Secure quantum network code

In partial fulfillment of the requirements
for the degree of

Master of Mathematical Science

Thesis by

Seunghoan Song

(Student ID: 321701139)

Advisor: Prof. Masahito Hayashi

Graduate School of Mathematics
Nagoya University

January 17, 2019

はじめに

ネットワーク符号

ネットワーク上で情報を送ることは, 通信の基本的なタスクの一つである. ネットワーク通信を効率的に行う方法の一つとして, ネットワーク符号 (network coding) が提案された. ネットワーク符号とは, ネットワーク上の中間ノードが情報を伝達するだけでなく, 情報処理も行うようにした通信方式である. その量子拡張として, 量子ネットワーク符号は, 量子通信路や量子演算を行う中間ノードで構成されたネットワーク上で, 量子状態を送る通信方式である.[*1] 量子ネットワーク符号は, Hayashi ら [10] によって提案された後, 多く研究されている [10, 11, 12, 14, 15, 13].

セキュア量子ネットワーク符号

ネットワーク符号を実際のネットワーク通信に用いるためには, ネットワーク符号のセキュリティーについて議論する必要がある. 文献 [7] は, 古典ネットワーク符号の秘匿性について初めて研究し, ネットワーク符号を使うことによって秘匿性が向上することを示した. 一方, 文献 [9] は, ネットワークを漸近的[*2]に使うことによって, 誤りを訂正するネットワーク符号を設計した. ネットワーク通信効率 m_0 が誤りのある通信路の最大数 m_1 より大きいとき ($m_1 < m_0$), 文献 [9] のネットワーク符号は符号化率[*3] $m_0 - m_1$ で漸近的に誤りを訂正する. さらに, 文献 [18] は文献 [9] の結果を拡張し, 秘匿性も得られるようにした: 前に定義された m_0, m_1 と情報漏れのある通信路の最大数 m_2 が $m_1 + m_2 < m_0$ を満たすとき, 文献 [18] のネットワーク符号は, 符号化率 $m_0 - m_1 - m_2$ で漸近的に誤りを訂正し, 漸近的に秘匿性を保証する.

一方, 量子ネットワーク符号のセキュリティに関する議論は, 文献 [19, 20] で始まった. しかし, 文献 [19, 20] のネットワーク符号は, 秘匿性だけを保証し, 訂正可能性を持たない. また, このネットワーク符号は, ネットワークの位相構造に依存し, 古典通信を必要とする.

私は, 林正人教授との共同研究 [1] で, これらの問題を解決し, 古典ネットワーク符号 [9, 18] の量子拡張として, 秘匿性と訂正可能性を持った量子ネットワーク符号を提案した. 文献 [9, 18] と類似した方法を使うため, 我々のネットワーク符号は, ネットワークを漸近的に使う. ネットワーク通信効率 m_0 と攻撃 (盗聴または改竄) されたチャンネルの最大数 m_1 が $2m_1 < m_0$ を満たすとき, 我々のネットワーク符号は, 符号化率 $m_0 - 2m_1$ で漸近的に正しいネットワーク通信を行う. また, 量子通信の正しさは秘匿性も保証するため, 我々のネットワーク符号は秘匿性も持つ.

我々のネットワーク符号は, 量子ネットワーク符号 [19, 20] と比べて以下の 3 つの利点がある. (1) 古典通信を要しない. 我々のネットワーク符号は, 符号に必要な送受信者間の共通乱数まで, 量子ネットワーク通信を用いて生成する. (2) $m_1 < m_0$ であれば, どのような攻撃に対しても秘匿性や訂正可能性を持つ. (3) ネットワークの位相構造に依存せず, 送受信者間の情報のみで設計できる.

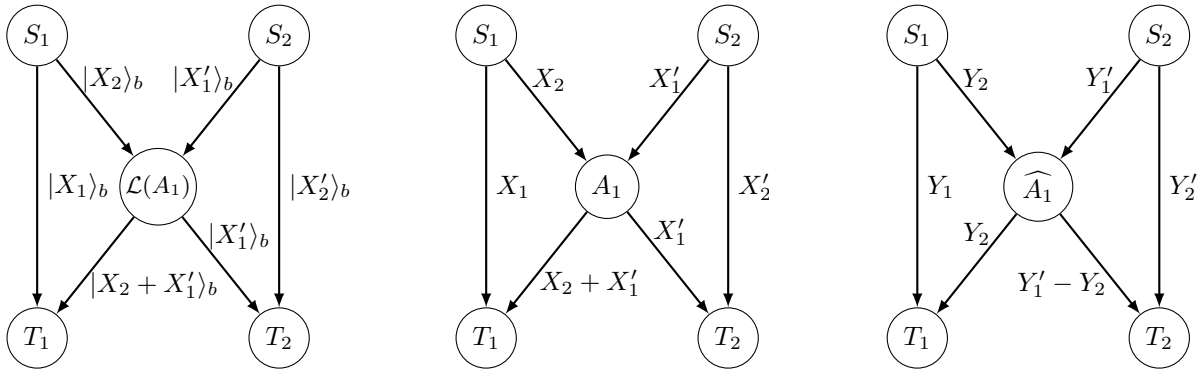
しかし, 文献 [19, 20] とは違い, 我々は, ネットワークノードの演算が量子線形可逆演算 (quantum invertible linear operation) であると制限をおく. 量子線形可逆演算とは, bit basis と呼ばれる一つの基底に対しての可逆線形演算であり, Chapter 3 で正確に定義される. この制限は, 古典ネットワーク符号 [9, 18] で, 中間ノード演算を可逆線形演算に制限したことに対応する.

我々のネットワーク符号は, honest-dealer verifiable quantum secret sharing (VQSS)[8] の一般化として扱うこと

[*1] 量子通信路, 量子演算, 量子状態は, Chapter 2 で定義される.

[*2] ここで漸近的とは, n 回のネットワーク通信で送られる情報を 1 ブロックとして符号化と復号化し, n が十分大きいことを意味する.

[*3] ネットワーク符号の符号化率は, ネットワーク一回利用あたりに伝送できる情報単位 (古典の場合は bit, 量子の場合は qubit) の数である.



(a) 量子ネットワーク (b) Bit classical network (c) Phase classical network

図 1: 多対多量子ネットワーク. 量子ネットワーク (a) で, $|\cdot\rangle_b$ は bit basis 量子状態, $\mathcal{L}(A_1)$ は中間ノードの量子演算を表す (Section 4.2 を参照). ネットワーク (b) と (c) は, (a) に対する bit classical network と phase classical network である.

ができる. 我々のネットワークを m_0 個の平行な量子通信路に適用することは, honest-dealer VQSS に対応するからである.

多対多量子ネットワーク符号

前節で提案されたセキュア量子ネットワーク符号 [1] は, 一組の送受信者がネットワークを使うときの符号である. しかし, 実際のネットワークは複数のユーザによって使われることが多い. そのため, 複数のユーザがネットワークを使う多対多ネットワーク符号が研究されている. 具体的には, 異なる r 組の送受信者 $(S_1, T_1), \ldots, (S_r, T_r)$ がそれぞれの通信を同時に行うネットワーク上でネットワーク符号が設計されている. 例えば, 前節で説明した秘匿性のみを持つ量子ネットワーク符号 [20] は, 多対多量子ネットワーク符号である.

私は, 林正人教授との共同研究 [2] で, 文献 [1] の結果を多対多量子ネットワーク通信に拡張した. 我々の符号は, 前節で述べた文献 [20] の問題点 (ネットワーク演算をネットワーク位相構造によって制御すること, 古典通信が必要であること) を解決した多対多量子ネットワーク符号である. 文献 [1] と同様に, 我々は中間ノード演算を量子可逆線形演算と制限し, ネットワークを複数回利用して符号を構成する. また, 量子状態の訂正可能性は秘匿性も保証するため [4], 我々の符号は秘匿性を持つ. 多対多のネットワークの場合, ネットワークの設計ミスにより, ネットワークの一部で混線が起きる可能性があるが, 混線の範囲が一定のレベル以下であれば, 訂正可能であることも, このネットワーク符号の利点である.

我々の符号の達成可能な符号化率について議論するために, すべての送信者の入力状態が bit basis state である状況を考える. すると, 我々のネットワークを古典ネットワークとして扱うことができる. 何故なら, ネットワークの中間ノード演算が量子可逆線形演算に制限されたため, 任意の bit basis state が他の bit basis state に変わるからである. このように構成された古典ネットワークを bit classical network と呼ぶ. Bit classical network で, 送信者 S_i から受信者 T_i への通信効率を m_i, S_i 以外の送信者から受信者 T_i への通信効率を a_i とする. 同様に, 量子系の phase basis が bit basis から定義され, phase basis に対しても古典ネットワーク phase classical network が定義される. Phase classical network で, 送信者 S_i から受信者 T_i への通信効率は bit clssical network と同じく m_i になると仮定し, S_i 以外の送信者から受信者 T_i への通信効率を a_i' と表す. すると, $a_i + a_i' < m_i$ のとき, 我々の符号は送信者 S_i から受信者 T_i までの量子通信を, 符号化率 $m_i - a_i - a_i'$ で漸近的に行う.

符号化率の理解のために, 図 1 の量子ネットワークを考える. Bit classical network と phase classical network は, 量子ネットワークによって決まる (Section 4.2 を参照). $X_1' = X_2' = Y_1' = Y_2' = 0$ のとき, 二つの classical network の S_1 から T_1 までの通信効率は 2 である. また, 二つの classical network の S_2 から T_1 までの通信効率はそれぞれ 1 と 0 である. よって, 我々の符号をパラメータ $(m_1, a_1, a_1') = (2, 1, 0)$ で利用することで, 符号化率 $m_1 - a_1 - a_1' = 1$ の量子ネットワーク通信を漸近的に行うことができる.

本稿の構成

本稿は次のように構成される.

Chapter 1 は, 英語の Introduction であり, 「はじめに」と同じ内容である.

Chapter 2 では, 量子情報理論を数学的に定式化する. そのため, 量子系, 量子状態, 量子演算, 測定に関する四つの量子情報理論の仮定を Sections 2.1, 2.2, 2.3, 2.4 で導入する. また, 通信の正しさと秘匿性について議論するために, 二つの状態の差と漏れる情報の量を, それぞれ Sections 2.5, 2.6 で定量化する.

Chapter 3 では, セキュア量子ネットワークについて述べる. 林正人教授との共同研究 [1] の結果である. Section 3.1 ではネットワークモデルを定義し, Section 3.2 で主定理を述べる. Section 3.3 で Preliminary を述べた後, Section 3.4 では, 送受信者が共有乱数を持つときに, 具体的に符号を設計する. Section 3.5 でネットワーク符号の誤り率が, bit basis error proabability と phase basis error probability の和より小さいことを示す. Section 3.6 では, bit basis error probability と phase basis error probability をそれぞれ求める. Section 3.7 では, セキュア古典ネットワーク符号 [16] を我々の量子ネットワーク符号に付け加えることで, 共有乱数なしでセキュア量子ネットワーク符号が設計できることを示す. Section 3.8 では, 我々の量子ネットワークが訂正可能性を持つことにより, 秘匿性も持つことを示す.

Chapter 4 では, 多対多量子ネットワークについて述べる. 林正人教授との共同研究 [2] の結果である. Chapter 4 は, Chapter 3 と同様な構成で記述されている. Section 4.1 では多対多ネットワークモデルを定義し, Section 4.2 で主定理を述べる. Section 4.4 では, 多対多量子ネットワーク符号を設計する. Section 4.5 で符号の性能を評価する.

Chapter 5 で結論を述べる.

Acknowledgements

First and the most, I want to thank my advisor Prof. Masahito Hayashi for his considerate guidance. He introduced me to the quantum information theory with his textbook "Quantum Information Theory: Mathematical Foundation" and my graduate study would not have been completed without the comments based on his deep and broad understandings on quantum and classical information theory. I am also grateful for him to allow me to attend to four international conferences.

I'm also grateful to the collegues in graduate school of mathematics, Nagoya university. Most of all, I want to thank to Yuuya Yoshida for all discussions. With his mathematical insights, I could successfully approach to mathematics though my undergraduate background was computer science. I want to thank Yu Saruta and Hayato Arai for their helpful comments and discussions.

The second year my graduate study was supported by Rotary Yoneyama Memorial Master Course Scholarship (YM).

Contents

Chapter 1

Introduction

1.1 Secure Quantum Network Code

Network coding is a coding method, addressed first by Ahlswede et al. [6], that allows network nodes to manipulate the information packets before forwarding. As a quantum analog, quantum network coding considers sending quantum states through a network which consists of quantum channels transmitting quantum states noiselessly and nodes performing quantum operations. Since quantum network coding was first discussed by Hayashi et al. [10], many other papers [10, 11, 12, 14, 15, 13] have studied quantum network codes.

In order to guarantee security in network communication, the security analysis of network codes is inevitable. The paper [7] started to discuss the secrecy of the classical network code and it was shown that the secrecy is improved by network coding. On the other hand, Jaggi et al. [9] constructed a classical network code with asymptotic error correctability. When transmission rate m_0 of network and the maximum rate m_1 of malicious injection satisfy $m_1 < m_0$, the code in [9] achieves correctability with rate $m_0 - m_1$ by asymptotic n uses of the network. Furthermore, Hayashi et al. [18] extended this result so that the secrecy is also guaranteed: when previously defined m_0, m_1 and the information leakage rate m_2 satisfy $m_1 + m_2 < m_0$, there exists a classical network code of rate $m_0 - m_1 - m_2$ which is asymptotically secret and correctable by n uses of the network.

The security analysis of quantum network codes was initiated in [19, 20]. However, the protocol in [19, 20] only keeps secrecy from the malicious adversary but the correctness of the state is not guaranteed if there is an attack. Moreover, this protocol depends on the network structure and requires classical communication.

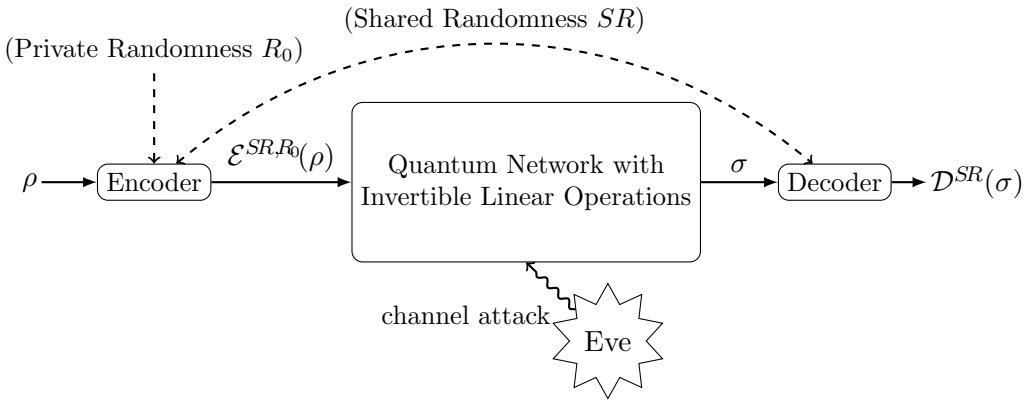


Figure 1.1: Protocol with negligible rate secret shared randomness. $\mathcal{S}(\mathcal{H})$ denotes the set of density matrices on a Hilbert space $\mathcal{H}$.

In the co-work [1] with my advisor Hayashi, to resolve these problems and as a natural quantum extension of the secure classical network codes [9, 18], we present a quantum network code which is secret and correctable [1]. Since we take a similar method to [9, 18], our code transmits a state by n uses of the quantum network. When the network transmission rate is m_0 and the maximum number m_1 of the attacked channels is restricted by $m_1 < m_0/2$, our protocol correctly transmits quantum information of rate $m_0 - 2m_1$ by asymptotic n uses of the network. Since the correctness of the transmitted quantum state guarantees the secrecy of the quantum channel [4], the secrecy of our protocol is guaranteed.

There are notable properties in our protocol. First, our protocol can be implemented without any classical communication. We generate the negligible rate secret shared randomness needed for our code by use of the quantum network. Secondly, our protocol is secure from any malicious operation on m_1 channels as long as $m_1 < m_0/2$ holds. That is, when $m_1 < m_0/2$, our protocol is safe from the strongest eavesdropper Eve who knows the network structure and the network operations, keeps classical information extracted from the wiretapped states, and applies quantum operations on the attacking channels adaptively by her wiretapped information. Thirdly, our protocol transmits a quantum state without the knowledge of the quantum network structure.

However, unlike [19, 20] and like [9, 18], we place a constraint on our network that every node operation is the application of an invertible matrix to bit basis states which is a fixed basis of the quantum system. We call the restricted quantum operations the *quantum invertible linear operations*.

Our protocol can be thought of as a generalization of the honest-dealer

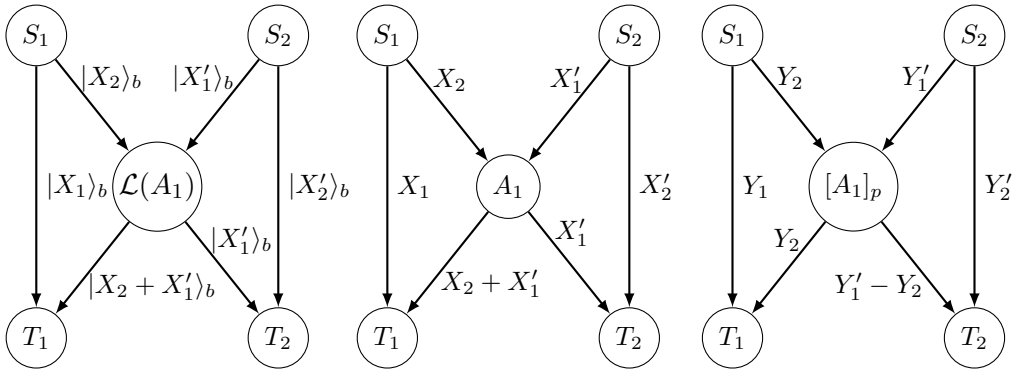
verifiable quantum secret sharing (VQSS) [8] because the honest-dealer VQSS corresponds to a special case of our protocol where the network consists of m_0 parallel quantum channels.

1.2 Multiple-Unicast Quantum Network Code

The proposed secure quantum network code in Section 1.1 is designed for the unicast network where the entire network is used by a sender and a receiver. However, since a network is used by several users in general, it is needed to treat the network model with multiple users instead of the unicast network. For this purpose, the multiple-unicast network has been researched, in which disjoint r sender-receiver pairs $(S_1, T_1), \ldots, (S_r, T_r)$ communicate over a network. The paper [20] studied a quantum network code for multiple-unicast network. The code in [20] transmits a state successfully for each use of the network. However, [20] has a limitation that the code should manipulate the node operations in the network and therefore the code depends on the network structure. In addition, the code in [20] requires the free use of classical communication.

In the co-work [2] with my advisor Hayashi, we propose a quantum network code for the multiple-unicast network which is a generalization of the unicast quantum network code in Section 1.1 and overcomes the shortcomings of the multiple-unicast quantum network code in [20]. In the same way as the code in Section 1.1, the given node operations are quantum invertible linear operations, our code requires the asymptotic n-use of the network for the correct transmission of the state, and the encoding and decoding operations are performed on the input and output quantum systems of the n-use of the network, respectively. On the other hand, differently from [20], our code can be implemented without any manipulation of the network operations and any classical communication. Moreover, our code makes no information leakage asymptotically from a sender S_i to the receivers other than T_i because the correctness of the transmitted state guarantees no information leakage [4].

To discuss the achievable rate by our code, we consider the situation that the input states of all senders are the bit basis states. Then, our network can be considered as a classical network, called *bit classical network*, because a bit basis state is transformed to another bit basis state by our quantum node operations. In the bit classical network, we assume that when the inputs of the senders other than S_i are zero, *the transmission rate* from S_i to T_i is m_i, which is the same as the number of outgoing edges of S_i and incoming edges of T_i. Also, when we define *the interference rate* by the



(a) Quantum network (b) Bit classical network (c) Phase classical network

Figure 1.2: Toy example of a multiple-unicast network. In quantum network (a), $|\cdot\rangle_b$ denote bit basis states and $\mathcal{L}(A_1)$ is the network operation. The network (b) and (c) is the bit and phase classical networks of the quantum network (a).

rate of the transmitted information to T_i from the senders other than S_i, we assume that the interference rate to T_i is at most a_i in the bit classical network. In the same way, in case that the input states of all senders are set to the phase basis states (defined in Section 3.1), we call the network a *phase classical network*. In the phase classical network, we also assume that the transmission rate from S_i to T_i is m_i when the inputs of the senders other than S_i are zero. Also, the interference rate to T_i is at most a_i' in the phase classical network. Under these constraints, if $a_i + a_i' < m_i$, our code achieves the rate $m_i - a_i - a_i'$ quantum communication from S_i to T_i asymptotically.

To help the understanding of the rates described above, we explain the achievable transmission rate from S_1 to T_1 in the network in Fig. 1.2. The bit and the phase classical networks (Fig. 1.2b and Fig. 1.2c) are determined from the quantum network (Fig. 1.2a) (see Section 3.1). When $X_1' = X_2' = Y_1' = Y_2' = 0$, the transmission rates from S_1 to T_1 are 2 for both networks, i.e., $m_1 = 2$, which is also the number of outgoing edges of S_1 and incoming edges of T_1. Also, the interference rates from S_2 to T_1 are 1 and 0 for the bit and the phase classical networks, respectively. On this network, if our code from S_1 to T_1 with the rates $(m_1, a_1, a_1') = (2, 1, 0)$ is constructed, the conditions $a_1 \geq 1$, $a_1' \geq 0$ and $a_1 + a_1' < m_1$ are satisfied, and therefore our code implements the rate $m_1 - a_1 - a_1' = 1$ quantum transmission from S_1 to T_1 asymptotically.

