Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations

Seunghoan Song
Graduate School of Mathematics, Nagoya University, Nagoya, Japan
m17021a@math.nagoya-u.ac.jp

Masahito Hayashi
Graduate School of Mathematics, Nagoya University, Nagoya, Japan
Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore
Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, China
masahito@math.nagoya-u.ac.jp

Abstract

This paper considers the communication over a quantum multiple-unicast network where r sender-receiver pairs communicate independent quantum states. We concretely construct a quantum network code for the quantum multiple-unicast network as a generalization of the code [Song and Hayashi, arxiv:1801.03306, 2018] for the quantum unicast network. When the given node operations are restricted to invertible linear operations between bit basis states and the rates of transmissions and interferences are restricted, our code certainly transmits a quantum state for each sender-receiver pair by n-use of the network asymptotically, which guarantees no information leakage to the other users. Our code is implemented only by the coding operation in the senders and receivers and employs no classical communication and no manipulation of the node operations. Several networks that our code can be applied are also given.

2012 ACM Subject Classification Hardware → Quantum communication and cryptography

Keywords and phrases Quantum network code, Multiple-unicast quantum network, Quantum invertible linear operation

Digital Object Identifier 10.4230/LIPIcs.TQC.2018.10

Acknowledgements SS is supported by Rotary Yoneyama Memorial Master Course Scholarship (YM). This work was supported in part by a JSPS Grant-in-Aids for Scientific Research (A) No.17H01280 and for Scientific Research (B) No.16KT0017, and Kayamori Foundation of Information Science Advancement.

1 Introduction

When we transmit information via network, it is useful to make codes by reflecting the network structure. Such type of coding is called network coding and was initiated by Ahlswede et al. [1]. This topic has been extensively researched by many researchers. Network coding employs computation-and-forward in intermediate nodes instead of the naive routing method in traditional network communication. For the quantum network, the paper [5] started the discussion of the quantum network coding, and many papers [2, 9–12] have advanced the study of quantum network coding.

In the network coding, unicast network is the most basic network model that the entire network is used by a sender and a receiver. As one of the remarkable achievements of network

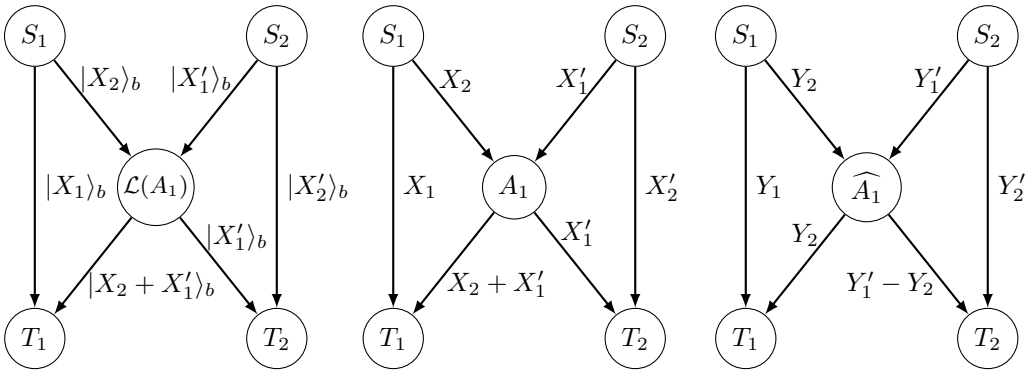
coding for the unicast network, on the classical linear network with malicious adversaries, the papers [6, 7] proposed codes that implement the classical communication by asymptotic n-use of the network. In [6, 7], when the transmission rate m in absence of attacks is at least the maximum rate a of attack (i.e., $a < m$), the codes in [6, 7] implement the rate $m - a$ communication asymptotically. As a quantum generalization of the codes in [6, 7], the paper [14] constructed a quantum network code that transmits a quantum state correctly and secretly by asymptotic n-use of the network. Similarly to [6, 7], when the transmission rate m without attacks is at least twice of the maximum number a of the attacked edges (i.e., $2a < m$), the code in [14] implements the rate $m-2a$ quantum communication asymptotically.

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 [8] studied a quantum network code for the multiple-unicast network. The code in [8] transmits a state successfully for each use of the network. However, [8] 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 [8] requires the free use of the classical communication.

This paper proposes a quantum network code for the multiple-unicast network which is a generalization of the unicast quantum network code in [14] and overcomes the shortcomings of the multiple-unicast quantum network code in [8]. In the same way as [14], the given node operations are invertible linear with respect to the bit basis states, which is called *quantum invertible linear operations* described in Section 2, 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 [8], 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 [13].

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 to 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 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 2), we call the network as *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. The bit and the phase classical networks (Fig. 1b and Fig. 1c) are determined from the quantum network (Fig. 1a) (see Section 2). 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



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

Figure 1 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 (see Section 2). The network (b) and (c) is the bit and phase classical networks of the quantum network (a).

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 the practical sense, our code can cope with the 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 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 the 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.

The remaining of this paper is organized as follows. Section 2 introduces the formal description of the quantum multiple-unicast network with quantum invertible linear operations. Section 3 gives the main results of this paper. Based on the preliminaries in Section 4, Section 5 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. Section 6 analyzes the correctness of the code in Section 5. Then, Section 7 constructs our code without the assumption of shared randomness by attaching the secret and correctable communication protocol [15] to the code given in Section 5, which proves the main result given in Section 3. Section 8 gives several examples of the network that our code can be applied. Section 9 is the conclusion of this paper.

2 Quantum Network with Invertible Linear Operations

Our code is designed on the 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 [14, Section II].

2.1 Classical 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 $S_1, \dots, S_r$ and r terminal nodes $T_1, \dots, T_r$. 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 $(= |V| - 2r)$ accordingly to the order of the transmission. The intermediate node numbered t has the same number k_t of incoming and outgoing edges where $1 \le k_t \le m$.

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

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

The second term $K_{i^c} z_{i^c}$ of (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 $X_1 \in \mathbb{F}_q^{m_1 \times n}, \dots, X_r \in \mathbb{F}_q^{m_r \times n}$, the output $Y_i \in \mathbb{F}_q^{m_i \times n}$ at the receiver T_i $(i = 1, \dots, r)$ is

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

2.2 Quantum 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 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 $\mathcal{H}_{T_i} := \mathcal{H}^{\otimes m_i \times n}$

To describe the quantum node operation, we define the following quantum operations.

▶ **Definition 2.1** (Quantum Invertible Linear Operation)**.** 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 for any $X \in \mathbb{F}_q^{m\times n}$ as

$$\mathcal{L}(A)|X\rangle_b := |AX\rangle_b, \quad \mathcal{R}(B)|X\rangle_b := |XB\rangle_b.$$

The operations $\mathcal{L}(A)$ and $\mathcal{R}(B)$ are called *quantum invertible linear operations.*

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 2.1. 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 [3, Section 8.1.2] by

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

where $\omega := \exp\frac{2\pi i}{p}$ 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 $\mathbb{F}_p^t$. For the analysis of the phase basis interference, we give Lemma 2.2 which explains how node operations $\mathcal{L}(A_t)$ are applied to the phase basis states.

