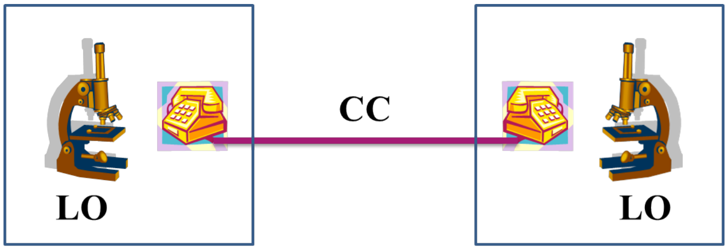

Figure 2.1: Paradigm of Local Operations and Classical Communication. Two separate parties might perform any operation which is localized to their own system (LO) and communicate information classically (CC). The parties are not allowed to exchange any quantum particles coherently. This is referred to as LOCC. [43]

When even the mixed state cannot be written as the convex sum of product states (i.e., is not separable), it is an entangled state. The entangled state (i.e., entanglement) is used as a resource for quantum computing and communication tasks such as quantum teleportation [6], superdense coding [7], and Ekert quantum key distribution [3].

The problem of determining whether a given state is entangled or separable is very difficult (i.e., it is known to be NP-hard) [44]. One of useful conditions for separability of density matrices is the positive partial transpose (PPT) criterion [45] [46]. The PPT criterion states that if the density matrix of a bipartite system $\mathscr{H}_A \otimes \mathscr{H}_B$ is separable, all eigenvalues of its partial transpose are not negative. It turns out that if a bipartite density matrix violates the PPT criterion (i.e., its partial transpose has any negative eigenvalue), it is entangled. The PPT criterion is just a necessary, but not a sufficient condition for separability in a high-dimensional bipartite system (i.e., $\dim(\mathscr{H}_A \otimes \mathscr{H}_B) > 6$), but for smaller systems it provides both a necessary and sufficient condition.

The density matrix is useful not only for describing a mixed state but also for describing the individual states of qubits in a composite system. For example, when the state of a bipartite system is given by ρ^{AB} on the Hilbert space $\mathscr{H}^A \otimes \mathscr{H}^B$, the state of a qubit on $\mathscr{H}^A$ can be represented by a reduced density matrix

$$\rho^A = \mathrm{tr}_B(\rho^{AB}) \tag{2.19}$$

where tr_B is the partial trace over another qubit B, defined as

$$\mathrm{tr}_B(|A_1\rangle\langle A_2| \otimes |B_1\rangle\langle B_2|) = |A_1\rangle\langle A_2|\langle B_1|B_2\rangle. \tag{2.20}$$

Finally, I explain a convenient mathematical technique—*purification*. Purification starts from the fact that for any mixed state ρ^A on a finite Hilbert space $\mathscr{H}_A$, there exists a pure state $|RA\rangle$ for a composite system $\mathscr{H}_R \otimes \mathscr{H}_A$ such that $\rho^A = \mathrm{tr}_R(|RA\rangle\langle RA|)$ [40]. R is called a reference system for A.

Suppose that the state ρ^A has an orthonormal decomposition $\rho^A = \sum_i p_i|i_A\rangle\langle i_A|$ where the vectors $\{|i_A\rangle\}$ form an orthonormal basis of $\mathscr{H}_A$. To purify ρ^A, R is chosen as a system that has the same Hilbert space as system A, with any orthonormal basis $\{|i_R\rangle\}$. Then, for a composite system of R and A the following pure state is introduced:

$$|RA\rangle = \sum_i \sqrt{p_i}|i_R\rangle|i_A\rangle \tag{2.21}$$

This is a purification of ρ^A. Indeed, the reduced density matrix of system A is

$$\begin{aligned}\mathrm{tr}_R(|RA\rangle\langle RA|) &= \sum_i \sum_{i'} \sqrt{p_i}\sqrt{p_{i'}}\langle i_R|i'_R\rangle|i_A\rangle\langle i'_A| \\ &= \sum_i \sum_{i'} \sqrt{p_i}\sqrt{p_{i'}}\delta_{ii'}|i_A\rangle\langle i'_A| \\ &= \sum_i p_i|i_A\rangle\langle i_A| = \rho^A\end{aligned} \tag{2.22}$$

2.2 Von Neumann Entropy and Mutual Information

Until now, I have seen how to represent and manipulate the states of qubits using state vectors, operators and density matrices. In this section, I quantify how much quantum information (i.e., how many qubits) is contained in quantum systems in terms of entropy.

First, consider a random variable chosen from a probability distribution of classical values. The random variable has an entropy (i.e., randomness or uncertainty) before measuring its value. *Shannon entropy* is a measure of the entropy in the unit of bit [47]. It can be interpreted as the number of bits needed to represent a variable. Shannon states that the entropy of a random variable is quantified as a function of its probability distribution. Given a probability distribution $\{p_x\} = \{p_1, p_2, \cdots, p_n\}$ of a random variable X, its Shannon entropy is

$$H(X) = H(p_1, p_2, \cdots, p_n) = -\sum_x p_x \log_2 p_x \tag{2.23}$$

If X has only one definite value, the entropy is $H(X) = 0$, but if it has perfectly random over all n values, $H(x)$ has the maximum value.

A characteristic property of the Shannon entropy is additivity. The term additivity means that the total randomness of independent variables is calculated by adding all entropies of the variables together. Thus, given two independent random variables X and Y with probability distributions $\{p_x\}$ and $\{p_y\}$, their joint entropy is

$$H(X, Y) = H(X) + H(Y) \tag{2.24}$$

where $H(X, Y) = -\sum_{x,y} p_{xy} \log_2 p_{xy}$ and $p_{xy} = p_x p_y$.

However, if the variables are not independent, their entropies will be somehow related to each other. The conditional entropy $H(X|Y)$ represents the entropy of X conditional on knowing Y. It is defined by

$$H(X|Y) = H(X, Y) - H(Y). \tag{2.25}$$

If $H(X|Y) = 0$, it means that one can determine X from Y. This entropy is very useful for describing recoverability and secrecy conditions of classical secret sharing [29].

The quantum analogue of the Shannon entropy is called *von Neumann entropy* [48]. This is described as the function of a density matrix because the density matrix itself captures the probabilistic feature of a quantum system. For a density matrix ρ, its von Neumann entropy is

$$S(\rho) = -\mathrm{tr}(\rho \log_2 \rho). \tag{2.26}$$

Note that if ρ is a pure state, $S(\rho) = 0$, and if a composite system of A and B is in a pure state, then $S(A) = S(B)$ [40].

The von Neumann entropy is also additive for independent systems. Given two independent systems A and B, the von Neumann entropy is

$$S(\rho^A \otimes \rho^B) = S(\rho^A) + S(\rho^B) \tag{2.27}$$

where ρ^A and ρ^B are the density matrices of two systems, respectively.

For a set of density matrices ρ_i with respective probabilities p_i satisfying $\sum_i p_i = 1$, the Shannon entropy H and the von Neumann entropy S have the following relationship:

$$S(\sum_i p_i \rho_i) \leq \sum_i p_i S(\rho_i) + H(p_i) \tag{2.28}$$

with the equality if and only if the density matrices ρ_i have support on mutually orthogonal subspace of the Hilbert space (i.e., the density matrices ρ_i are perfectly distinguishable from each other) [40].

By analogy with the Shannon entropy, the quantum joint entropy is

$$S(A, B) = -\mathrm{tr}(\rho^{AB} \log_2 \rho^{AB}) \tag{2.29}$$

where ρ^{AB} is the density matrix of a composite system of A and B, and the quantum conditional entropy is

$$S(A|B) = S(A, B) - S(B). \tag{2.30}$$

It is important to note that some properties of the Shannon entropy do not apply to its quantum counterpart in spite of the similarities in the definitions [40]. For example, the classical conditional entropy is always non-negative, whereas the quantum conditional entropy can be negative for an entangled state. Consequently, some analysis of classical secret sharing does not hold in quantum secret sharing because they are often built on the non-negativity of the classical conditional entropy [38]. Therefore, the quantum mutual information is used to study quantum secret sharing, instead of the quantum conditional entropy [38]. The quantum mutual information $S(A : B)$ is defined by

$$S(A : B) = S(A) + S(B) - S(A, B) \geq 0. \tag{2.31}$$

It can be interpreted as the amount of information on A that is revealed by B. If ρ^{AB} is a product state, $S(A : B) = 0$.

2.3 Entanglement Measures

As mentioned in Subsec. 2.1.4, entanglement is an important resource in quantum information tasks. Thus, it is necessary to quantify the amount of entanglement required to carry out the tasks. This can be achieved by *entanglement measures*: entanglement cost, distillable entanglement, relative entropy of entanglement and *et al.* (various entanglement measures and their properties are well explained in [43]). Entanglement measures E have different definitions and characterizations, but they commonly satisfy the following properties [43];

1. For a maximally entangled state of two qudits,

   $$|\psi\rangle = \frac{1}{\sqrt{d}}(|00\rangle + |11\rangle + \cdots + |d-1, d-1\rangle)$$

   any bipartite entanglement measure is $E(|\psi\rangle\langle\psi|) = \log_2 d$.

2. $E(\rho) = 0$ if the state ρ is separable.

3. E does not increase under deterministic LOCC transformations.

4. For the pure state $|\psi\rangle$ of a composite system, any entanglement measure reduces to the entropy of its subsystem;

$$E(|\psi\rangle\langle\psi|) = S(\mathrm{tr}_B|\psi\rangle\langle\psi|) \tag{2.32}$$

where tr_B denotes partial trace over subsystem B.

Note that a unit of entanglement is an *ebit*. For example, a Bell state is one ebit.

Next, I introduce one of entanglement measures, a *relative entropy of entanglement*, which quantifies entanglement in terms of the entropy. The relative entropy of entanglement has an interesting property of *non-lockability* [37] [43].

2.3.1 Relative Entropy of Entanglement

In the study of entanglement, there is a question about how much entanglement of a composite system can be changed when one qubit is discarded. The answer clearly depends on what entanglement measure is used. An entanglement measure is said to be lockable when the measured entanglement is reduced by an arbitrarily large amount after one qubit is removed [43]. Most fundamental measures such as entanglement cost and entanglement of formation have lockability, but the relative entropy of entanglement is not lockable [37].

The relative entropy of entanglement is described as the *quantum relative entropy.* Quantum relative entropy $S(\rho||\sigma)$ represents how distinguishable a density matrix ρ is from another density matrix σ, and is defined as

$$S(\rho||\sigma) = \mathrm{tr}(\rho\log_2\rho) - \mathrm{tr}(\rho\log_2\sigma). \tag{2.33}$$

Note that the quantum relative entropy is non-negative, i.e., $S(\rho||\sigma) \geq 0$ with equality if and only if $\rho = \sigma$.

Suppose that a bipartite system $H_A \otimes H_B$ is in the state ρ^{AB}, and let X be the set of all possible separable states in this system. Then, the relative entropy of entanglement E_R measures the smallest quantum relative entropy from ρ^{AB} to a separable state taken from the set X, which is defined as

$$E_R(\rho^{AB}) = \inf_{\sigma \in X} S(\rho^{AB} || \sigma). \tag{2.34}$$

In [37], it was proven that the relative entropy of entanglement is not lockable because it drops at most by two when one qubit is traced out. For any composite state ρ, its relative entropy of entanglement satisfies

$$E_R(\rho) - E_R(\mathrm{tr}_A(\rho)) \leq 2 \tag{2.35}$$

where A denotes a one qubit system.

2.4 Quantum Teleportation

Quantum teleportation is one of the most important entanglement-based protocols [6]. Suppose that there are two parties, Alice and Bob, who want to communicate the state of a qubit to each other. Alice and Bob initially share a pair of maximally entangled qubits

$$|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.36}$$

and Alice prepares a qubit in the arbitrary state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ which she wants to teleport to Bob. Now, their joint state is $|\psi\rangle|\beta_0\rangle$. This state can be rewritten as

$$|\psi\rangle|\beta_0\rangle = \frac{1}{2}|\beta_0\rangle|\psi\rangle + \frac{1}{2}|\beta_1\rangle(X|\psi\rangle) + \frac{1}{2}|\beta_2\rangle(Z|\psi\rangle) + \frac{1}{2}|\beta_3\rangle(XZ|\psi\rangle). \tag{2.37}$$

Then, Alice performs a joint measurement on her two qubits in the Bell basis. After measurement, the joint state is collapsed into one of the four states,

$$|\beta_0\rangle|\psi\rangle \qquad |\beta_1\rangle(X|\psi\rangle) \qquad |\beta_2\rangle(Z|\psi\rangle) \qquad |\beta_3\rangle(XZ|\psi\rangle) \tag{2.38}$$

with the equal probability $\frac{1}{4}$, and Alice obtains the measurement outcome of two classical bits. If the state is collapsed to $|\beta_0\rangle|\psi\rangle$, the outcome is 00, if it is $|\beta_1\rangle(X|\psi\rangle)$, the outcome is 01, and so on. Finally, Alice communicates the outcome to Bob over a classical channel and Bob performs a proper local operation on his qubit to transform his state into $|\psi\rangle$. For example, if he receives 01, he would learn that his state is $X|\psi\rangle$. Therefore, he can recover $|\psi\rangle$ by applying the X operator to his state.

Theoretically, entanglement enables one party to transmit quantum information to another party, no matter how far they are separated. Quantum teleportation can be extensively applied to implement primitive gates for universal quantum computation. For example, a CNOT gate (i.e., a controlled-NOT quantum gate) is hard to implement optically because it would need a strong optical non-linearity [40], but it can be replaced by a Gottesman-Chuang gate [10] which exploits quantum teleportation.

2.5 Classical Secret Sharing

Secret sharing was first introduced by Shamir [17] and Blakley [18]. They proposed a (k, n) classical threshold scheme wherein a classical secret is encoded in a set of n shares in a way that any k or more shares are able to recover the secret completely but less than k shares contain no information about the secret. Classical secret sharing schemes exist for all positive values of k and n with $k \leq n$, provided access structures are monotone [19].