In a practical sense, our code can cope with node malfunctions in the following case: on the multiple-unicast network with quantum invertible linear operations, the network operations are well-determined so that there is

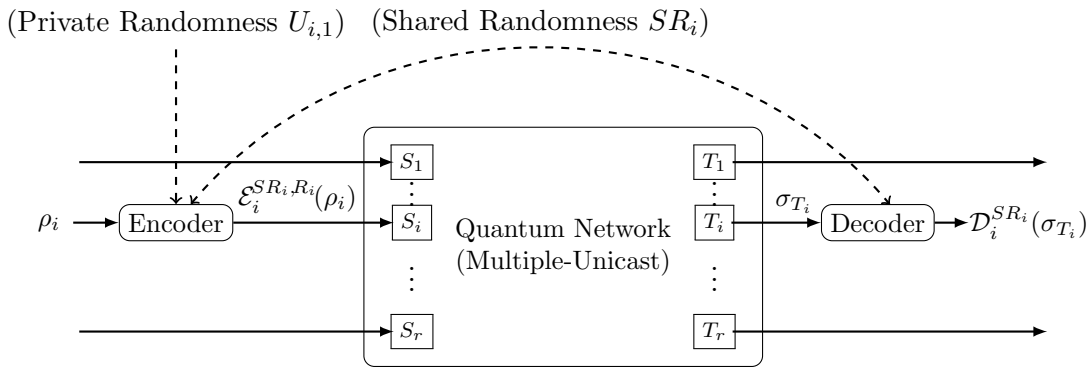


Figure 1.3: Overview of code protocol from a sender S_i to a receiver T_i. States ρ_i and $\mathcal{D}_i^{SR_i}(\sigma_{T_i})$ are in code space $\mathcal{H}'_{\text{code}}$.

no interference between all sender-receiver pairs, but three broken nodes apply quantum invertible linear operations different from the determined ones. Moreover, let the transmission rate m_1 without interferences from S_1 to T_1 be 100 and the number of outgoing edges of the three broken nodes be 4. In this case, $3 \times 4 = 12$ outgoing edges of the three broken nodes transmit unexpected information which implies the bit (phase) interference rate is at most 12. Therefore, by our code with $m_1 = 100$ and $a_1, a'_1 > 12$, the sender S_1 can transmit quantum states to the receiver T_1 correctly with the rate $100 - a_1 - a'_1 < 76$ by asymptotically many uses of the network.

1.3 Outline

The remainder of this thesis is organized as follows. Based on existing results, in Chapter 2, we give the mathematical basis of quantum information theory. Four postulates of quantum information theory are introduced in Sections 2.1, 2.2, 2.3 and 2.4. To prove the correctness and the security of quantum network codes, it is needed to define measures for the difference of two states and measures for leaked information. Section 2.5 defines measures for difference of two quantum states and propose several properties of these measures. Section 2.6 defines several informations measures which is related to the measure of leaked information.

In Chapter 3, the secure quantum network code introduced in Section 1.1 is constructed. Section 3.1 gives the network structure and Section 3.2 formally states two main theorems of this chapter. Based on the preliminaries in Section 3.3, our code is constructed in Section 3.4. In Section 3.5, we

suggest the transmission protocol with our code and show that the entanglement fidelity is upper bounded by the sum of the bit error probability and the phase error probability. In Section 3.6, we derive the bit error probability and the phase error probability. In Section 3.7, by attaching the secure classical network code presented in [16] to our quantum network protocol, we show that the secure quantum network code without classical communication can be implemented. Section 3.8 explains how correctness implies secrecy in our protocol.

In Chapter 4, the quantum network code for multiple-unicast network introduced in Section 1.2 is constructed. Section 4.1 introduces the formal description of the quantum multiple-unicast network with quantum invertible linear operations. Section 4.2 gives the main theorem of this chapter. Section 4.4 concretely constructs our code with the free use of negligible rate shared randomness. The encoder and decoder of our code is given in this section. The performance of our code is analyzed in Section 4.5.

Chapter 5 is the conclusion of this thesis.

Chapter 2

Quantum Information Theory

Quantum information theory is a theoretical framework to treat physical quantum systems and it is mathematically defined from four postulates of quantum systems, quantum states, quantum operation and measurement.

2.1 Quantum System and Quantum State

A quantum system is defined as a finite-dimensional Hilbert space $\mathcal{H}$, which is a complex vector space with standard inner product $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$.

Postulate 1 (Quantum system)**.** *Any quantum system is described by a finite-dimensional Hilbert space.*

We will use the bra-ket notation to describe vectors in $\mathcal{H}$ and vectors in the dual space $\mathcal{H}^*$. From one-to-one correspondence between $\mathcal{H}$ and $\mathcal{H}^*$, for any vector $|x\rangle := (x_1, \ldots, x_d)^\top$ in $\mathcal{H}$, there is a unique vector $\langle x| \in \mathcal{H}^*$ defined by

$$\langle x|y\rangle := \sum_{i=1}^{d} \bar{x}_i y_i, \quad \forall y \in \mathcal{H}\,.$$

For any $|x\rangle = (x_1, \ldots, x_d)^\top \in \mathcal{H}$, $|\bar{x}\rangle := (\bar{x}_1, \ldots, \bar{x}_d)^\top$. Throughout this thesis, we will use the term a *basis* to denote a orthonormal basis, $\mathcal{M}(\mathcal{H})$ denotes the set of square matrices on $\mathcal{H}$. Moreover, d denotes the dimension of the quantum system $\mathcal{H}$ if it is not specified.

For a square matrix X on $\mathcal{H}$, the adjoint matrix is defined by $X^* := \bar{X}^\top$ A matrix X on $\mathcal{H}$ is called a *Hermitian matrix* if $X = X^*$. A Hermitian matrix X is called positive definite if

$$\langle x|X|x\rangle > 0, \quad \text{for any } |x\rangle \in \mathcal{H},$$

and it is denoted by $X > 0$. Similarly, a Hermitian matrix X is called positive semidefinite if

$$\langle x|X|x\rangle \geq 0, \quad \text{for any } |x\rangle \in \mathcal{H},$$

and it is denoted by $X \geq 0$.

Quantum states are defined by desity matrices.

Definition 2.1.1 (Density matrix on $\mathcal{H}$)**.** *A matrix $\rho \in \mathcal{M}(\mathcal{H})$ is called a density matrix on the quantum system $\mathcal{H}$ if*

$$\operatorname{Tr}\rho = 1 \quad \textit{and} \quad \rho \geq 0.$$

Postulate 2 (Quantum state)**.** *Any quantum state on a quantum system $\mathcal{H}$ is described by a density matrix on $\mathcal{H}$.*

The set of states on a quantum system $\mathcal{H}$ is denoted as $\mathcal{S}(\mathcal{H})$ for the following.

A state that can be represented by a probabilistic mixture of other states is called a *mixed state* and a state which is not a mixed state is called a *pure state*. Any state ρ is pure state if and only if ρ is a rank-one matrix. Since the set of states of a quantum system is a convex set, it can also be regarded that pure states are the extremal points of this set and the mixed states are the inner points.

2.2 Composite System

Consider the case where we treat several quantum systems simultaneously. A composite system of quantum systems is given as a tensor product of the quantum systems, e.g. $\mathcal{H}_A \otimes \mathcal{H}_B$ is the composite system of $\mathcal{H}_A$ and $\mathcal{H}_B$.

Throughout this thesis, we use single lettered subscripts to differentiate quantum systems, e.g. $\mathcal{H}_A, \mathcal{H}_B, \ldots$ and multi-lettered subscript to denote composite systems, e.g. $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$. Furthermore, we use the notation $|x_A, x_B\rangle := |x_A\rangle \otimes |x_B\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.

States on a composite system are defined in the same way as states on a single system. Note that the states are not necessarily the tensor product of those in each subsystems. States which are written as tensor products of states on subsystems are called *seperable states*: a state ρ is separable if

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad \sum_i p_i = 1, \quad p_i \geq 1,$$

where ρ_A^i and ρ_B^i are states on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. States which are not seperable are called *entangled states*.

For any state ρ in $\mathcal{H}_{AB}$, the states $\rho_A := \mathrm{Tr}_B\,\rho$ and $\rho_B := \mathrm{Tr}_A\,\rho$ are states on $\mathcal{H}_A$ and $\mathcal{H}_B$, called *reduced states*, where the partial trace Tr_B (Tr_A) is defined as follows.

Definition 2.2.1 (Partial trace)**.** *Let $\{|e_i^B\rangle\}$ be a basis of the system $\mathcal{H}_B$. For any $X \in \mathcal{M}(\mathcal{H}_{AB})$,*

$$\operatorname*{Tr}_B X \stackrel{\text{def}}{=} \sum_i (I \otimes \langle e_i^B|) X (I \otimes |e_i^B\rangle),$$

or alternatively, $\mathrm{Tr}_B : \mathcal{H}_{AB} \to \mathcal{H}_A$ is a linear operator such that

$$\operatorname*{Tr}_B X \otimes Y \stackrel{\text{def}}{=} X \,\mathrm{Tr}\, Y, \quad \forall X \in \mathcal{M}(\mathcal{H}_A), Y \in \mathcal{M}(\mathcal{H}_B).$$

Given any $\rho \in \mathcal{S}(\mathcal{H}_A)$, a state $\tilde{\rho} \in \mathcal{S}(\mathcal{H}_{AR})$ is called an *extension* of ρ if

$$\operatorname*{Tr}_R \tilde{\rho} = \rho.$$

Especially, if an extension $\tilde{\rho}$ of ρ is a pure state, the state $\tilde{\rho}$ is called a *purification* of ρ.

Maximally entangled states and completely mixed states are the most important states in quantum information theory. Given a quantum system $\mathcal{H}$ spanned by a basis $\{e_i : i = 1, \ldots, d\}$, the maximally entangled state is defined by $|\Phi\rangle := \sum_{i=1}^d |e_i, e_i\rangle\langle e_i, e_i| \in \mathcal{S}(\mathcal{H} \otimes \mathcal{H})$ and the completely mixed state is $\rho_{\text{mix}} := I = \sum_{i=1}^d |e_i\rangle\langle e_i| \in \mathcal{S}(\mathcal{H})$. The maximally entangled state $|\Phi\rangle$ is a purification of the completely mixed state ρ_{mix} and conversely, the latter is a reduced state of the former.

2.3 Quantum Operation

Quantum operations describe the dynamics between two quantum systems. First, we will give several conditions that quantum operations between two systems should satisfy and define quantum operations by trace preserving completely positve (TP-CP) maps.

Quantum operations are maps κ from $\mathcal{S}(\mathcal{H}_A)$ to $\mathcal{S}(\mathcal{H}_B)$ satisfying the following conditions.

Condition 1 Quantum operations are affine maps.

A map f is called an affine map if

$$f(px_1 + (1-p)x_2) = pf(x_1) + (1-p)f(x_2), \quad p \in (0,1).$$

Since the mixed states are no other than the probabilistic mixture of other states, the quantum operation should act in the same way on the states composing the mixed states. Therefore, when ρ_1 and ρ_2 are states on $\mathcal{H}_A$, the following condition for affine maps should hold:

$$\kappa(p\rho_1 + (1-p)\rho_2) = p\kappa(\rho_1) + (1-p)\kappa(\rho_2), \quad p \in (0,1).$$

Condition 1' Quantum operations are linear maps.

Condition 1' is the generalization from the affinity to the linearity.

Condition 2 Quantum operations are positive maps.

A positive map is a map that maps a positive semidefinite matrix to a positive semidefinite matrix. Considering quantum states are positive semidefinite matrices, the quantum operations should be positive maps.

Condition 2' Quantum operations are completely positive maps.

Even in the case that the quantum opration κ from $\mathcal{H}_A$ is considered as an operation from the larger system $\mathcal{H}_A \otimes \mathbb{C}^n$ by applying identity operator to $\mathbb{C}^n$, the quantum operation κ should still be a positive map, i.e. $\kappa \otimes \iota_{\mathbb{C}^n}$ should be positive for any n where $\iota_{\mathbb{C}^n}$ is the identity map on $\mathbb{C}^n$. When $\kappa \otimes \iota_{\mathbb{C}^n}$ is a positive map, the operation κ is called n-positive map. When κ is n-positive for any dimension n, the operation κ is called a completely positive map. Therefore quantum operations should be completely positive maps.

Condition 3 Quantum operations are trace-preserving maps.

The resultant state $\kappa(\rho)$ should be traced to 1.

To summarize, quantum operations should satisfy the above Condition 1', Condition 2', and Condition 3. The maps satisfying these three conditions are called *trace-preserving completely positive (TP-CP) maps.*

Quantum information theory postulates that the set of TP-CP maps is the same as the set of quantum operations.

Postulate 3. *Any quantum operations are described by trace-preserving completely positive (TP-CP) maps.*

One of the most important result for describing quantum operations is that we have two detailed representations for TP-CP maps. To see this result, we introduce the following theorem which characterizes the TP-CP maps.

Theorem 2.3.1 (Equivalent conditions on TP-CP maps)**.** *Given a quantum operation $\kappa : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$, the followings are equivalent. The dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ are denoted by d_A and d_B, respectively.*

1. *κ is a TP-CP map.*
2. *κ is a TP $(\min\{d_A, d_B\})$-positive map.*
3. *(Stinespring representation) For $\mathcal{H}_C \simeq \mathcal{H}_B$, there exist a pure state $\rho_0 \in \mathcal{H}_{BC}$ and unitary matrix U on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ such that*
$$\kappa(\rho) = \operatorname*{Tr}_{AC} U(\rho \otimes \rho_0)U^*.$$
4. *(Choi-Kraus representation) There exists a set $\{F_i\}_{i=1}^{d_A d_B}$ of linear maps from $\mathcal{H}_A$ to $\mathcal{H}_B$ satisfying $\sum_i F_i F_i^* = I_A$ such that*
$$\kappa(\rho) = \sum_i F_i \rho F_i^*.$$

Stinespring representation shows that quantum operations are nothing other than multiplying a unitary matrix and its adjoint on both sides of the states and focusing on the subsystem.

2.4 Measurement

In this section, we discuss measurements to quantum systems. Measurement to a quantum system is an essential tool to extract classical information from the quantum state.[1] If a measurement is performed, the measurement outcome is obtained probabilistically and it also disturbs the state of the system. Therefore, to model the measurement, it needs to describe both of the probability distribution and the change of the state.

Given a set Ω of measurement outcomes, consider describing a measurement by a set of maps $\kappa_\Omega := \{\kappa_\omega : \omega \in \Omega\}$ such that the probability to obtain $\omega \in \Omega$ is $\operatorname{Tr} \kappa_\omega(\rho)$ and the resultant state is $(1/\operatorname{Tr} \kappa_\omega(\rho))\kappa_\omega(\rho)$. Similarly to the conditions for quantum operations, the maps $\{\kappa_\omega : \omega \in \Omega\}$ should satisfy the following conditions.

Condition 1 κ_ω are linear maps.

Condition 2 κ_ω are completely positive (CP) maps.

[1] Extracting classical information is important because all the information recognizable by humans is not quantum states but classical information.

Condition 3 $\sum_{\omega\in\Omega} \operatorname{Tr} \kappa_\omega(\rho) = 1$.

The set of maps κ_ω that satisfies the Condition 1, Condition 2, Condition 3 are defined as an instrument.

Definition 2.4.1 (Instrument κ_Ω)**.** *A set $\kappa_\Omega = \{\kappa_\omega : \omega \in \Omega\}$ of linear CP-maps is called an* instrument *if $\sum_\omega \kappa_\omega$ is TP-CP map.*

The last postulate of quantum information theory is given as follows.

Postulate 4 (Measurement)**.** *Any measurement is described by an instrument $\kappa_\Omega := \{\kappa_\omega : \omega \in \Omega\}$. When a measurement κ_Ω is applied, the probability to obtain $\omega \in \Omega$ is $\operatorname{Tr} \kappa_\omega(\rho)$ and the resultant state is $(1/\operatorname{Tr} \kappa_\omega(\rho))\kappa_\omega(\rho)$.*

If our interest is only the probabilistic distribution of the measurement outcome, it is enough to treat positive operator-valued measurement (POVM).

Definition 2.4.2 (Positive Operator-Valued Measurement (POVM) $\mathbf{M}_\Omega$)**.** *A set of matrices $\mathbf{M}_\Omega := \{M_\omega \in \mathcal{M}(\mathcal{H}) : \omega \in \Omega\}$ is called a POVM on the quantum system $\mathcal{H}$ if*

$$\sum_\omega \operatorname{Tr} \rho M_\omega = 1 \quad \textit{and} \quad M_\omega \geq 0 \quad \textit{for any } M_\omega \in \mathbf{M}_\Omega.$$

Given a state ρ and a POVM $\mathbf{M} = \{M_\omega : \omega \in \Omega\}$ on $\mathcal{H}$, the probability for obtaining ω is $\operatorname{Tr} \rho M_\omega$.

2.5 Measures of Difference of Two States

In this section, we introduce two measures for difference of two states, *fidelity* and *entanglement fidelity*.

2.5.1 Fidelity

Fidelity is defined as follows: for any two states ρ_1 and ρ_2 on $\mathcal{H}$,

$$F(\rho_1, \rho_2) \stackrel{\text{def}}{=} ||\sqrt{\rho_1}\sqrt{\rho_2}||_1 = \operatorname{Tr} |\sqrt{\rho_1}\sqrt{\rho_2}|$$

Theorem 2.5.1 ([3])**.** *For any two states ρ_1 and ρ_2 on $\mathcal{H}$,*

$$F(\rho_1, \rho_2) = \max\{|\langle u_1|u_2\rangle| : |u_1\rangle, |u_2\rangle \textit{ are purification of } \rho_1, \rho_2\}.$$

Corollary 2.5.1. *Let ρ_1 and ρ_2 be states on $\mathcal{H}_A$. Given a purification $|x\rangle$ of ρ_1, there exists a purification $|y\rangle$ of ρ_2 such that*

$$F(\rho_1, \rho_2) = |\langle x|y\rangle| = \langle x|y\rangle.$$

From the above corollary, several useful properties of fidelity are derived.

Corollary 2.5.2 (Properties of fidelity)**.** *1. (Symmetricity)* $F(\rho,\sigma) = F(\sigma,\rho)$.

2. (Range of fidelity) $F(\rho,\sigma) \in [0,1]$

3. (Maximum condition) $F(\rho,\sigma) = 1$ *if and only if* $\rho = \sigma$.

4. (Monotonicity) $F(\rho_1,\rho_2) \leq F(\kappa(\rho_1),\kappa(\rho_2))$ *for any TP-CP map* κ.

2.5.2 Entanglement Fidelity

In many contexts of quantum information theory, it is important to measure the difference of the states before and after applying quantum operation κ. For this reason, the measure F_e is defined as follows as a measure of the most destructive operation including κ.

$$\begin{aligned} F_e(\rho,\kappa) &:= \min_{\tilde{\rho},\kappa_R} F\Big((\iota_A \otimes \kappa_R)\tilde{\rho}, (\kappa \otimes \kappa_R)\tilde{\rho}\Big) \\ &= \min_{\tilde{\rho}} F\Big(\tilde{\rho}, (\kappa \otimes \iota_R)\tilde{\rho}\Big) \\ &= F\Big(|x\rangle\langle x|, (\kappa \otimes \iota_R)(|x\rangle\langle x|)\Big) \end{aligned}$$

where $\tilde{\rho}$ is an extension of ρ and $|x\rangle\langle x|$ is a purification of the state ρ. From this reasoning, entanglement fidelity is defined as follows.

Definition 2.5.1 (Entanglement fidelity)**.** *Given a CP-map* $\kappa : \mathcal{H}_A \to \mathcal{H}_A$*, for any purification* x *of* ρ*, the following is uniquely defined and called entanglement fidelity:*

$$\begin{aligned} F_e(\rho,\kappa) &\stackrel{\text{def}}{=} F\Big(|x\rangle\langle x|, \kappa \otimes \iota_R(|x\rangle\langle x|)\Big) \\ &= \sqrt{\langle x|\kappa \otimes \iota_R(|x\rangle\langle x|)|x\rangle} \\ &= \sqrt{\sum_j |\operatorname{Tr} E_j\rho|^2}. \end{aligned} \tag{2.1}$$

where $\{E_j\}$ *is Choi-Kraus representation of* κ.

Proof of (2.1).

$$\begin{aligned}
\langle x|\kappa \otimes \iota_R(|x\rangle\langle x|)|x\rangle &= \operatorname{Tr} \kappa \otimes \iota_R(|x\rangle\langle x|)|x\rangle\langle x| \\
&= \sum_i \operatorname{Tr}(E_i \otimes I_R)|x\rangle\langle x|(E_i^* \otimes I_R)|x\rangle\langle x| \\
&= \sum_i (\operatorname{Tr}(E_i^* \otimes I_R)|x\rangle\langle x|)(\operatorname{Tr}(E_i \otimes I_R)|x\rangle\langle x|) \\
&= \sum_i \operatorname*{Tr}_A E_i^* \rho \operatorname*{Tr}_A E_i \rho \\
&= \sum_i (\operatorname*{Tr}_A E_i \rho)^* \operatorname*{Tr}_A E_i \rho \\
&= \sum_i |\operatorname*{Tr}_A E_i \rho|^2
\end{aligned}$$

□

The square of entanglement fidelity is convex with respect to states.