▶ **Lemma 2.2** ([14, Appendix A])**.** *Let $A \in \mathbb{F}_q^{m\times m}$ and $B \in \mathbb{F}_q^{n\times n}$ be invertible matrices. For any $M \in \mathbb{F}_q^{m\times n}$, we have*

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

For notational convenience, we denote $\widehat{A} := (A^{\mathrm{T}})^{-1}$. 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 $\mathcal{L}(K)|M\rangle_p = |\widehat{K}M\rangle_p$. In this case, this quantum network can also be considered as a classical network with network operation $\widehat{K} = \widehat{A_c}\cdots\widehat{A_1}$. Then, $\widehat{K}_{i,j}$ is defined from $\widehat{K}$ in the same way as $K_{i,j}$.

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

$$\widehat{K}_{i^c} := [\widehat{K}_{i,1} \ \cdots \ \widehat{K}_{i,i-1} \ \widehat{K}_{i,i+1} \ \cdots \ \widehat{K}_{i,r}].$$

Similarly to the condition $\operatorname{rank} K_{i,i} = m_i$, we also assume $\operatorname{rank}\widehat{K}_{i,i} = m_i$. We also call $\operatorname{rank}\widehat{K}_{i^c}$ the rate of phase interference to T_i. The transmission rates from S_i to T_i are summarized in Table 1.

Table 1 Definitions of Information Rates.

Rate	Meaning
$m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} \widehat{K}_{i,i}$	Bit (phase) transmission rates from S_i to T_i without interference
$\operatorname{rank} K_{i^c}$	Rate of interference to T_i
$\operatorname{rank} \widehat{K}_{i^c}$	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

3 Main Results

In this section, we propose two main theorems of this paper. 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 5 and 7, respectively. The theorems are stated with respect to the completely mixed state ρ_{mix} and the *entanglement fidelity* $F_e^2(\rho, \kappa) := \langle x|\kappa \otimes \iota_R(|x\rangle\langle x|)|x\rangle$ for the quantum channel κ and a purification $|x\rangle$ of the state ρ.

▶ **Theorem 3.1.** *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 2. Let m_i be the bit and phase transmission rates from S_i to T_i without interferences ($m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} \widehat{K}_{i,i}$), and a_i, a'_i be the upper bounds of the bit and phase interferences, respectively ($\operatorname{rank} K_{i^c} \le a_i$, $\operatorname{rank} \widehat{K}_{i^c} \le a'_i$). When the condition $a_i + a'_i < m_i$ holds and the sender S_i and receiver T_i can share the 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 $F_e^2(\rho_{mix}, \kappa_i)$ satisfies $n(1 - F_e^2(\rho_{mix}, \kappa_i)) \to 0$ where κ_i is the quantum code protocol from sender S_i to receiver T_i.*

Section 5 constructs the code stated in Theorem 3.1 and Section 6 shows that this code has the performance in Theorem 3.1. 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. As explained in [14, Section III], our code has no information leakage from the condition $n(1 - F_e^2(\rho_{mix}, \kappa_i)) \to 0$.

Although Theorem 3.1 assumed the free use of the negligible rate shared randomness, it is possible to design the code of the same performance without negligible rate shared randomness as follows. The paper [15] gives the secret and correctable classical network communication protocol for the 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 [15] to our quantum network with bit basis states, the negligible rate shared randomness can be generated. By this method, we have the following Theorem 3.2 and the details are explained in Section 7.

▶ **Theorem 3.2.** *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 2. Let m_i be the bit and phase transmission rates from S_i to T_i without interferences ($m_i = \operatorname{rank} K_{i,i} = \operatorname{rank} \widehat{K}_{i,i}$), and a_i, a'_i be the upper bounds of the bit and phase interferences, respectively ($\operatorname{rank} K_{i^c} \le a_i$, $\operatorname{rank} \widehat{K}_{i^c} \le a'_i$). 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 $F_e^2(\rho_{mix}, \kappa_i)$ satisfies $n(1 - F_e^2(\rho_{mix}, \kappa_i)) \to 0$ where κ_i is the quantum code protocol from sender S_i to receiver T_i.*

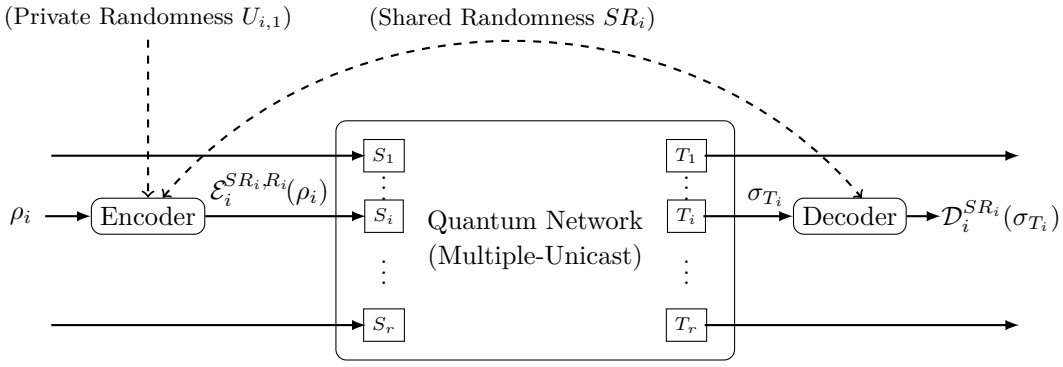


Figure 2 Overview of code protocol from a sender S_i to a receiver T_i. States ρ_i and $\mathcal{D}_i^{SR_i}(\sigma_{T_i})$ are in code space $\mathcal{H}'_{\rm code}$.

4 Preliminaries for Code Construction

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

4.1 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, dependently 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 2.1) 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

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

4.2 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

$$\begin{bmatrix} |\phi\rangle \\ |\psi\rangle \\ |\varphi\rangle \end{bmatrix} := |\phi\rangle \otimes |\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}'_{\mathcal{A}} \,. \tag{2}$$

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

$$\left| \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \right\rangle_b := \begin{bmatrix} |X\rangle_b \\ |Y\rangle_b \\ |Z\rangle_b \end{bmatrix}, \quad \left| \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \right\rangle_p := \begin{bmatrix} |X\rangle_p \\ |Y\rangle_p \\ |Z\rangle_p \end{bmatrix}. \tag{3}$$

We also introduce notations for the states in $\mathcal{H}'_{\mathcal{B}}$ and $\mathcal{H}'_{\mathcal{C}}$ in the same way as (2) and (3). In the following, we denote the $k \times l$ zero matrix as $\mathbf{0}_{k,l}$.

4.3 CSS Code in Our Code

In our code construction, we use the CSS code defined in this subsection which is similarly defined from [14, Subsection IV-B]. Define two classical codes $C_1, C_2 \subset \mathbb{F}_{q'}^{m_i \times (n'-2m_i)}$ which satisfy $C_1 \supset C_2^{\perp}$ as

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

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

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

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

With the above definitions, the code space is given as $\mathcal{H}'_{\text{code}} := \mathcal{H}'_{\mathcal{C}2} = \mathcal{H}'^{\otimes (m_i - a_i - a'_i) \times (n'-2m_i)}$ 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

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

5 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).

5.1 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 and the quantum systems $\mathcal{H}'_{\mathcal{A}}$ and $\mathcal{H}'_{\mathcal{B}}$ as

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

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 $U_{i,2}^{V_i} \in \mathbb{F}_{q'}^{n'\times n'}$ as

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

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

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

5.2 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

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

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

$$P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} O_{i,1} = \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix}, \quad P_{\mathcal{W}_{i,2}} D_{i,2}^{R_{i,2},O_{i,2}} O_{i,2} = \begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i} \end{bmatrix}. \tag{4}$$

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), the decoder applies $\mathcal{L}'(D_{i,1}^{R_{i,1},O_{i,1}})$ and $\mathcal{L}'(\widehat{D_{i,2}^{R_{i,2},O_{i,2}}})$ 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 $D_i^{R_i}$:

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

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

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

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.

