Secure Quantum Network Code without Classical Communication

Seunghoan Song and Masahito Hayashi, Fellow, IEEE

Abstract—We consider the secure quantum communication over a network with the presence of a malicious adversary who can eavesdrop and contaminate the states. The network consists of noiseless quantum channels with the unit capacity and the nodes which applies noiseless quantum operations. As the main result, when the maximum number $m_1$ of the attacked channels over the entire network uses is less than a half of the network transmission rate $m_0$ (i.e., $m_1 < m_0/2$), our code implements secret and correctable quantum communication of the rate $m_0 - 2m_1$ by using the network asymptotic number of times. Our code is universal in the sense that the code is constructed without the knowledge of the specific node operations and the network topology, but instead, every node operation is constrained to the application of an invertible matrix to the basis states. Moreover, our code requires no classical communication. Our code can be thought of as a generalization of the quantum secret sharing.

Index Terms—quantum network code, quantum error-correction, CSS code, universal construction, malicious adversary.

I. INTRODUCTION

NETWORK coding is a coding method, addressed first by Ahlswede et al. [1], that allows network nodes to manipulate information packets before forwarding. As a quantum analog, quantum network coding considers sending quantum states through a network which consists of noiseless quantum channels and nodes performing quantum operations. Since it was first discussed by Hayashi et al. [2], many other papers [3–9] have studied quantum network codes.

Classical network codes with security have been studied by two different methods. One method is to combine the network node controls and an end-to-end code. In this method, the sender and receiver know the network topology, control the node operations, and construct an end-to-end code between them. The use of the end-to-end code is important because it generates the redundancy which is necessary for the security guarantee. By this method, Cai and Yeung [10] first devised a classical network code which guarantees the secrecy of the communication. Secure classical network codes by this method have been further studied in [11, 12].

The other method for secure classical network codes is to use only an end-to-end code without controlling node operations. In this method, the node operations are not directly controlled but constrained, and an end-to-end code is constructed with the knowledge of the constraints without specific knowledge of the underlying node operations and the network topology. Although the codes [13–16] by this method do not control the node operations, which differs from the original definition of the network code in [1], these codes are also called network codes. By this method, Jaggi et al. [13] constructed a classical network code with asymptotic error correctability. In the paper [13], all node operations are not controlled but constrained to be linear operations, and the code is universal in the sense that the code is constructed independently of the network topology and the particular node operations. When the transmission rate $m_0$ of the network and the maximum rate $m_1$ of the malicious injection satisfy $m_1 < m_0$, the code in [13] achieves the correctability with the rate $m_0 - m_1$ by asymptotic $n$ uses of the network. Furthermore, Hayashi et al. [16] extended the result in [13] so that the secrecy is also guaranteed: when previously defined $m_0$, $m_1$, and the information leakage rate $m_2$ satisfy $m_1 + m_2 < m_0$, the classical network code in [16] achieves the secrecy and the correctability with the rate $m_0 - m_1 - m_2$ by asymptotic $n$ uses of the network.

On the other hand, secure quantum network codes have been designed by Owari et al. [8] and Kato et al. [9]. However, the codes in [8, 9] only keep secrecy from the malicious adversary but do not guarantee the correctness of the transmitted state if there is an attack. Moreover, this code depends on the network topology and requires classical communication.

In this paper, to resolve these problems and as a natural quantum extension of the secure classical network codes [13, 16], we present a quantum network code which is secret and correctable. Since we take a similar method to [13, 16], our code consists only of an end-to-end code without node operation controls and transmits a state by multiple $n$ uses of the quantum network. When the network transmission rate is $m_0$ and the maximum number $m_1$ of the attacked channels satisfy $m_1 < m_0/2$, our code transmits quantum information of the rate $m_0 - 2m_1$ with high fidelity by asymptotic $n$ uses of the network. Since the high fidelity of the transmitted quantum state guarantees the secrecy of the transmission [17], the secrecy of our code is guaranteed.

There are several notable properties in our code. First, our code is universal in the sense that the code construction does not depend on the network topology and the particular node operations. Instead, we place two constraints on the network topology and node operations. That is, at every node, the number of incoming edges is the same as the number of
outgoing edges, and, similarly to [13], [16] but differently from [8], [9], every node operation is the application of an invertible matrix to basis states. Then, our code is constructed by using the constraints but without any knowledge of the network topology and operations. Secondly, our code can be constructed without any classical communication. Though a negligible rate secret shared randomness is necessary for our code construction, we attach a subprotocol in order for sharing the randomness by use of the quantum network, and therefore no classical communication or no assumption of shared randomness is needed. Thirdly, our code is secure from any malicious operation on \( m_1 \) channels if \( m_1 < m_0/2 \). That is, when \( m_1 < m_0/2 \), our code is secure from the strongest eavesdropper who knows the network topology 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. Fourthly, when the network consists of parallel \( m_0 \) quantum channels, our code can be thought of as an error-tolerant quantum secret sharing [13].