Theorem 2.5.2 (Convexity of squared entanglement fidelity with respect to states)**.** *F_e^2 is convex with respect to states:*

$$F_e^2(\lambda\rho + (1-\lambda)\sigma, \kappa) \leq \lambda F_e^2(\rho, \kappa) + (1-\lambda) F_e^2(\sigma, \kappa).$$

Proof. Note on $F_e^2(\rho, \kappa) = \sum_j |\operatorname{Tr} E_j \rho|^2$. Since x^2 and $|x|$ are convex and trace operator is linear, $F_e^2(\rho, \kappa)$ is convex with respect to ρ. □

Convexity of squared entanglement fidelity implies Corollary 2.5.3.

Corollary 2.5.3. *Let ρ be any state on $\mathcal{H}$. There exists $\lambda_0 \geq 0$ and $\sigma \in \mathcal{S}(\mathcal{H})$ such that*

$$1 - F_e^2(\rho_{\mathrm{mix}}, \kappa) \geq \lambda_0(1 - F_e^2(\rho, \kappa)) + (1-\lambda_0)(1 - F_e^2(\sigma, \kappa)). \tag{2.2}$$

Proof. Let ρ is diagonalized as $\rho = \sum_i p_i |u_i\rangle\langle u_i|$. The values $\lambda_0 \leq 1/(d \cdot \max_i p_i)$ and $\sigma := \sum_i q_i |u_i\rangle\langle u_i|$ for $q_i := -\lambda_0/(1-\lambda_0)p_i + 1/(d(1-\lambda_0))$ satisfy the inequality (2.2). □

Corollary 2.5.3 implies that if $1 - F_e^2(\rho_{\mathrm{mix}}, \kappa)$ is close to 0, $1 - F_e^2(\rho, \kappa)$ is also close to 0 for any state ρ. Therefore, the invariance of arbitrary states by κ can be evaluated by that of the completely mixed state ρ_{mix}. This fact is important in the error analysis of quantum network codes in Chapters 3 and 4.

Moreover, squared entanglement fidelity can be evaluated with the special bases called mutually unbiased bases.

Definition 2.5.2 (Mutually unbiased basis)**.** *Two orthonormal bases* $\{|e_i\rangle\}$ *and* $\{|u_i\rangle\}$ *of Hilbert space* $\mathcal{H}$ *are called mutually unbiased if and only if*

$$|\langle e_i|u_i\rangle| = \frac{1}{\sqrt{d}}.$$

Given mutually unbiased bases $\mathcal{B}_1 = \{|e_i\rangle\}$ and $\mathcal{B}_2 = \{|u_i\rangle\}$ of $\mathcal{H}$, consider two maximally entangled states on $\mathcal{H} \otimes \mathcal{H}$.

$$|\Phi_1\rangle = \sum_i \frac{1}{d}|e_i, \bar{e}_i\rangle, \quad |\Phi_2\rangle = \sum_i \frac{1}{d}|u_i, \bar{u}_i\rangle,$$

and projections

$$P_1 = \sum_i |e_i, \bar{e}_i\rangle\langle e_i, \bar{e}_i|, \quad P_2 = \sum_i |u_i, \bar{u}_i\rangle\langle u_i, \bar{u}_i|.$$

By a change of basis matrix $\mathcal{F} := \sum_i |u_i\rangle\langle e_i|$, we have the relations $|\Phi_2\rangle = (\mathcal{F} \otimes \bar{\mathcal{F}})|\Phi_1\rangle$ and $P_2 = (\mathcal{F} \otimes \bar{\mathcal{F}})|\Phi_1\rangle\langle\Phi_1|(\mathcal{F} \otimes \bar{\mathcal{F}})^*$.

Theorem 2.5.3. *The following properties hold for the above maximally entangled states and projections.*

1. $\Phi_1 = \Phi_2$. *Thus, define* $\Phi := \Phi_1 = \Phi_2$.
2. $P_1 P_2 = |\Phi\rangle\langle\Phi|$.
3. $\frac{1}{2}((I - P_1) + (I - P_2)) \leq I - P_1 P_2 \leq (I - P_1) + (I - P_2)$.

Proof. 1. $\langle\Phi_1|\Phi_2\rangle = 1$.

2. Simple calculation.

3. (right inequality) $(I - P_1)(I - P_2) \geq 0$.

   (left inequality) Since P_1 and P_2 are orthogonal projections, $P_1 - P_2$ is Hermitian and diagonalizable. Therefore, $(P_1 - P_2)^2 \geq 0$ holds and it proves the left inequality.

□

The above proposition implies the following theorem for bounds of entanglement fidelity.

Theorem 2.5.4. *For* $i = 1, 2$*, define* the error probability with respect to the i-th basis *by* $\mathcal{E}_i := 1 - \operatorname{Tr} P_i \kappa \otimes \iota(|\Phi\rangle\langle\Phi|)$*. Then, the above proposition implies*

$$\frac{1}{2}(\mathcal{E}_1 + \mathcal{E}_2) \leq 1 - F_e^2(\rho_{\mathrm{mix}}, \kappa) \leq (\mathcal{E}_1 + \mathcal{E}_2).$$

Proof. From $F_e^2(\rho_{\mathrm{mix}}, \kappa) = \mathrm{Tr}\,|\Phi\rangle\langle\Phi|\kappa \otimes \iota(|\Phi\rangle\langle\Phi|)$, we have the theorem by applying the above proposition. □

Corollary 2.5.4. *$\mathcal{E}_1 + \mathcal{E}_2 \to 0$ if and only if $1 - F_e^2(\rho_{\mathrm{mix}}, \kappa) \to 0$.*

2.6 Quantum Information Measures

Definition 2.6.1 (von Neumann entropy)**.** *For a state ρ on $\mathcal{H}_A$,*

$$H(\rho) \stackrel{\mathrm{def}}{=} \mathrm{Tr}\,\rho \log \rho.$$

Definition 2.6.2 (Quantum mutual entropy)**.** *For a state ρ on $\mathcal{H}_{AB}$,*

$$I_\rho(A; B) \stackrel{\mathrm{def}}{=} H(\rho_A) + H(\rho_B) - H(\rho).$$

Definition 2.6.3 (Quantum entropy exchange)**.**

$$H_e(\rho, \kappa) \stackrel{\mathrm{def}}{=} H(\kappa \otimes \iota(|x\rangle\langle x|)).$$

Theorem 2.6.1 (Quantum Fano's inequality)**.** *Given $\rho \in \mathcal{S}(\mathcal{H})$*

$$H_e(\rho, \kappa) \leq h(F_e^2(\rho, \kappa)) + (1 - F_e^2(\rho, \kappa)) \log(d^2 - 1)$$

where $d = \dim \mathcal{H}$.

2.6.1 Leaked Information

Suppose a set of input states $W := \{\rho_x\}$ is generated with the probabilistic distribution $p = \{p_x\}$. In this case, the composite state of quantum states and classical probabilistic distribution can be written as

$$\rho = \sum_x p_x \rho_x \otimes |x\rangle\langle x| \in \mathcal{S}(\mathcal{H}_{AR}).$$

If a quantum operation κ is applied to the state ρ, the leaked information about x by the quantum state ρ_x is measured by mutual information $I(p, W)$:

$$I(p, W) := I_\rho(A; R) = H\Big(\kappa_E\Big(\sum_x p_x \rho_x\Big)\Big) - \sum_x p_x H(\kappa_E(\rho_x)).$$

Since $H_e(\rho, \kappa) = H(\kappa_E(\sum_x p_x \rho_x))$ in our choice of ρ, we have the inqualities

$$I(p, W) \leq H_e(\rho, \kappa) \leq h(F_e^2(\rho, \kappa)) + (1 - F_e^2(\rho, \kappa)) \log(d^2 - 1),$$

where d is the dimension of the input system of κ and the second inequality follows from quantum Fano's inequality.

Chapter 3

Secure Quantum Network Code on Unicast Network

In this chapter, we construct a secure quantum network code.

3.1 Quantum Network and Attack Model

We give the formal description of our quantum network which is defined as a natural quantum extension of a classical network. The information rates related to network transmission and malicious attack are summarized in Table 3.1.

3.1.1 Network Structure and Transmission

We consider the network described by a directed acyclic graph $G_N = (V, E)$ where V is the set of nodes (vertices) and E is the set of channels (edges). The network G_N has one source node v_0 which has m_0 outgoing channels and one sink node v_{c+1} which has m_0 incoming channels. The nodes, which are not source or sink, are called intermediate nodes and denoted as $v_1, v_2, \ldots, v_c$ where $c := |V| - 2$ according to the order of the information conversion. An intermediate node v_t has the same number k_t of incoming and outgoing channels where $1 \leq k_t \leq m_0$. For convenience, we define $k_0 = k_{c+1} := m_0$.

The transmission on the network G_N is described as follows. Each channel transmits information noiselessly unless the channel is attacked, and each node applies information conversion noiselessly at any time. At time 0, the source node transmits the input information along m_0 outgoing channels. At time t where $1 \leq t \leq c$, the node v_t applies information conversion to the information from k_t incoming channels, and outputs conversion outcome

Table 3.1: Definitions and notations

m_0	Network transmission rate
m_1 $(< m_0/2)$	Maximum number of attacked channels
m_a $(\leq m_1)$	The number of the attacked channels
$\mathcal{H}$	Unit quantum system
q	Dimension of $\mathcal{H}$ (prime power)
n	Block-length
$\mathcal{H}'$	Extended unit quantum system
α	Dimension of extension
q'	Dimension of $\mathcal{H}'$
n'	Block-length with respect to $\mathcal{H}'$
$\mathcal{H}_{\rm code}^{(n)}$	Code space with block-length n
$\kappa^{(n)}$	Code protocol with block-length n
$\|x\rangle_b$ $(x \in \mathbb{F}_q$ $(\mathbb{F}_{q'}))$	Bit basis element of $\mathcal{H}$ $(\mathcal{H}')$
$\|z\rangle_p$ $(z \in \mathbb{F}_q$ $(\mathbb{F}_{q'}))$	Phase basis element of $\mathcal{H}$ $(\mathcal{H}')$

along k_t outgoing channels. After time c, the sink node receives the output information from the m_0 incoming channels. The details of the transmitted information and information conversion are described in the following subsections.

The m_0 outgoing channels of the source node are numbered to $1, \ldots, m_0$ and after the conversion in the node v_t, the assigned numbers are moved from k_t incoming channels to k_t outgoing channels.

3.1.2 Classical Network

To explain our model of the quantum network, we consider the classical case. When we use the channel only once, each channel transmits one symbol of the finite field $\mathbb{F}_q$. Hence, the information at each time is described by the vector space $\mathbb{F}_q^{m_0}$. We assume that the information conversion at each intermediate node is an invertible and linear operation. That is, the information conversion at intermediate node v_t is written as an invertible $k_t \times k_t$ matrix A_t acting only on the k_t components of the vector space $\mathbb{F}_q^{m_0}$. Therefore, combining all the conversions, the relation between the input information $x \in \mathbb{F}_q^{m_0}$ and the output information $y \in \mathbb{F}_q^{m_0}$ can be characterized by an invertible $m_0 \times m_0$

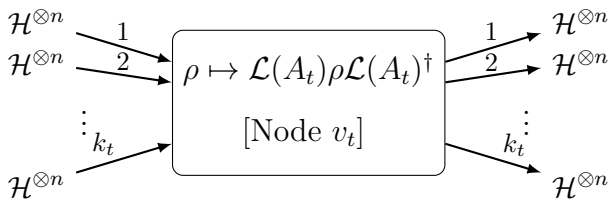


Figure 3.1: Transmission and operation at the intermediate node v_t in quantum network by using the network n times. Both ρ and $\mathcal{L}(A_t)\rho\mathcal{L}(A_t)^\dagger$ are density matrices on $\mathcal{H}^{\otimes k_t \times n}$.

matrix K as

$$y = Kx.$$

We extend the above discussion to the case of n uses of the network, i.e., each channel trasmits n symbols of $\mathbb{F}_q$. We assume that every intermediate node v_t applies the matrix A_t n times. When the input and output informations are written as $m_0 \times n$ matrices X and Y, respectively, we have the relation

$$Y = KX. \tag{3.1}$$

Next, we discuss the case where Eve attacks m_a ($\leq m_1$) channels. Since all the node operations are linear, there is a linear relation between the information on each channel and output information. That is, there are m_a vectors $w_1, \ldots, w_{m_a}$ in $\mathbb{F}_q^{m_0}$ satisfying the following condition: when Eve adds the noise $z_1, \ldots, z_{m_a} \in \mathbb{F}_q^n$ on the m_a attacked channels, the relation (3.1) is changed to

$$Y = KX + \sum_{j=1}^{m_a} w_j z_j^\top = KX + WZ, \tag{3.2}$$

where $W = [w_1, \ldots, w_{m_a}]$ and $Z = [z_1, \ldots, z_{m_a}]^\top$. Here, the vectors $w_1, \ldots, w_{m_a}$ are determined by the network topology and a linear operation on each node. For the detail, see [20, Section 2.2]. Even when Eve chooses the noise dependently of the input information, the output Y is always written in the form (3.2) while Z might depend on X. That is, the noise is given by the subspace $\mathcal{W}_C \otimes \mathbb{F}_q^n$, where $\mathcal{W}_C$ is defined as the subspace spanned by columns of W.

3.1.3 Quantum Network

We consider a natural quantum extension of the above classical network. Each single use of quantum channel transmits a quantum system $\mathcal{H}$ of dimenension q spanned by $\{|x\rangle_b\}_{x\in\mathbb{F}_q}$. In n uses of the network, the whole system

to be transmitted is written as $\mathcal{H}^{\otimes m_0 \times n}$ spanned $\{|X\rangle_b\}_{X \in \mathbb{F}_q^{m_0 \times n}}$. To describe the node operations, we introduce the following unitary operations called *quantum invertible linear operations*

Definition 3.1.1 (Quantum Invertible Linear Operation)**.** *For an invertible $m \times m$ matrix A and an invertible $n \times n$ matrix B, two unitaries $\mathcal{L}(A)$ and $\mathcal{R}(B)$ are defined as*

$$\mathcal{L}(A)|X\rangle_b = |AX\rangle_b,\ \mathcal{R}(B)|X\rangle_b = |XB\rangle_b,\ \ \textit{for any}\, X \in \mathbb{F}_q^{m \times n}.$$

Node v_t converts the information on the subsystem $\mathcal{H}^{\otimes k_t \times n}$ by applying the unitary $\mathcal{L}(A_t)$. When there is no attack, the operation of the whole network is the application of the unitary $\mathcal{L}(K)$.

Next, consider the malicious attack when the maximum number of the attacked channel is m_1 over n uses of the network. To describe the network transmission where Eve attacks m_a ($\leq m_1$) quantum channels in n uses of the network, we introduce the following assumption and notations. Assume that Eve possesses a large quantum system $\mathcal{H}_{\mathcal{W}}$. Denote the set of attacked channels as $E_A := \{e_{a,1}, \ldots, e_{a,m_a}\} \subset E$. The quantum systems possessed by $e_{a,1}, \ldots, e_{a,m_a}$ are spanned by $\{|z^\top\rangle_b\}_{z \in \mathbb{F}_q^n}$ and denoted by $\mathcal{H}_{a,1}, \ldots, \mathcal{H}_{a,m_a}$, respectively. Define a function $\tau : \{1, \ldots, m_a\} \to \{0, \ldots, c\}$ so that the input nodes of the edges $e_{a,1}, \ldots, e_{a,m_a}$ are $v_{\tau(1)}, \ldots, v_{\tau(m_a)}$, respectively. Moreover, define $\mathcal{O}_t := \{i \in \{1, \ldots, m_a\} \mid \tau(i) = t\}$ for $t = 0, \ldots, c$. Then, $\mathcal{H}_{\mathcal{O}_t} := \otimes_{i \in \mathcal{O}_t} \mathcal{H}_{a,i}$ denotes the quantum system of channels attacked at time t by the discussion below.

The transmission on our quantum network with m_a channel attacks is described by the iteration of the following process from time $t = 0$ to $t = c$. At time t, after node v_t applies the node operation $\mathcal{L}(A_t)$ on the quantum system $\mathcal{H}^{\otimes k_t \times n}$ of k_t incoming channels (no operation if $t = 0$), the quantum system $\mathcal{H}^{\otimes k_t \times n}$ is sent through outgoing k_t channels. Among the k_t outgoing channels, the channels $e_{a,i}$ with $i \in \mathcal{O}_t$ are corrupted by Eve's arbitrary operations on $\mathcal{H}_{\mathcal{O}_t} \otimes \mathcal{H}_{\mathcal{W}}$, and then the corrupted quantum systems arrive at the next nodes. Eve's operations can be any trace preserving and completely positive (TP-CP) maps, measurements or both. It can also be adaptive on the previous measurement outcomes and Eve is assumed to know the topology of the network and the node operations in the network. After all of k_t systems arrive at the next nodes, the process at time t ends.

3.2 Main Results

Our code is a pair of an encoder and a decoder and it is constructed without any knowledge of the network: the node operations $\mathcal{L}(A_t)$, network operation

$\mathcal{L}(K)$ nor the topology of the network. In the following, we use the given quantum network n times, i.e., the block-length is n.

Main Idea in Our Code: Our quantum code is designed based on the classical network codes in [9, 18] which correct malicious injection by finding the subspace of injection from the received message and then recovering the original message from the information not in the injected subspace. In the analysis of our code, we reduce the correctness of our code to that of two classical codes with respect to bit basis and phase basis. In that reduction, our quantum code is sophisticatedly defined so that the two classical codes are similar to the codes in [9, 18]. A difficult point in this reduction to the classical codes is that the accessible information from the network output state is restricted since measurement disturbs the quantum states, whereas the classical codes [9, 18] have access to all information of the network output. Our code circumvents this difficulty by attaching to the codeword the ancilla whose measurement outcome contains sufficient information for finding the subspace of injection.

Main Results: First, we present the coding theorem with use of the secret shared randomness of negligible rate. The shared randomness between the encoder and the decoder plays a crucial role in our code. The results are stated with respect to the entanglement fidelity for the quantum protocol $\kappa^{(n)}$, a purification $|x\rangle$ of the state ρ and the identity operator ι_R on the reference system. Here, the quantum protocol $\kappa^{(n)}$ is the combination of the encoding, network tranmission with attack and the decoding, and it is formally defined in Section 3.5. The completely mixed state is denoted as ρ_{mix}.

Theorem 3.2.1 (Quantum Network Code with Negligible Rate Secret Shared Randomness)**.** *Suppose that the operation of the whole network is the application of the unitary $\mathcal{L}(K)$ of an invertible matrix $K \in \mathbb{F}_q^{m_0 \times m_0}$ and at most m_1 channels are attacked over the entire uses of the network. When $m_1 < m_0/2$ holds and the sender and the receiver can share the secret randomness with a negligible rate in comparison with the block-length n, independently of the invertible matrix K, there exists a sequence of quantum network codes which implements the quantum transmission TP-CP map $\kappa^{(n)}$ from $\mathcal{H}_{\mathrm{code}}^{(n)}$ to itself where $\lim_{n\to\infty}(1/n)\cdot \log_q \dim \mathcal{H}_{\mathrm{code}}^{(n)} = m_0 - 2m_1$ holds and the entanglement fidelity $F_e^2(\rho_{\mathrm{mix}}, \kappa^{(n)})$ satisfies $\lim_{n\to\infty} n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa^{(n)})) = 0$.* □

Notice that this code depends only on the rates m_0 and m_1, and does not depend on the detailed structure of the network. Section 3.4 gives the code realizing the performance mentioned in Theorem 3.2.1. In Sections 3.5 and 3.6 it is proved that the code given in Section 3.4 satisfies the performance mentioned in Theorem 3.2.1.

Indeed, it is known that there exists a classical network code to transmit classical information securely when the number of attacked channels is less than a half of the transmission rate from the sender to the receiver [16]. Although Theorem 3.2.1 requires secure transmission of classical information with negligible rate, the result [16] mentioned that such secure transmission can be realized by using our quantum network in bit basis states with the negligible number of times. Hence, as shown in Section 3.7, the combination of the result [16] and Theorem 3.2.1 yields the following theorem.

Theorem 3.2.2 (Quantum Network Code without Classical Communication)**.** *Suppose that the operation of the whole network is the application of the unitary $\mathcal{L}(K)$ of an invertible matrix $K \in \mathbb{F}_q^{m_0 \times m_0}$ and at most m_1 channels are attacked over the entire uses of the network. When $m_1 < m_0/2$, independently of the invertible matrix K, there exists a sequence of quantum network codes which implements the quantum transmission TP-CP map $\kappa^{(n)}$ from $\mathcal{H}_{\rm code}^{(n)}$ to itself where $\lim_{n\to\infty}(1/n)\cdot \log_q \dim \mathcal{H}_{\rm code}^{(n)} = m_0 - 2m_1$ holds and the entanglement fidelity $F_e^2(\rho_{\rm mix}, \kappa^{(n)})$ satisfies $\lim_{n\to\infty} n(1 - F_e^2(\rho_{\rm mix}, \kappa^{(n)})) = 0$.* □

Connection to Code in [8] : The quantum error-correcting code in [8] asymptotically corrects arbitrary errors when the number of errors is less than a half of the code length. Therefore, if the network consists of parallel m_0 channels (i.e., $\mathcal{L}(K)$ is the identity operator), the code in [8] can be applied to our network. However, if $\mathcal{L}(K)$ is not the identity, the code in [8] cannot be applied because even one network channel attack might corrupt all m_0 network outputs by error propagation. In this sense, our code generalizes the result in [8], but instead, we employ the secret shared randomness between the encoder and the decoder. As mentioned above, however, we can share the secret randomness necessary for our code without losing any asympototic rate by attaching the protocol in [16].