6 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 3, 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 5 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 $\mathcal{H}'_{\rm code}$,

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

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 [14, Section IV], $1-F_e^2(\rho_{mix},\kappa_i)$ 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 $|X\rangle_b\in\mathcal{H}'_{\rm code}$ 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. We will show in Subsections 6.2 and 6.3 that the bit and phase error probabilities are upper bounded by $O\Big(\max\Big\{\frac{1}{q'},\frac{(n')^{m_i}}{(q')^{m_i-a_i}}\Big\}\Big)$ and $O\Big(\max\Big\{\frac{1}{q'},\frac{(n')^{m_i}}{(q')^{m_i-a'_i}}\Big\}\Big)$, respectively. Therefore, we have

$$n(1-F_e^2(\rho_{mix},\kappa_i)) \le nO\Big(\max\Big\{\frac{1}{q'},\frac{(n')^{m_i}}{(q')^{m_i-\max\{a_i,a'_i\}}}\Big\}\Big). \tag{5}$$

Since q' is taken in Section 4 to satisfy $\frac{n\cdot(n')^{m_i}}{(q')^{m_i-\max\{a_i,a'_i\}}}\to 0$, the RHS of (5) converges to 0 and therefore $n(1-F_e^2(\rho_{mix},\kappa_i))\to 0$. This completes the proof of Theorem 3.1.

6.1 Notation and Lemmas for Bit and Phase Error Probabilities

In this subsection, we prepare a notation and lemmas for proving the upper bounds of the bit and phase error probabilities. The upper bounds of these probabilities are shown separately in Subsections 6.2 and 6.3.

We introduce the notation $X := (X^{\mathcal{A}},X^{\mathcal{B}},X^{\mathcal{C}})\in\mathbb{F}_{q'}^{k\times m_i}\times\mathbb{F}_{q'}^{k\times m_i}\times\mathbb{F}_{q'}^{k\times(n'-2m_i)}$ for $X\in\mathbb{F}_{q'}^{k\times n'}$ with arbitrary positive integer k. Also, we prepare the following lemmas.

▶ **Lemma 6.1.** *For integers $d_0\ge d_1+d_2$, let $\mathcal{W}_1\subset\mathbb{F}_{q'}^{d_0}$ be a d_1-dimensional subspace and $\mathcal{W}_2\subset\mathbb{F}_{q'}^{d_0}$ be a d_2-dimensional subspace. Assume the following three conditions.*
(Γ1) $\mathcal{W}_1\cap\mathcal{W}_2=\{\mathbf{0}_{d_0,1}\}$.

(Γ2) *Let $\bar{m} \geq d_1 + d_2$. The vectors $x_1, \ldots, x_{\bar{m}} \in \mathcal{W}_1$ and $y_1, \ldots, y_{\bar{m}} \in \mathcal{W}_2$ satisfy*

$$\mathrm{span}((x_1, y_1), \ldots, (x_{\bar{m}}, y_{\bar{m}})) = \mathcal{W}_1 \oplus \mathcal{W}_2.$$

(Γ3) *Let $W_1' \subset \mathbb{F}_{q'}^{d_0}$ be a d_1-dimensional subspace and $r_1, \ldots, r_{\bar{m}} \in \mathcal{W}_1'$. There exists an invertible linear map $A : \mathcal{W}_1' \to \mathcal{W}_1$ which maps*

$$[x_1, \ldots, x_{\bar{m}}] = A[r_1, \ldots, r_{\bar{m}}].$$

Then, the following two statements hold.

(Δ1) *There exists invertible linear map $D : \mathbb{F}_{q'}^{d_0} \to \mathbb{F}_{q'}^{d_0}$ that*

$$P_{\mathcal{W}_1'} D[(x_1, y_1), \ldots, (x_{\bar{m}}, y_{\bar{m}})] = A^{-1}[x_1, \ldots, x_{\bar{m}}] = [r_1, \ldots, r_{\bar{m}}]. \tag{6}$$

(Δ2) *For the above linear map D, it holds for any $x \in \mathcal{W}_1$ and $y \in \mathcal{W}_2$ that*

$$P_{\mathcal{W}_1'} D(x, y) = A^{-1} x. \tag{7}$$

Proof. First, we show the item (Δ1). Let $\mathcal{W}_3$ be a subspace of $\mathbb{F}_{q'}^{d_0}$ that satisfies $\mathcal{W}_1 \oplus \mathcal{W}_2 \oplus \mathcal{W}_3 = \mathbb{F}_{q'}^{d_0}$. If D is defined as $D|_{\mathcal{W}_1} = A^{-1}$ and $D|_{\mathcal{W}_2 \oplus \mathcal{W}_3}(\mathcal{W}_2 \oplus \mathcal{W}_3) = \mathcal{W}_1'^{\perp}$, we obtain (6), i.e., (Δ1) from

$$P_{\mathcal{W}_1'} D((x_i, y_i)) = P_{\mathcal{W}_1'}(D|_{\mathcal{W}_1}(x_i) + D|_{\mathcal{W}_2 \oplus \mathcal{W}_3}(y_i)) = A^{-1} x_i = r_i.$$

Next, we show that the item (Δ2). Since arbitrary $(x, y) \in \mathcal{W}_1 \oplus \mathcal{W}_2$ is spanned by $(x_1, y_1), \ldots, (x_{\bar{m}}, y_{\bar{m}})$, Eq. (6) implies (7), which yields (Δ2). ◀

▶ **Lemma 6.2** ([14, Lemma 7.1]). *For integers $d_a \geq d_b + d_c$, fix a d_b-dimensional subspace $\mathcal{W} \subset \mathbb{F}_{q'}^{d_a}$, and randomly choose a d_c-dimensional subspace $\mathcal{R} \subset \mathbb{F}_{q'}^{d_a}$ with the uniform distribution. Then, we have*

$$\Pr[\mathcal{W} \cap \mathcal{R} = \{\mathbf{0}_{d_a,1}\}] = 1 - O(q'^{d_b + d_c - d_a - 1}).$$

▶ **Lemma 6.3.** *For $d \geq d'$,*

$$\Pr\left[\mathrm{rank}[t_1, \ldots, t_d] = d' \;\middle|\; t_1, \ldots, t_d \in \mathbb{F}_{q'}^{d'}\right] \geq 1 - O\left(\frac{1}{q'}\right).$$

Proof. From $d \geq d'$, we have

$$\Pr\left[\mathrm{rank}[t_1, \ldots, t_d] = d' \;\middle|\; t_1, \ldots, t_d \in \mathbb{F}_{q'}^{d'}\right] \geq \Pr\left[\mathrm{rank}[t_1, \ldots, t_{d'}] = d' \;\middle|\; t_1, \ldots, t_{d'} \in \mathbb{F}_{q'}^{d'}\right]. \tag{8}$$

On the other hand, the RHS of (8) is equivalent to the probability to choose d' independent vectors in $\mathbb{F}_{q'}^{d'}$:

$$\Pr\left[\mathrm{rank}[t_1, \ldots, t_{d'}] = d' \;\middle|\; t_1, \ldots, t_{d'} \in \mathbb{F}_{q'}^{d'}\right] = \frac{q'^{d'}}{q'^{d'}} \cdot \frac{q'^{d'} - q'}{q'^{d'}} \cdots \frac{q'^{d'} - q'^{d'-1}}{q'^{d'}} = 1 - O\left(\frac{1}{q'}\right).$$