Suppose that a dealer shares a classical secret (e.g., a password) with seven players, one of whom is dishonest (i.e., the dishonest player might leak the secret to an enemy). Hence, the dealer wants to encode the secret in such a way that at least two of the players must collaborate to recover the secret and any player alone is completely denied the secret.

Let the secret be encoded in the slope of a line. The dealer picks seven random points on the line as shares $\{x_1, x_2, \ldots, x_7\}$ and equally distributes the shares among the players. Then, any two players can know the slope together, but any single player cannot have any knowledge about it from a single point on the line. This is an example of a $(2, 7)$ Shamir's threshold scheme.

Shamir generalized this observation using polynomial interpolation [17]. A secret S is encoded in a polynomial of degree $k-1$ such that

$$f(x) = S + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \tag{2.39}$$

where the coefficients $a_1 \ldots a_{k-1}$ are randomly picked in a finite field $\mathbb{F}_q = Z/qZ$ for a prime number $q > S,\ n$. Given k points $(x_i,\ y_i)$ for $i = 1 \ldots k$, the polynomial function can be uniquely determined as follows

$$f(x) = \sum_{j=1}^{k} y_j \prod_{i=1, i \neq j}^{k} \frac{x_i - x}{x_i - x_j} \tag{2.40}$$

where the x_i's are all distinct for $\mathbb{F}_q$. However, with any $k-1$ points, there still remains a degree of freedom of $f(x)$. It means that all possible values for the coefficient are equally likely and thus secrecy holds as desired.

All (k, n) threshold schemes are secure and reliable [17] [18]. Even though $n-k$ out of n shares are destroyed, the original secret can be recovered perfectly with the remaining shares. Furthermore, the secret can be securely protected from adversaries, even when $k-1$ of the remaining k shares are exposed.

Finally, I give the information theoretical description of classical secret sharing schemes as was done in [29]. Suppose that a secret S is encoded in shares $V = \{V_1, V_2, \cdots, V_n\}$. For a classical secret sharing scheme with an access structure $\mathcal{A}$, the following requirement must be satisfied.

1. For $\forall\, \Gamma \in \mathcal{A}, \quad H(S \mid \Gamma) = 0.$

2. For $\forall\, \Gamma \notin \mathcal{A}, \quad H(S \mid \Gamma) = H(S)$.

Note that each share must be at least as long as the secret,

$$|V_i| \geq |S| \tag{2.41}$$

for any $1 \leq i \leq n$ [29] [30] [31]. The size of the shares is one of the most important issues in secret sharing. A small size of shares is desirable to reduce the communication complexity [49]. In the next section, I describe classical ramp secret sharing which achieves a small size of shares at a cost of perfect secrecy.

2.6 Classical Ramp Secret Sharing

Ramp secret sharing reduces the size of shares by leaking some information to unauthorized sets [32] [33] [34]. A set of players which obtains partial information about the secret is called an intermediate set, and the collection of all intermediate sets is called an intermediate structure.

A (k, L, n) ramp scheme was first devised as an extension of the Shamir's threshold scheme [32]. Let a secret $S = (S_0, S_1, \cdots, S_{L-1})$ where $S_i \in \mathbb{F}_q$ for some prime number q. A dealer picks $k - L$ coefficients in $\mathbb{F}_q$ randomly, and creates the $k - 1$ degree polynomial function,

$$f(x) = S_0 + S_1 x + \cdots + S_{L-1} x^{L-1} + a_L x^L + \cdots + a_{k-1} x^{k-1}. \tag{2.42}$$

Then, n shares are given by $f(i)$ modulo q for $1 \leq i \leq n$. The function can be fully determined with any k shares, but with any $k - L$ or fewer shares, L elements of the secret are totally random over $\mathbb{F}_q$. However, a set of shares Γ can narrow down the range of the secret if $k - L < |\Gamma| < k$. This means that some information about the secret is leaked to the set.

As in classical secret sharing, a classical ramp scheme can be described by the conditional entropy [31]. Let $V = \{V_1, V_2, \cdots, V_n\}$ be a set of shares. Given access, intermediate and forbidden structures $\mathcal{A}$, $\mathcal{I}$ and $\mathcal{F}$, repectively, a classical ramp secret sharing scheme fulfills the following requirements.

1. For $\forall\, \Gamma \in \mathcal{A}, \quad H(S|\, \Gamma) = 0$.
2. For $\forall\, \Gamma \in \mathcal{I}, \quad 0 < H(S|\, \Gamma) < H(S)$.
3. For $\forall\, \Gamma \in \mathcal{F}, \quad H(S|\, \Gamma) = H(S)$.

In this description, the amount of leaked information for an intermediate set Γ can be measured by the conditional entropy $H(S|\ \Gamma)$ and the leaked information must be classical. Similarly, in quantum ramp secret sharing, leaked information can be quantified by the quantum mutual information. However, it is hard to determine whether it is quantum or classical or how much quantum information is leaked. The quantum case will be discussed in Chapter 4.

Finally, I explain the size of shares in (k, L, n) ramp secret sharing schemes. For any (k, L, n) ramp scheme, the following relationship holds.

$$\log |V_i| \geq \frac{1}{L} \log |S| \tag{2.43}$$

for any $1 \leq i \leq n$ [35]. In the ramp scheme using a polynomial fucntion, the size of each share is indeed $|V_i| = q$, whereas the size of the secret is $|S| = q^L$.

2.7 The Size of Shares in QSS and QRSS Schemes

As in classical secret sharing, quantum secret sharing is also limited by the large size of shares. Let a quantum secret be an arbitrary quantum state on $\mathscr{H}_S$. In general, a quantum secret sharing scheme encodes the quantum secret in a composite system of n shares corresponding to $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_n$ where $\mathscr{H}_i$ is the Hilbert space of the ith share. For any quantum secret sharing scheme, it is proven that

$$\log(\dim(\mathscr{H}_{\mathrm{S}})) \leq \log(\dim(\mathscr{H}_i)) \tag{2.44}$$

for any $1 \leq i \leq n$ [16] [20]. That is, the size of each share must be at least as large as the size of a secret. For example, if the secret is two qubits (i.e., $\dim(\mathscr{H}_{\mathrm{S}}) = 2^2$), each share should be at least two qubits (i.e., $2^2 \leq \dim(\mathscr{H}_i)$). To overcome this limitation, quantum ramp secret sharing schemes have been studied.

For a (k, L, n) quantum ramp secret sharing scheme [34], it was shown that

$$\frac{1}{L}\log(\dim(\mathscr{H}_{\mathrm{S}})) \leq \frac{1}{n}\sum_i \log(\dim(\mathscr{H}_i)). \tag{2.45}$$

As L increases (i.e., the range of an intermediate structure expands), the size of shares can be reduced by $1/L$. For example, in a $(6, 3, 9)$ quantum ramp secret sharing scheme, the size of a secret is three qubits and each share can be one qubit at most.

2.8 Quantum error correcting Codes

In this section, I provide basic results of quantum error correction. The aim of error correction is protecting information against errors. Errors can occur on quantum systems due to imperfect physical devices, undesired interaction with an environment or interruption from a third party (e.g., an eavesdropper). In error correction, information is transformed into a *codeword* (i.e., the encoded form which can detect and correct errors). The set of codewords is called a *code*.

In Subsec. 2.8.1, I show how a simple code can correct errors occurring on a single bit. After that, I consider a sufficient and necessary condition for more general codes in

Subsec. 3.11.

2.8.1 A simple code

The simplest error correcting code can be obtained by copying the value of an input bit onto two ancillary bits (i.e., $0 \mapsto 000$, $1 \mapsto 111$). In this case, we can correct a single bit flip error in a codeword (i.e., the resulting string of bits) by looking at the majority of the bit values. However, in a quantum case, it is impossible to simply copy an arbitrary state of qubits. According to the no-cloning theorem of quantum mechanics, there is no unitary operation satisfying

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \tag{2.46}$$

where U is a generally unknown operator and $|\psi\rangle$ is an arbitrary state of qubits.

Quantum error correcting codes (QECCs) can be obtained by a unitary operation that maps a quantum state into a subspace of a larger-dimensional Hilbert space. The subspace is called a *coding space*, denoted by C. For example, a three-qubit code can be implemented via a unitary operation which encodes an arbitrary state of a qubit with two ancillary qubits in the codeword of three qubits as follows:

$$U_{\text{enc}} : (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \mapsto \alpha|000\rangle + \beta|111\rangle. \tag{2.47}$$

In this case, a coding space C spanned by this codeword is the two-dimensional subspace of a larger 2^3-dimensional Hilbert space. Note that this encoding operation does not violate the no-cloning theorem: $\alpha|000\rangle + \beta|111\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3}$.

The three-qubit code can correct a bit flip error occurring on a single qubit. Suppose that the first qubit has been flipped (i.e., switching between $|0\rangle$ and $|1\rangle$). In this case, one can know on which qubit the error occurs by comparing the state of the first qubit with other two qubits via measurements; in order not to disturb a superposition of the codeword, one measures the differences between two states, but does not measures the states individually.

Qubits have not only the bit flip errors but also phase flip errors. The phase flip error switches between $(|0\rangle + |1\rangle)$ and $(|0\rangle - |1\rangle)$. The three-qubit code can correct a phase flip error by performing the encoding operation with respect to the different basis:

$$U'_{\text{enc}} : (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \mapsto \alpha| + ++\rangle + \beta| - --\rangle. \tag{2.48}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In this basis, the phase flip error has the same effect as the bit flip error in the previous basis; thus, detection of the phase flip error is achieved in the same manner as one of the bit flip error.

However, the three-qubit code cannot correct a bit flip error and a flip error at the same time. To correct both bit flip and phase flip errors occurring on a single qubit, the state of a qubit can be encoded as follows

$$|0\rangle \mapsto |\bar{0}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \tag{2.49}$$

$$|1\rangle \mapsto |\bar{1}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \tag{2.50}$$

This is a Shor's 9-qubit code [50] defined by a coding space that is a two-dimensional subspace of a 2^9-dimensional Hilbert space.

2.8.2 Conditions for Quantum Error Correction

Now, let me consider conditions for successful error correction of a coding space C [51] [52]. At first, errors are correctable when they can be distinguished from each other. That is, for arbitrary errors E_a and E_b occurring on two different basis codewords $|\psi_i\rangle$ and $|\psi_j\rangle$, respectively, $E_a|\psi_i\rangle$ must be orthogonal to $E_b|\psi_j\rangle$:

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = 0 \tag{2.51}$$

where $i \neq j$. Also, when a measurement is performed to detect errors on a codeword, it must not reveal any information about the actual state of codeword; otherwise, the measurement will collapse a superposition of codewords. Therefore, the result of the measurement depends on the errors, but not on the codeword:

$$\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle = C_{ab} \tag{2.52}$$

where $|\psi_i\rangle$ is a codeword in C and $\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle$ is an expectation value (i.e., mean value) of an observable $E = E_a^\dagger E_b$. Combining Eq. 2.51 and Eq. 2.52, we can have a necessary and sufficient condition for the code to correct the errors $\{E_a\}$; the errors $\{E_a\}$ occurring on any states in the coding space C are correctable iff

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ab}\delta_{ij} \tag{2.53}$$

where $\{|\psi_i\rangle\}$ are basis codewords in C [28]. This condition will be connected with the condition of quantum secret sharing in Sec. 2.10.

The minimum weight of errors that do not satisfy Eq. 2.53 is called the *distance* of a code. A code with a distance d can correct $d-1$ erasure errors. Note that an erasure error is a general error occurring on a known location. A quantum error correcting code encoding k qubits in n qubits can be described as a $[[n, k, d]]$ code where d is its distance. This code has a coding space that is a 2^k-dimensional subspace of a 2^n-dimensional Hilbert space.

2.9 Stabilizer Codes

In this section, I give an overview of stabilizer codes. One promising way to construct a quantum error correcting code is choosing a coding space C that is stabilized by an Abelian subgroup (i.e., all its elements commute with each other) of the Pauli group.

g_1	Z	Z	I	I	I	I	I	I	I
g_2	Z	I	Z	I	I	I	I	I	I
g_3	I	I	I	Z	Z	I	I	I	I
g_4	I	I	I	Z	I	Z	I	I	I
g_5	I	I	I	I	I	I	Z	Z	I
g_6	I	I	I	I	I	I	Z	I	Z
g_7	X	X	X	X	X	X	I	I	I
g_8	I	I	I	X	X	X	X	X	X

Table 2.1: The stabilizer for Shor's 9-qubit code

The Pauli group G_n is the set of all the tensor products of the Pauli operators and the identity matrix with a possible overall factor of ± 1 or $\pm i$;

$$G_n = \{i^a \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n \mid \sigma_j \in \{I, X, Y, Z\}\} \tag{2.54}$$

Quantum error correcting codes defined by such a coding space are called *stabilizer codes* [28]. The stabilizer formalism provides a compact way to describe quantum error correcting codes. Not all quantum error correcting codes are stabilizer codes, but most of the well-known quantum codes are. For example, Shor's 9-qubit code is in fact a $[[9, 1, 3]]$ stabilizer code.

A stabilizer S is the Abelian subgroup of the Pauli group G_n which does not contain the element $-I$;

$$S = \{g_i \mid g_i \in G_n \text{ s.t. } g_i \neq -I,\ [g_i, g_j] = 0 \text{ for } \forall g_i\} \tag{2.55}$$

Note that we usually specify generators $\langle S_i \rangle$ of the stabilizer; all the elements of the stabilizer can be described as products of these generators. The generators of Shor's 9-qubit code are listed in Table 2.1.