3.3 Preliminaries

3.3.1 Phase Basis

We discuss the operation on the phase basis $\{|z\rangle_p\}_{z\in\mathbb{F}_q}$ defined as [17, Section 8.1.2]

$$|z\rangle_p := \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \omega^{-\operatorname{tr}(xz)} |x\rangle_b,$$

where $\omega := \exp(2\pi i/p)$ and $\operatorname{tr} y := \operatorname{Tr} M_y$ ($y \in \mathbb{F}_q$) with the multiplication map $M_y : x \mapsto yx$ identifying the finite field $\mathbb{F}_q$ with the vector space $\mathbb{F}_p^t$. The following Lemma 3.3.1 shows the application of the unitaries $\mathcal{L}(A)$ and $\mathcal{R}(A)$ to the phase basis states, and is proved in Appendix A.

Lemma 3.3.1. *When $A \in \mathbb{F}_q^{m\times m}$ and $B \in \mathbb{F}_q^{n\times n}$ are invertible matrices, any $M \in \mathbb{F}_q^{m\times n}$ satisfies*

$$\mathcal{L}(A)|M\rangle_p = |(A^\top)^{-1}M\rangle_p, \quad \mathcal{R}(B)|M\rangle_p = |M(B^\top)^{-1}\rangle_p.$$

We use notation $[C]_p := (C^{-1})^\top = (C^\top)^{-1}$ for an invertible matrix C.

3.3.2 Extended Quantum System in Our Code

In our code, the extended quantum system $\mathcal{H}'$, described below, is considered as a unit quantum system of encoding and decoding operations. Dependently of the block-length n, we choose an integer α such that α and the power $q' := q^\alpha$ of q satisfy the conditions $\lim_{n\to\infty} \alpha/n = 0$ and $\lim_{n\to\infty} n \cdot (n')^{m_0}/(q')^{m_0-m_1} = 0$ (e.g. $\alpha = \lceil (1+(2+m_1)/(m_0-m_1)) \log_q n \rceil$) where $n = n'\alpha$. We identify the system $\mathcal{H}' := \mathcal{H}^{\otimes\alpha}$ with the system spanned by $\{|x\rangle_b\}_{x\in\mathbb{F}_{q'}}$. Then, n uses of our quantum network can be regarded as n' uses of quantum network over the quantum system $\mathcal{H}'$. Similarly to the system $\mathcal{H}$, for invertible matrices $A \in \mathbb{F}_{q'}^{m\times m}$ and $B \in \mathbb{F}_{q'}^{n\times n}$, two unitaries $\mathcal{L}'(A)$ and $\mathcal{R}'(B)$ are defined as

$$\mathcal{L}'(A)|X\rangle_b = |AX\rangle_b,\ \mathcal{R}'(B)|X\rangle_b = |XB\rangle_b, \ \text{ for any} X \in \mathbb{F}_{q'}^{m\times n}.$$

Lemma 3.3.1 is also satisfied for $\mathcal{L}'(A)$ and $\mathcal{R}'(B)$.

3.3.3 Notations for Quantum Systems

By n uses of the network, the quantum system $\mathcal{H}^{\otimes m_0\times n} = (\mathcal{H}')^{\otimes m_0\times n'}$ is transmitted. We denote

$$(\mathcal{H}')^{\otimes m_0\times n'} = \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}} := (\mathcal{H}')^{\otimes m_0\times m_0} \otimes (\mathcal{H}')^{\otimes m_0\times m_0} \otimes (\mathcal{H}')^{\otimes m_0\times(n'-2m_0)}.$$

Moreover, for $\mathcal{X} \in \{\mathcal{A}, \mathcal{B}, \mathcal{C}\}$ and $(m_{\mathcal{A}}, m_{\mathcal{B}}, m_{\mathcal{C}}) := (m_0, m_0, n' - 2m_0)$, we define

$$\mathcal{H}'_{\mathcal{X}} = \mathcal{H}'_{\mathcal{X}1} \otimes \mathcal{H}'_{\mathcal{X}2} \otimes \mathcal{H}'_{\mathcal{X}3} := (\mathcal{H}')^{\otimes m_1\times m_{\mathcal{X}}} \otimes (\mathcal{H}')^{\otimes(m_0-2m_1)\times m_{\mathcal{X}}} \otimes (\mathcal{H}')^{\otimes m_1\times m_{\mathcal{X}}}.$$

The tensor product state on $\mathcal{H}'_{\mathcal{X}}$ of $|\phi\rangle \in \mathcal{H}'_{\mathcal{X}1}, |\psi\rangle \in \mathcal{H}'_{\mathcal{X}2}$, and $|\varphi\rangle \in \mathcal{H}'_{\mathcal{X}3}$ is denoted as

$$\begin{bmatrix} |\phi\rangle \\ |\psi\rangle \\ |\varphi\rangle \end{bmatrix} := |\phi\rangle \otimes |\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}'_{\mathcal{X}}.$$

The bit or phase basis state of block matrix is denoted by

$$\left|\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right\rangle_b := \begin{bmatrix} |X\rangle_b \\ |Y\rangle_b \\ |Z\rangle_b \end{bmatrix}, \quad \left|\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right\rangle_p := \begin{bmatrix} |X\rangle_p \\ |Y\rangle_p \\ |Z\rangle_p \end{bmatrix},$$

where $(X, Y, Z) \in \mathbb{F}_q^{m_1 \times m_{\mathcal{X}}} \times \mathbb{F}_q^{(m_0-2m_1)\times m_{\mathcal{X}}} \times \mathbb{F}_q^{m_1 \times m_{\mathcal{X}}}$.

On the other hand, $\mathbf{0}_{k,l}$ denotes the $k \times l$ zero matrix in $\mathbb{F}_q^{k\times l}$ and $|i,j\rangle := |i\rangle \otimes |j\rangle$.

3.3.4 CSS code in our quantum network code

In our code, we employ CSS code described in this subsection. Define classical codes $C_1, C_2 \subset \mathbb{F}_{q'}^{m_0\times(n'-2m_0)}$ by

$$C_1 := \left\{ \begin{bmatrix} \mathbf{0}_{m_1,n'-2m_0} \\ X_2 \\ X_3 \end{bmatrix} \in \mathbb{F}_{q'}^{m_0\times(n'-2m_0)} \middle| X_2 \in \mathbb{F}_{q'}^{(m_0-2m_1)\times(n'-2m_0)}, X_3 \in \mathbb{F}_{q'}^{m_1\times(n'-2m_0)} \right\},$$

$$C_2 := \left\{ \begin{bmatrix} X_1 \\ X_2 \\ \mathbf{0}_{m_1,n'-2m_0} \end{bmatrix} \in \mathbb{F}_{q'}^{m_0\times(n'-2m_0)} \middle| X_1 \in \mathbb{F}_{q'}^{m_1\times(n'-2m_0)}, X_2 \in \mathbb{F}_{q'}^{(m_0-2m_1)\times(n'-2m_0)} \right\}.$$

Classical codes C_1 and C_2 satisfy $C_1 \supset C_2^{\perp}$. For any coset $[M_1] \in C_1/C_2^{\perp}$ containing $M_1 \in \mathbb{F}_{q'}^{(m_0-2m_1)\times(n'-2m_0)}$, define a quantum state $|[M_1]\rangle_b \in \mathcal{H}'_{\mathcal{C}}$ by

$$|[M_1]\rangle_b := \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{Y\in C_2^{\perp}} \left| \begin{bmatrix} \mathbf{0}_{m_1,n'-2m_0} \\ M_1 \\ \mathbf{0}_{m_1,n'-2m_0} \end{bmatrix} + Y \right\rangle_b = \begin{bmatrix} |\mathbf{0}_{m_1,n'-2m_0}\rangle_b \\ |M_1\rangle_b \\ |\mathbf{0}_{m_1,n'-2m_0}\rangle_p \end{bmatrix}.$$

With the above definitions, the code space is given as $\mathcal{H}_{\text{code}}^{(n)} := \mathcal{H}'_{\mathcal{C}2} = (\mathcal{H}')^{\otimes(m_0-2m_1)\times(n'-2m_0)}$, and a state $|\phi\rangle \in \mathcal{H}_{\text{code}}^{(n)}$ is encoded as

$$\begin{bmatrix} |\mathbf{0}_{m_1,n'-2m_0}\rangle_b \\ |\phi\rangle \\ |\mathbf{0}_{m_1,n'-2m_0}\rangle_p \end{bmatrix} \in \mathcal{H}'_{\mathcal{C}}.$$

3.4 Code Construction with Negligible Rate Secret Shared Randomness

Now, we describe the quantum network code with the secret shared randomness of negligible rate. In our code, the encoder and decoder are determined by secret random variables $SR = (R_2, V)$ and R_0. These random variables are chosen uniformly and independently satisfying the following conditions: the random variable $R_2 = (R_{2,b}, R_{2,p}) \in \mathbb{F}_{q'}^{(m_0-m_1)\times m_0} \times \mathbb{F}_{q'}^{(m_0-m_1)\times m_0}$ consists of two random matrices $R_{2,b}, R_{2,p}$ of rank $m_0 - m_1$, the random variable $V = (V_1, \ldots, V_{4m_0})$ consists of $4m_0$ random variables $V_1, \ldots, V_{4m_0} \in \mathbb{F}_{q'}$, and the random variable $R_0 \in \mathbb{F}_{q'}^{m_0\times m_0}$ is an $m_0 \times m_0$ invertible matrix. Before the encoding, the random variable SR is shared between encoder and decoder, and R_0 is owned by encoder. Note that the size of the shared secret random variable SR is negligible with respect to n.

Depending on the secret random variables SR and R_0, the encoder $\mathcal{E}^{SR,R_0}$ is defined as an isometry quantum channel from $\mathcal{H}_{\rm code}^{(n)}$ to

$$\mathcal{H}^{\otimes m_0\times n} = (\mathcal{H}')^{\otimes m_0\times n'} = \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}.$$

Depending on the secret shared random variable SR, the decoder $\mathcal{D}^{SR}$ is defined as a TP-CP map from $\mathcal{H}^{\otimes m_0\times n}$ to $\mathcal{H}_{\rm code}^{(n)}$. We give the details of the encoder $\mathcal{E}^{SR,R_0}$ and the decoder $\mathcal{D}^{SR}$ in the following subsections.

3.4.1 Encoder $\mathcal{E}^{SR,R_0}$

We give the encoding operation when the input state is a state $|\phi\rangle \in \mathcal{H}_{\rm code}^{(n)}$.

Encode 1 (Check Bit Embedding) Encode the input state $|\phi\rangle$ by an isometry map $U_1^{R_2} : \mathcal{H}_{\rm code}^{(n)} \to \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{B} \otimes \mathcal{H}'_{\mathcal{C}}$ defined as

$$|\phi_1\rangle := U_1^{R_2}|\phi\rangle = \left|\begin{bmatrix}\mathbf{0}_{m_1,m_0}\\ R_{2,b}\end{bmatrix}\right\rangle_b \otimes \left|\begin{bmatrix}R_{2,p}\\ \mathbf{0}_{m_1,m_0}\end{bmatrix}\right\rangle_p \otimes \begin{bmatrix}|\mathbf{0}_{m_1,n'-2m_0}\rangle_b\\ |\phi\rangle\\ |\mathbf{0}_{m_1,n'-2m_0}\rangle_p\end{bmatrix}.$$

Encode 2 (Vertical Mixing) Encode $|\phi_1\rangle$ with the unitary map $\mathcal{L}'(R_0) := \sum_{X\in\mathbb{F}_{q'}^{m_0\times n'}} |R_0X\rangle\langle X|$ as

$$|\phi_2\rangle := \mathcal{L}'(R_0)|\phi_1\rangle \in \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}.$$

Encode 3 (Horizontal Mixing) From the shared randomness V, define matrices $Q_{1;i,j} := (V_j)^i$, $Q_{2;i,j} := (V_{m_0+j})^i$ for $1 \le i \le n' - 2m_0$,

$1 \leq j \leq m_0$, and $Q_{3;i,j} := (V_{2m_0+j})^i$, $Q_{4;i,j} := (V_{3m_0+j})^i$ for $1 \leq i \leq m_0$ and $1 \leq j \leq m_0$. With these matrices, define the random matrix $R_1^V \in \mathbb{F}_{q'}^{n' \times n'}$ as

$$R_1^V := \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ Q_3^\top Q_4 & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & Q_2^\top \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ Q_1 & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix},$$

where I_d is the d-dimensional identity matrix.

Encode $|\phi_2\rangle$ with the unitary map $\mathcal{R}'(R_1^V) := \sum_{X \in \mathbb{F}_{q'}^{m_0 \times n'}} |XR_1^V\rangle\langle X|$ as

$$|\phi_3\rangle := \mathcal{R}'(R_1^V)|\phi_2\rangle \in \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}.$$

Therefore, the encoder $\mathcal{E}^{SR,R_0}$ is the isometry map written as

$$\mathcal{E}^{SR,R_0} : |\phi\rangle \mapsto \mathcal{R}'(R_1^V)\mathcal{L}'(R_0)U_1^{R_2}|\phi\rangle \in \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}.$$

3.4.2 Decoder $\mathcal{D}^{SR}$

We give the decoding operation when the input state is a state $|\psi\rangle \in \mathcal{H}^{m_0 \times n} = \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$.

Decode 1 (Decoding of Encode 3) Construct $(R_1^V)^{-1}$ from the shared randomness $V = (V_1, \ldots, V_{4m_0})$ as

$$(R_1^V)^{-1} := \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ -Q_1 & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & -Q_2^\top \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ -Q_3^\top Q_4 & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix}.$$

The unitary map $\mathcal{R}'(R_1^V)^\dagger = \sum_{X \in \mathbb{F}_{q'}^{m_0 \times n'}} |X(R_1^V)^{-1}\rangle\langle X|$ is the decoder for the encoder $\mathcal{R}'(R_1^V)$. By applying $\mathcal{R}'(R_1^V)^\dagger$, the state $|\psi\rangle$ is decoded as

$$|\psi_1\rangle := \mathcal{R}'(R_1^V)^\dagger |\psi\rangle \in \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}.$$

Decode 2 (Error Correction) Perform the bit and the phase basis measurements on the systems $\mathcal{H}'_{\mathcal{A}}$ and $\mathcal{H}'_{\mathcal{B}}$, respectively. The measurement outcomes are denoted as $O_b, O_p \in \mathbb{F}_{q'}^{m_0 \times m_0}$. With these measurement outcomes, find the invertible matrices $D_{3,b}^{R_2,O_b}, D_{3,p}^{R_2,O_p} \in \mathbb{F}_{q'}^{m_0 \times m_0}$ as the solutions to satisfy

$$P_{\mathcal{W}_b} D_{3,b}^{R_2,O_b} O_b = \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix}, \tag{3.3}$$

$$P_{\mathcal{W}_p} [D_{3,p}^{R_2,O_p}]_p O_p = \begin{bmatrix} R_{2,p} \\ \mathbf{0}_{m_1,m_0} \end{bmatrix}, \tag{3.4}$$

where $P_{\mathcal{W}_b}$ and $P_{\mathcal{W}_p}$ are projections to the subspaces $\mathcal{W}_b, \mathcal{W}_p \subset \mathbb{F}_{q'}^{m_0}$ whose 1-st, ..., (m_1)-th elements are 0 and $(m_0 - m_1 + 1)$-st, ..., (m_0)-th elements are 0, respectively.

If the invertible matrix $D_{3,b}^{R_2,O_b}$ or $D_{3,p}^{R_2,O_p}$ does not exist, decoder applies no operation. Otherwise, apply the unitary maps $\mathcal{L}'(D_{3,b}^{R_2,O_b})$ and $\mathcal{L}'(D_{3,p}^{R_2,O_p})$ to the system $\mathcal{H}'_{\mathcal{C}}$ (if the solution $D_{3,b}^{R_2,O_b}$ of (3.3) or $D_{3,p}^{R_2,O_p}$ of (3.4) is not unique, decide $D_{3,b}^{R_2,O_b}$ or $D_{3,p}^{R_2,O_p}$ deterministically depending on R_2, O_b, O_p). After applying $\mathcal{L}'(D_{3,b}^{R_2,O_b})$ and $\mathcal{L}'(D_{3,p}^{R_2,O_p})$, Decode 2 outputs the reduced state on $\mathcal{H}'_{\mathcal{C}2} = \mathcal{H}_{\rm code}^{(n)}$.

The above process in Decode 2 is summarized as a TP-CP map $\mathcal{D}_2$ from $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$ to $\mathcal{H}_{\rm code}^{(n)}$ by

$$\mathcal{D}_2(|\psi_1\rangle\langle\psi_1|) := \operatorname*{Tr}_{\mathcal{C}1,\mathcal{C}3} \sum_{X_b, X_p \in \mathbb{F}_{q'}^{m_0 \times m_0}} \mathbf{D}_3^{R_2,X_b,X_p} \rho_{X_b,X_p|\psi_1\rangle} (\mathbf{D}_3^{R_2,X_b,X_p})^\dagger,$$

where the matrix $\rho_{X_b,X_p|\psi_1\rangle}$ and the unitary $\mathbf{D}_3^{R_2,X_b,X_p}$ are defined as

$$\rho_{X_b,X_p|\psi_1\rangle} := \operatorname*{Tr}_{\mathcal{A},\mathcal{B}} |\psi_1\rangle\langle\psi_1| (|X_b\rangle_{bb}\langle X_b| \otimes |X_p\rangle_{pp}\langle X_p| \otimes I_{\mathcal{C}}),$$
$$\mathbf{D}_3^{R_2,X_b,X_p} := \mathcal{L}'(D_{3,p}^{R_2,X_p}) \mathcal{L}'(D_{3,b}^{R_2,X_b}).$$

Therefore, the decoder $\mathcal{D}^{SR}$ is a TP-CP map written as

$$\mathcal{D}^{SR}(|\psi\rangle\langle\psi|) = \mathcal{D}_2\big(\mathcal{R}'(R_1^V)^\dagger|\psi\rangle\langle\psi|\mathcal{R}'(R_1^V)\big).$$

Since the size of the shared randomness SR is sublinear with respect to n, our code is constructed with a shared randomness of negligible rate. Moreover, since the dimension of the code space $\mathcal{H}_{\text{code}}^{(n)}$ is $(q')^{(m_0-2m_1)(n'-2m_0)} = q^{(m_0-2m_1)(n-2\alpha m_0)}$ and α is taken as to satisfy $\lim_{n\to\infty}\alpha/n = 0$ in Section 3.3.2, the code rate is $m_0 - 2m_1$, i.e., $\lim_{n\to\infty}\frac{1}{n}\log_q \dim \mathcal{H}_{\text{code}}^{(n)} = m_0 - 2m_1$.

3.5 Correctability of Our Code

For analysis of the correctability of our code, we consider the situation that the authorized sender, Alice, sends quantum information to the authorized receiver, Bob, through the quantum network with the existence of Eve who attacks the network. To keep security from Eve's attack, Alice and Bob communicate using the secure quantum network code introduced in Section 3.4.

Let Γ be the TP-CP map of the given quantum network with malicious attacks. If the encoder and the decoder are defined as a probabilistic mixture by the uniformly chosen random variables SR and R_0, the entire protocol is written as

$$\kappa^{(n)}(\rho) = \sum_{SR,R_0}\frac{1}{N}\mathcal{D}^{SR}\circ\Gamma\circ\mathcal{E}^{SR,R_0}(\rho),$$

where N is the size of the random variables written as $N := (q')^{4m_0} + 2\cdot|\{X \in \mathbb{F}_{q'}^{(m_0-m_1)\times m_0} \mid \operatorname{rank} X = m_0 - m_1\}| + |\{R_0 \in \mathbb{F}_{q'}^{m_0\times m_0} \mid R_0 \text{ is invertible}\}|$.

The correctability of the transmission is evaluated by the entanglement fidelity $F_e(\rho_{\text{mix}}, \kappa^{(n)})$ for the channel $\kappa^{(n)}$ with respect to the completely mixed state ρ_{mix} on $\mathcal{H}_{\text{code}}^{(n)}$, which is defined by

$$F_e^2(\rho_{\text{mix}}, \kappa^{(n)}) = \langle\Phi|\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)|\Phi\rangle,$$

where $|\Phi\rangle := \frac{1}{\sqrt{(q')^m}}\sum_{M\in\mathbb{F}_{q'}^m}|M,M\rangle_b$ and $m := (m_0-2m_1)\times(n'-2m_0)$. This value is evaluated by

$$\begin{aligned}
1 - F_e^2(\rho_{\text{mix}}, \kappa^{(n)}) &= 1 - \langle\Phi|\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)|\Phi\rangle \\
&= \operatorname{Tr}\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I - P_bP_p) \qquad (3.5)\\
&\le \operatorname{Tr}\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I-P_b) + \operatorname{Tr}\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I-P_p). \qquad (3.6)
\end{aligned}$$

where $P_b := \sum_{M\in\mathbb{F}_{q'}^m} |M,M\rangle_{bb}\langle M,M|$, $P_p := \sum_{M\in\mathbb{F}_{q'}^m} |M,\bar{M}\rangle_{pp}\langle M,\bar{M}|$, and $|\bar{M}\rangle_p$ is complex conjugate of $|M\rangle_p \in \mathcal{H}_{\rm code}^{(n)} = (\mathcal{H}')^{\otimes m}$. Eq. (3.5) holds from $P_bP_p = |\Phi\rangle\langle\Phi|$ proved in Lemma A.2.2.