By combining the above inequality and equality, we have the lemma. ◀

▶ **Lemma 6.4** ([14, Lemmas 7.2 and 7.4]). *For the random matrix $U_{i,2}^{V_i}$ defined in Step E3, we have*

$$\max_{\mathbf{0}_{n',1} \neq x \in \mathbb{F}_{q'}^{n'}} \Pr[x^{\mathrm{T}}((U_{i,2}^{V_i})^{-1})^{\mathcal{A}} = \mathbf{0}_{1,m_i}] \leq \left(\frac{n' - 2m_i}{q'}\right)^{m_i},$$

$$\max_{\mathbf{0}_{n',1} \neq x \in \mathbb{F}_{q'}^{n'}} \Pr[x^{\mathrm{T}}((\widehat{U_{i,2}^{V_i}})^{-1})^{\mathcal{B}} = \mathbf{0}_{1,m_i}] \leq \left(\frac{n' - 2m_i}{q'}\right)^{m_i}.$$

6.2 Bit Error Probability

In this subsection, we show that when arbitrary bit basis state $|M\rangle_b \in \mathcal{H}'_{\rm code}$ is the input state of the sender S_i, the original message M is correctly recovered with probability at least $1 - O\Big(\max\Big\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a_i}}\Big\}\Big)$.

Step 1: We derive a necessary condition for correct decoding of the original message M in bit basis. When arbitrary bit basis state $|M\rangle_b \in \mathcal{H}'_{\rm code}$ is the input state of the sender S_i, the encoded state is written as

$$\mathcal{E}_i^{SR_i,R_i}(|M\rangle_b) = \sum_{\bar{E}_1 \in \mathbb{F}_{q'}^{m_i\times m_i}, \bar{E}_2 \in \mathbb{F}_{q'}^{a'_i\times(n'-2m_i)}} \left| U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} & & \mathbf{0}_{a_i,n'-2m_i} \\ R_{i,1} & \bar{E}_1 & M \\ & & \bar{E}_2 \end{bmatrix} U_{i,2}^{V_i} \right\rangle_b ,$$

where we ignore the normalizing factors and phase factors.

Note that bit state measurement on network output system $\mathcal{H}_{T_i} = \mathcal{H}'^{\otimes m_i\times n'_i}$ commutes with the decoding operation $\mathcal{D}_i^{SR_i}$ on $\mathcal{H}_{T_i}$. Therefore, in the analysis of the bit error probability, we take the method to perform bit state measurement to $\mathcal{H}_{T_i}$ first, and then apply the decoding operation corresponding to $\mathcal{D}_i^{SR_i}$, instead of decoding first and performing bit state measurement.

By performing the bit basis measurement to the network output $\sigma_{T_i} = \kappa_i(|M\rangle_{bb}\langle M|)$, we have the following measurement outcome Y:

$$Y = K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} & & \mathbf{0}_{a_i,n'-2m_i} \\ R_{i,1} & \bar{E}_1 & M \\ & & \bar{E}_2 \end{bmatrix} U_{i,2}^{V_i} + K_{i^c}Z,$$

where $\bar{E}_1 \in \mathbb{F}_{q'}^{m_i\times m_i}$, $\bar{E}_2 \in \mathbb{F}_{q'}^{a'_i\times(n'-2m_i)}$ and $Z \in \mathbb{F}_{q'}^{(m-m_i)\times n'}$. By Step D1, Y is decoded to

$$\bar{Y} = Y(U_{i,2}^{V_i})^{-1} = K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} & & \mathbf{0}_{a_i,n'-2m_i} \\ R_{i,1} & \bar{E}_1 & M \\ & & \bar{E}_2 \end{bmatrix} + K_{i^c}Z(U_{i,2}^{V_i})^{-1}.$$

The measurement outcome $O_{i,1}$ in Step D2 is

$$O_{i,1} = \bar{Y}^{\mathcal{A}} = K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix} + (K_{i^c}Z(U_{i,2}^{V_i})^{-1})^{\mathcal{A}}.$$

Since the decoder knows $O_{i,1}$ and $R_{i,1}$, the matrix $D_{i,1}^{R_{i,1},O_{i,1}}$ is found by Gaussian elimination to the left equation of (4) which is written as

$$P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} O_{i,1} = P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} \left(K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix} + (K_{i^c}Z(U_{i,2}^{V_i})^{-1})^{\mathcal{A}} \right) = \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix}. \quad (9)$$

Therefore, if the matrix $D_{i,1}^{R_{i,1},O_{i,1}}$ derived in (9) satisfies the following equation

$$P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} \bar{Y}^{\mathcal{C}} = P_{\mathcal{W}_{i,1}} D_{i,1}^{R_{i,1},O_{i,1}} \left(K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,n'-2m_i} \\ M \\ \bar{E}_2 \end{bmatrix} + (K_{i^c}Z(U_{i,2}^{V_i})^{-1})^{\mathcal{C}} \right) = \begin{bmatrix} \mathbf{0}_{a_i,n'-2m_i} \\ M \\ \bar{E}_2 \end{bmatrix}, \quad (10)$$

the original message M is correctly recovered.

Step 2: In the next step, we show that the conditions (Γ1), (Γ2) and (Γ3) of Lemma 6.1 in the following case imply Eq. (10);

$$\mathcal{W}_1 := \mathrm{col}\left(K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix} \right), \quad \mathcal{W}_2 := \mathrm{col}\big(K_{i^c} Z (U_{i,2}^{V_i})^{-1}\big), \quad \mathcal{W}_1' := \mathcal{W}_{i,1}, \quad \bar{m} := m_i,$$

$$[x_1, \dots, x_{\bar{m}}] := K_{i,i}U_{i,1} \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix}, \quad [y_1, \dots, y_{\bar{m}}] := (K_{i^c} Z (U_{i,2}^{V_i})^{-1})^{\mathcal{A}},$$

$$[r_1, \dots, r_{\bar{m}}] := \begin{bmatrix} \mathbf{0}_{a_i,m_i} \\ R_{i,1} \end{bmatrix}, \quad A := (K_{i,i}U_{i,1})|_{\mathcal{W}_1'}, \quad (d_0, d_1, d_2) := (m_i, m_i - a_i, \mathrm{rank}\, K_{i^c} Z),$$

where $\mathrm{col}(T)$ of the matrix T is the column space of T and $\mathcal{W}_{i,1}$ is defined in Step D2 of Subsection 5.2.

Applying Lemma 6.1, we show that Eq. (10) holds if the conditions (Γ1), (Γ2) and (Γ3) are satisfied. Assume that (Γ1), (Γ2) and (Γ3) are satisfied. Then, the condition (Δ1) holds which implies the existence of $D_{i,1}^{R_{i,1},O_{i,1}}$ in (9). Moreover, (Δ2) implies that for any $r \in \mathcal{W}_1', y \in \mathcal{W}_2$ and $x = K_{i,i}U_{i,1}r \in \mathcal{W}_1$, it holds

$$P_{\mathcal{W}_1'} D_{i,1}^{R_{i,1},O_{i,1}}(x+y) = A^{-1}x = \big((K_{i,i}U_{i,1})|_{\mathcal{W}_1'}\big)^{-1}(K_{i,i}U_{i,1}r) = r,$$

and this yields (10).