Given a stabilizer S, we can define a coding space C as the set of states fixed by the elements of the stabilizer;

$$C = \{|\psi\rangle \mid g|\psi\rangle = |\psi\rangle\ \forall g \in S,\ |\psi\rangle \in \mathscr{H}\} \tag{2.56}$$

That is, codewords spanning C are eigenvectors of the elements of the stabilizer with eigenvalue $+1$.

A natural question to be followed is what kinds of errors can be detected in the coding space C. If an error E on a codeword anti-commutes with an element g of the stabilizer S, it will move the codeword to the (-1)-eigenvalue subspace of S; $g(E|\psi\rangle) = -Eg|\psi\rangle = -(E|\psi\rangle)$. Thus, we can detect the error by measuring the eigenvalue of g. Also, if an error itself is an element of the stabilizer S, it cannot change the codewords at all. It follows that a stabilizer code with stabilizer S can correct the following errors,

$$E = \{E_a \mid E_a g = -gE_a \text{ for some } g \in S \text{ or } E_a \in S\}. \tag{2.57}$$

That is, this code can detect all errors E that are either in S or anti-commutes with any element of S [28]. The errors satisfy Eq. 2.53.

A $[[n, k, d]]$ stabilizer code is bounded by the quantum singleton bound (also called Knill-Laflamme bound). The quantum singleton bound states that $n - k \geq 2\ (d - 1)$ for any $[[n, k, d]]$ stabilizer code [51]. According to this bound, $n = 9$ (i.e., a Shor's 9-qubit code) is not the minimum value for $d = 3$ and $k = 1$; in this case $n = 5$ is the minimum value (i.e., a $[[5, 1, 3]]$ stabilizer code).

2.10 Relationship between QSS and QECC

In this section, I show the remarkable relationship between quantum secret sharing and quantum error correction. It is known that a $[[2k - 1, 1, k]]$ stabilizer code is equivalent to a $(k, 2k - 1)$ quantum threshold scheme [16] [20]. For example, a $[[5, 1, 3]]$ stabilizer code exactly yields a $(3, 5)$ threshold scheme. The $[[5, 1, 3]]$ stabilizer code can correct two erasure errors by encoding one qubit in five qubits. Thus, an initial state can be constructed from any three qubits. On the other hand, any two qubits provide no information about the state, as learning some information from the qubits necessarily disturbs a superposition of the initial state. It is possible to see this relationship more deeply.

Let an operation encode a quantum secret to a composite system of n shares, and the composite system be spanned by $\{|\psi_i\rangle\}$. The operation is a pure-state quantum secret sharing scheme iff for any $|\psi_i\rangle, |\psi_j\rangle \in \{|\psi_i\rangle\}$ and all operators E acting on the complement of an authorized set,

$$\langle\psi_i|E|\psi_j\rangle = c(E)\delta_{ij} \tag{2.58}$$

where $c(E)$ is the function of E [16] [20].

For $i \neq j$, $\langle\psi_i|E|\psi_j\rangle = 0$ means that an authorized set can correct any erasure error occurring on the state of its complement, i.e., an unauthorized set. That is, the authorized set can distinguish all different bases $\{|\psi_i\rangle\}$ for any operator on its complement. For $i = j$, the condition becomes $\langle\psi_i|E|\psi_i\rangle = c(E)$. It means that an unauthorized set cannot learn any information about a quantum secret encoded in $\{|\psi_i\rangle\}$ because the expectation value $\langle\psi_i|E|\psi_i\rangle$ is independent of $|\psi_i\rangle$.

The necessary and sufficient condition of Eq. 2.58 is exactly included in the quantum error correcting condition of Eq. 2.53. It follows that every quantum secret sharing scheme is in fact a quantum error correcting code (strictly speaking, the encoding operation of quantum secret sharing is quantum error correction) [16] [20].

2.11 Summary

In this chapter, I have provided basics of quantum information theory, classical secret sharing and quantum error correction. The elements of this chapter are summarized as follows. A pure state of qubits is well described by a vector in a Hilbert space, but a density matrix is more suitable to express the mixed state (i.e., the statistical ensemble of pure states). Then, the evolution and the measurement of a quantum system is described by means of operators. In a composite system of multiple qubits, a composite state might be entangled. The entangled state is used as an important resource in quantum communication protocols such as quantum teleportation.

Von Neumann entropy measures how much uncertainty there is in a density matrix, and mutual information of two quantum systems measures how much information the systems have in common. Entanglement measures are useful tools for quantifying entanglement in a density matrix. Particularly, the relative entropy of entanglement is one of entanglement measures, which has the property of non-lockability; the removal of one qubit reduces the amount of relative entropy of entanglement at most by two.

Classical secret sharing allows a dealer to distribute a classical secret among players such that some specific sets of players can reconstruct the secret, but the other sets gain no information about the secret. In classical secret sharing schemes, there is a critical limitation on the size of shares. Thus, classical ramp secret sharing has been proposed. For (k, L, n) ramp schemes, the size of each share can be reduced by $1/L$. Instead, there is some leaked information to unauthorized sets, but the leaked information can be quantified by the conditional entropy.

A quantum error correcting code can correct some errors occurring on the state of qubits, and is defined by a coding space. A coding space is sometimes determined by a stabilizer. The stabilizer formalism provides a compact way to describe quantum error correcting codes. Quantum error correction is closely related to quantum secret sharing. In quantum secret sharing, an authorized set can correct any erasure error acting on its complement. This is exactly what quantum error correcting codes do. In fact, it is proven that any quantum secret sharing scheme is equivalent to a quantum error correcting code. This relationship gives rise to a central idea to prove the existence of entanglement sharing in Chapter 3.

Chapter 3

Entanglement Sharing Schemes

In this chapter, I introduce an *entanglement sharing scheme*. An entanglement sharing scheme allows a dealer to distribute entanglement among players in such a way that authorized sets of players can have the original entanglement fully with the dealer, but unauthorized sets are totally denied any entanglement. Entanglement is a necessary resource required for quantum information tasks such as quantum teleportation [6], superdense coding [7] and device-independent quantum key distribution [8] [9]. An entanglement sharing scheme enables a dealer to perform such quantum tasks with only authorized sets of players in a network consisting of multiple players. Each of player cannot be trusted but their collaborating groups might be trusted. The definition of entanglement sharing is given in Sec. 3.1.

Entanglement sharing can be designed by employing quantum error correcting codes. In Sec. 3.2, I show how to use a quantum error correcting code for implementing an entanglement sharing scheme, with an example of the Shor's 9-qubit code. Then, I prove that the size of shares is at least half the size of the initially shared entanglement in Sec. 3.3. When an entanglement sharing scheme has the minimum size of shares, it is said to be optimal. In Sec. 3.4, I show that an optimal entanglement sharing scheme can be constructed from a $[[4, 2, 2]]$ stabilizer code.

3.1 Definition of Entanglement Sharing

Entanglement sharing has many similarities with quantum secret sharing in the concept of distributing a secret among multiple players. However, they are basically designed with different systems. Let D denote a dealer and $P = \{P_1, P_2, \cdots, P_n\}$ a set of players. Quantum secret sharing concerns a single-party system of a dealer or a set of players. In quantum secret sharing, an arbitrary quantum state in a Hilbert space $\mathscr{H}_\mathrm{D}$ is encoded in the Hilbert space of players $\mathscr{H}_\mathrm{P}$ (i.e., a tensor product of the Hilbert spaces of players). In contrast, entanglement sharing is based on a bipartite system of a dealer and a set of players, and encodes a maximally entangled state in $\mathscr{H}_\mathrm{D} \otimes \mathscr{H}_\mathrm{D}$ into $\mathscr{H}_\mathrm{D} \otimes \mathscr{H}_\mathrm{P}$.

Let me explain the encoding procedure of entanglement sharing in details. A dealer initially prepares a pair of qubits in a maximally entangled state. One of the pair is held in his place, and the other is encoded into the n shares of players. Entanglement sharing has recoverability and secrecy conditions. The recoverability condition is that any authorized set of players can recover the initial maximally entangled state fully using local operations (the local operations mean joint operations on the qubits of an authorized set and single-qubit operations), and the secrecy condition is that any unauthorized set cannot be entangled with the dealer whatsoever. Every subset of players must be either an authorized set or an unauthorized set. The collection of all authorized sets is an access structure $\mathcal{A}$ and the collection of all unauthorized sets is an adversary structure $\mathcal{U}$. As in quantum secret sharing, the access structure must be monotone. A schematic picture of entanglement sharing schemes is shown in Fig. 3.1.

Note that if a subset of players is partially entangled with the dealer, the corresponding scheme will be said to be non-perfect. I discuss non-perfect entanglement sharing schemes in Chapter 5.

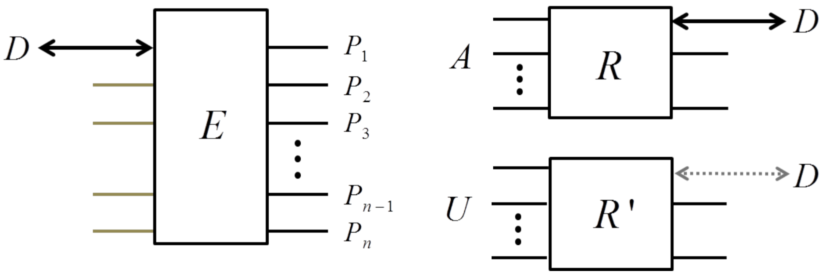

Figure 3.1: Schematic picture of an entanglement sharing scheme. Arrows indicate pairs of qubits. A rigid arrow refers to a pair of qubits in a maximally entangled state and a dotted arrow is a pair in either a separable state or a product state. E is an encoding circuit of the scheme, which encodes half of the pair and some ancillary qubits into n shares of players. R and R' are properly chosen recovery circuits for an authorized set A and an unauthorized set U, respectively.

3.2 Entanglement Sharing with Quantum Error Correcting Codes

Recall that quantum secret sharing has a close relationship with quantum error correction. A quantum secret sharing scheme can be constructed from any quantum error correcting code that satisfies the condition of Eq. 2.58. For example, as a $[[2k-1,1,k]]$ stabilizer code corrects any $k-1$ erasure errors, a secret is constructed from any k qubits and no information about the secret is obtained from any $k-1$ shares. This is equivalent to a $(k, 2k-1)$ quantum threshold scheme [16]. As in quantum secret sharing, entanglement sharing is also related to quantum error correction. Any authorized set of shares in entanglement sharing can reconstruct an initial maximally entangled state by correcting erasure errors on its complement. This means that the encoding operation of any entanglement sharing scheme is in fact quantum error correction.

In this section, I guess entanglement sharing schemes based on the existing stabilizer codes. I implement a scheme that encodes a maximally entangled state in the coding space of a quantum error correcting code and assess whether or not the induced scheme satisfies the recoverability and secrecy conditions of entanglement sharing. The recoverability condition is naturally fulfilled from the coding space. However, the secrecy condition might be violated if the coding space yields the unauthorized sets that obtain *partially* entangled states (i.e., neither maximally entangled nor separable) with dealer. At this point, it is helpful to investigate methods for determining the separability of a reduced density matrix. Finally, I show that Shor's 9-qubit code indeed induces an entanglement sharing scheme.

First, consider a quantum error correcting code that encodes k in n qubits. A dealer prepares a maximally entangled state,

$$|S\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |j\rangle_{\mathrm{D}} |j\rangle_{\mathrm{D}} \tag{3.1}$$

in a bipartite system $\mathscr{H}_{\mathrm{D}} \otimes \mathscr{H}_{\mathrm{D}}$ where $\mathscr{H}_{\mathrm{D}}$ is a 2^k-dimensional Hilbert space. One component system is held in the dealer's place, and another system is encoded in the coding space C. Then, the mapping of $|S\rangle$ is given by

$$|S\rangle \ \mapsto \ |\Psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |j\rangle_{\mathrm{D}} |C_j\rangle_P \tag{3.2}$$

where $C = \mathrm{span}\{C_j\}_{j=0\cdots 2^k-1}$. Each qubit of the code is taken as a share (i.e., $C = \mathscr{H}_{P_1} \otimes \mathscr{H}_{P_2} \otimes \cdots \otimes \mathscr{H}_{P_n}$)

An access structure $\mathcal{A}$ is determined from the coding space C. A set K of shares reconstructs $|S\rangle$ through a recovery operation of the code if C can correct erasure errors on the complement of K. That is, K is an authorized set and the access structure consists of all sets K.

On the other hand, the complement of K must have a non-entangled state (i.e., either a separable state or a product state) with the dealer, due to *monogamy of entanglement.* According to monogamy, if two systems are maximally entangled, they cannot be entangled with any third system [53] [54]. For example, monogamy is expressed as the following inequality,

$$E(\rho^{XY}) + E(\rho^{XZ}) \leq E(\rho^{X(YZ)}) \tag{3.3}$$

for any composite system of X, Y and Z. This inequality holds for some entanglement measures such as the one-way distillable entanglement and the squashed entanglement [54]. Let X be the dealer, Y an authorized set and Z the complement of Y. As ρ^{XY} can be transformed into $\rho^{X(YZ)}$ by LOCC and vice versa, ρ^{XY} has the same amount of entanglement as $\rho^{X(YZ)}$. Therefore, the complement of any authorized set is an unauthorized set, i.e., $E(\rho^{XZ}) = 0$. It turns out that an access structure in entanglement sharing cannot have two disjoint sets due to monogamy. This is analogous to quantum secret sharing not allowing an access structure to have two disjoint sets due to the no-cloning theorem.

Now, consider another class of sets $\{B\}$, which is neither an authorized set nor the complement of any authorized set. Any set in this class is unauthorized to have any entanglement with the dealer. For a set B in this class, the reduced density matrix is given by

$$\rho^B = \mathrm{tr}_{\bar{B}}\big(|\Psi\rangle\langle\Psi|\big) \tag{3.4}$$

where $\bar{B}$ denotes the complement of B. As B is an unauthorized set, ρ^B must be a non-entangled state with the dealer. However, it is a NP-hard problem to determine whether or not a bipartite density matrix is entangled [44]; thus, it is not easy to verify the secrecy of entanglement sharing.