We show that the first term $\mathrm{Tr}\,\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I-P_b)$ of (3.6) is *the bit error probability* which is defined as the average probability that the bit basis state $|M\rangle_b \in \mathcal{H}_{\rm code}^{(n)}$ is sent but the bit measurement outcome on the protocol output is not M. For a bit basis state $|M\rangle_b \in \mathcal{H}_{\rm code}^{(n)}$, we have

$$\mathrm{Tr}(P_b\cdot\kappa^{(n)}\otimes\iota_R(|M,M\rangle_{bb}\langle M,M|)) = {}_b\langle M|\kappa^{(n)}(|M\rangle_{bb}\langle M|)|M\rangle_b.$$

Since the entangled state $|\Phi\rangle$ is a superposition of bit basis states $|i,i\rangle_b$, the bit error probability is given as the first term $\mathrm{Tr}\,\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I-P_b)$ of (3.6). Similarly, since the entangled state $|\Phi\rangle$ is given as the superposition of the phase basis state $|i,\bar{i}\rangle_p$ (see Lemma A.2.1), the second term $\mathrm{Tr}\,\kappa^{(n)}\otimes\iota_R(|\Phi\rangle\langle\Phi|)(I-P_p)$ of (3.6) is *the phase error probability* defined in the same way as the bit error probability. Therefore, we can bound the entanglement fidelity as

$$1-F_e^2(\rho_{\rm mix},\kappa^{(n)}) \le (\text{bit error prob.}) + (\text{phase error prob.}).$$

As shown in the next section, the bit and the phase error probabilities are upper bounded by $O\Big(\max\Big\{\frac{1}{q'},\frac{(n')^{m_0}}{(q')^{m_0-m_1}}\Big\}\Big)$. That is,

$$1-F_e^2(\rho_{\rm mix},\kappa^{(n)}) \le O\left(\max\left\{\frac{1}{q'},\frac{(n')^{m_0}}{(q')^{m_0-m_1}}\right\}\right).$$

Since q' is taken to satisfy $\lim_{n\to\infty}\frac{n\cdot(n')^{m_0}}{(q')^{m_0-m_1}} = 0$ in Section 3.3.2 and this implies $\lim_{n\to\infty} n/q' = 0$, the protocol satisfies $\lim_{n\to\infty} n(1-F_e^2(\rho_{\rm mix},\kappa^{(n)})) = 0$. Hence, our proof of Theorem 3.2.1 is completed.

Remark 3.5.1. *Since the bit and phase bases are mutually unbiased bases, the evaluation in this section is a special case of Corollary 2.5.3 and Theorem 2.5.3.*

3.6 Bit and Phase Error Probabilities

In this section, we bound separately the bit error probability and the phase error probability. Throughout in this section, we assume $m_a \le m_1 < m_0/2$. For notational convenience, for any integer k and any matrix $X \in \mathbb{F}_{q'}^{k\times n'}$, we denote

$$X = (X^{\mathcal{A}}, X^{\mathcal{B}}, X^{\mathcal{C}}) \in \mathbb{F}_{q'}^{k\times m_0}\times\mathbb{F}_{q'}^{k\times m_0}\times\mathbb{F}_{q'}^{k\times(n'-2m_0)}.$$

3.6.1 Application of the Protocol in Bit Basis

We first calculate the bit error probability. Assume that the input state is a bit basis state $|M\rangle_b \in \mathcal{H}_{\text{code}}^{(n)}$. When Alice sends $\mathcal{E}^{SR,R_0}(|M\rangle_{bb}\langle M|)$ over the network, Bob receives the state $\rho_{\text{receive}} := \Gamma \circ \mathcal{E}^{SR,R_0}(|M\rangle_{bb}\langle M|)$ on $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$.

Note that the bit basis measurement on $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$ commutes with the decoding operation $\mathcal{D}^{SR}$. That is, applying the quantum decoder $\mathcal{D}^{SR}$ and then performing the bit basis measurement on $\mathcal{H}_{\text{code}}^{(n)}$ is equivalent to performing the bit basis measurement on $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$ and then applying the classical decoding corresponding to the quantum decoder $\mathcal{D}^{SR}$. Therefore, we adopt the latter method to calculate the bit error probability.

After ρ_{receive} is received, perform the bit basis measurement on $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$ and denote the measurement outcome as a matrix $Y \in \mathbb{F}_{q'}^{m_0 \times n'}$. From (3.2), Y is written as

$$Y := \tilde{K}X' + \tilde{W}, \tag{3.7}$$

where $\tilde{K} \in \mathbb{F}_{q'}^{m_0 \times m_0}$ and $\tilde{W} \in \mathbb{F}_{q'}^{m_0 \times n'}$ are matrices equivalent to $K \in \mathbb{F}_q^{m_0 \times m_0}$ and $WZ \in \mathbb{F}_q^{m_0 \times n}$ in (3.2) by field extension, respectively, and $X' := R_0 X R_1^V \in \mathbb{F}_{q'}^{m_0 \times n'}$ for $X \in \mathbb{F}_{q'}^{m_0 \times n'}$ defined with some matrices $\bar{E}_1 \in \mathbb{F}_{q'}^{(m_0-m_1)\times m_0}$, $\bar{E}_2 \in \mathbb{F}_{q'}^{m_1 \times m_0}$, and $\bar{E}_3 \in \mathbb{F}_{q'}^{m_1 \times (n'-2m_0)}$ by

$$X := \left[\begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix}, \begin{bmatrix} \bar{E}_1 \\ \bar{E}_2 \end{bmatrix}, \begin{bmatrix} \mathbf{0}_{m_1,n'-2m_0} \\ M \\ \bar{E}_3 \end{bmatrix} \right]. \tag{3.8}$$

On the other hand, the decoder decodes Y to

$$Y' := D_{3,b}^{R_2,O_b} Y (R_1^V)^{-1} = D_{3,b}^{R_2,O_b} (\tilde{K} R_0 X + \tilde{W}(R_1^V)^{-1}).$$

If the original message $M \in \mathbb{F}_{q'}^{(m_0-2m_1)\times(n'-2m_0)}$ is contained in Y', the decoding succeeds. We calculate the probability that $[M^\top, \bar{E}_3^\top]^\top \in \mathbb{F}_{q'}^{(m_0-m_1)\times(n'-2m_0)}$ in the rightmost block matrix of (3.8) is recovered instead of M. Then, the decoding success probability is lower bounded by this probability.

3.6.2 Existence of Recovery Map (bit error)

In this subsection, we show that there exists a recovery map to the original message M if we assume

$$\operatorname{Im} \tilde{K} R_0|_{\mathcal{W}_b} \cap \operatorname{Im} \tilde{W} = \{\mathbf{0}_{m_0,1}\}. \tag{3.9}$$

If (3.9) is assumed, a map $D_b : \operatorname{Im}\tilde{K}R_0|_{\mathcal{W}_b} \oplus \operatorname{Im}\tilde{W} \to \mathbb{F}_{q'}^{m_0}$ can be defined which is an inverse map of $\tilde{K}R_0$ for the vectors in $\operatorname{Im}\tilde{K}R_0|_{\mathcal{W}_b}$ and a map into $\mathcal{W}_b^{\perp}$ for the vectors in $\operatorname{Im}\tilde{W}$. Then, for any $x \in \mathcal{W}_b$ and any $r \in \mathbb{F}_{q'}^{n'}$, we have $P_{\mathcal{W}_b} D_b(\tilde{K}R_0 x + \tilde{W}r) = x$. Therefore, for any $M \in \mathbb{F}_{q'}^{(m_0-2m_1)\times(n'-2m_0)}$ and any $\bar{E}_3 \in \mathbb{F}_{q'}^{m_1\times(n'-2m_0)}$, the map D_b recovers the original message M as

$$\begin{aligned}(P_{\mathcal{W}_b} D_b Y (R_1^V)^{-1})^{\mathcal{C}} =& P_{\mathcal{W}_b} D_b Y ((R_1^V)^{-1})^{\mathcal{C}} \\ =& P_{\mathcal{W}_b} D_b \left(\tilde{K}R_0 \begin{bmatrix} \mathbf{0}_{m_1,n'-2m_0} \\ M \\ \bar{E}_3 \end{bmatrix} + \tilde{W}((R_1^V)^{-1})^{\mathcal{C}} \right) \\ =& \begin{bmatrix} \mathbf{0}_{m_1,n'-2m_0} \\ M \\ \bar{E}_3 \end{bmatrix}. \end{aligned} \tag{3.10}$$

On the other hand, Eq. (3.9) holds with probability at least $1 - O(1/q')$ as follows. It is shown by the following Lemma 3.6.1 applied with $\mathcal{V} = \mathbb{F}_{q'}^{m_0}$, $\mathcal{W} = \operatorname{Im}\tilde{W}$, and $\mathcal{R} = \operatorname{Im}\tilde{K}R_0|_{\mathcal{W}_b}$. In this case, $n_1 = \operatorname{rank}\tilde{W} \le m_a \le m_1$ from $\operatorname{rank}\tilde{W} \le \operatorname{rank} WZ \le \operatorname{rank} W \le m_a \le m_1$, and $n_2 = \operatorname{rank}\tilde{K}R_0|_{\mathcal{W}_b} = m_0 - m_1$ because $\tilde{K}, R_0$ are invertible and $\dim \mathcal{W}_b = m_0 - m_1$. Therefore,

$$\Pr[(3.9)] = 1 - O\Big((q')^{\dim\tilde{W}-m_1-1}\Big) \ge 1 - O\left(\frac{1}{q'}\right). \tag{3.11}$$

Lemma 3.6.1. *For integers $n_0 \ge n_1 + n_2$, we fix an n_0-dimensional vector space $\mathcal{V}$ over $\mathbb{F}_q$ and an n_1-dimensional subspace $\mathcal{W} \subset \mathcal{V}$, and randomly choose an n_2-dimensional subspace $\mathcal{R} \subset \mathcal{V}$ with the uniform distribition. Then, we have*

$$\Pr[\mathcal{W} \cap \mathcal{R} = \{0\}] = 1 - O(q^{n_1+n_2-n_0-1}).$$

Proof. The probability $\Pr[\mathcal{W} \cap \mathcal{R} = \{0\}]$ is the same as the probability to choose n_2 linearly independent vectors so that they do not intersect with $\mathcal{R}$. Therefore, we have

$$\begin{aligned}\Pr[\mathcal{W} \cap \mathcal{R} = \{0\}] &= \left[\frac{q^{n_0} - q^{n_1}}{q^{n_0}}\right] \cdot \left[\frac{q^{n_0} - q^{n_1+1}}{q^{n_0} - q^1}\right] \cdot \cdots \cdot \left[\frac{q^{n_0} - q^{n_1+n_2-1}}{q^{n_0} - q^{n_2-1}}\right] \\ &= 1 - O(q^{n_1+n_2-n_0-1}).\end{aligned}$$

□

3.6.3 Discoverability of Recovery Map (bit error)

In this subsection, we calculate the probability that the solution $D_{3,b}^{R_2,O_b}$ of (3.3) is a recovery map. Throughout this subsection, we assume (3.9) holds, i.e., a recovery map exists.

Since the bit measurement outcome O_b in Decode 2 is $(Y(R_1^V)^{-1})^{\mathcal{A}} = Y((R_1^V)^{-1})^{\mathcal{A}}$, Eq. (3.3) is written as

$$P_{\mathcal{W}_b} D_{3,b}^{R_2 O_b}\left(\tilde{K} R_0 \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix} + \tilde{W}((R_1^V)^{-1})^{\mathcal{A}}\right) = \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix}. \tag{3.12}$$

If it holds that

$$\mathrm{rank}\left(\tilde{K} R_0 \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix} + \tilde{W}((R_1^V)^{-1})^{\mathcal{A}}\right) = \mathrm{rank} R_{2,b} + \mathrm{rank}\tilde{W}, \tag{3.13}$$

the columns of $\tilde{K} R_0 [\mathbf{0}_{m_1,m_0}^\top, R_{2,b}^\top]^\top + \tilde{W}((R_1^V)^{-1})^{\mathcal{A}}$ span $\mathrm{Im}\, \tilde{K} R_0|_{\mathcal{W}_b} \oplus \mathrm{Im}\, \tilde{W}$. Therefore, if Eq. (3.13) holds, the solution $D_{3,b}^{R_2,O_b}$ of (3.12) satisfies (3.10) with $D_b := D_{3,b}^{R_2,O_b}$, i.e., the bit error is corrected. That is, the bit decoding success probability is bounded as

$$\text{(bit success prob.)} = 1 - \text{(bit error prob.)} \geq \Pr[(3.9)] \cdot \Pr[(3.13)|(3.9)]. \tag{3.14}$$

In the following, we bound the probability (3.13) when (3.9) is satisfied, by two steps.

Step 1: First, we give one necessary condition for (3.13) and calculate the probability that the condition is satisfied. Since it holds that

$$\begin{aligned} \mathrm{rank}\left(\tilde{K} R_0 \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,b} \end{bmatrix} + \tilde{W}((R_1^V)^{-1})^{\mathcal{A}}\right) &\leq \mathrm{rank}\, R_{2,b} + \mathrm{rank}\, \tilde{W}((R_1^V)^{-1})^{\mathcal{A}} \\ &\leq \mathrm{rank}\, R_{2,b} + \mathrm{rank}\, \tilde{W}, \end{aligned} \tag{3.15}$$

the following condition is a necessary condition for (3.13):

$$\mathrm{rank}\, \tilde{W}((R_1^V)^{-1})^{\mathcal{A}} = \mathrm{rank}\, \tilde{W}. \tag{3.16}$$

The condition (3.16) holds if and only if $x^\top \tilde{W}((R_1^V)^{-1})^{\mathcal{A}} \neq \mathbf{0}_{1,m_0}$ holds for any $x \in \mathbb{F}_{q'}^{m_0}$ satisfying $x^\top \tilde{W} \neq \mathbf{0}_{1,n'}$. By applying the following Lemma 3.6.2

to all $(q')^{\operatorname{rank}\tilde{W}}$ vectors in $\{x^\top\tilde{W}\neq\mathbf{0}_{1,n'}|x\in\mathbb{F}_{q'}^{m_0}\}$, we have

$$\begin{aligned}\Pr[(3.16)|(3.9)]\geq&1-(q')^{\operatorname{rank}\tilde{W}}\left(\frac{n'-2m_0}{q'}\right)^{m_0}\\ \geq&1-(q')^{m_1}\left(\frac{n'-2m_0}{q'}\right)^{m_0}\\ \geq&1-\frac{(n')^{m_0}}{(q')^{m_0-m_1}}.\end{aligned}$$

Lemma 3.6.2. *For $n'>3m_0$,*

$$\max_{\mathbf{0}_{1,n'}\neq x\in\mathbb{F}_{q'}^{n'}}\Pr\left[x^\top((R_1^V)^{-1})^{\mathcal{A}}=\mathbf{0}_{1,m_0}\right]\leq\left(\frac{n'-2m_0}{q'}\right)^{m_0}. \tag{3.17}$$

The proof of Lemma 3.6.2 is in Appendix A.3.

Step 2: In this step, we calculate the probability that (3.13) holds under the assumptions (3.9) and (3.16). We introduce notations with column vectors $u_k,v_k\in\mathbb{F}_{q'}^{m_0}(k=1,\ldots,m_0)$ as

$$\begin{aligned}&[u_1,\ldots,u_{m_0}]:=\tilde{K}R_0\begin{bmatrix}\mathbf{0}_{m_1,m_0}\\R_{2,b}\end{bmatrix},\\&[v_1,\ldots,v_{m_0}]:=\tilde{W}((R_1^V)^{-1})^{\mathcal{A}},\\&m_2:=\operatorname{rank}R_{2,b}+\operatorname{rank}\tilde{W},\end{aligned}$$

and define an injective index function $i:\{1,...,m_0\}\to\{1,...,m_0\}$ so that $\operatorname{rank}(v_{i(1)},\ldots,v_{i(m_2)})=\operatorname{rank}\tilde{W}$. Note that the condition (3.13) holds if m_2 vectors $(u_{i(1)}+v_{i(1)}),\ldots,(u_{i(m_2)}+v_{i(m_2)})$ are linearly independent. Moreover, the condition (3.9) guarantees that m_2 vectors $(u_{i(1)}+v_{i(1)}),\ldots,(u_{i(m_2)}+v_{i(m_2)})$ are linearly independent if the following condition holds:

$$\mathcal{S}_u^\perp\cap\mathcal{S}_v^\perp=\{\mathbf{0}_{m_2,1}\}, \tag{3.18}$$

where

$$\begin{aligned}\mathcal{S}_u^\perp:=&\left\{x\in\mathbb{F}_{q'}^{m_2}\middle|[u_{i(1)},\ldots,u_{i(m_2)}]x=\mathbf{0}_{m_0,1}\right\},\\ \mathcal{S}_v^\perp:=&\left\{x\in\mathbb{F}_{q'}^{m_2}\middle|[v_{i(1)},\ldots,v_{i(m_2)}]x=\mathbf{0}_{m_0,1}\right\}.\end{aligned}$$

Then, we calculate the probability (3.18) holds. It follows from the definitions of $u_1,\ldots,u_{m_0},v_1,\ldots,v_{m_0}$ and the index function i that

$$\begin{aligned}&\dim\mathcal{S}_u^\perp\geq m_2-\operatorname{rank}[u_{i(1)},\ldots,u_{i(m_2)}]\geq\operatorname{rank}\tilde{W},\\&\dim\mathcal{S}_v^\perp=m_2-\operatorname{rank}[v_{i(1)},\ldots,v_{i(m_2)}]=\operatorname{rank}R_{2,b}.\end{aligned}$$

This implies $\dim \mathcal{S}_u^\perp + \dim \mathcal{S}_v^\perp \geq m_2$ and therefore (3.18) holds only if $\dim \mathcal{S}_u^\perp = \operatorname{rank} \tilde{W}$. We calculate the probability (3.18) holds by the following relation:

$$\begin{aligned}\Pr[(3.18)|(3.9) \cap (3.16)] = &\Pr[(3.18)|\dim \mathcal{S}_u^\perp = \operatorname{rank} \tilde{W} \cap (3.9) \cap (3.16)] \\ &\cdot \Pr[\dim \mathcal{S}_u^\perp = \operatorname{rank} \tilde{W} \cap (3.9) \cap (3.16)].\end{aligned}$$

Applying Lemma 3.6.1 with $(n_0, \mathcal{W}, \mathcal{R}) := (m_2, \mathcal{S}_v^\perp, \mathcal{S}_u^\perp)$,

$$\Pr[(3.18)|\dim \mathcal{S}_u^\perp = \operatorname{rank} \tilde{W} \cap (3.9) \cap (3.16)] = 1 - O\left(\frac{1}{q'}\right).$$

Moreover, the following inequality is proved in Appendix A.4:

$$\Pr[\dim \mathcal{S}_u^\perp = \operatorname{rank} \tilde{W} \cap (3.9) \cap (3.16)] \geq 1 - O\left(\frac{1}{q'}\right). \tag{3.19}$$

Therefore,

$$\Pr[(3.18)|(3.9) \cap (3.16)] \geq 1 - O\left(\frac{1}{q'}\right). \tag{3.20}$$

To summarize, from the two probabilities derived above two steps, we have

$$\begin{aligned}\Pr[(3.13)|(3.9)] &= \Pr[(3.13) \cap (3.16)|(3.9)] \\ &= \Pr[(3.13)|(3.16) \cap (3.9)] \cdot \Pr[(3.16)|(3.9)] \\ &\geq \Pr[(3.18)|(3.16) \cap (3.9)] \cdot \Pr[(3.16)|(3.9)] \\ &\geq \left(1 - \frac{(n')^{m_0}}{(q')^{m_0 - m_1}}\right)\left(1 - O\left(\frac{1}{q'}\right)\right) \\ &= 1 - O\Big(\max\Big\{\frac{1}{q'}, \frac{(n')^{m_0}}{(q')^{m_0 - m_1}}\Big\}\Big).\end{aligned}$$

Combining (3.11), (3.14) and the inequality above, we have

$$(\text{bit error prob.}) \leq O\Big(\max\Big\{\frac{1}{q'}, \frac{(n')^{m_0}}{(q')^{m_0 - m_1}}\Big\}\Big).$$

3.6.4 Phase Error Probability

Since coding and node operations are considered as classical linear operations even in the phase basis from Lemma 3.3.1, we can apply similar analysis to the phase basis errors as bit basis errors in Subsections 3.6.1, 3.6.2 and 3.6.3.

Consider the situation that a phase basis state $|M\rangle_p \in \mathcal{H}_{\text{code}}^{(n)}$ is encoded and transmitted through the quantum network. As we analyzed for bit basis states, we also perform the phase basis measurement first and then apply the decoding process. When ρ_{receive} is received, the phase measurement outcome Y_p on $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}$ is written similarly to (3.7) as

$$Y_p := [\tilde{K}]_p [R_0]_p X_p [R_1^V]_p + \tilde{W}',$$

where $\tilde{W}' \in \mathbb{F}_{q'}^{m_0 \times n'}$ and

$$X_p := \left[\begin{bmatrix} \bar{E}'_1 \\ \bar{E}'_2 \end{bmatrix}, \begin{bmatrix} R_{2,p} \\ \mathbf{0}_{m_1,m_0} \end{bmatrix}, \begin{bmatrix} \bar{E}'_3 \\ M \\ \mathbf{0}_{m_1,n'-2m_0} \end{bmatrix} \right] \in \mathbb{F}_{q'}^{m_0 \times n'}$$

for some matrices $\bar{E}'_1 \in \mathbb{F}_{q'}^{m_1 \times m_0}$, $\bar{E}'_2 \in \mathbb{F}_{q'}^{(m_0-m_1)\times m_0}$, and $\bar{E}'_3 \in \mathbb{F}_{q'}^{m_1 \times (n'-2m_0)}$. By the decoder, Y_p is decoded to

$$Y'_p := [D_{3,p}^{R_2,O_p}]_p \Big([\tilde{K}]_p [R_0]_p X_p + \tilde{W}' [(R_1^V)^{-1}]_p \Big).$$

If we assume

$$\operatorname{Im}[\tilde{K}]_p [R_0]_p |_{\mathcal{W}_p} \cap \operatorname{Im} \tilde{W}' = \{\mathbf{0}_{m_0,1}\}, \tag{3.21}$$

there exists a recovery map from phase errors. In the same way as Subsection 3.6.2, we have $\Pr[(3.21)] \geq 1 - O(1/q')$.