Step 3: In the third step, we show that the relations (Γ1), (Γ2) and (Γ3) hold at least with probability $1 - O\Big(\max\Big\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a_i}}\Big\}\Big)$, which proves the desired statement by combining the conclusion of Steps 1 and 2.

Step 3-1: In this substep, we show that the probability satisfying (Γ1), (Γ2) and (Γ3) is obtained by

$$\Pr[(\Gamma1) \cap (\Gamma2) \cap (\Gamma3)] = \Pr[(\Gamma1)] \cdot \Pr[(\Gamma2')] \cdot \Pr[(\Gamma2)|(\Gamma2') \cap (\Gamma1)], \tag{11}$$

where the condition (Γ2′) is given as
(Γ2′) $\mathrm{rank}\, K_{i^c} Z((U_{i,2}^{V_i})^{-1})^{\mathcal{A}} = \mathrm{rank}\, K_{i^c} Z$.
Eq. (11) is derived by the following reductions:

$$\begin{aligned} &\Pr[(\Gamma1) \cap (\Gamma2) \cap (\Gamma3)] \overset{(a)}{=} \Pr[(\Gamma1) \cap (\Gamma2)] \overset{(b)}{=} \Pr[(\Gamma1)] \cdot \Pr[(\Gamma2)|(\Gamma1)] \\ &\overset{(c)}{=} \Pr[(\Gamma1)] \cdot \Pr[(\Gamma2) \cap (\Gamma2')|(\Gamma1)] \overset{(d)}{=} \Pr[(\Gamma1)] \cdot \Pr[(\Gamma2')|(\Gamma1)] \cdot \Pr[(\Gamma2)|(\Gamma2') \cap (\Gamma1)] \\ &\overset{(e)}{=} \Pr[(\Gamma1)] \cdot \Pr[(\Gamma2')] \cdot \Pr[(\Gamma2)|(\Gamma2') \cap (\Gamma1)]. \end{aligned}$$

The equality (a) follows from the fact that (Γ3) is always satisfied for A defined in Step 2, and (b) and (d) are trivial. (c) is obtained because (Γ2′) is a necessary condition for (Γ2). Since $\mathrm{span}(y_1, \dots, y_{\bar{m}}) = \mathcal{W}_2$ is a necessary condition for (Γ2) in Lemma 6.1, the condition (Γ2′) is also necessary for (Γ2) from

$$\begin{aligned} \mathrm{rank}\, K_{i^c} Z((U_{i,2}^{V_i})^{-1})^{\mathcal{A}} &= \mathrm{rank}(K_{i^c} Z (U_{i,2}^{V_i})^{-1})^{\mathcal{A}} = \mathrm{dimspan}(y_1, \dots, y_{\bar{m}}) \\ &= \dim \mathcal{W}_2 = \mathrm{rank}\, K_{i^c} Z (U_{i,2}^{V_i})^{-1} = \mathrm{rank}\, K_{i^c} Z. \end{aligned}$$

The equality (e) follows from the fact that (Γ1) and (Γ2′) are independent, which will be shown by $\Pr[(\Gamma1)|(\Gamma2')] = \Pr[(\Gamma1)]$ in Step 3-2.

Step 3-2: In this step, we prove $\Pr[(\Gamma 1)] \geq 1 - O(1/q')$ and $\Pr[(\Gamma 1)|(\Gamma 2')] = \Pr[(\Gamma 1)]$. Fix $R_{i,1}$ and $U_{i,2}^{V_i}$. Then, $\mathcal{W}_1$ is randomly chosen d_1-dimensional subspace under uniform distribution and $\mathcal{W}_2$ is fixed d_2-dimensional subspace. Therefore, Lemma 6.2 can be applied with $(d_a, d_b, d_c, \mathcal{W}) := (d_0, d_2, d_1, \mathcal{W}_2)$ and $\Pr[(\Gamma 1)] = 1 - O(q'^{d_2+d_1-d_0-1}) \geq 1 - O(1/q')$. On the other hand, since $\Pr[(\Gamma 1)]$ does not depend on $U_{i,2}^{V_i}$ but $\Pr[(\Gamma 2)]$ depends only on $U_{i,2}^{V_i}$, we have $\Pr[(\Gamma 1)|(\Gamma 2')] = \Pr[(\Gamma 1)]$.

Step 3-3: In this step, we show $\Pr[(\Gamma 2')] \geq 1 - \frac{n'^{m_i}}{q'^{m_i - a_i}}$. The condition $(\Gamma 2')$ holds if and only if $x^{\mathrm{T}} K_{i^c} Z ((U_{i,2}^{V_i})^{-1})^{\mathcal{A}} \neq \mathbf{0}_{1,m_i}$ for any vector $x \in \mathbb{F}_{q'}^{m_i}$ satisfying $x^{\mathrm{T}} K_{i^c} Z \neq \mathbf{0}_{1,n'}$ (considering K_{i^c}, Z and $((U_{i,2}^{V_i})^{-1})^{\mathcal{A}}$ as linear maps on row vector spaces, this is equivalent that $((U_{i,2}^{V_i})^{-1})^{\mathcal{A}}$ has trivial kernel $\{\mathbf{0}_{1,n'}\}$ for the image of $K_{i^c} Z$). Therefore, by applying Lemma 6.4 for all distinct $x^{\mathrm{T}} K_{i^c} Z$ which is not zero vector, we have

$$\Pr[(\Gamma 2')] \geq 1 - q'^{\operatorname{rank} K_{i^c} Z} \left(\frac{n' - 2m_i}{q'} \right)^{m_i} \geq 1 - q'^{a_i} \left(\frac{n' - 2m_i}{q'} \right)^{m_i} \geq 1 - \frac{n'^{m_i}}{q'^{m_i - a_i}}.$$

Step 3-4: Now we evaluate the probability $\Pr[(\Gamma 2)|(\Gamma 2') \cap (\Gamma 1)] \geq 1 - O(1/q'^{-1})$. Fix the random variable $U_{i,2}^{V_i}$ so that $(\Gamma 2')$ holds in the following. Define matrices $T_x = [x_{i(1)}, \ldots, x_{i(d_1+d_2)}]$, $T_y = [y_{i(1)}, \ldots, y_{i(d_1+d_2)}]$ and $T = T_x + T_y \in \mathbb{F}_{q'}^{d_0 \times (d_1+d_2)}$ where $i : \{1, \ldots, d_1 + d_2\} \to \{1, \ldots, \bar{m}\}$ is an injective index function such that $y_{i(1)}, \ldots, y_{i(d_2)}$ are linearly independent i.e., $\operatorname{rank} T_y = d_2$. Then, we have

$$\begin{aligned}
&\Pr\big[(\Gamma 2)|(\Gamma 2') \cap (\Gamma 1)\big] \geq \Pr[\operatorname{span}\big((x_{i(1)}, y_{i(1)}), \ldots, (x_{i(d_1+d_2)}, y_{i(d_1+d_2)})\big) = \mathcal{W}_1 \oplus \mathcal{W}_2 \,|\, (\Gamma 2') \cap (\Gamma 1)] \\
&\overset{(a)}{=} \Pr\big[\operatorname{rank} T = d_1 + d_2 \mid (\Gamma 2') \cap (\Gamma 1)\big] = \Pr\big[\ker T = \{\mathbf{0}_{d_1+d_2,1}\} \mid (\Gamma 2') \cap (\Gamma 1)\big] \\
&\overset{(b)}{=} \Pr\big[\ker T_x \cap \ker T_y = \{\mathbf{0}_{d_1+d_2,1}\} \mid (\Gamma 2') \cap (\Gamma 1)\big],
\end{aligned}$$