One possible way to determine whether or not the set B has some entanglement with the dealer is measuring the amount of entanglement between B and the dealer by means of any entanglement measure. For a pure state $|\psi\rangle$ in a bipartite system of X and Y, every entanglement measure simply reduces to the entropy of entanglement [43], as follows.

$$E(|\psi\rangle\langle\psi|) = S(\mathrm{tr}_X|\psi\rangle\langle\psi|) \tag{3.5}$$

However, most entanglement measures for a mixed state are very difficult to compute, except some special cases (various entanglement measures and their computable classes of states are well surveyed in [43]).

The PPT criterion can also be used in checking the absence of entanglement in a reduced density matrix, as it has the advantage of being easily checked in many computation programs such as Mathematica$^{\text{TM}}$. As I explained in Sec. 2.1.4, the PPT criterion is a necessary but not sufficient condition for the separability of the reduced density matrix in the bipartite system of a more than six dimension.

For some stabilizer codes such as Shor's 9-qubit code (i.e., a $[[9, 1, 3]]$ stabilizer code), the separability of ρ^B is directly shown from its form. Now, I encode a maximally entangled state using the Shor's 9-qubit code.

Consider a Bell state,

$$|S\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_{\text{D}}|0\rangle_{\text{D}} + |1\rangle_{\text{D}}|1\rangle_{\text{D}}\big). \tag{3.6}$$

According to the encoding shown in Eq. 2.49, $|S\rangle$ is encoded such that

$$|S\rangle \mapsto |\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle_{\text{D}}|G_0\rangle_{123}|G_0\rangle_{456}|G_0\rangle_{789} + |1\rangle_{\text{D}}|G_1\rangle_{123}|G_1\rangle_{456}|G_1\rangle_{789}\Big) \tag{3.7}$$

where $|G_0\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|G_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. This code consists of three triplets, each of which corresponds to three qubits in the same G-state. Each qubit in this code is allocated to a player. Let $P = \{1, 2, 3, \cdots, 9\}$ be a set of the labels of qubits in the code, or equivalently, a set of players.

The stabilizer of the Shor's 9-qubit code (see Table. 2.1) can correct erasure errors on $K \subseteq P$ if K is a set of

1. any one or two qubits
2. two qubits in one triplet and single qubit in other triplet (e.g., $\{1, 2, 4\}$)
3. two qubits in one triplet and two qubits in other triplet (e.g., $\{1, 2, 4, 5\}$)

For any K, every erasure error on K is either in the stabilizer or anti-commutes with some element in the stabilizer. This means that the complement of K can correct the erasure errors and recover the original entanglement with the dealer, whereas K is not entangled with the dealer due to monogamy. The complement of K might use the following recovery process. Consider $K = \{6, 8, 9\}$ of the second case. The complement of K (i.e., $\{1, 2, 3, 4, 5, 7\}$) has the reduced density matrix

$$\frac{1}{4}|\phi\rangle\langle\phi|\otimes\Big(|000\rangle\langle 000|_{457}+|111\rangle\langle 111|_{457}\Big)+\frac{1}{4}|\bar{\phi}\rangle\langle\bar{\phi}|\otimes\Big(|110\rangle\langle 110|_{457}+|001\rangle\langle 001|_{457}\Big) \quad (3.8)$$

where $|\phi\rangle$ and $|\bar{\phi}\rangle$ are $\frac{1}{\sqrt{2}}\Big(|0\rangle_{\mathrm{D}}|G_0\rangle_{123} \pm |1\rangle_{\mathrm{D}}|G_1\rangle_{123}\Big)$, respectively. In this case, the entire system can be collapsed into one of two states $|\phi\rangle$ and $|\bar{\phi}\rangle$ through a projection measurement on qubits of the last three players (i.e., $\{4, 5, 7\}$). The collapsed state is transformed to the original maximally entangled state by performing a proper local unitary operation.

For Shor's 9-qubit code, every set in $\{B\}$ has a separable state with the dealer. For example, the reduced density matrix of $B = \{1, 2, 3, 4, 5, 6\}$ can be written as

$$\mathrm{tr}_{789}\Big(|\Psi\rangle\langle\Psi|\Big) = \frac{1}{2}\sum_{i=0}^{1}|i\rangle\langle i|_{\mathrm{D}} \otimes |G_i\rangle\langle G_i|_{123} \otimes |G_i\rangle\langle G_i|_{456}. \quad (3.9)$$

The form of the reduced density matrix directly shows that B is separable with the dealer. In a similar way, it can be shown that the other sets in $\{B\}$ also have separable states with the dealer, as investigated in Appendix A. Therefore, an entanglement sharing scheme with a general access structure is constructed from Shor's 9-qubit code.

3.3 The Size of Shares in Entanglement Sharing

In this section, I prove that the size of shares in an entanglement sharing scheme must be at least half the size of an initial entanglement. Let T be an unauthorized set such that $A = T \cup r$ is authorized where r is a share of one qubit. This means that the state ρ^{DA} has the same amount of entanglement as ρ^{DP}, but the amount of entanglement must go to zero by discarding the share r. In this case, the share r acts like a key that locks the initial entanglement. According to [37], the amount of entanglement can decrease at most by two upon discarding one qubit with respect to *the relative entropy of entanglement.* This observation leads to the following theorem.

Theorem 3.3.1. *For any entanglement measure E, every entanglement sharing scheme satisfies*

$$E(\rho^{DP}) \leq 2q \tag{3.10}$$

where ρ^{DP} is an initial maximally entangled state and q is the size of each share (i.e., the number of qubits in a share).

Proof. Let Γ be an unauthorized set satisfying that $\Gamma \cup u = A$ where $u \notin \Gamma$ is one share and A is an authorized set, and let $\rho^{\mathrm{D}\Gamma u}$ be the reduced density matrix of the authorized set A with a dealer. Assume that total dephasing (i.e., twirling) is performed on the share u; that is, the unitary operators $g_i^u \in \{I, X, Y, Z\}^{\otimes q}$ are applied to u with equal probabilities. Then, the following inequality for the relative entropy of entanglement E_R is obtained:

$$\sum_i p_i E_R(\rho_i) - E_R(\sum_i p_i \rho_i) \leq S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \tag{3.11}$$

where $\rho_i = (I^{\mathrm{D}\Gamma} \otimes g_i^u)\rho^{\mathrm{D}\Gamma u}(I^{\mathrm{D}\Gamma} \otimes g_i^u)$ and $p_i = \frac{1}{4^q}$. The derivation of this inequality is shown in Appendix B. Due to the total dephasing,

$$\sum_i p_i \rho_i = \frac{1}{4^q} \sum_i (I^{\mathrm{D}\Gamma} \otimes g_i^u)\rho^{\mathrm{D}\Gamma u}(I^{\mathrm{D}\Gamma} \otimes g_i^u) = \mathrm{tr}_u(\rho^{\mathrm{D}\Gamma u}) \otimes \frac{1}{2^k} I^u. \tag{3.12}$$

Now, the share u does not affect the amount of the entire entanglement because it is independent of the other shares and the dealer. It follows that $E_R(\sum_i p_i \rho_i) = E_R(\mathrm{tr}_u(\rho^{\mathrm{D}\Gamma u}))$. Also, as the relative entropy of entanglement is invariant under local unitary transformations,

$$\sum_i p_i E_R(\rho_i) = \sum_i p_i E_R(\rho^{\mathrm{D}\Gamma u}) = E_R(\rho^{\mathrm{D}\Gamma u}). \tag{3.13}$$

Thus, the inequality is rewritten as

$$E_R(\rho^{\mathrm{D}\Gamma u}) - E_R(\mathrm{tr}_u(\rho^{\mathrm{D}\Gamma u})) \leq S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \leq H(p_i) = 2q \tag{3.14}$$

with Eq.2.28.

As Γ is an unauthorized set, its reduced density matrix $\mathrm{tr}_u(\rho^{\mathrm{D}\Gamma u})$ is not entangled with the dealer; i.e., $E_R(\mathrm{tr}_u(\rho^{\mathrm{D}\Gamma u})) = 0$. On the other hand, $\rho^{\mathrm{D}\Gamma u}$ has the same amount of entanglement as ρ^{DP} because $\rho^{\mathrm{D}\Gamma u}$ can be transformed into ρ^{DP} by LOCC and vice versa. Furthermore, any entanglement measure has the same value for a maximally entangled state. Therefore, the following inequality is obtained:

$$E(\rho^{\mathrm{DP}}) = E_R(\rho^{\mathrm{DP}}) = E_R(\rho^{\mathrm{D}\Gamma u}) \leq 2q. \tag{3.15}$$

□

In the trivial case where the initial entanglement is one ebit (i.e., any maximally entangled state unitarily equivalent to one Bell state), the size of the shares is just one qubit because 0.5 qubit is not defined. However, for entanglement of more than one ebit, the size of each share is bounded by half of the number of ebits according to Theorem 3.3.1. An entanglement sharing scheme is said to be *optimal* if the size of its shares is half the size of the initial entanglement.

3.4 Optimal Entanglement Sharing

In this section, I present an optimal entanglement sharing scheme using the $[[4, 2, 2]]$ stabilizer code. The coding space C_{op} of the $[[4, 2, 2]]$ stabilizer code can correct erasure errors on a single qubit by encoding two qubits in four qubits. The codewords of the $[[4, 2, 2]]$ stabilizer code are

$$\{|\beta_i\rangle|\beta_i\rangle\}_{i=0,1,2,3} \tag{3.16}$$

where $\{|\beta_i\rangle\}$ are a set of Bell states.

Let D be a dealer and $P = \{1, 2, 3, 4\}$ be a set of 4 players. For a bipartite system $\mathscr{H}_{\mathrm{D}} \otimes \mathscr{H}_{\mathrm{D}}$, the dealer prepares a maximally entangled state

$$|S\rangle = \frac{1}{2}\sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|i\rangle_{\mathrm{D}} \tag{3.17}$$

where $\mathscr{H}_{\mathrm{D}}$ is a 4-dimensional Hilbert space. Note that $|S\rangle$ is local unitarily equivalent to a tensor product of two Bell states $|\beta\rangle \otimes |\beta\rangle$ (more precisely, the density matrix of $|S\rangle$ is local unitarily equivalent to $|\beta\rangle\langle\beta| \otimes |\beta\rangle\langle\beta|$).

According to the $[[4, 2, 2]]$ stabilizer code, half of $|S\rangle$ is encoded as follows:

$$|S\rangle \;\rightarrow\; |\Psi\rangle = \frac{1}{2}\sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|\beta_i\rangle_{12}|\beta_i\rangle_{34}. \tag{3.18}$$

where the index of $|\beta\rangle_{xy}$ refers to the x-th and y-th players. Note that each player receives a single qubit. As C_{op} corrects erasure errors on a single qubit, any three players can recover the original maximally entangled state $|S\rangle$. They might use the following recovery process. For $\Gamma = \{2, 3, 4\}$, $|\Psi\rangle$ can be rewritten as

$$|\Psi\rangle = \frac{1}{2\sqrt{2}}\Bigg[|0\rangle_1\Big(\sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|p_i\rangle_2|\beta_i\rangle_{34}\Big) + |1\rangle_1\Big(\sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|q_i\rangle_2|\beta_i\rangle_{34}\Big)\Bigg] \tag{3.19}$$

where the $|p_i\rangle_2$'s and $|q_i\rangle_2$'s are either $|0\rangle_2$ or $|1\rangle_2$, satisfying $\langle q_i|p_i\rangle = 0$ for all i. After tracing out the first player, the reduced density matrix of the remaining players is

$$\mathrm{tr}_1\Big(|\Psi\rangle\langle\Psi|\Big) = \frac{1}{2}\Big(|\gamma\rangle\langle\gamma| + |\gamma'\rangle\langle\gamma'|\Big) \tag{3.20}$$

where $|\gamma\rangle = \sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|p_i\rangle_2|\beta_i\rangle_{34}$ and $|\gamma'\rangle = \sum_{i=0}^{3} |i\rangle_{\mathrm{D}}|q_i\rangle_2|\beta_i\rangle_{34}$. As two possible subspaces of Γ are orthogonal, the entire system can be collapsed to one of two states $|\gamma\rangle$ and $|\gamma'\rangle$, through a projection measurement on Γ. Then, the three players of Γ can transform the collapsed state to $|S\rangle$ by applying unitary operators on their qubits. A similar recovery process can be applied to any three players. On the other hand, any single player cannot be entangled with the dealer according to monogamy. In fact, any single player has a product state with the dealer, which is of the form

$$\Big(\frac{1}{4}\sum_i |i\rangle\langle i|_{\mathrm{D}}\Big) \otimes \frac{1}{2} I_x \tag{3.21}$$

where I_x is the identity matrix of a single player x.