For the map $[D_{3,p}^{R_2,O_p}]_p$ in (3.4) to be a recovery map, it needs to be satisfied that

$$\operatorname{rank} \left([\tilde{K}]_p [R_0]_p \begin{bmatrix} \mathbf{0}_{m_1,m_0} \\ R_{2,p} \end{bmatrix} + \tilde{W}' ([R_1^V]_p^{-1})^{\mathcal{A}} \right) = \operatorname{rank} R_{2,p} + \operatorname{rank} \tilde{W}'. \tag{3.22}$$

Applying the same discussion in Step 1 of Subsection 3.6.3 to the phase basis, we have

$$\operatorname{rank} \tilde{W}' ([R_1^V]_p^{-1})^{\mathcal{B}} = \operatorname{rank} \tilde{W}', \tag{3.23}$$

with probability at least $1 - \frac{(n')^{m_0}}{(q')^{m_0-m_1}}$ by applying Lemma 3.6.3 to $(q')^{\operatorname{rank} \tilde{W}'}$ vectors in $\{x^\top \tilde{W}' \neq \mathbf{0}_{1,n'} | x \in \mathbb{F}_{q'}^{m_0}\}$.

Lemma 3.6.3. *For $n' > 3m_0$,*

$$\max_{\mathbf{0}_{n',1} \neq x \in \mathbb{F}_{q'}^{n'}} \Pr[x^\top ([R_1^V]_p^{-1})^{\mathcal{B}} = \mathbf{0}_{1,m_0}] \leq \left(\frac{n'-2m_0}{q'} \right)^{m_0}. \tag{3.24}$$

Proof. Proof is in Appendix A.3 □

Assuming (3.21) and (3.23), the condition (3.22) holds with probability at least $1 - O(1/q')$, in the similar way to Step 2 of Subsection 3.6.3.

From the probabilities derived above, in the same way as the bit success probability, the phase decoding error probability is derived as

$$\begin{aligned}(\text{phase error prob.}) &= 1 - \Pr[(3.21)] \cdot \Pr[(3.23)|(3.21)] \cdot \Pr[(3.22)|(3.21) \cap (3.23)] \\ &\leq 1 - \left(1 - \frac{(n')^{m_0}}{(q')^{m_0 - m_1}}\right)\left(1 - O\left(\frac{1}{q'}\right)\right) \\ &= O\Big(\max\Big\{\frac{1}{q'}, \frac{(n')^{m_0}}{(q')^{m_0 - m_1}}\Big\}\Big).\end{aligned}$$

3.7 Secure Quantum Network Code without Classical Communication

In the secure quantum network code given in Theorem 3.2.1, we assumed that the encoder and the decoder share the negligible rate randomness SR secretly. The secret shared randomness can be realized by secure communication. The paper [16] provided a secure classical communication protocol for the classical network as Proposition 3.7.1.

Proposition 3.7.1 ([16, Theorem 1])**.** *Let q_1 be the size of the finite field which is the information unit of the network channel. We assume the inequality $c_1 + c_2 < c_0$ for the classical network code where c_0 is transmission rate from Alice to Bob, c_1 is the rate of noise injected by Eve, and c_2 is the rate of information leakage to Eve. When $q_2 := q_1^{c_0}$, there exists a k-bit transmission protocol of block-length $n_2 := c_0(c_0 - c_2 + 1)k$ over $\mathbb{F}_{q_2}$ such that*

$$P_{err} \leq k\frac{c_0}{q_2} \text{ and } I(M; E) = 0,$$

where P_{err} is the error probability and $I(M; E)$ is the mutual information between the message $M \in \mathbb{F}_2^k$ and the Eve's information E. □

By attaching the protocol in Proposition 3.7.1 as a quantum protocol, we can share the negligible rate randomness secretly as the following proof of Theorem 3.2.2.

Proof of Theorem 3.2.2. Since the protocol of Proposition 3.7.1 can be implemented with the quantum network by sending bit basis states, the following protocol implements the code satisfying the conditions of Theorem 3.2.2.

Given a block-length n, we choose the prime power $q' = q^\alpha$ such that $\alpha = \lfloor \frac{3\log_2 n}{\log_2 q} \rfloor$ i.e., $q'/n^3 \to 1$. Hence, as the implementation of protocol in Theorem 3.2.1 with the extension field of size q', the sender and the receiver need to share the secret randomness of $4m_0 + 2m_0(m_0 - m_1)$ elements of $\mathbb{F}_{q'}$ Hence, using the protocol given in Proposition 3.7.1 with $(c_0, c_1, c_2) := (m_0, m_1, m_1)$, the sender secretly sends the receiver $k := \lceil (4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil$ bits, which is called the preparation protocol. To guarantee that the error of the preparation protocol goes to zero, we choose the other prime power $q_2 = q^{\alpha_2}$ such that $\alpha_2 = \lfloor \frac{2\log_2 \log_2 n}{\log_2 q} \rfloor$ i.e., $q_2/(\log n)^2 \to 1$. Since k is evaluated as $k = \lceil (4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil = \lceil (4m_0 + 2m_0(m_0 - m_1)) \lfloor \frac{3\log_2 n}{\log_2 q} \rfloor \log_2 q \rceil \le \lceil 3(4m_0 + 2m_0(m_0 - m_1)) \log_2 n \rceil$, we have $P_{err} \le O(\frac{\log_2 n}{(\log_2 n)^2}) \to 0$. Also, the preparation protocol requires the transmission of $n_2 = m_0(m_0 - m_1 + 1)k\alpha_2$ elements of $\mathbb{F}_q$. That is, n_2 is evaluated as

$$n_2 \le m_0(m_0 - m_1 + 1)\lceil 3(4m_0 + 2m_0(m_0 - m_1)) \log_2 n \rceil \cdot \Big\lfloor \frac{2\log_2 \log_2 n}{\log_2 q} \Big\rfloor. \tag{3.25}$$

Then, we define $n_1 := n - n_2$, which implies $n_1/n \to 1$. Finally, we apply the protocol given in Theorem 3.2.1 with $n = n_1$, $n' := n_1/\alpha$, and the above chosen α and q'. Since the relation $n_1/n \to 1$ guarantees the condition $\frac{n_1 \cdot (n_1/\alpha)^{m_0}}{(q')^{m_0 - m_1}} \to 0$, this protocol realizes the required conditions. □

3.8 Secrecy of our code

We mention that the condition $n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa^{(n)})) \to 0$ in Theorems 3.2.1 and 3.2.2 guarantees the secrecy of the protocol. As explained in Section 2.6, the leaked information of a quantum protocol $\kappa^{(n)}$ is upper bounded by entropy exchange $H_e(\rho, \kappa^{(n)}) := H(\kappa^{(n)} \otimes \iota_R(|x\rangle\langle x|)) = H(\kappa_E^{(n)}(\rho))$ as follows, where $|x\rangle$ is a purification of the state ρ and $\kappa_E^{(n)}$ is the channel to the environment. When the input state ρ_x is generated subject to the distribution p_x, the mutual information between the input system and the environment is given as $H(\kappa_E^{(n)}(\sum_x p_x \rho_x)) - \sum_x p_x H(\kappa_E^{(n)}(\rho_x))$, which is upper bounded by $H_e(\kappa^{(n)}, \sum_x p_x \rho_x)$. By entanglement fidelity, the entropy exchange is upper bounded as [4]

$$H_e(\rho, \kappa^{(n)}) \le h(F_e^2(\rho, \kappa^{(n)})) + (1 - F_e^2(\rho, \kappa^{(n)})) \log(d-1)^2$$

where $h(p)$ is the binary entropy defined as $h(p) := p \log p + (1-p)\log(1-p)$ for $0 \le p \le 1$ and d is the dimension of the input space of $\kappa^{(n)}$. Hence,

when the mixture distribution is the completely mixed state ρ_{mix}, because $d = \dim \mathcal{H}_{\mathrm{code}}^{(n)} = O\big(q^{(m_0-2m_1)n}\big)$ in our protocol, the condition

$$n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa^{(n)})) \to 0$$

leads that the entropy exchange of the protocol is asymptotically 0, i.e., there is no leakage in the protocol. Thus, the asymptotic correctability $n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa^{(n)})) \to 0$ also guarantees the secrecy of the protocol in Theorems 3.2.1 and 3.2.2.

Chapter 4

Quantum Network Code for Multiple-Unicast Network

In this chapter, we propose a multiple-unicast quantum network code which implements resilient quantum communication.

4.1 Quantum Multiple-Unicast Network

Our code is designed as a quantum network which is a generalization of a classical multiple-unicast network. In this section, we first introduce the multiple-unicast network with classical invertible linear operations and generalize this network as a network with quantum invertible linear operations. The node operations introduced in this section are identical to the operations in Definition 3.1.1.

4.1.1 Classical Multiple-Unicast Network with Invertible Linear Operations

First, we describe the multiple-unicast network with classical invertible linear operations. The network topology is given as a directed graph $G = (V, E)$. The r senders and r receivers are given as r source nodes $S_1, \ldots, S_r$ and r terminal nodes $T_1, \ldots, T_r$. The sender S_i has m_i outgoing edges and the receiver T_i has m_i incoming edges. Define $m := m_1 + \cdots + m_r$. The intermediate nodes are numbered from 1 to c $(= |V| - 2r)$ according to the order of the transmission. The intermediate node numbered t has the same number k_t of incoming and outgoing edges where $1 \leq k_t \leq m$.

Next, we describe the transmission and the operations on this network. Each edge sends an element of the finite field $\mathbb{F}_q$ where q is a power of

a prime number p. The t-th node operation is described as an invertible linear operation A_t from the information on k_t incoming edges to that of k_t outgoing edges. Since node operations are invertible linear, the entire network operation is written as $K = A_c \cdots A_1 \in \mathbb{F}_q^{m\times m}$. For the network operation K, we introduce the following notation:

$$K := \begin{bmatrix} K_{1,1} & K_{1,2} & \cdots & K_{1,r} \\ K_{2,1} & K_{2,2} & \cdots & K_{2,r} \\ \vdots & \ddots & & \vdots \\ K_{r,1} & K_{r,2} & \cdots & K_{r,r} \end{bmatrix}, \quad K_{i,j} \in \mathbb{F}_q^{m_i\times m_j}.$$

Then, $K_{i,j}$ is the network operation from S_i to T_j. We assume $\operatorname{rank} K_{i,i} = m_i$ which means the information from S_i to T_i is completely transmitted if there is no interference.

When the network inputs by senders $S_1, \ldots, S_r$ are $x_1 \in \mathbb{F}_q^{m_1}, \ldots, x_r \in \mathbb{F}_q^{m_r}$, the output $y_i \in \mathbb{F}_q^{m_i}$ at the receiver T_i $(i = 1, \ldots, r)$ is written as

$$\begin{aligned} y_i =& \sum_{j=1}^{r} K_{i,j}x_j = K_{i,i}x_i + K_{i^c}z_{i^c}, \qquad (4.1)\\ K_{i^c} :=& [K_{i,1} \ \cdots \ K_{i,i-1} \ K_{i,i+1} \ \cdots \ K_{i,r}] \in \mathbb{F}_q^{m_i\times(m-m_i)},\\ z_{i^c} :=& [x_1^\top \ \cdots \ x_{i-1}^\top \ x_{i+1}^\top \ \cdots \ x_r^\top]^\top \in \mathbb{F}_q^{m-m_i}. \end{aligned}$$

The second term $K_{i^c}z_{i^c}$ of (4.1) is called the interference to T_i, and $\operatorname{rank} K_{i^c}$ is called the rate of the interference to T_i.

Consider the n-use of the above network. When the inputs by senders $S_1, ..., S_r$ are $X_1 \in \mathbb{F}_q^{m_1\times n}, \ldots, X_r \in \mathbb{F}_q^{m_r\times n}$, the output $Y_i \in \mathbb{F}_q^{m_i\times n}$ at the receiver T_i $(i = 1, \ldots, r)$ is

$$\begin{aligned} Y_i =& \sum_{j=1}^{r} K_{i,j}X_j = K_{i,i}X_i + K_{i^c}Z_{i^c},\\ Z_{i^c} :=& [X_1^\top \ \cdots \ X_{i-1}^\top \ X_{i+1}^\top \ \cdots \ X_r^\top]^\top \in \mathbb{F}_q^{(m-m_i)\times n}. \end{aligned}$$

4.1.2 Quantum Multiple-Unicast Network with Invertible Linear Operations

We generalize the multiple-unicast network with classical invertible linear operations to the network with quantum invertible linear operations. In this quantum network, the network topology is the same graph $G = (V, E)$. Each edge transmits a quantum system $\mathcal{H}$ which is q-dimensional Hilbert

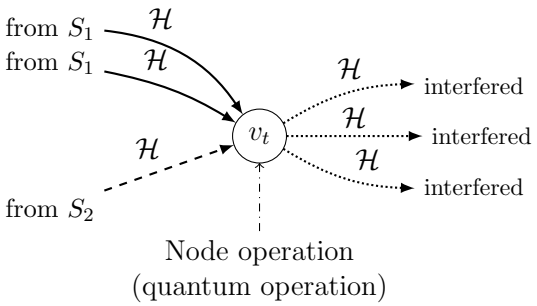


Figure 4.1: Interference of information in network nodes.

space spanned by the bit basis $\{|x\rangle_b\}_{x\in\mathbb{F}_q}$. In n-use of the network, we treat the quantum system $\mathcal{H}^{\otimes m_i\times n}$ spanned by the bit basis $\{|X\rangle_b\}_{X\in\mathbb{F}_q^{m_i\times n}}$. The sender S_i sends a quantum system $\mathcal{H}_{S_i} := \mathcal{H}^{\otimes m_i\times n}$ and the receiver T_i receives a quantum system $\mathcal{H}_{T_i} := \mathcal{H}^{\otimes m_i\times n}$

The t-th node operation is given as $\mathcal{L}(A_t)$ and it is called quantum invertible linear operation. The entire network operation is written as the unitary $\mathcal{L}(K) = \mathcal{L}(A_c\cdots A_1) = \mathcal{L}(A_c)\cdots\mathcal{L}(A_1)$. When a state ρ on $\mathcal{H}_{S_1}\otimes\cdots\otimes\mathcal{H}_{S_r}$ is transmitted by senders $S_1,\ldots,S_r$, the network output σ_{T_i} at $\mathcal{H}_{T_i}$ is written as

$$\sigma_{T_i} := \operatorname*{Tr}_{T_1,\ldots,T_{i-1},T_{i+1},\ldots,T_r} \mathcal{L}(K)\rho\mathcal{L}(K)^\dagger,$$

where $\mathrm{Tr}_{T_1,\ldots,T_{i-1},T_{i+1},\ldots,T_r}$ is the partial trace on the system

$$\mathcal{H}_{T_1}\otimes\ldots\otimes\mathcal{H}_{T_{i-1}}\otimes\mathcal{H}_{T_{i+1}}\otimes\ldots\otimes\mathcal{H}_{T_r}\,.$$

When the input state on the network is $|M\rangle_b$ on $\mathcal{H}_{S_1}\otimes\cdots\otimes\mathcal{H}_{S_r}$, this quantum network can be considered as the classical network in Subsection 4.1.1. In the same way as the classical network, we assume $\operatorname{rank} K_{i,i} = m_i$ which means S_i transmits any bit basis states completely to T_i if the input states on source nodes S_j $(j\neq i)$ are zero bit basis states. Similarly, $\operatorname{rank} K_{i^c}$ is called the rate of the bit interference to T_i.

We can discuss the interference similarly on the phase basis $\{|z\rangle_p\}_{z\in\mathbb{F}_q}$ defined in Section 3.3. When the input state is a phase basis state $|M\rangle_p$ on $\mathcal{H}_{S_1}\otimes\cdots\otimes\mathcal{H}_{S_r}$, the network operation $\mathcal{L}(K)$ is applied by $\mathcal{L}(K)|M\rangle_p = |[K]_pM\rangle_p$. In this case, this quantum network can also be considered as a classical network with network operation $[K]_p = [A_c]_p\cdots[A_1]_p$. Then, $[K]_{p_{i,j}}$

Table 4.1: Definitions of Information Rates

Rate	Meaning
$m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} [K_{i,i}]_p$	Bit (phase) transmission rates
$\operatorname{rank} K_{i^c}$	Rate of interference to T_i
$\operatorname{rank} [K_{i^c}]_p$	Rate of phase interference to T_i
a_i	Maximum rate of bit interference to T_i
a'_i	Maximum rate of phase interference to T_i

is defined from $[K]_p$ in the same way as $K_{i,j}$.

$$[K]_p := \begin{bmatrix} [K_{1,1}]_p & [K_{1,2}]_p & \cdots & [K_{1,r}]_p \\ [K_{2,1}]_p & [K_{2,2}]_p & \cdots & [K_{2,r}]_p \\ \vdots & \ddots & & \vdots \\ [K_{r,1}]_p & [K_{r,2}]_p & \cdots & [K_{r,r}]_p \end{bmatrix}, \quad [K_{i,j}]_p \in \mathbb{F}_q^{m_i \times m_j},$$

$$[K_{i^c}]_p := [[K_{i,1}]_p \ \cdots \ [K_{i,i-1}]_p \ [K_{i,i+1}]_p \ \cdots \ [K_{i,r}]_p].$$

Similarly to the condition $\operatorname{rank} K_{i,i} = m_i$, we also assume $\operatorname{rank} [K_{i,i}]_p = m_i$. We also call $\operatorname{rank} [K_{i^c}]_p$ the rate of phase interference to T_i. The transmission rates from S_i to T_i are summarized in Table 4.1.

4.2 Main Results

In this section, we propose the two main theorems of this chapter. The two theorems state the existence of our code with and without negligible rate shared randomness, respectively. The codes stated in the theorems are concretely constructed in Section 4.4. The theorems are stated with respect to the completely mixed state ρ_{mix} and the entanglement fidelity for the quantum channel κ and a purification $|x\rangle$ of the state ρ.

Theorem 4.2.1. *Consider the transmission from the sender S_i to the receiver T_i over a quantum multiple-unicast network with quantum invertible linear operations given in Section 4.1. Let m_i be the bit and phase transmission rates from S_i to T_i without interferences ($m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} [K]_{p_{i,i}}$), and a_i, a'_i be the upper bounds of the bit and phase interferences, respectively ($\operatorname{rank} K_{i^c} \leq a_i$, $\operatorname{rank} [K_{i^c}]_p \leq a'_i$). When the condition $a_i + a'_i < m_i$ holds and the sender S_i and receiver T_i can share a randomness whose rate is negligible in comparison with the block-length n, there exists a quantum network code*

whose rate is $m_i - a_i - a'_i$ *and the entanglement fidelity* $F_e^2(\rho_{\mathrm{mix}}, \kappa_i)$ *satisfies* $n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa_i)) \to 0$ *where* κ_i *is the quantum code protocol from sender* S_i *to receiver* T_i.

Section 4.4 constructs the code stated in Theorem 4.2.1 and Section 4.5 shows that this code has the performance in Theorem 4.2.1. Note that this code does not depend on the detailed network structure, but depends only on the information rates m_i, a_i and a'_i. By the same analysis as in Chapter 3, our code has no information leakage from the condition $n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa_i)) \to 0$.

Although Theorem 4.2.1 assumed the free use of a negligible rate shared randomness, it is possible to design a code of same performance without this negligible rate shared randomness as follows. The paper [16] gives the secret and correctable classical network communication protocol for a classical network with malicious attacks, when the transmission rate is more than the sum of the rate of attacks and the rate of information leakage. By applying the protocol in [16] to our quantum network with bit basis states, the negligible rate shared randomness can be generated. By this method, we have the following Theorem 4.2.2.

Theorem 4.2.2. *Consider the transmission from the sender* S_i *to the receiver* T_i *over a quantum multiple-unicast network with quantum invertible linear operations given in Section 4.1. Let* m_i *be the bit and phase transmission rates from* S_i *to* T_i *without interferences* ($m_i = \mathrm{rank}\, K_{i,i} = \mathrm{rank}\, [K]_{p_{i,i}}$), *and* a_i, a'_i *be the upper bounds of the bit and phase interferences, respectively* ($\mathrm{rank}\, K_{i^c} \le a_i$, $\mathrm{rank}\, [K_{i^c}]_p \le a'_i$). *When* $a_i + a'_i < m_i$, *there exists a quantum network code whose rate is* $m_i - a_i - a'_i$ *and the entanglement fidelity* $F_e^2(\rho_{\mathrm{mix}}, \kappa_i)$ *satisfies* $n(1 - F_e^2(\rho_{\mathrm{mix}}, \kappa_i)) \to 0$ *where* κ_i *is the quantum code protocol from sender* S_i *to receiver* T_i.

4.3 Preliminaries for Code Construction

Before code construction, we prepare the extended quantum system, notations, and CSS code used in our code.

4.3.1 Extended Quantum System

Although the unit quantum system for the network transmission is $\mathcal{H}$, our code is constructed based on the extended quantum system $\mathcal{H}'$ described below.