where (a) follows from $\operatorname{span}\big((x_{i(1)}, y_{i(1)}), \ldots, (x_{i(d_1+d_2)}, y_{i(d_1+d_2)})\big) \subset \mathcal{W}_1 \oplus \mathcal{W}_2$, and (b) follows from the condition $(\Gamma 1)$. Since $\operatorname{rank} T_x \leq d_1$ follows from its definition and the dimension of $\ker T_y$ is d_1, the condition $\operatorname{rank} T_x = d_1$ is a necessary condition for $\ker T_x \cap \ker T_y = \{\mathbf{0}_{d_1+d_2,1}\}$. Therefore, we have

$$\begin{aligned}
&\Pr[\ker T_x \cap \ker T_y = \{\mathbf{0}_{d_1+d_2,1}\} \mid (\Gamma 2') \cap (\Gamma 1)] \\
&= \Pr[\ker T_x \cap \ker T_y \mid \operatorname{rank} T_x = d_1 \cap (\Gamma 2') \cap (\Gamma 1)] \cdot \Pr[\operatorname{rank} T_x = d_1 \mid (\Gamma 2') \cap (\Gamma 1)]. \quad (12)
\end{aligned}$$

By applying Lemma 6.2 for $(d_a, d_b, d_c, \mathcal{W}) := (d_1 + d_2, d_1 = \dim \ker T_y, d_2 = \dim \ker T_x, \ker T_y)$, the first multiplicand of (12) equals to $1 - O(1/q'^{-1})$. From $\Pr[\operatorname{rank} T_x = d_1 \mid (\Gamma 2') \cap (\Gamma 1)] \geq \Pr\left[\operatorname{rank}[t_1, \ldots, t_{d_1+d_2}] = d_1 \mid t_1, \ldots, t_{d_1+d_2} \in \mathbb{F}_{q'}^{d_1}\right]$ and Lemma 6.3, the second multiplicand of (12) is greater than or equal to $1 - O(1/q'^{-1})$. Therefore, $\Pr[(\Gamma 2)|(\Gamma 2') \cap (\Gamma 1)] \geq 1 - O(1/q'^{-1})$.

In summary, we obtain

$$\begin{aligned}
&\Pr[(\Gamma 1) \cap (\Gamma 2) \cap (\Gamma 3)] = \Pr[(\Gamma 1)] \cdot \Pr[(\Gamma 2')] \cdot \Pr[(\Gamma 2)|(\Gamma 2') \cap (\Gamma 1)] \\
&\geq \left(1 - O\left(\frac{1}{q'}\right)\right) \cdot \left(1 - \frac{n'^{m_i}}{q'^{m_i - a_i}}\right) \cdot \left(1 - O\left(\frac{1}{q'}\right)\right) = 1 - O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i - a_i}}\right\}\right).
\end{aligned}$$

6.3 Phase Error Probability

In this subsection, we show that the original message M' in the phase basis is correctly recovered with probability at least $1 - O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i - a_i'}}\right\}\right)$.

Step 1: We derive a necessary condition for correct decoding of the original message M' in phase basis. For the analysis of the phase error probability, we apply the same discussion as the bit error probability. When a phase basis state $|M'\rangle_p \in \mathcal{H}'_{\rm code}$ is the input state of sender S_i, the encoded state is written as

$$\mathcal{E}_i^{SR_i,R_i}(|M'\rangle_p) = \sum_{\bar{E}'_1\in\mathbb{F}_{q'}^{m_i\times m_i},\bar{E}'_2\in\mathbb{F}_{q'}^{a_i\times(n'-2m_i)}} \left|\widehat{U_{i,1}}\begin{bmatrix} \bar{E}'_1 & R_{i,2} & \bar{E}'_2 \\ & \mathbf{0}_{a'_i,m_i} & M' \\ & & \mathbf{0}_{a'_i,n'-2m_i}\end{bmatrix}\widehat{U_{i,2}^{V_i}}\right\rangle_p,$$

where we ignore normalizing factors and phase factors.

Since phase basis measurement and decoding operation $\mathcal{D}_i^{SR_i}$ commutes, we first apply phase basis measurement, and then decode the measurement outcome for the analysis of the phase error probability. Then, the phase basis measurement outcome Y' on the network output of T_i is written as

$$Y' = \widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} \bar{E}'_1 & R_{i,2} & \bar{E}'_2 \\ & \mathbf{0}_{a'_i,m_i} & M' \\ & & \mathbf{0}_{a'_i,n'-2m_i}\end{bmatrix}\widehat{U_{i,2}^{V_i}} + \widehat{K}_{i^c}Z,$$

where $\bar{E}'_1 \in \mathbb{F}_{q'}^{m_i\times m_i}$, $\bar{E}'_2 \in \mathbb{F}_{q'}^{a_i\times(n'-2m_i)}$ and $Z \in \mathbb{F}_{q'}^{(m-m_i)\times n'}$. By Step D1, Y' is decoded to

$$\bar{Y}' = Y'(\widehat{U_{i,2}^{V_i}})^{-1} = \widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} \bar{E}'_1 & R_{i,2} & \bar{E}'_2 \\ & \mathbf{0}_{a'_i,m_i} & M' \\ & & \mathbf{0}_{a'_i,n'-2m_i}\end{bmatrix} + \widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1}.$$

By Step D2, the measurement outcome $O_{i,2}$ is given as $O_{i,2} = \bar{Y}'^{\mathcal{B}} = \widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix} + (\widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1})^{\mathcal{B}}$, and $D_{i,2}^{R_{i2},O_{i2}}$ is found by Gaussian elimination to the right equation of (4) which is written as

$$P_{\mathcal{W}_{i,2}}D_{i,2}^{R_{i2},O_{i2}}O_{i,2} = P_{\mathcal{W}_{i,2}}D_{i,2}^{R_{i2},O_{i2}}\left(\widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix} + (\widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1})^{\mathcal{B}}\right) = \begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix}. \quad (13)$$

Thus, the correct estimate of M' is obtained when the following relation holds for $D_{i,2}^{R_{i2},O_{i2}}$ derived in (13):

$$P_{\mathcal{W}_{i2}}D_{i2}^{R_{i2},O_{i2}}\bar{Y}'^{\mathcal{C}} = P_{\mathcal{W}_{i2}}D_{i2}^{R_{i2},O_{i2}}\left(\widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} \bar{E}'_2 \\ M' \\ \mathbf{0}_{a'_i,n'-2m_i}\end{bmatrix} + (\widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1})^{\mathcal{C}}\right) = \begin{bmatrix} \bar{E}'_2 \\ M' \\ \mathbf{0}_{a'_i,n'-2m_i}\end{bmatrix}. \quad (14)$$

Step 2: In the next step, we show that the equation (14) holds with probability at least $1 - O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a'_i}}\right\}\right)$, which shows the desired statement by combining Step 1.