Let us look at the cases of two players. It is clear from Eq. 3.18 that two players of $\{1, 2\}$ or $\{3, 4\}$ have a separable state with the dealer. The following analysis shows that all other sets of two players are also separable with the dealer. Note that the state $|\beta_i\rangle_{12}|\beta_i\rangle_{34}$ can reorder the indices of qubits as

$$|\beta_i\rangle_{12}|\beta_i\rangle_{34} = \sum_i c_{ij}|\beta_j\rangle_{kl}|\beta_j\rangle_{mn} \tag{3.22}$$

where $\{k, l, m, n\}$ is a permutation of $\{1, 2, 3, 4\}$. Substituting this into Eq. 3.18, $|\Psi\rangle$ can be rewritten as

$$\frac{1}{2}\sum_i |i\rangle_{\mathrm{D}}|\beta_i\rangle_{12}|\beta_i\rangle_{34} = \frac{1}{2}\sum_i |i\rangle_{\mathrm{D}} \sum_j c_{ij}|\beta_j\rangle_{kl}|\beta_j\rangle_{mn}. \tag{3.23}$$

By tracing out two arbitrary players $\{k, l\}$, a separable state can be obtained as follows.

$$\begin{aligned}
\mathrm{tr}_{kl}\Big(|\Psi\rangle\langle\Psi|\Big) &= \frac{1}{4}\sum_j\sum_{j'} {}_{kl}\langle\beta_j|\beta_{j'}\rangle_{kl}\Big(\sum_i\sum_{i'} c_{ij}c_{i'j'}|i\rangle\langle i'|_{\mathrm{D}} \otimes |\beta_j\rangle\langle\beta_{j'}|_{mn}\Big) \\
&= \frac{1}{4}\sum_j\Big(\sum_i\sum_{i'} c_{ij}c_{i'j}|i\rangle\langle i'|_{\mathrm{D}}\Big) \otimes |\beta_j\rangle\langle\beta_j|_{mn} \\
&= \frac{1}{4}\sum_j |a_j\rangle\langle a_j|_{\mathrm{D}} \otimes |\beta_j\rangle\langle\beta_j|_{mn}
\end{aligned} \tag{3.24}$$

where $|a_j\rangle = \sum_i c_{ij}|i\rangle_{\mathrm{D}}$.

A stabilizer of the [[4, 2, 2]] stabilizer code is $XXXX$ and $ZZZZ$ [28]. The permutation invariance of the elements of its stabilizer leads to a threshold entanglement sharing scheme such that any three or more players are authorized to recover the original entanglement, any two players have a separable state with the dealer and any single player have a product state. A schematic picture of this scheme is shown in Fig. 3.2.

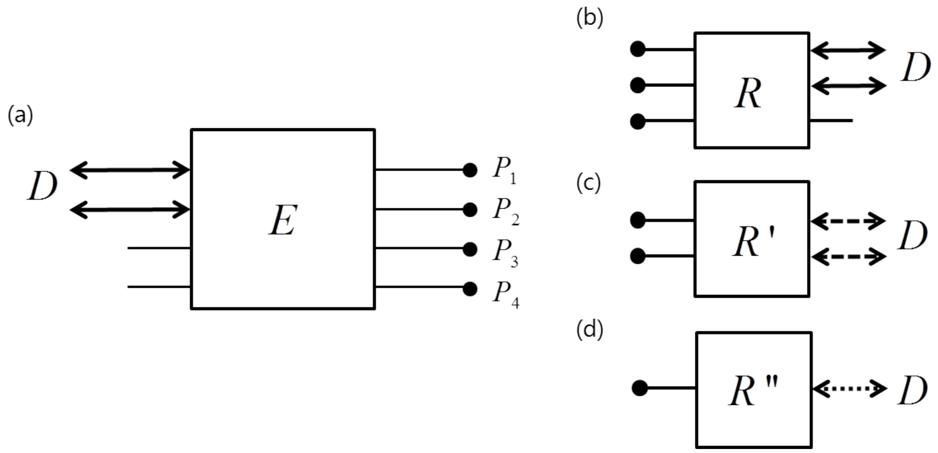

Figure 3.2: Schematic picture for an optimal entanglement sharing scheme with a $[[4, 2, 2]]$ stabilizer code. Arrows indicate bipartite states of a dealer and a set of players. (a) A pair of rigid arrows is two ebits (i.e., a four-qubit maximally entangled state). E is an encoding operation that encodes half of two ebits in four shares using ancillary qubits. (b) R is a recovery operation that reconstructs the initial two ebits from three shares. (c) A pair of dashed arrows is a separable state with the dealer. R' is any recovery operation that outputs only separable states with the dealer from two shares. (d) A dotted arrow is a product state with the dealer. R'' is any recovery operation. It is impossible to have nothing other than a product state from a single share.

3.5 Summary

In this chapter, I has introduced entanglement sharing as a new cryptographic scheme to share maximally entangled states with multiple players, which are used as central resources of quantum information protocols. In entanglement sharing, any authorized set of players can be maximally entangled with a dealer (recoverability condition), but any unauthorized set must be separable with the dealer (secrecy condition).

Entanglement sharing naturally has an access structure that is monotone, as in quantum secret sharing. I have seen that the access structure cannot have two disjoint sets as monogamy of entanglement prohibits the complement of any authorized set from having entanglement with a dealer.

Quantum error correcting codes recover original quantum states by correcting erasure errors. In this sense, entanglement sharing is related to quantum error correcting because any authorized set recovers the original maximally entangled state by correcting erasure errors on its complement. Thus, I considered a way to share maximal entanglement using the existing stabilizer codes, and constructed an entanglement sharing scheme from Shor's 9-qubit code, which has a general access structure.

Then, I proved that the size of shares must be at least half the size of the initial entanglement. Furthermore, I showed that a $[[4, 2, 2]]$ stabilizer code induces an optimal entanglement sharing scheme that has the minimum size of shares with respect to the initial entanglement. The induced optimal entanglement sharing scheme has a threshold structure due to the prefect symmetry in the stabilizer of the code.

Chapter 4

A Secrecy Condition of QRSS

Quantum ramp secret sharing schemes reduce the size of shares by leaking some information to intermediate sets. As the leaked information directly affects the secrecy of schemes, it is desirable to characterize information leakage and develop secrecy conditions for quantum ramp secret sharing schemes. However, the characterization of information leakage is a challenging problem. For stabilizer encoding, it is possible to characterize the leaked information through the notion of an information group [39], but this approach requires the details of the encoding operation to obtain the information group. In this chapter, I propose a different approach to characterize the leaked information by exploiting entanglement sharing.

In Sec. 4.1, I start by defining the intermediate sets based on quantum mutual information. The quantum mutual information can determine whether or not a set of players learns some information about the secret, but it is not suitable to characterize the information. In general, quantum information is considered to include classical information. However, defining classical and quantum information separately can help to characterize information. Thus, I show how classical and quantum information was defined in [57] and briefly explain the method of an information group based on this definition, as was shown in [39].

In Sec. 4.2, I define classical and quantum information in the context of channels used to transmit information. Then, I show how entanglement sharing can be used to determine whether any quantum information is leaked or not. Finally, I introduce a new secrecy condition of quantum ramp secret sharing schemes.

4.1 Discussion on Leaked Information

Information theory has played a crucial role in defining and evaluating secret sharing schemes [29] [31] [38] [34]. Classical secret sharing was defined by the conditional entropy [29] and it simply extended to classical ramp secret sharing [31]. In the quantum setting, the quantum mutual information has been used to describe quantum secret sharing [38] [34]. As in classical secret sharing, the descriptions of quantum secret sharing can be also extended to quantum ramp secret sharing. Before doing it, I first consider the recoverability and secrecy conditions of quantum secret sharing as was done in [38].

Suppose that a quantum secret X is given by the density matrix ρ^X in a q-dimensional Hilbert space $\mathscr{H}_X$. The density matrix ρ^X can be described by its orthonormal decomposition,

$$\rho^X = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle\langle i| \tag{4.1}$$

where $\alpha_i \in [0,1]$ for $i \in \mathbb{F}_q$ and $\{|i\rangle\}$ are orthonormal basis vectors of $\mathscr{H}_X$. For instance, when $q = 2$, the density matrix can be represented by $\rho^X = \alpha_0|0\rangle\langle 0| + \alpha_1|1\rangle\langle 1|$.

Let R be the reference system for X. The composite system of R and X is in a pure state $|RX\rangle \in \mathscr{H}_R \otimes \mathscr{H}_X$, according to the purification (see Sec. 2.1.4). The state $|RX\rangle$ is reduced to ρ^X after tracing out R.

In a quantum secret sharing scheme, the secret X is distributed among a set of n players, $P = \{1, 2, 3, \ldots, n\}$. If a subset $\Gamma \subseteq P$ satisfies

$$S(R:\Gamma) = 0 \quad \text{(secrecy condition)}, \tag{4.2}$$

then it cannot obtain any information about ρ^X. This condition means that a composite system of Γ and R is in a product state. As Γ is totally independent of R, it cannot gain any information about a system that is correlated to R. In quantum ramp secret sharing, such a subset is called a forbidden set.

On the other hand, if a subset Γ satisfies

$$S(R:\Gamma) = S(R:X) \quad \text{(recoverability condition)}, \tag{4.3}$$

it can recover ρ^X perfectly. Let $\mathcal{E} : \mathscr{H}_X \to \mathscr{H}_\Gamma$ be a quantum operation such that $\mathcal{E}(\rho^X) = \rho^\Gamma$ where $\mathscr{H}_\Gamma$ is the Hilbert space of Γ and ρ^Γ is the reduced density matrix of Γ. In [56], it was proven that $\mathcal{E}$ is perfectly reversible if and only if

$$S(X) = S(\Gamma) - S(R,\Gamma). \tag{4.4}$$

This means that there exists a quantum operation $\mathcal{R} : \mathscr{H}_\Gamma \to \mathscr{H}_X$ such that $\mathcal{R}(\rho^\Gamma) = \rho^X$. Eq. 4.4 is equivalent to the recoverability condition as shown by

$$\begin{aligned} S(R:\Gamma) - S(R:X) &= S(R) + S(\Gamma) - S(R,\Gamma) - \big(S(R) + S(X) - S(R,X)\big) \\ &= S(\Gamma) - S(X) - S(R,\Gamma) \\ &= 0 \end{aligned} \tag{4.5}$$

where $S(R,X) = 0$ as ρ^{RX} is a pure state.

Next, consider a subset of players, which satisfies neither the secrecy nor the recoverability condition. If $0 < S(R:\Gamma) < S(R:X)$, a subset Γ will learn some information about ρ^X, but cannot recover it perfectly. In quantum ramp secret sharing, such a subset is called an intermediate set [34]. Now, I can describe a quantum ramp secret sharing scheme as follows.

A (k, L, n) pure-state quantum ramp secret sharing scheme distributes a quantum secret ρ^X among n players satisfying the following conditions:

1. For $|\Gamma| \geq k, \quad S(R:\Gamma) = S(R:X)$
2. For $k - L < |\Gamma| < k, \quad 0 < S(R:\Gamma) < S(R:X)$
3. For $|\Gamma| \leq k - L, \quad S(R:\Gamma) = 0$

where R is a reference system for X. By this description, a $[[4,2,2]]$ stabilizer code is in fact a $(3,2,4)$ quantum ramp scheme as follows.

Consider a secret in the four-dimensional Hilbert space $\mathscr{H}_X$, given by

$$\rho^X = \frac{1}{4}\sum_{i=0}^{3} |i\rangle\langle i|. \tag{4.6}$$

The purification of ρ^X is

$$|RX\rangle = \frac{1}{2}\sum_{i=0}^{3} |i\rangle|i\rangle. \tag{4.7}$$

and therefore $S(R:X) = S(R) + S(X) - S(R,X) = 2S(X) = 4$. Suppose that the secret X is distributed among four players by the $[[4,2,2]]$ stabilizer code. The encoding operation of the $[[4,2,2]]$ stabilizer code is

$$V_X \ : \ \sum_{i=0}^{3} \alpha_i|i\rangle \mapsto \sum_{i=0}^{3} \alpha_i|\beta_i\rangle|\beta_i\rangle. \tag{4.8}$$

where $\{|\beta_i\rangle\}$ are Bell states. After the encoding operation, the composite state of R and P can be described by

$$|RP\rangle = (I_R \otimes V_X)|RX\rangle = \frac{1}{2}\sum_{i=0}^{3} |i\rangle|\beta_i\rangle|\beta_i\rangle. \tag{4.9}$$

Let $P = \{1,2,3,4\}$ be a set of four players. The $[[4,2,2]]$ stabilizer code can correct erasure errors on any single player. It turns out that any three players Γ_3 are authorized. In fact, the recoverability condition holds for any three players as shown by

$$S(R:\Gamma_3) = 2 + 3 - 1 = 4 = S(R:X). \tag{4.10}$$

On the other hand, any single player is a forbidden set because it satisfies the secrecy condition,

$$S(R:\Gamma_1) = 2 + 1 - 3 = 0. \tag{4.11}$$

Any two players obtain some information about the secret. For any two players, we have

$$\rho^{R\Gamma_2} = \frac{1}{4}\sum_{i=0}^{3} |i'\rangle\langle i'| \otimes |\beta_i\rangle\langle\beta_i| \tag{4.12}$$

and

$$\rho^{\Gamma_2} = \frac{1}{4}\sum_{i=0}^{3} |\beta_i\rangle\langle\beta_i|. \tag{4.13}$$

It follows that

$$\begin{aligned} S(R:\Gamma_2) &= S(R) + S(\Gamma_2) - S(R,\Gamma_2) \\ &= 2 + 2 - 2 = 2. \end{aligned} \tag{4.14}$$

Therefore, any two players form an intermediate set as $0 < S(R:\Gamma_2) < S(R:X)$.

So far, I have shown that the quantum mutual information is an important tool for determining an intermediate structure in quantum ramp secret sharing. The quantum mutual information can tell us whether or not some information on the secret is leaked to a subset of players. Now, consider how to characterize the leaked information. The characterization of leaked information is important because if the leaked information includes any useful clue on the secret it might be possible to narrow down the range of the secret significantly. I investigate whether or not the information leakage includes any quantum information. The quantum mutual information is not suitable for this problem, as it cannot distinguish quantum from classical information. It just measures both classical and quantum information together. To solve this problem, first I need to clearly define classical and quantum information in quantum ramp secret sharing. In [57], it was shown that classical and quantum information can be defined by incompatible *types* of information. Based on this definition, the leaked information can be characterized for the stabilizer encoding through the notion of an information group [39]. Let me briefly explain this method below.