First, depending on the block-length n, we choose a power $q' := q^\alpha$ to satisfy $n \cdot (n')^{m_i} / (q')^{m_i - \max\{a_i, a'_i\}} \to 0$ (e.g. $q' = O(n^{1+(\max\{a_i, a'_i\}+2)/(m_i - \max\{a_i, a'_i\})})$

) where $n' := n/\alpha$. Let $\mathbb{F}_{q'}$ be the α-dimensional field extension of $\mathbb{F}_q$. Similarly, let $\mathcal{H}' := \mathcal{H}^{\otimes\alpha}$ be the quantum system spanned by $\{|x\rangle_b\}_{x\in\mathbb{F}_{q'}}$. Then, the n-use of the network over $\mathcal{H}$ can be considered as the n'-use of the network over $\mathcal{H}'$. The quantum invertible linear operations (Definition 3.1.1) can also be defined for invertible matrices $A' \in \mathbb{F}_{q'}^{m\times m}$ and $B' \in \mathbb{F}_{q'}^{n\times n}$ as

$$\mathcal{L}'(A)|X\rangle_b = |AX\rangle_b,\ \ \mathcal{R}'(B)|X\rangle_b = |XB\rangle_b, \quad \text{for any } X \in \mathbb{F}_{q'}^{m\times n}.$$

4.3.2 Notations for Quantum Systems and States in Our Code

We introduce notations used in our code. By the n-use of the network, the sender S_i transmits the system $\mathcal{H}_{S_i} = \mathcal{H}^{\otimes m_i\times n}$ and the receiver T_i receives the system $\mathcal{H}_{T_i} = \mathcal{H}^{\otimes m_i\times n}$, which are identical to $\mathcal{H}'^{\otimes m_i\times n'}$. We partition the quantum system $\mathcal{H}'^{\otimes m_i\times n'}$ as $\mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}} := \mathcal{H}'^{\otimes m_i\times m_i} \otimes \mathcal{H}'^{\otimes m_i\times m_i} \otimes \mathcal{H}'^{\otimes m_i\times(n'-2m_i)}$. Furthermore, we partition the systems $\mathcal{H}'_{\mathcal{A}}, \mathcal{H}'_{\mathcal{B}}, \mathcal{H}'_{\mathcal{C}}$ by

$$\begin{aligned}
\mathcal{H}'_{\mathcal{A}} &= \mathcal{H}'_{\mathcal{A}1} \otimes \mathcal{H}'_{\mathcal{A}2} \otimes \mathcal{H}'_{\mathcal{A}3} := \mathcal{H}'^{\otimes a_i\times m_i} \otimes \mathcal{H}'^{\otimes(m_i-a_i-a'_i)\times m_i} \otimes \mathcal{H}'^{\otimes a'_i\times m_i},\\
\mathcal{H}'_{\mathcal{B}} &= \mathcal{H}'_{\mathcal{B}1} \otimes \mathcal{H}'_{\mathcal{B}2} \otimes \mathcal{H}'_{\mathcal{B}3} := \mathcal{H}'^{\otimes a_i\times m_i} \otimes \mathcal{H}'^{\otimes(m_i-a_i-a'_i)\times m_i} \otimes \mathcal{H}'^{\otimes a'_i\times m_i},\\
\mathcal{H}'_{\mathcal{C}} &= \mathcal{H}'_{\mathcal{C}1} \otimes \mathcal{H}'_{\mathcal{C}2} \otimes \mathcal{H}'_{\mathcal{C}3} := \mathcal{H}'^{\otimes a_i\times(n'-2m_i)} \otimes \mathcal{H}'^{\otimes(m_i-a_i-a'_i)\times(n'-2m_i)} \otimes \mathcal{H}'^{\otimes a'_i\times(n'-2m_i)}.
\end{aligned}$$

For states $|\phi\rangle \in \mathcal{H}'_{\mathcal{A}1}, |\psi\rangle \in \mathcal{H}'_{\mathcal{A}2}$, and $|\varphi\rangle \in \mathcal{H}'_{\mathcal{A}3}$, the tensor product state in $\mathcal{H}'_{\mathcal{A}}$ is denoted as

$$\begin{bmatrix} |\phi\rangle \\ |\psi\rangle \\ |\varphi\rangle \end{bmatrix} := |\phi\rangle \otimes |\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}'_{\mathcal{A}}\,. \tag{4.2}$$

The bit or phase basis state of $(X, Y, Z) \in \mathbb{F}_{q'}^{a_i\times m_i} \times \mathbb{F}_{q'}^{(m_i-a_i-a'_i)\times m_i} \times \mathbb{F}_{q'}^{a'_i\times m_i}$ is denoted as

$$\left|\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right\rangle_b := \begin{bmatrix} |X\rangle_b \\ |Y\rangle_b \\ |Z\rangle_b \end{bmatrix}, \quad \left|\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right\rangle_p := \begin{bmatrix} |X\rangle_p \\ |Y\rangle_p \\ |Z\rangle_p \end{bmatrix}. \tag{4.3}$$

We also introduce notations for the states in $\mathcal{H}'_{\mathcal{B}}$ and $\mathcal{H}'_{\mathcal{C}}$ in the same way as (4.2) and (4.3). In the following, we denote the $k \times l$ zero matrix as $\mathbf{0}_{k,l}$.

4.3.3 CSS Code in Our Code

In our code construction, we use the CSS code defined in this subsection which is defined similarly to Section 3.3.4. Define two classical codes $C_1, C_2 \subset$

$\mathbb{F}_{q'}^{m_i\times(n'-2m_0)}$ which satisfy $C_1 \supset C_2^{\perp}$ as

$$C_1 := \left\{ \begin{bmatrix} \mathbf{0}_{a_i,n'-2m_0} \\ X_2 \\ X_3 \end{bmatrix} \in \mathbb{F}_{q'}^{m_i\times(n'-2m_0)} \middle| X_2 \in \mathbb{F}_{q'}^{(m_i-a_i-a_i')\times(n'-2m_0)}, X_3 \in \mathbb{F}_{q'}^{a_i'\times(n'-2m_0)} \right\},$$

$$C_2 := \left\{ \begin{bmatrix} X_1 \\ X_2 \\ \mathbf{0}_{a_i',n'-2m_0} \end{bmatrix} \in \mathbb{F}_{q'}^{m_i\times(n'-2m_0)} \middle| X_1 \in \mathbb{F}_{q'}^{a_i\times(n'-2m_0)}, X_2 \in \mathbb{F}_{q'}^{(m_i-a_i-a_i')\times(n'-2m_0)} \right\}.$$

For any $[M_1] \in C_1/C_2^{\perp}$ where $M_1 \in \mathbb{F}_{q'}^{(m_i-a_i-a_i')\times(n'-2m_0)}$, define the quantum state $|[M_1]\rangle_b \in \mathcal{H}_{\mathcal{C}}$ by

$$|[M_1]\rangle_b := \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{Y\in C_2^{\perp}} \left| \begin{bmatrix} \mathbf{0}_{a_i,n'-2m_0} \\ M_1 \\ \mathbf{0}_{a_i',n'-2m_0} \end{bmatrix} + Y \right\rangle_b = \begin{bmatrix} |\mathbf{0}_{a_i,n'-2m_0}\rangle_b \\ |M_1\rangle_b \\ |\mathbf{0}_{a_i',n'-2m_0}\rangle_p \end{bmatrix}.$$

With the above definitions, the code space is given as $\mathcal{H}'_{\text{code}} := \mathcal{H}'_{\mathcal{C}2} = \mathcal{H}'^{\otimes(m_i-a_i-a_i')\times(n'-2m_0)}$ and a pure state $|\phi\rangle \in \mathcal{H}'_{\text{code}}$ is encoded as a superposition of the states $|[M_1]\rangle_b$ in this CSS code by

$$\begin{bmatrix} |\mathbf{0}_{a_i,n'-2m_0}\rangle_b \\ |\phi\rangle \\ |\mathbf{0}_{a_i',n'-2m_0}\rangle_p \end{bmatrix} \in \mathcal{H}_{\mathcal{C}}.$$

4.4 Code Construction with Negligible Rate Shared Randomness

In this section, we construct our code that allows a sender S_i to transmit a state ρ_i on $\mathcal{H}'_{\text{code}} = \mathcal{H}'^{\otimes(m_i-a_i-a_i')\times(n'-2m_i)}$ correctly to a receiver T_i by n-use of the network when the encoder and decoder share the negligible rate random variable $SR_i := (R_i, V_i)$.

The encoder and decoder are defined depending on the private randomness $U_{i,1}$ owned by encoder and the randomness SR_i shared between the encoder and decoder. These random variables are uniformly chosen from the values or matrices satisfying the following respective conditions: the variable $R_i := (R_{i,1}, R_{i,2}) \in \mathbb{F}_{q'}^{(m_i-a_i)\times m_i} \times \mathbb{F}_{q'}^{(m_i-a_i')\times m_i}$ satisfies $\operatorname{rank} R_{i,1} = m_i - a_i$ and $\operatorname{rank} R_{i,2} = m_i - a_i'$, the random variable $V_i := (V_{i,1}, \ldots, V_{i,4m_i})$ consists of $4m_i$ values $V_{i,1}, \ldots, V_{i,4m_i} \in \mathbb{F}_{q'}^{4m_i}$ and the random variable $U_{i,1} \in \mathbb{F}_{q'}^{m_i\times m_i}$ satisfies $\operatorname{rank} U_{i,1} = m_i$.

Next, we construct the encoder $\mathcal{E}_i^{SR_i,U_{i,1}}$ and decoder $\mathcal{D}_i^{SR_i}$. Depending on SR_i and $U_{i,1}$, the encoder $\mathcal{E}_i^{SR_i,U_{i,1}}$ of the sender S_i is defined as an isometry

channel from $\mathcal{H}'_{\rm code}$ to $\mathcal{H}_{S_i} = \mathcal{H}'^{\otimes m_i \times n'}$. Depending on SR_i, the decoder $\mathcal{D}_i^{SR_i}$ of the receiver T_i is defined as a TP-CP map from $\mathcal{H}_{T_i} = \mathcal{H}'^{\otimes m_i \times n'}$ to $\mathcal{H}'_{\rm code}$. Note that the randomness SR_i is shared between the encoder and the decoder. Because SR_i consists of $\alpha m_i(2m_i - a_i - a'_i + 4)$ elements of $\mathbb{F}_q$, the size of the shared randomness SR_i is sublinear with respect to n (i.e., negligible).

4.4.1 Encoder $\mathcal{E}_i^{SR_i,U_{i,1}}$ of the sender S_i

The encoder $\mathcal{E}_i^{SR_i,U_{i,1}}$ consists of three steps. In the following, we describe the encoding of the state $|\phi\rangle$ in $\mathcal{H}'_{\rm code}$.

Step E1 The isometry map $U_{i,0}^{R_i}$ encodes the state $|\phi\rangle$ with the CSS code defined in Subsection 4.3.3 and the quantum systems $\mathcal{H}'_{\mathcal{A}}$ and $\mathcal{H}'_{\mathcal{B}}$ as

$$|\phi_1\rangle := U_{i,0}^{R_i}|\phi\rangle = \left|\begin{bmatrix}\mathbf{0}_{a_i,m_i}\\ R_{i,1}\end{bmatrix}\right\rangle_b \otimes \left|\begin{bmatrix}R_{i,2}\\ \mathbf{0}_{a'_i,m_i}\end{bmatrix}\right\rangle_p \otimes \begin{bmatrix}|\mathbf{0}_{a_i,m_i}\rangle_b\\ |\phi\rangle\\ |\mathbf{0}_{a'_i,m_i}\rangle_p\end{bmatrix} \in \mathcal{H}'_{\mathcal{A}} \otimes \mathcal{H}'_{\mathcal{B}} \otimes \mathcal{H}'_{\mathcal{C}}\,.$$

Step E2 By quantum invertible linear operation $\mathcal{L}'(U_{i,1})$, the encoder maps $|\phi_1\rangle$ to $|\phi_2\rangle := \mathcal{L}'(U_{i,1})|\phi_1\rangle$.

Step E3 From random variable $V_i = (V_{i,1}, \ldots, V_{i,4m_i})$, define matrices $Q_{i,1;j,k} := (V_{i,k})^j$, $Q_{i,2;j,k} := (V_{i,m_i+k})^j$ for $1 \le j \le n' - 2m_i$, $1 \le k \le m_i$, and $Q_{i,3;j,k} := (V_{i,2m_i+k})^j$, $Q_{i,4;j,k} := (V_{i,3m_i+k})^j$ for $1 \le j, k \le m_i$. With these matrices, define the matrix $U_{i,2}^V \in \mathbb{F}_{q'}^{n' \times n'}$ as

$$U_{i,2}^V := \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0}\\ Q_{i,3}^{\rm T}Q_{i,4} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0}\\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0}\end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0}\\ \mathbf{0}_{m_0,m_0} & I_{m_0} & Q_{i,2}^{\rm T}\\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0}\end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0}\\ \mathbf{0}_{m_0,m_0} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0}\\ Q_{i,1} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0}\end{bmatrix},$$

where I_d is the identity matrix of size d. By quantum invertible linear operation $\mathcal{R}'(U_{i,2}^{V_i})$, the encoder maps $|\phi_2\rangle$ to $\mathcal{R}'(U_{i,2}^{V_i})|\phi_2\rangle$.

By the above three steps, the encoder $\mathcal{E}_i^{SR_i,U_{i,1}}$ is described as an isometry map

$$\mathcal{E}_i^{SR_i,U_{i,1}} : |\phi\rangle \mapsto \mathcal{R}'(U_{i,2}^{V_i})\mathcal{L}'(U_{i,1})U_{i,0}^{R_i}|\phi\rangle \in \mathcal{H}_{S_i}\,.$$

4.4.2 Decoder $\mathcal{D}_i^{SR_i}$ of the receiver T_i

Decoder $\mathcal{D}_i^{SR_i}$ consists of two steps. In the following, we describe the decoding of the state $|\psi\rangle \in \mathcal{H}_{T_i}$.

Step D1 Since $(U_{i,2}^{V_i})^{-1}$ can be constructed from shared randomness V_i by

$$(U_{i,2}^{V})^{-1}=\begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ -Q_{i,1} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{m_0,m_0} & I_{m_0} & -Q_{i,2}^{\mathrm{T}} \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix} \cdot \begin{bmatrix} I_{m_0} & \mathbf{0}_{m_0,m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ -Q_{i,3}^{\mathrm{T}}Q_{i,4} & I_{m_0} & \mathbf{0}_{m_0,n'-2m_0} \\ \mathbf{0}_{n'-2m_0,m_0} & \mathbf{0}_{n'-2m_0,m_0} & I_{n'-2m_0} \end{bmatrix},$$

the decoder applies the reverse operation $\mathcal{R}'(U_{i,2}^{V_i})^\dagger = \mathcal{R}'((U_{i,2}^{V_i})^{-1})$ of Step E3 as $|\psi_1\rangle := \mathcal{R}'(U_{i,2}^{V_i})^\dagger|\psi\rangle$.

Step D2 Perform the bit and phase basis measurements on $\mathcal{H}'_{\mathcal{A}}$ and $\mathcal{H}'_{\mathcal{B}}$, respectively, and let $O_{i,1}, O_{i,2} \in \mathbb{F}_{q'}^{m_i \times m_i}$ be the respective measurement outcomes. By Gaussian elimination, find invertible matrices $D_{i,1}^{R_{i,1},O_{i,1}}, D_{i,2}^{R_{i,2},O_{i,2}} \in \mathbb{F}_{q'}^{m_i \times m_i}$ satisfying

$$P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} O_{i,1} = \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix}, \quad P_{\mathcal{W}_{i,2}} D_{i,2}^{R_{i,2},O_{i,2}} O_{i,2} = \begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i} \end{bmatrix}. \tag{4.4}$$

where $P_{\mathcal{W}}$ is the projection from $\mathbb{F}_{q'}^{m_i}$ to the subspace $\mathcal{W}$, the subspace $\mathcal{W}_{i,1}$ consists of the vectors whose 1-st, ..., a_i-th elements are zero and the subspace $\mathcal{W}_{i,2}$ consists of the vectors whose $(m_i - a'_i + 1)$-st, ..., m_i-th elements are zero. The case of non-existence of $D_{i,1}^{R_{i,1},O_{i,1}}$ nor $D_{i,2}^{R_{i,2},O_{i,2}}$ means decoding failure, which implies that the decoder performs no more operations. Also, when $D_{i,1}^{R_{i,1},O_{i,1}}$ and $D_{i,2}^{R_{i,2},O_{i,2}}$ are not determined uniquely, the decoder chooses $D_{i,1}^{R_{i,1},O_{i,1}}$ and $D_{i,2}^{R_{i,2},O_{i,2}}$ deterministically depending on $O_{i,1}, R_{i,1}$ and $O_{i,2}, R_{i,2}$, respectively.

Based on $D_{i,1}^{R_{i,1},O_{i,1}}$ and $D_{i,2}^{R_{i,2},O_{i,2}}$ found by (4.4), the decoder applies $\mathcal{L}'(D_{i,1}^{R_{i,1},O_{i,1}})$ and $\mathcal{L}'([D_{i,2}^{R_{i,2},O_{i,2}}]_p)$ consecutively to $|\psi_1\rangle$, and the resultant state on $\mathcal{H}_{\mathrm{code}}$ is the output of Step D2. Then, Step D2 is written as the following TP-CP map $D_i^{R_i}$:

$$D_i^{R_i}(|\psi_1\rangle\langle\psi_1|) := \operatorname*{Tr}_{\mathcal{C}1,\mathcal{C}3} \sum_{O_{i,1},O_{i,2} \in \mathbb{F}_{q'}^{m_i \times m_0}} U_D^{R_i,O_{i,1},O_{i,2}} \sigma_{O_{i,1},O_{i,2}} (U_D^{R_i,O_{i,1},O_{i,2}})^\dagger,$$

where the matrices $U_D^{R_i,O_{i,1},O_{i,2}}$ and $\sigma_{O_{i,1},O_{i,2}}$ are defined as

$$\begin{aligned} U_D^{R_i,O_{i,1},O_{i,2}} :=& \mathcal{L}'([D_{i,2}^{R_{i,2},O_{i,2}}]_p)\mathcal{L}'(D_{i,1}^{R_{i,1},O_{i,1}}), \\ \sigma_{O_{i,1},O_{i,2}} :=& \operatorname*{Tr}_{\mathcal{A},\mathcal{B}} |\psi_1\rangle\langle\psi_1|(|O_{i,1}\rangle_{bb}\langle O_{i,1}| \otimes |O_{i,2}\rangle_{pp}\langle O_{i,2}| \otimes I_{\mathcal{C}}), \end{aligned}$$

with the identity operator $I_{\mathcal{C}}$ on $\mathcal{H}_{\mathcal{C}}$.

By above two steps, the decoder $\mathcal{D}_i^{SR_i}$ is described as

$$\mathcal{D}_i^{SR_i}(|\psi\rangle\langle\psi|) := D_i^{R_i}\big(\mathcal{R}'(U_{i,2}^{V_i})^\dagger|\psi\rangle\langle\psi|\mathcal{R}'(U_{i,2}^{V_i})\big).$$

Since the size of the shared randomness SR_i is sublinear with respect to n, our code is implemented with negligible rate shared randomness.

4.5 Correctness of Our Code

In this section, we confirm that our code correctly transmits the state from the sender S_i to the receiver T_i. As is mentioned in Section 4.2, we show the condition $n(1 - F_e^2(\rho_{mix}, \kappa_i)) \to 0$ which implies the correctness of our code.

First, we describe the quantum code protocol κ_i from S_i to T_i, which is an integration of the encoding, transmission, and decoding. The encoding and decoding in κ_i is given by the probabilistic mixture of the code in Section 4.4 depending on the uniformly chosen random variables SR_i and $U_{i,1}$. Then, the code protocol κ_i is written as, for the state ρ_i on $\mathcal{H}'_{\text{code}}$,

$$\kappa_i(\rho_i) := \sum_{SR_i,U_{i,1}} \frac{1}{N}\mathcal{D}_i^{SR_i}\left(\operatorname*{Tr}_{T_1,\dots,T_{i-1},T_{i+1},\dots,T_r} \mathcal{L}(K)\Big(\mathcal{E}_i^{SR_i,U_{i,1}}(\rho_i)\otimes\rho_{i^c}\Big)\mathcal{L}(K)^\dagger\right),$$

where ρ_{i^c} is the state in $\mathcal{H}_{S_1}\otimes\cdots\otimes\mathcal{H}_{S_{i-1}}\otimes\mathcal{H}_{S_{i+1}}\otimes\cdots\otimes\mathcal{H}_{S_r}$ of senders other than S_i, and $N := q'^{4m_i} + |\{U_{i,1} \in \mathbb{F}_{q'}^{m_i\times m_i} | \operatorname{rank} U_{i,1} = m_i\}| + |\{R_{i,1} \in \mathbb{F}_{q'}^{(m_i-a_i)\times m_i} | \operatorname{rank} R_{i,1} = m_i - a_i\}| + |\{R_{i,2} \in \mathbb{F}_{q'}^{(m_i-a'_i)\times m_i} | \operatorname{rank} R_{i,1} = m_i - a'_i\}|$.

As explained in Section 3.5, $1 - F_e^2(\rho_{mix}, \kappa_i)$ is upper bounded by the sum of the bit error probability and the phase error probability. The bit error probability is the probability that a bit basis state $|X\rangle_b \in \mathcal{H}'_{\text{code}}$ is sent but the bit basis measurement outcome on the decoder output is not X. In the similar way, the phase error probability is defined for the phase basis.

Similarly to Subsections 3.6.1 and 3.6.4, the bit and phase error probabilities are upper bounded by

$$O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a_i}}\right\}\right) \text{ and } O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a'_i}}\right\}\right),$$

respectively. Therefore, we have

$$n(1 - F_e^2(\rho_{mix}, \kappa_i)) \leq nO\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i - \max\{a_i, a_i'\}}}\right\}\right). \tag{4.5}$$

Since q' is taken in Section 4.3 to satisfy $\frac{n \cdot (n')^{m_i}}{(q')^{m_i - \max\{a_i, a_i'\}}} \to 0$, the RHS of (4.5) converges to 0 and therefore $n(1 - F_e^2(\rho_{mix}, \kappa_i)) \to 0$. This completes the proof of Theorem 4.2.1.