The rest of this paper is organized as follows. Section II formally describes the quantum network and the attack model. Section III presents two main results of the paper, and compares our quantum network code with the quantum maximum distance separable (MDS) codes and quantum secret sharing. Based on the preliminaries in Section IV, Section V constructs our code when a negligible rate secret shared randomness is needed. Thirdly, our code is secure from the strongest eavesdropper who knows the network topology 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. Fourthly, when the network consists of parallel \( m_0 \) quantum channels, our code can be thought of as an error-tolerant quantum secret sharing [13]. Section VI evaluates the performance of our code without assuming any negligible rate secret shared randomness. Section VII derives upper bounds of the bit error probability and phase error probability, respectively. Section VIII constructs our code without assuming any negligible rate secret shared randomness. Section IX analyzes the secrecy of our code. Section X is the conclusion of the paper.

### II. 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 notations in the network and attack model are summarized in Table I, and an example of the quantum network is given in Fig. I.

#### A. Network structure and transmission

We consider the network described by a directed acyclic graph \( G_{m_0} = (V, E) \) where \( V \) is the set of nodes (vertices) and \( E \) is the set of channels (edges). The network \( G_{m_0} \) has one source node \( v_0 \), intermediate nodes \( v_1, \ldots, v_c \) (\( c := |V| - 2 \)), and one sink node \( v_{c+1} \), where the subscript represents the order of the information conversion. The source node \( v_0 \) and the sink node \( v_{c+1} \) have \( m_0 \) outgoing and incoming channels, respectively, and each intermediate node \( v_t \) has the same number \( k_t \in \{1, \ldots, m_0 \} \) of incoming and outgoing channels. For convenience, we define \( k_0 = k_{c+1} := m_0 \).

The transmission on the network \( G_{m_0} \) is described as follows. Each channel transmits information noiselessly unless the channel is attacked, and each node applies an information conversion noiselessly at any time. At time 0, the source node transmits the input information along the \( m_0 \) outgoing channels. At time \( t \in \{1, \ldots, c\} \), the node \( v_t \) applies an information conversion to the information from the \( k_t \) incoming channels, and outputs the conversion outcome along the \( k_t \) outgoing channels. At time \( c + 1 \), the sink node receives the output information from the \( m_0 \) incoming channels. The detailed constraints of the transmitted information and information conversion are described in the following subsections.

The \( m_0 \) outgoing channels of the source node are numbered from 1 to \( m_0 \), and after the conversion in the node \( v_t \), the assigned numbers are changed from \( k_t \) incoming channels to \( k_t \) outgoing channels deterministically.

#### B. Classical network

To explain our model of the quantum network, we first consider the classical network. Every single use of a channel transmits one symbol of the finite field \( \mathbb{F}_q \) of order \( q \). 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 linear operation. That is, the information conversion at each intermediate node \( v_t \), which 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 \( m_0 \times m_0 \) matrix \( K \) as

\[
y = Kx.
\]

We extend the above discussion to the case of \( n \) network uses, i.e., the input and output informations are written as \( X = [x_1, \ldots, x_n] \in \mathbb{F}_q^{m_0 \times n} \) and \( Y = [y_1, \ldots, y_n] \in \mathbb{F}_q^{m_0 \times n} \). We assume that every intermediate node \( v_t \) applies the invertible matrix \( A_t \) at \( n \) times and the matrix \( A_t \) is not changed during the \( n \) transmissions. In addition, we assume that the inputs

### TABLE I

#### SUMMARY OF NOTATIONS

| Symbol | Description |
|--------|-------------|
| \( m_0 \) | Network transmission rate without attack |
| \( m_1 \) | Maximum number of attacked channels |
| \( m_0 \) | Number of attacked channels |
| \( H \) | Unit quantum system |
| \( q \) | Dimension of \( H \) (prime power) |
| \( \tau \) | Block-length |
| \( F \) | Network structure |
| \( S \) | Strategy of malicious attack |
| \( \mathbb{F}^n, S_n \) | Network operation |
| \( C \) | Quantum network code |
| \( P_c \) | Code space |
| \( \Lambda_n = \Lambda(\mathbb{F}_q, \mathbb{F}^n, S_n) \) | Averaged protocol by code randomness |
| \( \mathcal{H}' \) | Extended unit quantum system |
| \( \alpha \) | Dimension of extension |
| \( q' \) | Dimension of \( \mathcal{H}' \) |
| \( \alpha' \) | Block-length with respect to \( \mathcal{H}' \) |
| \( \omega_p \) | Bit basis element of \( \mathcal{H} (\mathcal{H}') \) |
| \( \omega_q \) | Phase basis element of \( \mathcal{H} (\mathcal{H}') \) |
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 node operations. For the detail, see [9] Section 2.2. Even in the case where Eve chooses the noise \( Z \) dependently of the input information \( X \), the output information \( Y \) is always written in the form (3).