In [57], it was shown that quantum information has different types corresponding to decompositions of the identity on a Hilbert space. A decomposition of the identity can be represented by a collection of mutually orthogonal projectors $\mathcal{J} = \{J_i\}$ where $I = \sum_j J_j$ and $J_j^\dagger = J_j = J_j^2$. For example, on a two-dimensional Hilbert space, there are two possible decompositions,

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \quad \text{and} \quad I = |+\rangle\langle +| + |-\rangle\langle -| \tag{4.15}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Then, $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ can be called the Z type and the X type of information, respectively. This means that one can determine whether a state is $|0\rangle$ or $|1\rangle$ ($|+\rangle$ or $|-\rangle$) by measuring Z (X).

Given a mapping $\mathcal{E} : \mathcal{L}(\mathscr{H}) \rightarrow \mathcal{L}(\mathscr{H}')$ where $\mathcal{L}(\mathscr{H})$ is the space of operators on the Hilbert space, the $\mathcal{J}$ type of information in $\mathscr{H}$ will be perfectly presented after the mapping if the output operators are all orthogonal with respect to $\{J_j\}$, i.e., $\mathcal{E}(J_j)\mathcal{E}(J_k) = 0$ for $j \neq k$. On the other hand, it will be absent after the mapping if $\mathcal{E}(J_j)$ is independent of j. More precise details were presented in [57].

Gheorghiu, Looi and Griffiths defined an information group $\mathcal{G}$ that represents the types of information in the coding space [39]. Some elements of this group might disappear by tracing out the subset of carriers Γ (equivalently, players in a secret sharing context), and the remaining elements form a subgroup of $\mathcal{G}$. Then, this subgroup represents what types of information are present in the complement of Γ [39].

Classical information is defined as a single type of information or equivalently, all compatible types of information [57]. Note that two types $\mathcal{J}$ and $\mathcal{J}'$ are compatible if all J_i commute with all J'_j. In this sense, if the types of information contained in a subset of carriers are all compatible, the information can be said to be classical. Otherwise, the subset contains quantum information. For example, in the $[[4, 2, 2]]$ stabilizer encoding, the types of information that are present in any two carriers are all compatible, and hence they contain only classical information [39].

The information group can characterize the information that appears in a subset of carriers for the stabilizer encoding. However, precise knowledge of the encoding operation (e.g., stabilizers) is required to generate the information group. It turns out that this method is not valid given the encoding operation is a black box (i.e., in this case, one must play only with inputs and outputs of the operation). In fact, it is not easy to characterize leaked information directly from the density matrix that is obtained after the operation. Thus, in the next section, I propose an indirect way to determine whether leaked information is classical or quantum by embedding the encoding operation of a quantum ramp secret sharing scheme in the bipartite setting of entanglement sharing.

4.2 A New Secrecy Condition of QRSS with Entanglement Sharing

Entanglement is the one way to realize a quantum channel. Quantum correlation that is inherent in entanglement enables us to achieve quantum communication. For example, in quantum teleportation, one party can transmit an arbitrary quantum state to another party by sharing a maximally entangled state and communicating two classical bits [6]. The terminology "quantum correlation" is justified by the observation that entangled states violate Bell's inequalities derived from hidden parameters [4]. On the other hand, separable states refer to classical correlation as they can be classically prepared by LOCC, and satisfy the Bell's inequalities [41]. A classical channel can be realized by separable states.

In this section, I define classical and quantum information with respect to what kind of channels information is transmitted through. Generally, we consider quantum information to include classical information. However, if quantum information can be transmitted through a classical channel, it will be effectively classical. Thus, I regard the transmitted information as classical information. On the other hand, if quantum information can be transmitted through a quantum channel but not through any classical channel, I will consider it quantum. These definitions can be understood in the following context.

Imagine a circuit implementing quantum teleportation, which successfully operates when a maximally entangled state is input. Alice inputs her quantum state to this circuit, and then the circuit outputs to Bob a density matrix associated with the input state. Given a maximally entangled state, the output density matrix is identical to the input state. If a product state is inserted instead of the maximally entangled state, this circuit will output the identity matrix and Bob cannot get any information about Alice's quantum state. The more interesting case is a separable state. If a separable state replaces the maximally entangled state, this circuit cannot achieve teleportation perfectly. For example, Alice inputs an arbitrary quantum state $|\phi\rangle_S = \alpha|0\rangle_S + \beta|1\rangle_S$ with a separable state given by

$$\rho_{SR} = \frac{1}{2}\Big(|0\rangle\langle 0|_S \otimes |0\rangle\langle 0|_R + |1\rangle\langle 1|_S \otimes |1\rangle\langle 1|_R\Big). \tag{4.16}$$

Then, the circuit outputs a density matrix,

$$\rho_R = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|. \tag{4.17}$$

Now, Bob has some information about the amplitudes of $|\phi\rangle_S$, but learns nothing about the relative phase of the amplitudes. According to my definitions, quantum information cannot be transmitted at all but only classical information appears in the output density matrix when any separable state is input into the quantum teleportation circuit. The method to classify information in the context of quantum teleportation is useful to determine the presence of quantum information in output states without ambiguity, as it relies on the clear definitions of bipartite states.

Let me revisit the $[[4,2,2]]$ stabilizer code. The $[[4,2,2]]$ stabilizer code is not only used to devise an optimal entanglement sharing scheme but also for a $(3,2,4)$ quantum ramp secret sharing scheme. Suppose that the optimal entanglement sharing scheme using the $[[4,2,2]]$ stabilizer code is applied to share a maximally entangled state in the quantum teleportation circuit. A dealer inputs his secret state into the circuit and encodes the maximally entangled state into four shares by the optimal entanglement sharing scheme. Each share is given to a player. Then, any three players can receive the secret fully through this circuit by recovering the original maximally entangled state from three shares and any single player is totally denied any information about the secret with a product state. On the other hand, any two players obtain only classical information after the circuit, as they cannot recover any entanglement with the dealer in this scheme. This observation corresponds to the result of [39], and it can extend to any quantum ramp secret sharing scheme.

Consider a quantum ramp secret sharing scheme that has the encoding operation $C : |j\rangle_{\mathrm{D}} \rightarrow |C_j\rangle_{\mathrm{P}}$. In this scheme, the encoded state $|C_j\rangle_{\mathrm{P}}$ is distributed among a set of players P. At first, prepare a maximally entangled state,

$$|S\rangle = \frac{1}{\sqrt{|C|}} \sum_j |j\rangle_{\mathrm{D}} |j\rangle_{\mathrm{D}}. \tag{4.18}$$

Then, half of $|S\rangle$ is left to a dealer D and the other half is encoded by the encoding operation C,

$$|\Psi\rangle = (I_{\mathrm{D}} \otimes C)|S\rangle|00\ldots0\rangle = \frac{1}{\sqrt{|C|}} \sum_j |j\rangle_{\mathrm{D}} |C_j\rangle_{\mathrm{P}} \tag{4.19}$$

where $|00\ldots0\rangle$ is an ancilla. Now, every intermediate set $\Gamma \in P$ obtains the reduced density matrix ρ^{Γ} after the operation. Next, check ρ^{Γ} for any entanglement between two parties D and Γ. If ρ^{Γ} has some entanglement with the dealer, Γ can get some quantum information from the dealer through a quantum teleportation circuit. This means that the encoding operation C leaks some quantum information to Γ. Otherwise, Γ is totally denied any quantum information. In this sense, I can propose a secrecy condition of quantum ramp secret sharing as follows.

Definition 4.2.1. *Given an encoding operation $C : \mathscr{H}_D \to \mathscr{H}_P$ mapping*

$$(I_D \otimes C) : |S\rangle = \frac{1}{\sqrt{|C|}} \sum_j |j\rangle_D |j\rangle_D \to |\Psi\rangle = \frac{1}{\sqrt{|C|}} \sum_j |j\rangle_D |C_j\rangle_P, \tag{4.20}$$

a quantum ramp secret sharing scheme described by C is secure from the leakage of quantum information if the reduced density matrix for every intermediate set $\Gamma \in P$, $\rho^{\Gamma} = tr_{\overline{\Gamma}}(|\Psi\rangle\langle\Psi|)$, is separable with the system D.

Furthermore, one might use entanglement measures to quantify how much quantum information is leaked, with respect to the amount of entanglement.

4.3 Summary

Quantum ramp secret sharing has the advantage of a small size of shares, but it necessarily leaks some information about a secret to intermediate sets. Characterizing the leaked information is one of the important issues in this field, as it is closely related to the secrecy of schemes. In this chapter, I addressed the problem of whether the leaked information is classical or quantum. First, I investigated the quantum mutual information and the method of an information group. The quantum mutual information well defines the intermediate sets, but it is not suitable to distinguish quantum from classical information. For the stabilizer encoding, it is possible to precisely characterize information from the subgroups of an information group, but this method requires some details of the encoding operation to generate the information group.

I dealt with this problem using entanglement sharing. First, I defined classical and quantum information separately with respect to classical and quantum channels. The idea is that quantum communication cannot be achieved with only classical channels. Then, I showed that the leakage of quantum information can be assessed by embedding a quantum ramp secret sharing scheme into the bipartite setting of entanglement sharing. Finally, I proposed a new secrecy condition of quantum ramp secret sharing.

Chapter 5

Hybrid Entanglement Sharing

In this chapter, I introduce *hybrid entanglement sharing*, which combines non-perfect entanglement sharing with classical secret sharing. Non-perfect entanglement sharing schemes leak some entanglement to unauthorized sets. However, it is possible to lock the leaked entanglement using a classical key. Classical secret sharing can distribute the key among a set of players in such a way that any unauthorized set is totally denied any access to entanglement. A similar technique was applied to non-perfect quantum secret sharing [58], and was generalized in [59].

In Sec. 5.1, I start by introducing non-perfect entanglement sharing schemes with an example that exploits the $[[6, 4, 2]]$ stabilizer code. Then, in Sec. 5.2, I introduce a technique that encrypts entanglement using classical information. Finally, in Sec. 5.3 I devise hybrid entanglement sharing schemes by introducing the technique in non-perfect entanglement sharing schemes.

5.1 Non-perfect Entanglement Sharing Schemes

As in quantum secret sharing, quantum error correcting codes are good candidates for the encoding operations in entanglement sharing as their coding spaces naturally yield access structures. As I showed in Chapter 3, the Shor 9-qubit code and the $[[4, 2, 2]]$ stabilizer code are indeed used to devise entanglement sharing schemes. However, not all quantum error correcting codes are suitable for entanglement sharing. Some quantum error correcting codes might leak partial entanglement to unauthorized sets. The entanglement leakage leads to non-perfect entanglement sharing schemes.

Non-perfect entanglement sharing mainly occurs when the underlying quantum error correcting code has a coding space of large dimension. The dimension of the coding space is directly related to the amount of initial entanglement. For example, a 2^k-dimensional coding space corresponds to k ebits of the initial entanglement, i.e., $E(\rho^{\mathrm{DP}}) = k$. In Sec. 3.3, I mentioned that a share r of one qubit acts as a key that locks at most the initial entanglement of two ebits (i.e., $k = 2$). If more than two ebits are initially shared, however, the important share cannot lock the entire amount of the initial entanglement. Thus, an unauthorized set will get some entanglement after discarding the share r from an authorized set.

Consider a non-perfect entanglement sharing scheme which is devised using the $[[6,4,2]]$ stabilizer code. A dealer encodes a maximally entangled state of four ebits by the $[[6,4,2]]$ code such that

$$\frac{1}{4}\sum_{i=1}^{16}|i\rangle|i\rangle \mapsto \frac{1}{4}\sum_{i=1}^{16}|i\rangle|\beta_{f(i)}\rangle|\beta_{g(i)}\rangle|\beta_{f(i)+g(i)}\rangle \tag{5.1}$$

where $f(i)$, $g(i) = \{0,1,2,3\}$ and $\{|\beta_j\rangle\}$ are Bell states. Note that each qubit in the code is allocated to a player. Threshold scheme arises because the stabilizer elements of the code are invariant under permutation, i.e., $S = \{XXXXXX, ZZZZZZ\}$.

Any five players can recover the original entanglement as this stabilizer code can correct erasure errors on a single qubit. However, the amount of initial entanglement is too large to be reduced to zero by discarding one player from the five players. Even though one player is excluded, some entanglement remains between any four players and the dealer. The reduced density matrix of four players indeed violates the PPT criterion. In the next section, I explain how to lock the remaining entanglement.

5.2 Locking of Entanglement with Classical Information

In this section, I show how to lock entanglement using classical information. In fact, classical information has been used to encrypt a quantum secret [58] [59]. Let us consider the following example. In quantum teleportation, Alice teleports an arbitrary quantum state $|\psi\rangle$ to Bob by communicating two classical bits, given a previously shared entanglement. As Alice performs a joint measurement on $|\psi\rangle$ and half of the entanglement, Bob's state is collapsed into one of the four states $|\psi\rangle$, $(X|\psi\rangle)$, $(Z|\psi\rangle)$ or $(XZ|\psi\rangle)$ with equal probability. Each state corresponds to the measurement outcome of two classical bits. Before communicating the classical bits, Bob's qubit is left in a maximally mixed state,

$$\frac{1}{4}(|\psi\rangle\langle\psi| + X|\psi\rangle\langle\psi|X + Z|\psi\rangle\langle\psi|Z + XZ|\psi\rangle\langle\psi|ZX). \tag{5.2}$$

However, with the knowledge of the two classical bits, he can determine into which state his qubit has been collapsed, and recover $|\psi\rangle$. In this example, classical bits act like a key that is used to encrypt and decrypt the quantum state. Similarly, entanglement can be encrypted by a classical key.