Chapter 5

Conclusion and Outlook

We have constructed a secure quantum network code in Chapter 3 and a multiple-unicast quantum network code in Chapter 4.

In Chapter 3, we have presented an asymptotically secret and correctable quantum network code as a quantum extension of the classical network codes given in [9, 18]. Under multiple uses of the network and a restriction on node operations, our code acheives rate $m_0 - 2m_1$ asymptotically without any classical communication, where m_0 is the transmission rate without attack and m_1 is the maximum number of the attacked channels. Our code needs secret shared randomness and it is implemented by attaching a known classical secret transmission protocol [16] in our quantum network code. In the analysis of the code, we only considered the correctability because the secrecy is guaranteed by the correctness of the recovered state. The correctability is derived analogously to the classical codes [9, 18] by evaluating bit and phase error probabilities separately.

In Chapter 4, we have proposed a quantum network code for a multiple-unicast network with quantum invertible linear operations. As constraints on information rates, we assumed that the bit and phase transmission rates from S_i to T_i without interference are m_i ($m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} [K]_{p_{i,i}}$), the upper bounds of the bit and phase interferences are a_i and a'_i, respectively ($\operatorname{rank} K_{i^c} \leq a_i$, $\operatorname{rank} [K]_{p_{i^c}} \leq a'_i$), and $a_i + a'_i < m_i$ holds. Under these constraints, our code achieves the rate $m_i - a_i - a'_i$ quantum communication by asymptotic n-use of the network. The negligible rate shared randomness plays a crucial role in our code, and it is realized by attaching the protocol in [16].

The codes in Chapters 3 and 4 can be integrated as a multiple-unicast network with a malicious adversary. When the eavesdropper attacks at most a''_i edges connected with the sender S_i and the receiver T_i, if $a_i + a'_i + 2a''_i < m_i$ holds, our code implements the rate $m_i - a_i - a'_i - 2a''_i$ quantum communi-

cations asymptotically. This fact can be shown by integrating the methods in Chapters 3 and 4.

Bibliography

[1] S. Song and M. Hayashi, "Secure Quantum Network Code without Classical Communication," *Proceedings of 2018 IEEE Information Theory Workshop (ITW 2018)*, pp. 126–130, 2018.

[2] S. Song and M. Hayashi, "Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations," *Proceedings of 13th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2018)*, vol. 111, pp 10:1–10:20, 2018.

[3] Uhlmann, A. "The "transition probability" in the state space of a *-algebra" Reports on Mathematical Physics. 9 (2): 273–279, 1976.

[4] B. Schumacher, "Sending quantum entanglement through noisy channels," *Phys. Rev. A*, 54, 2614–2628, 1996.

[5] M. A. Nielsen, "The entanglement fidelity and quantum error correction", quant-ph/9606012, 1996.

[6] R. Ahlswede, N. Cai, S. -Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, 1204 – 1216, 2000.

[7] N. Cai and R. Yeung, "Secure network coding," in *Proceedings of 2002 IEEE International Symposium on Information Theory (ISIT)*, pp. 323, 2002.

[8] C. Crepeau, D. Gottesman, and A. Smith, "Approximate quantum error-correcting codes and secret sharing schemes," in Proc. Eurocrypt 2005, pp. 285-301. Springer-Verlag, 2005.

[9] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros, "Resilient Network Coding in the Presence of Byzantine Adversaries," *IEEE Transactions on Information Theory*, vol. 54, no. 6, 2596–2603, 2008.

[10] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum Network Coding," in *STACS 2007 SE - 52* (W. Thomas and P. Weil, eds.), vol. 4393 of *Lecture Notes in Computer Science*, pp. 610–621, Springer Berlin Heidelberg, 2007.

[11] M. Hayashi, "Prior entanglement between senders enables perfect quantum network coding with modification," *Phys. Rev. A*, vol. 76, no. 4, 40301, 2007.

[12] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rötteler, "General Scheme for Perfect Quantum Network Coding with Free Classical Communication," in *Automata, Languages and Programming SE - 52* (S. Albers, A. Marchetti-Spaccamela, Y. Matias, S. Nikoletseas, and W. Thomas, eds.), vol. 5555 of *Lecture Notes in Computer Science*, pp. 622–633, Springer Berlin Heidelberg, 2009.

[13] D. Leung, J. Oppenheim, and A. Winter, "Quantum Network Communication; The Butterfly and Beyond," *IEEE Transactions on Information Theory*, vol. 56, no. 7, 3478–3490, 2010.

[14] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, "Perfect quantum network communication protocol based on classical network coding," in *Proceedings of 2010 IEEE International Symposium on Information Theory (ISIT)*, pp. 2686–2690, 2010.

[15] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, "Constructing quantum network coding schemes from classical nonlinear protocols," in *Proceedings of 2011 IEEE International Symposium on Information Theory (ISIT)*, pp. 109–113, 2011.

[16] H. Yao, D. Silva, S. Jaggi, and M. Langberg, "Network Codes Resilient to Jamming and Eavesdropping," IEEE/ACM Transactions on Networking, vol. 22, no. 6, 1978-1987, 2014.

[17] M. Hayashi, *Group Representation for Quantum Theory*, Springer, 2017.

[18] M. Hayashi, M. Owari, G. Kato, and N. Cai, "Secrecy and Robustness for Active Attack in Secure Network Coding," in *IEEE International Symposium on Information Theory (ISIT2017)*, Aachen, Germany, June, 25 – 30, 2017. pp. 1172-1177; The long version is available as arXiv: 1703.00723, 2017.

[19] M. Owari, G. Kato, and M. Hayashi, "Secure Quantum Network Coding on Butterfly Network," *Quantum Science and Technology*, Vol. 3, 014001, 2017.

[20] G. Kato, M. Owari, and M. Hayashi, "Single-Shot Secure Quantum Network Coding for General Multiple Unicast Network with Free Public Communication," In: Shikata J. (eds) 10th International Conference on Information Theoretic Security (ICITS2017). Lecture Notes in Computer Science, vol 10681. Springer, pp. 166-187, 2017.

[21] M. Hayashi, Quantum Information Theory: Mathematical Foundation, Graduate Texts in Physics, Springer, (Second edition of Quantum Information: An Introduction Springer), 2017.

Appendix A

Proofs in Chapter 3

A.1 Proof of Lemma 3.3.1

Proof of Lemma 3.3.1. For $x = (x_1, ..., x_m), y = (y_1, ..., y_m) \in \mathbb{F}_q^m$, define an inner product

$$(x, y) := \sum_{i=1}^{m} \operatorname{tr} x_i y_i = \operatorname{tr} \sum_{i=1}^{m} x_i y_i. \tag{A.1}$$

Let T be a $m \times m$ matrix ove $\mathbb{F}_q$. If x, y are considered as column vectors, it holds that $(Tx, y) = (x, T^\top y)$. On the other hand, if x, y are considered as row vectors, it holds that $(xT, y) = (x, yT^\top)$.

First, we show $\mathcal{L}(A)|M\rangle_p = |(A^{-1})^\top M\rangle_p$ by considering $\mathbb{F}_q^m$ as a column vector space. For $\mathcal{L}^{(1)}(A) := \sum_{x \in \mathbb{F}_q^m} |Ax\rangle_{bb}\langle x|$ and $z \in \mathbb{F}_q^m$,

$$\begin{aligned}
\mathcal{L}^{(1)}(A)|z\rangle_p &= \frac{1}{\sqrt{q^m}} \sum_{x \in \mathbb{F}_q^m} \omega^{-(x,z)} |Ax\rangle_b \\
&= \frac{1}{\sqrt{q^m}} \sum_{x' \in \mathbb{F}_q^m} \omega^{-(A^{-1}x', z)} |x'\rangle_b \\
&= \frac{1}{\sqrt{q^m}} \sum_{x' \in \mathbb{F}_q^m} \omega^{-(x', (A^{-1})^\top z)} |x'\rangle_b \\
&= |(A^{-1})^\top z\rangle_p.
\end{aligned}$$

Since $\mathcal{L}(A) := \left(\mathcal{L}^{(1)}(A)\right)^{\otimes n}$, we have $\mathcal{L}(A)|M\rangle_p = |(A^{-1})^\top M\rangle_p$.

Next, consider $\mathbb{F}_q^n$ as an n-dimensional row vector space over $\mathbb{F}_q$. For

$\mathcal{R}^{(1)}(B) := \sum_{x\in\mathbb{F}_q^n} |xB\rangle_{bb}\langle x|$ and $z \in \mathbb{F}_q^n$,

$$\begin{aligned}
\mathcal{R}^{(1)}(B)|z\rangle_p &= \frac{1}{\sqrt{q^n}} \sum_{x\in\mathbb{F}_q^n} \omega^{-(x,z)}|xB\rangle_b \\
&= \frac{1}{\sqrt{q^n}} \sum_{x''\in\mathbb{F}_q^n} \omega^{-(x''B^{-1},z)}|x''\rangle_b \\
&= \frac{1}{\sqrt{q^n}} \sum_{x''\in\mathbb{F}_q^n} \omega^{-(x'',z(B^{-1})^\top)}|x''\rangle_b \\
&= |z(B^{-1})^\top\rangle_p.
\end{aligned}$$

Since $\mathcal{R}(B) := \big(\mathcal{R}^{(1)}(B)\big)^{\otimes m}$, we have $\mathcal{R}(B)|M\rangle_p = |M(B^{-1})^\top\rangle_p$. □

A.2 Proof of (3.5)

In this section, we show Lemmas A.2.1 and A.2.2 which shows the relationship between two maxially entangled states and projections P_b, P_p defined by the bit and the phase bases.

Define the following maxially entangled states with respect to the bit and phase bases:

$$|\Phi^b\rangle := \frac{1}{\sqrt{q^m}} \sum_{i\in\mathbb{F}_q^m} |i,i\rangle_b, \quad |\Phi^p\rangle := \frac{1}{\sqrt{q^m}} \sum_{z\in\mathbb{F}_q^m} |z,\bar{z}\rangle_p.$$

We use the inner product $(\cdot,\cdot)$ defined in (A.1) for the proofs.

Lemma A.2.1. $|\Phi^p\rangle = |\Phi^b\rangle$.

Proof.

$$\begin{aligned}
|\Phi^p\rangle &= \frac{1}{\sqrt{q^m}}\Big(\sum_{z\in\mathbb{F}_q^m}\Big(\sum_{j\in\mathbb{F}_q^m}\frac{w^{-(z,j)}}{\sqrt{q^m}}|j\rangle_b\Big)\otimes\Big(\sum_{l\in\mathbb{F}_q^m}\frac{w^{(z,l)}}{\sqrt{q^m}}|l\rangle_b\Big)\Big) \\
&= \frac{1}{\sqrt{q^m}} \sum_{z,j,l\in\mathbb{F}_q^m} \frac{\omega^{-(z,j-l)}}{q^m}|j,l\rangle_b \\
&= \frac{1}{\sqrt{q^m}} \sum_{j\in\mathbb{F}_q^m} |j,j\rangle_b. \qquad \text{(A.2)}
\end{aligned}$$

Eq. (A.2) holds because

$$\sum_{z\in\mathbb{F}_q^m}\frac{\omega^{-(z,j-l)}}{q^m}=\begin{cases}0 & \text{if } j\neq l,\\ 1 & \text{otherwise.}\end{cases}$$

□

From the above lemma, we denote $|\Phi\rangle := |\Phi^b\rangle = |\Phi^p\rangle$. Eq. (3.5) is proved by the following lemma.

Lemma A.2.2. *$P_bP_p = P_pP_b = |\Phi\rangle\langle\Phi|$.*

Proof.

$$\begin{aligned}P_bP_p &= \sum_{i,z\in\mathbb{F}_q^m} {}_b\langle i,i|z,\bar{z}\rangle_p|i,i\rangle_{bp}\langle z,\bar{z}|\\ &= \sum_{i,z\in\mathbb{F}_q^m}\frac{\omega^{-(z,i-i)}}{q^m}\sum_{j,l\in\mathbb{F}_q^m}\frac{\omega^{(z,j-l)}}{q^m}|i,i\rangle_{bb}\langle j,l|\\ &= \sum_{i,j,l,z\in\mathbb{F}_q^m}\frac{\omega^{(z,j-l)}}{q^{2d}}|i,i\rangle_{bb}\langle j,l|\\ &= \sum_{i,j\in\mathbb{F}_q^m}\frac{1}{q^m}|i,i\rangle_{bb}\langle j,j|.\end{aligned}$$

□

A.3 Proofs of Lemmas 3.6.2 and 3.6.3

We prepare Lemma A.3.1 to prove Lemmas 3.6.2 and 3.6.3.

Lemma A.3.1 ([9])**.** *Suppose independent m random variables $V_1,\ldots,V_m\in\mathbb{F}_q$ are uniformly chosen in $\mathbb{F}_q$ and define the random matrix $Q\in\mathbb{F}_q^{l\times m}$ as $Q_{i,j} := (V_j)^i$. For arbitrary row vectors $x\in\mathbb{F}_q^m$ and $y\in\mathbb{F}_q^l\backslash\{\mathbf{0}_{1,l}\}$ $(l\geq m)$, we have*

$$\Pr[x=yQ]\leq\left(\frac{l}{q}\right)^m. \tag{A.3}$$

For arbitrary row vectors $x\in\mathbb{F}_q^m\backslash\{\mathbf{0}_{1,m}\}, y\in\mathbb{F}_q^l(l\geq m)$,

$$\Pr[y=xQ^\top]\leq\frac{1}{q}. \tag{A.4}$$

Proof. We only show (A.4) because the inequality (A.3) was shown in [9, Claim 5].

For $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$, the Hadamard product and dot product are defined as $a \circ b := (a_1 b_1, \ldots, a_m b_m)$ and $a \cdot b := \sum_{i=1}^{m} a_i b_i$, respectively. Then, we have the following inclusion: for $V := (V_1, \ldots, V_m) \in \mathbb{F}_q^m$,

$$\begin{aligned}\{V \mid y = xQ^\top\} =& \{V \mid y_1 = x \cdot V,\ y_2 = x \cdot (V \circ V), \ldots, y_l = x \cdot (V^{\circ l})\} \\ \subset& \{V \mid y_1 = x \cdot V\}, \end{aligned} \tag{A.5}$$

where $V^{\circ l} := \underbrace{V \circ V \circ \cdots \circ V}_{l}$. Since the hyperplane (A.5) is $(m-1)$-dimensional, we have

$$\Pr[y = xQ^\top] \leq \Pr[y_1 = x \cdot V] \leq \frac{q^{m-1}}{q^m} = \frac{1}{q}.$$

□

Now we prove Lemmas 3.6.2 and 3.6.3.

Proofs of Lemmas 3.6.2 and 3.6.3. Let $x = (x^{\mathcal{A}}, x^{\mathcal{B}}, x^{\mathcal{C}}) \in \mathbb{F}_{q'}^{m_0} \times \mathbb{F}_{q'}^{m_0} \times \mathbb{F}_{q'}^{n'-2m_0}$ be a nonzero row vector. It holds from definition of R_1^V that

$$x((R_1^V)^{-1})^{\mathcal{A}} = x^{\mathcal{A}} - x^{\mathcal{B}} Q_3^\top Q_4 - x^{\mathcal{C}} Q_1, \tag{A.6}$$

$$x([R_1^V]_p^{-1})^{\mathcal{B}} = x^{\mathcal{B}} + x^{\mathcal{A}} Q_4^\top Q_3 + (x^{\mathcal{A}} Q_1^\top + x^{\mathcal{C}}) Q_2. \tag{A.7}$$

Lemma 3.6.2 is proved as follows. The condition $x((R_1^V)^{-1})^{\mathcal{A}} = \mathbf{0}_{1,m_0}$ holds only in the following three cases from (A.6), and in each case, the probability for $x((R_1^V)^{-1})^{\mathcal{A}} = \mathbf{0}_{1,m_0} = \mathbf{0}_{1,m_0}$ is calculated by Lemma A.3.1 as follows.

1. If $x^{\mathcal{B}} \neq \mathbf{0}_{1,m_0}$ and $x^{\mathcal{C}} = \mathbf{0}_{1,n'-2m_0}$,
$$\Pr[x^{\mathcal{A}} = x^{\mathcal{B}} Q_3^\top Q_4] \leq \left(\frac{m_0}{q'}\right)^{m_0}.$$
2. If $x^{\mathcal{B}} = \mathbf{0}_{1,m_0}$ and $x^{\mathcal{C}} \neq \mathbf{0}_{1,n'-2m_0}$,
$$\Pr[x^{\mathcal{A}} = x^{\mathcal{C}} Q_1] \leq \left(\frac{n'-2m_0}{q'}\right)^{m_0}.$$
3. If $x^{\mathcal{B}} \neq \mathbf{0}_{1,m_0}$ and $x^{\mathcal{C}} \neq \mathbf{0}_{1,n'-2m_0}$,
$$\Pr[x^{\mathcal{A}} - x^{\mathcal{C}} Q_1 = x^{\mathcal{B}} Q_3^\top Q_4] \leq \left(\frac{m_0}{q'}\right)^{m_0}.$$

Since $n' > 3m_0$, we obtain the inequality (3.17) in Lemma 3.6.2.

In the same way, we show Lemma 3.6.3 as follows. The condition $x([R_1^V]_p^{-1})^{\mathcal{B}} = \mathbf{0}_{1,m_0}$ holds only in the following two cases from (A.7), and in each case, the probabilitiy that this condition holds is calculated by Lemma A.3.1 as follows.

1. If $x^{\mathcal{A}}Q_1^\top + x^{\mathcal{C}} = \mathbf{0}_{1,n'-2m_0}$, it should hold that $x^{\mathcal{B}} + x^{\mathcal{A}}Q_4^\top Q_3 = \mathbf{0}_{1,m_0}$. The probability is derived as

$$\begin{aligned}&\Pr[x^{\mathcal{B}} = -x^{\mathcal{A}}Q_4^\top Q_3 \cap x^{\mathcal{C}} = -x^{\mathcal{A}}Q_1^\top]\\ =&\Pr[x^{\mathcal{B}} = -x^{\mathcal{A}}Q_4^\top Q_3] \cdot \Pr[x^{\mathcal{C}} = -x^{\mathcal{A}}Q_1^\top] \le \frac{1}{q'}\Big(\frac{m_0}{q'}\Big)^{m_0}.\end{aligned}$$

2. If $x^{\mathcal{A}}Q_1^\top + x^{\mathcal{C}} \neq \mathbf{0}_{1,n'-2m_0}$, we have

$$\Pr[x^{\mathcal{B}} + x^{\mathcal{A}}Q_4^\top Q_3 = -(x^{\mathcal{C}} + x^{\mathcal{A}}Q_1^\top)Q_2] \le \Big(\frac{n'-2m_0}{q'}\Big)^{m_0}.$$

Since $\frac{1}{q'}\big(\frac{m_0}{q'}\big)^{m_0} < \big(\frac{m_0}{q'}\big)^{m_0} < \big(\frac{n'-2m_0}{q'}\big)^{m_0}$ from $n' > 3m_0$, we have the inequality (3.24) in Lemma 3.6.3. □

A.4 Proof of (3.19)

From $\dim \mathcal{S}_u^\perp = m_2 - \operatorname{rank}[u_{i(1)}, \ldots, u_{i(m_2)}]$, we have

$$\Pr\big[\dim\mathcal{S}_u^\perp = \operatorname{rank}\tilde{W}\big] = \Pr\big[\operatorname{rank}[u_{i(1)}, \ldots, u_{i(m_2)}] = \operatorname{rank} R_{2,b}\big].$$

Since $R_{2,b} = [u_{i(1)}, \ldots, u_{i(m_0)}]$ is a random matrix with $\operatorname{rank} R_{2,b} = m_0 - m_1$, this probability is equivalent to

$$\begin{aligned}&\Pr\big[\operatorname{rank}[u_{i(1)}, \ldots, u_{i(m_2)}] = \operatorname{rank} R_{2,b}\big]\\ =&\Pr\big[\operatorname{rank}[v_1, \ldots, v_{m_2}] = m_0 - m_1 \,\big|\, \operatorname{rank}[v_1, \ldots, v_{m_0}] = m_0 - m_1, v_k \in \mathbb{F}_{q'}^{m_0-m_1}\big].\end{aligned}$$

Therefore, it holds that

$$\begin{aligned}&\Pr\big[\operatorname{rank}[u_{i(1)}, \ldots, u_{i(m_2)}] = \operatorname{rank} R_{2,b}\big]\\ &\ge \Pr\big[\operatorname{rank}[v_1, \ldots, v_{m_2}] = m_0 - m_1 \big| v_k \in \mathbb{F}_{q'}^{m_0-m_1}\big]\\ &\ge \Pr\big[\operatorname{rank}[v_1, \ldots, v_{m_0-m_1}] = m_0 - m_1 \big| v_k \in \mathbb{F}_{q'}^{m_0-m_1}\big]. \qquad \text{(A.8)}\end{aligned}$$

The probability (A.8) is equivalent to the probability to choose $m_0 - m_1$ independent vectors in $\mathbb{F}_{q'}^{m_0-m_1}$:

$$\begin{aligned}
&\Pr\big[\operatorname{rank}[v_1, \ldots, v_{m_0-m_1}] = m_0 - m_1 \big| v_k \in \mathbb{F}_{q'}^{m_0-m_1}\big] \\
&= \Big(\frac{(q')^{m_0-m_1}}{(q')^{m_0-m_1}}\Big) \cdot \Big(\frac{(q')^{m_0-m_1} - q'}{(q')^{m_0-m_1}}\Big) \cdots \Big(\frac{(q')^{m_0-m_1} - (q')^{m_0-m_1-1}}{(q')^{m_0-m_1}}\Big) \\
&= 1 - O(1/q').
\end{aligned}$$

Therefore, (3.19) holds with probability at least $1 - O(1/q')$.