In the same way as Subsection 6.2, the conditions (Γ1), (Γ2) and (Γ3) of Lemma 6.1 in

the following case imply Eq. (14);

$$\mathcal{W}_1 := \mathrm{col}\left(\widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix}\right), \quad \mathcal{W}_2 := \mathrm{col}\left(\widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1}\right), \quad \mathcal{W}'_1 := \mathcal{W}_{i,2}, \quad \bar{m} := m_i,$$

$$[x_1,\ldots,x_{\bar{m}}] := \widehat{K}_{i,i}\widehat{U_{i,1}}\begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix}, \quad [y_1,\ldots,y_{\bar{m}}] := (\widehat{K}_{i^c}Z(\widehat{U_{i,2}^{V_i}})^{-1})^{\mathcal{B}},$$

$$[r_1,\ldots,r_{\bar{m}}] := \begin{bmatrix} R_{i,2} \\ \mathbf{0}_{a'_i,m_i}\end{bmatrix}, \quad A := (\widehat{K}_{i,i}\widehat{U_{i,1}})|_{\mathcal{W}'_1}, \quad (d_0,d_1,d_2) := (m_i, m_i - a'_i, \mathrm{rank}\,\widehat{K}_{i^c}Z),$$

where $\mathcal{W}_{i,2}$ is defined in Step D2 of Subsection 5.2. Also, in the same way, the conditions (Γ1), (Γ2) and (Γ3) holds with probability at least $1 - O\left(\max\left\{\frac{1}{q'}, \frac{(n')^{m_i}}{(q')^{m_i-a'_i}}\right\}\right)$.

7 Code Construction Without Free Classical Communication

We show that our code in Theorem 3.1 can be implemented without the assumption of negligible rate shared randomness. The paper [15] shows the following Proposition 7.1 by constructing a secret and correctable classical communication protocol for the classical unicast linear network. Due to the relation between the phase error and the information leakage in the bit basis [4, Lemma 5.9], we find that the dimension of leaked information is a'_i in the information transmission from the sender S_i to the receiver T_i. We apply Proposition 7.1 to the sender-receiver pair (S_i, T_i) with $c_1 := a_i$ and $c_2 := a'_i$. Therefore, the protocol of Proposition 7.1 can be implemented in our multiple-unicast network by preparing the input state of S_i in the bit basis. By attaching Proposition 7.1 to our code in the above method, we can implement our code satisfying Theorem 3.2.

▶ **Proposition 7.1** ([15, Theorem 1]). *Let q_1 be the size of the finite field which is the information unit of the network edges. We assume the inequality $c_1 + c_2 < c_0$ for the classical network where c_0 is the transmission rate from the sender S to the receiver T, c_1 is the rate of noise injection, and c_2 is the rate of information leakage. Define $q_2 := q_1^{c_0}$. Then, there exists a k-bit transmission protocol of block-length $n_1 := c_0(c_0 - c_2 + 1)k$ over $\mathbb{F}_{q_2}$ such that $P_{err} \le kc_0/q_2$ 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 leaked information E.*

The proof of Theorem 3.2 takes a similar method to the proof of [14, Theorem 3.2].

Proof of Theorem 3.2. To construct the code satisfying the conditions of Theorem 3.2, we generate the shared randomness SR_i by Proposition 7.1 and then apply the code in Section 5. To apply Proposition 7.1 in our quantum network, we prepare the input state as a bit basis state. Given a block-length n, we take $q_1 = q^\beta$ such that $\beta = \lfloor \frac{2\log_2\log_2 n}{m_i \log_2 q} \rfloor$ i.e., $q_2/(\log n)^2 = q_1^{m_i}/(\log n)^2 \to 1$, and $q' = q^\alpha$ such that $\alpha = \lfloor \frac{(m_i+2)\log_2 n}{\log_2 q} \rfloor$ i.e., $q'/n^{m_i+2} \to 1$.

First, by the protocol of Proposition 7.1 with $(c_0, c_1, c_2) := (m_i, a_i, a'_i)$, the sender S_i and the receiver T_i share the randomness SR_i. Since SR_i consists of $m_i(2m_i - a_i - a'_i + 4)$ elements of $\mathbb{F}_{q'}$, the number of bits to be shared is

$$\begin{aligned} k = \lceil m_i(2m_i - a_i - a'_i + 4)\log_2 q' \rceil &= \left\lceil m_i(2m_i - a_i - a'_i + 4)\left\lfloor \frac{(m_i+2)\log_2 n}{\log_2 q}\right\rfloor \log_2 q \right\rceil \\ &\le \lceil m_i(m_i+2)(2m_i - a_i - a'_i + 4)\log_2 n \rceil. \end{aligned}$$

The error probability is $P_{err} \le (m_i/q_1^{m_i}) \cdot \lceil m_i(m_i+2)(2m_i-a_i-a_i'+4)\log_2 n \rceil = O\left(\frac{\log_2 n}{(\log_2 n)^2}\right) \to 0$, and the block-length over $\mathbb{F}_q$ is

$$n_1 = m_i(m_i-a_i'+1)k\beta \le m_i(m_i-a_i'+1) \cdot \lceil m_i(m_i+2)(2m_i-a_i-a_i'+4)\log_2 n \rceil \cdot \left\lfloor \frac{2\log_2 \log_2 n}{m_i \log_2 q} \right\rfloor,$$

which implies $n_1/n \to 0$. Therefore, the sharing protocol is implemented with negligible rate uses of the network.

Next, we apply the code in Section 5 with the extended field of size q' and $n_2 := n - n_1$ uses of the network. The relation $n_2/n = (n-n_1)/n \to 1$ holds and therefore the field size q' satisfies $n_2 \cdot (n_2')^{m_i}/(q')^{m_i - \max\{a_i, a_i\}} \to 0$ where $n_2' := n_2/\alpha$. Thus, this code implements the code in Theorem 3.2. ◀

8 Examples of Network

In this section, we give several network examples that our code can be applied.

First, as the most trivial case, if $\operatorname{rank} K_{i,i} = m_i$ and any distinct sender-receiver pairs do not interfere with each other, i.e, $K_{i,j}$ $(i \neq j)$ are zero matrices, the network operation K is a block matrix. This is the case where each pair independently communicates. In this case, our code is implemented with the rate m_i.

8.1 Simple Network in Fig. 1

In the network in Fig. 1, the network and node operations are described as

$$K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \widehat{K} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

When we consider the transmission from S_1 to T_1, the rates of bit and phase interferences are

$$\operatorname{rank} K_{1^c} = \operatorname{rank} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = 1, \quad \operatorname{rank} \widehat{K}_{1^c} = \operatorname{rank} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0.$$

In this network, by constructing our code with $(m_1, a_1, a_1') := (2, 1, 0)$, our coding protocol transmits the state of rate $m_1 - a_1 - a_1' = 1$ asymptotically from S_1 to T_1.

8.2 Network with Bit Interference from One Sender

As a generalization of the network in Fig. 1, consider the case where the network consists of two sender-receiver pairs, and there is no bit interference from the sender S_1 to receiver T_2. The network operation of this network can be described by $\mathcal{L}(K)$ with

$$K = \begin{bmatrix} K_{1,1} & K_{1,2} \\ \mathbf{0}_{m_2,m_1} & K_{2,2} \end{bmatrix}, \quad \widehat{K} = \begin{bmatrix} (K_{1,1}^{\mathrm{T}})^{-1} & \mathbf{0}_{m_1,m_2} \\ -(K_{2,2}^{\mathrm{T}})^{-1} K_{1,2}^{\mathrm{T}} (K_{1,1}^{\mathrm{T}})^{-1} & (K_{2,2}^{\mathrm{T}})^{-1} \end{bmatrix}.$$

In this network, there is no phase interference from the sender S_2 to receiver T_1, and the other two rates $\operatorname{rank} K_{1,2}$ and $\operatorname{rank}(K_{2,2}^{\mathrm{T}})^{-1} K_{1,2}^{\mathrm{T}} (K_{1,1}^{\mathrm{T}})^{-1}$ coincide from $\operatorname{rank} K_{1,2} = \operatorname{rank} K_{1,2}^{\mathrm{T}} = \operatorname{rank}(K_{2,2}^{\mathrm{T}})^{-1} K_{1,2}^{\mathrm{T}} (K_{1,1}^{\mathrm{T}})^{-1}$. Therefore, by implementing our code with a_i, a_i' $(i = 1, 2)$ satisfying $\operatorname{rank} K_{1,2} \le a_1, a_2' < m_i$ and $a_1' = a_2 := 0$, each sender-receiver pair can transmit the states.