Consider a maximally entangled state in a bipartite system of two 2^k-dimensional Hilbert spaces $\mathscr{H}_A \otimes \mathscr{H}_B$,

$$|S\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |a_j\rangle|b_j\rangle. \tag{5.3}$$

Here, I introduce an unitary mapping $U^l : \mathscr{H}_A \otimes \mathscr{H}_B \to \mathscr{H}_A \otimes \mathscr{H}_B$ such that

$$U^l : |S\rangle \mapsto |S^l\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} \alpha_{jl}|a_j\rangle|b_j\rangle \tag{5.4}$$

where $\alpha_{jl} = \exp(2i\pi jl/2^k)$ and $l \in \mathbf{Z}_{2^k}$ is randomly chosen. As in quantum teleportation, the entanglement $|S^l\rangle$ is totally randomized without knowing the classical information l, as follows.

$$\begin{aligned}\rho^S &= \sum_{l=0}^{2^k-1} |S^l\rangle\langle S^l| \\ &= \frac{1}{2^k}\sum_{j,j'=0}^{2^k-1}\Big(\sum_{l=0}^{2^k-1} e^{i\frac{2\pi(j-j')l}{2^k}}\Big)|a_j\rangle\langle a_{j'}| \otimes |b_j\rangle\langle b_{j'}| \\ &= \frac{1}{2^k}\sum_{j,j'=0}^{2^k-1} \delta(j-j')|a_j\rangle\langle a_{j'}| \otimes |b_j\rangle\langle b_{j'}| \\ &= \frac{1}{2^k}\sum_{j=0}^{2^k-1} |a_j\rangle\langle a_j| \otimes |b_j\rangle\langle b_j|.\end{aligned} \tag{5.5}$$

Now, the bipartite system can be written in terms of separable states. That is, the classical information effectively encrypts the maximal entanglement. Also, the encrypted entanglement can be always decrypted with knowledge of the classical information used for encryption. In the next section, I use this technique to lock leaked entanglement in a non-perfect entanglement sharing scheme.

5.3 Construction of Hybrid Entanglement Sharing Schemes

In hybrid entanglement sharing schemes, the essential idea to lock leaked entanglement is to encrypt the initial entanglement by a classical key and distribute the key such that any unauthorized set is totally denied the key. This can be achieved by classical secret sharing. Hybrid schemes distribute the encrypted entanglement and a classical key using entanglement sharing and classical secret sharing, respectively. That is, each player receives both quantum and classical shares. Then, any authorized set can recover the initial entanglement by knowing the classical key, but unauthorized sets cannot have any access to the entanglement without knowing the classical key. If the entanglement sharing scheme used to distribute the encrypted entanglement is non-perfect, the unauthorized sets might have some entanglement without hybridizing. However, distribution of a classical key effectively locks the leaked entanglement in hybrid schemes. In this sense, the hybrid schemes can be understood like "double doors". Even though the inner door is a little bit open, one cannot enter the room without passing the outer door. Now, I implement a hybrid scheme from any given quantum error correcting code, as follows.

1. A dealer prepares a maximally entangled state
$$|S\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |j\rangle|j\rangle$$
in the bipartite system $\mathscr{H}_{\mathrm{D}} \otimes \mathscr{H}_{\mathrm{D}}$ where $\mathscr{H}_{\mathrm{D}}$ is a 2^k-dimensional Hilbert space.

2. The dealer is given a quantum error correcting code that encodes k in n qubits. Its coding space C induces an access structure Q; e.g., for a $[[n,k,d]]$ stabilizer code, Q consists of any $n-d+1$ or more shares. Then, the dealer encodes half of $|S\rangle$ in the coding space C by mapping
$$|S\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |j\rangle|j\rangle \mapsto |\Psi\rangle = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} |j\rangle|C_j\rangle$$
where $C = \mathrm{span}\{C_j\}_{j=0\cdots 2^k-1}$.

3. The dealer selects a classical key l randomly in $\mathbf{Z}_{2^k}$ and performs U^l on $|\Psi\rangle$. Then, the dealer has
$$\frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^k-1} e^{i\frac{2\pi jl}{2^k}} |j\rangle|C_j\rangle.$$
Now, the dealer takes the last n qubits as quantum shares.

4. The dealer encodes the classical key l in n classical shares using a classical secret sharing scheme with an access structure $Q' \subseteq Q$.

5. Classical and quantum shares are separately distributed among n players. If a subset of players is an element of Q', they can recover both the classical key l and the initial maximally entangled state $|S\rangle$. Otherwise, they cannot have any entanglement with the dealer.

Hybrid entanglement sharing makes construction and verification of secrecy easier than entanglement sharing. For entanglement sharing, it is comparatively hard to verify its secrecy because it is very difficult to determine whether or not a given density matrix is separable. Also, not all quantum error correcting code can be used to construct entanglement sharing schemes. However, hybrid entanglement sharing can be constructed from any quantum error correcting code by choosing suitable classical secret sharing schemes. This can be achieved, for instance, by simply using polynomial functions [17] [18]. Furthermore, its secrecy is easily determined according to whether or not every unauthorized set is denied any information about the classical key.

5.4 Summary

In this chapter, I proposed a method for locking leaked information in non-perfect entanglement sharing schemes. Entanglement can be locked by classical information through unitary operations. I showed that unauthorized sets of players can be effectively excluded from getting access to entanglement by properly distributing the classical information among players. The distribution of classical information can be achieved by classical secret sharing. Then, I presented how to construct hybrid entanglement sharing schemes from any quantum error correcting codes. This construction is summarized as follows.

First, a dealer encodes a maximally entangled state in a given coding space, and then performs a unitary operation on the encoded entanglement with respect to a randomly selected classical key. Without knowing the key, the resultant state is totally randomized and becomes a separable state. The classical key is distributed among a set of players by a properly selected classical secret sharing scheme, in such a way that only authorized sets of players can get the key and recover the original entanglement, but other sets are totally denied any access to the entanglement.

Chapter 6

Conclusions and Future Work

Quantum secret sharing is one of the most important cryptographic protocols, which is closely related to quantum error correction. The main results of quantum secret sharing naturally follow from the theory of quantum error correction. Moreover, quantum secret sharing schemes can be constructed from quantum error correcting codes.

In this thesis, I introduced a new cryptographic protocol that shares a maximally entangled state with a set of players in such a way that some sets of players are authorized to recover the original entangled state fully, but the other sets are totally denied any entanglement. This protocol is called "entanglement sharing". As in quantum secret sharing, quantum error correcting codes play a crucial role in entanglement sharing. I constructed entanglement sharing based on the existing stabilizer code, and found two examples of entanglement sharing using the Shor's 9-qubit code and the $[[4,2,2]]$ stabilizer code, respectively. In each example, the secrecy was verified by directly computing the reduced density matrix of each subset of players. I used permutation invariance in stabilizers and monogamy of entanglement to reduce the number of computations. In particular, I derived from monogamy that an access structure in entanglement sharing cannot have two disjoint sets. Also, I proved by using the lockability of the relative entropy of entanglement that the size of shares must be at least half the amount of initial entanglement (Theorem 3.3.1). An entanglement sharing scheme is said to be optimal if it has the minimum size of shares with respect to the initial amount of entanglement. Then, I showed that the $[[4,2,2]]$ stabilizer code induces an optimal entanglement sharing scheme with a threshold access structure.

With the bipartite setting of entanglement sharing, I proposed a new secrecy condition of quantum ramp secret sharing. In quantum ramp secret sharing, one of the important issues is characterizing the leaked information. Particularly, I focused on how to determine whether the leaked information is classical or quantum. Intermediate sets were clearly described by the quantum mutual information by extending the description of quantum secret sharing in [38]. However, the quantum mutual information was not suitable to determine what kind of information is leaked, as the mutual information cannot distinguish between classical and quantum information but measures both at the same time. For the stabilizer encoding, the leaked information can be characterized using the notion of an information group [39]. This method seemed to provide a precise characterization of leaked information, but it required details of the underlying encoding operation. From a practical point of view, it might be more desirable to examine leaked information with only input and output states of the encoding operation because it is not easy to fully characterize quantum operations in general.

I came up with a new approach that can be applied to any quantum ramp secret sharing without requiring details of its encoding operation. I first defined quantum information as the information that can be transmitted through a quantum channel, but not through a classical channel. Quantum and classical channels can be realized by entangled and separable states, respectively. Thus, I examined the bipartite states of intermediate sets by embedding quantum ramp secret sharing into the bipartite setting of entanglement sharing. This led to the secrecy condition that every intermediate set must not have any entangled state with a dealer in order for a quantum ramp secret sharing scheme to be secure from leakage of quantum information. Under this condition, I showed that the $[[4,2,2]]$ stabilizer code does not leak any quantum information and this corresponds to the result of [39].

At this point, I remark that the proposed secrecy condition is in fact equivalent to the secrecy condition of entanglement sharing, as shown in the case of the $[[4,2,2]]$ stabilizer code. This means that every quantum error correcting code used for entanglement sharing is a quantum ramp scheme which is secure against quantum leakage. Similarly, every quantum error correcting code corresponding to quantum secret sharing is a strict case of entanglement sharing, in which unauthorized sets have only product states. These relationships are summarized in Fig. 6.1

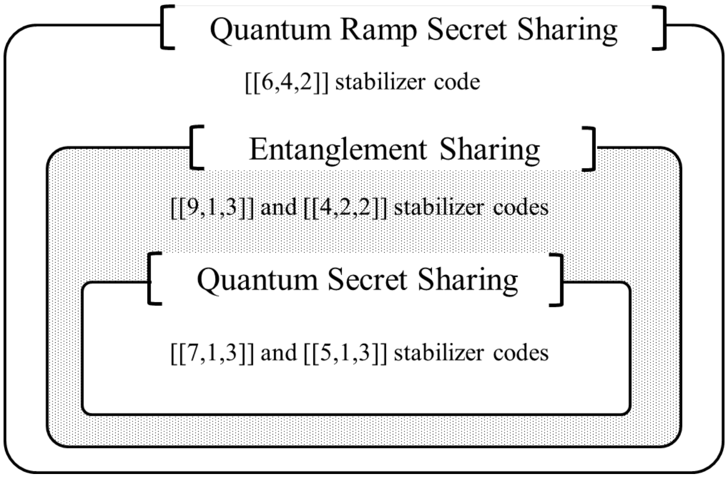
Quantum Ramp Secret Sharing
[[6,4,2]] stabilizer code
Entanglement Sharing
[[9,1,3]] and [[4,2,2]] stabilizer codes
Quantum Secret Sharing
[[7,1,3]] and [[5,1,3]] stabilizer codes

Figure 6.1: Relationship among entanglement sharing, quantum secret sharing and quantum ramp secret sharing schemes in terms of quantum error correcting codes. Some existing stabilizer codes are given as examples.

Next, I hybridized entanglement sharing to make construction and verification of its secrecy easier alternatively. In hybrid schemes, a maximally entangled state was locked by classical information and the classical information was properly distributed using classical secret sharing. Any unauthorized set was left in a separable state with a dealer because it could not recover any information about the classical information. Hybrid entanglement sharing can be constructed from any quantum error correcting code.

Finally, I give some suggestion for a future work. The structure of quantum error correcting codes determines whether the induced entangled sharing scheme is perfect or non-perfect, or whether it is a threshold scheme or a scheme with a general access structure. In this sense, future work can move the research toward the precise relationship between quantum error correcting codes and entanglement sharing schemes. We might consider the relationship in stabilizer formalism because it can provide a more compact picture to understand the structure of a code.

Bibliography

[1] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 124 (1994)

[2] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175 (1984)

[3] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991)

[4] J. S. Bell, On the Einstein Podolsky Rosen Paradox, Physics **1**, 195 (1964)

[5] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880 (1969)

[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. **70**, 1895 (1993)

[7] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. **69**, 2881 (1992)

[8] A. Acín, N. Brunner, N. Gisin, S. Pironio and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007)

[9] L. Masanes, S. Pironio and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nature Communications **2**,

238 (2011)

[10] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature **402**, 390 (1999)

[11] E. Knill, R. Laflamme and G. J. Milburn, A scheme for efficient quantum computation with linear optics, Nature **409**, 46 (2001)

[12] D. T. Pegg, L. S. Phillips and S. M. Barnett, Optical state truncation by projection synthesis, Phys. Rev. Lett. **81**, 1604 (1998)

[13] S. A. Babichev, J. Ries and A. I. Lvovsky, Quantum scissors: teleportation of single-mode optical states by means of a nonlocal single photon, Europhysics Letters **64**, 1 (2003)

[14] M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert, "Event-ready-detectors" Bell experiment via entanglement swapping, Phys. Rev. Lett. **71**, 4287 (1993)

[15] N. Zhou, G. Zeng and J. Xiong, Quantum key agreement protocol, Electronics Letters **40**, 18, 1149 (2004)

[16] R. Cleve, D. Gottesman, H.-K. Lo, How to share a quantum secret, Phys. Rev. Lett. **83**, 648 (1999)

[17] A. Shamir, How to share a secret, Commumications of the ACM **22**, 612 (1979)

[18] G. R. Blakley, Safeguarding cryptographic keys, AFIPS Conference Proceeding **48**, 313-317 (1979)

[19] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, Proceedings of CRYPTO '88, Lecture Notes in Computer Science **403**, Springer Berlin, 27 (1990)

[20] D. Gottesman, Theory of quantum secret sharing, Phys. Rev. A **61**, 042311 (2000)

[21] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008)

[22] M. Hillery, V. Bužek and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999)

[23] A. Karlsson, M. Koashi and N. Imoto, Quantum entanglement for secret sharing and secret splitting, Phys. Rev. A **59**, 162 (1999)

[24] L. Xiao, G. L. Long, F-G. Deng and J-W. Pan, Efficient multiparty quantum-secret-sharing schemes, Phys. Rev. A **69**, 052307 (2004)

[25] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum cryptography, Review of Modern Physics **74**, 145 (2002)

[26] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders and P. K. Lam, Continuous variable $(2, 3)$ threshold quantum secret sharing schemes, New Journal of Physics **5**, 4 (2003)

[27] A. M. Lance, T. Symul, W. Bowen, B. C. Sanders and P. K. Lam, Tripartite quantum state sharing, Phys. Rev. Lett. **92**, 177903 (2004)

[28] D. Gottesman, Stabilizer codes and quantum error correction, quant-ph/9705052, Caltech Ph. D. thesis

[29] E. Karnin, J. Green and M. Hellman, On secret sharing systems, IEEE Transaction on Information Theory **29**, 35 (1982)

[30] R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, Journal of Cryptology **6**, 157 (1993)

[31] K. Kurosawa, K. Okada, K. Sakano, W. Ogata and S. Tsujii, Nonperfect secret sharing schemes and matroids, Proceedings of EUROCRYPT '93, Lecture Notes in Computer Science **765**, Springer Berlin, 126 (1993)

[32] G. R. Blakley and C. Meadows, Security of ramp schemes, Advances in Cryptology, Proceedings of CRYPTO '84, Lecture Notes in Computer Science **196**, Springer Berlin, 242 (1985)

[33] H. Yamamoto, Secret sharing system using (k, L, n) threshold scheme, Electronics and Communications in Japan (Part I: Communications) **69**, 46 (1986)

[34] T. Ogawa, A. Sasaki, M. Iwamoto and H. Yamamoto, Quantum secret sharing schemes and reversibility of quantum operations, Phys. Rev. A **72**, 032318 (2005)

[35] C. Blundo, A. De Santis and U. Vaccaro, Efficient sharing of many secrets, Proceedings of STACS '93, Lecture Notes in Computer Science **665**, Springer Berlin, 692 (1993)

[36] A. S. Holevo, Some estimates for information quantity transmitted by quantum communication channel, Problems of Information Transmission **9**, 3 (1973)

[37] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Locking entanglement with a single qubit, Phys. Rev. Lett. **94**, 200501 (2005)

[38] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls and A. Winter, A quantum information theoretical model for quantum secret sharing schemes, quant-ph/0311136 (2003)

[39] V. Gheorghiu, S. Y. Looi and R. B. Griffiths, Location of quantum information in additive graph codes, Phys. Rev. A **81**, 032326 (2010)

[40] M. A. Nielsen and I. L. Chuang, Quantum comutation and quantum information, Cambridge University Press, Cambridge, (2000)

[41] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989)

[42] A. Einstein, B. Podolsky and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. **47**, 777 (1935)

[43] M. B. Plenio and S. Virmani, An introduction to entanglement measures, Quantum information & Computation **7**, 1, (2007)

[44] L. Gurvits. Classical deterministic complexity of edmonds problem and quantum entanglement, Proceedings of the 35th ACM symposium on Theory of computing, STOC'03, ACM Press, 10 (2003)

[45] A. Peres, Separability criterion for density matrices, Phys. Rev. Lett. **77**, 1413 (1996)

[46] M. Horodecki, P. Horodecki and R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996)

[47] C. E. Shannon, A mathematical theory of communication, Bell System Technical Journal **27**, 379 (1948)

[48] V. N. John, Mathematical foundation of quantum mechanics, Princeton University Press, Princeton (1996)

[49] M. Franklin and M. Yung, Communication complexity of secure computation, Proceedings of the 24th annual ACM symposium on Theory of computing, STOC'92, ACM Press, 699 (1992)

[50] P. W. Shor, Scheme for reducing decohoerence in quantum computer memory, Phys. Rev. A **52**, 2493 (1995)

[51] E. Knill and R. Laflamme, A theory of quantum error correcting codes, Phys. Rev. A **55**, 900 (1997)

[52] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Mixed state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996)

[53] V. Coffman, J. Kundu and W. K. Wootters, Distributed entanglement, Phys. Rav. A **61**, 052306 (2000)

[54] M. Koashi and A. Winter, Monogamy of entanglement and other correlations, Phys. Rev. A **69**, 022309 (2004)

[55] N. Linden, S. Popescu, B. Schumacker and M. Westmoreland, Reversibility of local transformations of multiparticle entanglement, quant-ph/9912039

[56] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, Phys. Rev. A **54**, 2629 (1996)

[57] R. B. Griffiths, Types of Quantum Information, Phys. Rev. A **76**, 062320 (2007)

[58] B. Fortescue and G. Gour, Reducing the quantum communication cost of quantum secret sharing, IEEE Transactions on Information Theory **PP**, 99, 1, (2012)

[59] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Improving quantum secret-sharing schemes, Phys. Rev. A **64**, 042311 (2001)

Appendix A

Investigation of Shor's code

In this appendix, I supplement Sec. 3.2 by investigating other sets in $\{B\}$. Recall the mapping in Eq. 3.7 according to the Shor's 9-qubit code.

$$|S\rangle \mapsto |\Psi\rangle = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} |j\rangle_{\mathrm{D}} |G_j\rangle_{123} |G_j\rangle_{456} |G_j\rangle_{789}. \tag{A.1}$$

As I show in Sec. 3.2, the reduced density matrix for $\{1, 2, 3, 4, 5, 6\}$ has a separable form. The reduced density matrices for $\{1, 2, 3, 7, 8, 9\}$ and $\{4, 5, 6, 7, 8, 9\}$ are also separable with a dealer D due to a permutation on the triplets. I define two subsets of players to be equivalent if the reduced density matrix of one subset can be obtained from the other by the permutation on the triplets. In this sense, the complements of $\{1, 2, 3, 4, 5, 6\}$, $\{1, 2, 3, 7, 8, 9\}$ and $\{4, 5, 6, 7, 8, 9\}$ are equivalent to each other so I look at only the complement of $B = \{1, 2, 3, 4, 5, 6\}$. In fact, the reduced density matrix for $\bar{B} = \{7, 8, 9\}$ (equivalently, for $\{1, 2, 3\}$ and $\{4, 5, 6\}$) is a separable state with the dealer, as shown as

$$\frac{1}{2} \sum_{i=0}^{1} |i\rangle\langle i|_{\mathrm{D}} \otimes |G_i\rangle\langle G_i|_{789}. \tag{A.2}$$

I regard these six sets as a class of $\{1, 2, 3\}$. Similarly, it is possible to define other classes in $\{B\}$. Note that a class of B consists of the equivalent sets of B and the complement of B. Every set in $\{B\}$ is classified into one of the following classes:

1. $\{1, 2, 3\}$

2. $\{1, 4, 7\}$

3. $\{1, 2, 3, 4\}$

4. $\{1, 4, 7, 8\}$

Let $\bar{B}$ denote the complement of B. For a class of B, it is enough to check whether or not the reduced density matrices of B and $\bar{B}$ are separable with the dealer D.

Let us look at the class of $\{1,4,7\}$. For the complement of $\{1,4,7\}$, the reduced density matrix of is a separable state, written as

$$\frac{1}{2}\Big(|+\rangle\langle+|_{\mathrm{D}}\otimes\rho_{235689}+|-\rangle\langle-|_{\mathrm{D}}\otimes\rho'_{235689}\Big) \tag{A.3}$$

where $|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{D}}\pm|1\rangle_{\mathrm{D}})$,

$$\rho_{235689}=\frac{1}{4}\Big(|000000\rangle\langle000000|+|001111\rangle\langle001111|+|110011\rangle\langle110011|+|111100\rangle\langle111100|\Big) \tag{A.4}$$

and

$$\rho'_{235689}=\frac{1}{4}\Big(|000011\rangle\langle000011|+|001100\rangle\langle001100|+|110000\rangle\langle110000|+|111111\rangle\langle111111|\Big). \tag{A.5}$$

Even when discarding three more qubits $\{2,5,8\}$ from Eq. A.3, the resulting density matrix (i.e., a reduced density matrix of $\{3,6,9\}$) still has a separable form. Note that $\{1,4,7\}$ is equivalent to $\{3,6,9\}$. Thus, all sets in this class are equivalently separable with the dealer.

Next, consider the class of $\{1,2,3,4\}$. The reduced density matrix for the complement of $\{1,2,3,4\}$ is given by

$$\frac{1}{2}\Big(\sum_{i=0}^{1}|i\rangle\langle i|_{\mathrm{D}}\otimes|G_i\rangle\langle G_i|_{789}\Big)\otimes\frac{1}{2}\Big(|00\rangle\langle00|_{56}+|11\rangle\langle11|_{56}\Big). \tag{A.6}$$

Here, $\{7,8,9\}$ is separable with the dealer, no matter whether or not $\{5,6\}$ is involved; $\{5,6\}$ is independent of other qubits. Thus, the separable form holds for the reduced density matrix of $\{6,7,8,9\}$. $\{6,7,8,9\}$ is equivalent to $\{1,2,3,4\}$.

Finally, consider the class of $\{1,4,7,8\}$. By tracing out $\{8\}$ from Eq. A.3, it is easily shown that the reduced density matrix of $\{2,3,5,6,9\}$ is a separable state with the dealer. The density matrix is still a separable state even after discarding $\{5\}$ again. As

$\{1,4,7,8\}$ is equivalent to $\{2,3,6,9\}$, the sets in this class are all separable with the dealer.

From all these cases, I conclude that any set of players has either authorized or unauthorized. The authorized sets can recover the maximally entangled state with the dealer: any 7, 8 and 9 players; $\{1,2,3,4,5,7\}$ and its equivalent sets; $\{1,2,3,4,7\}$ and its equivalent sets. Some unauthorized sets have a separable state with the dealer: $\{1,2,3\}$, $\{1,4,7\}$, $\{1,2,3,4\}$, $\{1,2,4,7\}$, $\{1,2,3,4,5\}$, $\{1,2,4,5,7\}$, $\{1,2,3,4,5,6\}$, $\{1,2,4,5,7,8\}$ and all their equivalent sets. The other unauthorized sets have a product state: any one or two players; $\{1,2,4\}$ and its equivalent sets; $\{1,2,4,5\}$ and its equivalent sets. Thus, entanglement sharing using a $[[9,1,3]]$ stabilizer code has a general access structure.

Appendix B

A property of the relative entropy of entanglement

In this Appendix, I derive the following property of the relative entropy of entanglement used in Sec. 3.3 [55]:

$$\sum_i p_i E_R(\rho_i) - E_R(\sum_i p_i\rho_i) \leq S(\sum_i p_i\rho_i) - \sum_i p_i S(\rho_i). \tag{B.1}$$

First, recall that the quantum relative entropy of ρ with respect to σ is

$$S(\rho||\sigma) = \mathrm{tr}(\rho\log_2\rho) - \mathrm{tr}(\rho\log_2\sigma). \tag{B.2}$$

Suppose that ρ is a mixture of density matrices, expressed by $\rho = \sum_i p_i\rho_i$. Then, the quantum relative entropy can be rewritten as

$$\begin{aligned}
S(\rho||\sigma) &= \mathrm{tr}(\rho\log\rho) - \mathrm{tr}(\rho\log\sigma)\\
&= \mathrm{tr}\Big(\sum_i p_i\rho_i\log\rho\Big) - \mathrm{tr}\Big(\sum_i p_i\rho_i\log\sigma\Big)\\
&= \sum_i p_i\mathrm{tr}(\rho_i\log\rho) - \sum_i p_i\mathrm{tr}(\rho_i\log\sigma)\\
&= \Big(\sum_i p_i\mathrm{tr}(\rho_i\log\rho_i) - \sum_i p_i\mathrm{tr}(\rho_i\log\sigma)\Big) - \Big(\sum_i p_i\mathrm{tr}(\rho_i\log\rho_i) - \sum_i p_i\mathrm{tr}(\rho_i\log\rho)\Big)\\
&= \sum_i p_i S(\rho_i||\sigma) - \sum_i p_i S(\rho_i||\rho)
\end{aligned} \tag{B.3}$$

because $\mathrm{tr}(\sum_i p_i\rho_i\log[\cdot]) = \sum_i \mathrm{tr}(p_i\rho_i\log[\cdot]) = \sum_i p_i\mathrm{tr}(\rho_i\log[\cdot])$ according to the properties of trace.

Now, consider a density matrix $\rho^{AB} = \sum_i p_i\rho_i^{AB}$ on the bipartite system $H_A\otimes H_B$. Then, we have

$$\sum_i p_i S(\rho_i^{AB}||\sigma^{AB}) = \sum_i p_i S(\rho_i^{AB}||\rho^{AB}) + S(\rho^{AB}||\sigma^{AB}) \tag{B.4}$$

where σ^{AB} is a separable state on $H_A \otimes H_B$. The relative entropy of entanglement E_R is defined as the smallest quantum relative entropy from a bipartite density matrix ρ^{AB} to all possible separable states on the system (see Eq. 2.34). Let σ^{AB} be a closest separable state to ρ^{AB}, satisfying $E_R(\rho^{AB}) = S(\rho^{AB}||\sigma^{AB})$. Since $E_R(\rho_i^{AB}) \leq S(\rho_i^{AB}||\sigma^{AB})$, we can have

$$\sum_i p_i E_R(\rho_i^{AB}) - E_R(\rho^{AB}) \leq \sum_i p_i S(\rho_i^{AB}||\rho^{AB}) \tag{B.5}$$

By the definition of von Neumann entropy (see Eq. 2.26), the right side of the above inequality can be written as

$$\begin{aligned} \sum_i p_i S(\rho_i^{AB}||\rho^{AB}) &= \sum_i p_i \mathrm{tr}(\rho_i^{AB} \log \rho_i^{AB}) - \sum_i p_i \mathrm{tr}(\rho_i^{AB} \log \rho^{AB}) \\ &= \sum_i p_i \mathrm{tr}(\rho_i^{AB} \log \rho_i^{AB}) - \mathrm{tr}(\rho^{AB} \log \rho^{AB}) \\ &= S(\rho^{AB}) - \sum_i p_i S(\rho_i^{AB}) \end{aligned} \tag{B.6}$$

Taking Eq. B.6 in Eq. B.5, we can derive the property of Eq. B.1:

$$\sum_i p_i E_R(\rho_i^{AB}) - E_R(\rho^{AB}) \leq S(\rho^{AB}) - \sum_i p_i S(\rho_i^{AB}) \tag{B.7}$$

where $\rho^{AB} = \sum_i p_i \rho_i^{AB}$ on the bipartite system $H_A \otimes H_B$.