Moreover, we generalize the above network for arbitrary r sender-receiver pairs where the interferences are generated only from one sender S_1. In this network, the network operation is given by the unitary operator $\mathcal{L}(K)$ with K defined as follows:

$$K = \begin{bmatrix} K_{1,1} & K_{1,2} & K_{1,3} & \cdots & K_{1,r} \\ \mathbf{0}_{m_2,m_1} & K_{2,2} & \mathbf{0}_{m_2,m_3} & \cdots & \mathbf{0}_{m_2,m_r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{m_r,m_1} & \mathbf{0}_{m_r,m_2} & \mathbf{0}_{m_r,m_3} & \cdots & K_{r,r} \end{bmatrix},$$

$$\widehat{K} = \begin{bmatrix} (K_{1,1}^{\mathrm{T}})^{-1} & & \mathbf{0}_{m_1,m_2} & \mathbf{0}_{m_1,m_3} & \cdots & \mathbf{0}_{m_1,m_r} \\ -(K_{2,2}^{\mathrm{T}})^{-1}K_{1,2}^{\mathrm{T}}(K_{1,1}^{\mathrm{T}})^{-1} & & (K_{2,2}^{\mathrm{T}})^{-1} & \mathbf{0}_{m_2,m_3} & \cdots & \mathbf{0}_{m_1,m_r} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ -(K_{r,r}^{\mathrm{T}})^{-1}K_{1,r}^{\mathrm{T}}(K_{1,1}^{\mathrm{T}})^{-1} & & \mathbf{0}_{m_r,m_2} & \mathbf{0}_{m_r,m_3} & \cdots & (K_{r,r}^{\mathrm{T}})^{-1} \end{bmatrix},$$

where the ranks of $m_i \times m_i$ matrices $K_{i,i}$ are m_i, resepctively. In this network, if a_i, a'_i $(i = 1, \ldots, r)$ are set to $a_1 \geq \mathrm{rank}[K_{1,2}\ K_{1,3}\ \cdots\ K_{1,r}]$, $a'_i \geq \mathrm{rank}\, K_{1,i}$ $(i = 2, \ldots, r)$, and $a'_1 = a_2 = a_3 = \cdots = a_r \geq 0$ and the condition $a_i + a'_i < m_i$ holds, the sender S_i can send to the receiver T_i the rate $m_i - a_i - a'_i$ state asymptotically by our code.

8.3 Network with Two Way Bit Interferences

In this subsection, we consider the code implementation over the network described as follows: The size q is 3, there exists two pairs (S_1, T_1) and (S_2, T_2) in the network, S_1, S_2, T_1, T_2 are connected to three edges, and the network operation is given by $\mathcal{L}(K)$ of

$$K = \begin{bmatrix} K_{1,1} & K_{1,2} \\ K_{2,1} & K_{2,2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \widehat{K} = \begin{bmatrix} 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ -2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then, differently from the previous examples, there are bit interferences both from S_1 to T_2 and from S_2 to T_1 because $K_{1,2}$ and $K_{2,1}$ are not zero matrix.

In the above network, we construct our code for S_1 to T_1 with $(m_1, a_1, a'_1) := (3, 1, 1)$. Then, our code implements the rate $m_i - a_i - a'_i = 3 - 1 - 1 = 1$ quantum communication asymptotically from the relations

$$\mathrm{rank}\, K_{11} = \mathrm{rank}\, \widehat{K}_{11} = m_1 = 3, \quad \mathrm{rank}\, K_{1^c} = \mathrm{rank} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 1, \quad \mathrm{rank}\, \widehat{K}_{1^c} = \mathrm{rank} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = 1.$$

9 Conclusion

In this paper, we have proposed a quantum network code for the multiple-unicast network with quantum invertible linear operations. As the constraints of information rates, we assumed that the bit and phase transmission rates from S_i to T_i without interference are m_i $(m_i = \mathrm{rank}\, K_{i,i} = \mathrm{rank}\, \widehat{K}_{i,i})$, the upper bounds of the bit and phase interferences are a_i, a'_i, respectively $(\mathrm{rank}\, K_{i^c} \leq a_i, \mathrm{rank}\, \widehat{K}_{i^c} \leq a'_i)$, 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 [15].

Our code can be applied for the multiple-unicast network with the 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 communications asymptotically. This fact can be shown by integrating the methods in this paper and [14].

References

1 Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung. Network information flow. *IEEE Transactions on information theory*, 46(4):1204–1216, 2000.

2 Masahito Hayashi. Prior entanglement between senders enables perfect quantum network coding with modification. *physical review A*, 76(4):040301, 2007.

3 Masahito Hayashi. *Group Representation for Quantum Theory*. Springer, 2017.

4 Masahito Hayashi. *Group Theoretic Approach to Quantum Information*. Springer, 2017.

5 Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. Quantum network coding. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 610–621. Springer, 2007.

6 Masahito Hayashi, Masaki Owari, Go Kato, and Ning Cai. Secrecy and robustness for active attack in secure network coding. In *Proceedings on 2017 IEEE International Symposium on Information Theory (ISIT)*, pages 1172–1176, 2017.

7 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*, 54(6):2596–2603, June 2008.

8 Go Kato, Masaki Owari, and Masahito Hayashi. Single-shot secure quantum network coding for general multiple unicast network with free public communication. In *International Conference on Information Theoretic Security*, pages 166–187. Springer, 2017.

9 Hirotada Kobayashi, François Le Gall, Harumichi Nishimura, and Martin Rötteler. General scheme for perfect quantum network coding with free classical communication. In *International Colloquium on Automata, Languages, and Programming*, pages 622–633. Springer, 2009.

10 Hirotada Kobayashi, François Le Gall, Harumichi Nishimura, and Martin Rötteler. Perfect quantum network communication protocol based on classical network coding. In *Proceedings of 2010 IEEE International Symposium on Information Theory (ISIT)*, pages 2686–2690, 2010.

11 Hirotada Kobayashi, François Le Gall, Harumichi Nishimura, and Martin Rötteler. Constructing quantum network coding schemes from classical nonlinear protocols. In *Proceedings of 2011 IEEE International Symposium on Information Theory (ISIT)*, pages 109–113, 2011.

12 Debbie Leung, Jonathan Oppenheim, and Andreas Winter. Quantum network communication—the butterfly and beyond. *IEEE Transactions on Information Theory*, 56(7):3478–3490, 2010.

13 Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54(4):2614, 1996.

14 Seunghoan Song and Masahito Hayashi. Secure quantum network code without classical communication. *arXiv:1801.03306*, 2018.

15 Hongyi Yao, Danilo Silva, Sidharth Jaggi, and Michael Langberg. Network codes resilient to jamming and eavesdropping. *IEEE/ACM Transactions on Networking*, 22(6):1978–1987, 2014.