C. Quantum network

We consider a natural quantum extension of the above classical network. Every single use of a quantum channel transmits a quantum system \( \mathcal{H} \) of dimension \( q \) spanned by a basis \( \{ |x\rangle \mid x \in \mathbb{F}_q \} \) which is called the bit basis. In \( n \) uses of the network, the whole system to be transmitted is written as \( \mathcal{H}^{\otimes n} \) spanned by \( \{ |X\rangle \mid X \in \mathbb{F}_q^{m_a \times n} \} \). To describe the node operations, we introduce the following unitary operations: for an invertible \( m \times n \) matrix \( A \) and an invertible \( n \times n \) matrix \( B \), two unitaries \( L(A) \) and \( R(B) \) are defined as

\[
L(A) := \sum_{X \in \mathbb{F}_q^{m \times n}} |AX\rangle \langle X|, \quad R(B) := \sum_{X \in \mathbb{F}_q^{m \times n}} |XB\rangle \langle X|. 
\]

Every node \( v_t \) converts the information on the subsystem \( \mathcal{H}_{X_t} \) by applying the unitary \( L(A_t) \). If there is no attack, the operation of the whole network is the application of the unitary \( L(K) \).

Next, we introduce Eve’s attack model. Eve attacks fixed \( m_a (\leq m_1) \) channels over \( n \) uses of the network. Whenever quantum systems are transmitted over the \( m_a \) attacked channels, Eve can perform on the systems any trace preserving and completely positive (TP-CP) maps, measurements defined by positive operator-valued measure (POVM), or both. We assume that Eve’s operations can be adaptive on the previous measurement outcomes and Eve knows the network topology and all node operations.

Consider the entire network operation with malicious attacks. When Eve attacks on channels, the network structure \( \mathcal{F} \) is characterized by the network topology \( G_{m_0} = (V, E) \), node operations \( A = (A_1, \ldots, A_c) \), and the set \( E_{\text{att}} \subset E \) of attacked channels, i.e., \( \mathcal{F} := (G_{m_0}, A, E_{\text{att}}) \). Given a network structure \( \mathcal{F} \), Eve’s strategy \( S_n \) over \( n \) network uses determines the TP-CP map of the entire network operation. Therefore, we denote the entire network operation over \( n \) network uses as a TP-CP map

\[
\Gamma[\mathcal{F}^n, S_n],
\]

where \( \mathcal{F}^n \) denotes the network structure \( \mathcal{F} \) is used \( n \) times. As a special case, if \( E_{\text{att}} = \emptyset \), we have \( \Gamma[\mathcal{F}^n, S_n] = L(K) \rho L(K)^\dagger \). Moreover, we define the set \( \zeta_{m_0, m_1}^{(n)} \) of all network structures and strategies of transmission rate \( m_0 \) without attacks, at most \( m_1 \) attacked channels, and block-length \( n \) as

\[
\zeta_{m_0, m_1}^{(n)} := \{ (\mathcal{F}, S_n) \mid \mathcal{F} = (G_{m_0}, A, E_{\text{att}}), m_a = |E_{\text{att}}| \leq m_1 \}.
\]
III. MAIN RESULTS

In this section, we present the two coding theorems with and without a negligible rate secret shared randomness. For any quantum network described in Section II, our code can be constructed only with the knowledge of $m_0$, $m_1$, and $q$, but without any specific knowledge of the node operations $L(A_i)$ and the network topology $G_{m_0}$.

A. Main idea in our code construction

In order to explain the main idea of our code, we briefly introduce the classical network codes in [13], [16]. In [13], [16], node operations are restricted to be linear operations. Therefore, malicious injections on channels form a subspace in the network output, in the same way as (3). Then, the codes in [13], [16] find the subspace of injections from the network output with the help of secret shared randomness between the sender and receiver. Finally, the codes recover the original message from the information not in the subspace of injections.

By the above method of the classical network codes in [13], [16], our quantum network code is designed in the following way. Since our quantum network in Section II is defined as a natural quantum extension of the classical networks in [13], [16], we can reduce the correctness of our code to that of two classical network codes which are defined on two bases of quantum systems (in Sections VI and VII-B). In this reduction, our quantum network code is sophisticatedly defined so that the two classical network codes are similar to the codes in [13], [16]. A difficult point in our code construction is that the accessible information from the network output state is restricted since a measurement disturbs the quantum states, whereas the classical network codes [13], [16] 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 injections.

B. Main theorems

In this subsection, we present two coding theorems with and without a negligible rate secret shared randomness.

Before we state the two coding theorems, we formulate a quantum network code of block-length $n$. Let $R_s$ and $R_e$ be sets for the secret shared randomness and the private randomness parameters, respectively. Let $\mathcal{H}_{\text{code}}^{(n)}$ be a quantum system called the code space. Given $(r_s, r_e) \in R_s \times R_e$, an encoder is defined as a TP-CP map $E^{(n)}_{r_s, r_e}$ from $\mathcal{H}_{\text{code}}^{(n)}$ to $\mathcal{H}_{\text{code}}^{(n) \otimes m_0 \otimes n}$, and a decoder is defined as a TP-CP map $D^{(n)}_{r_s}(\sigma)$ from $\mathcal{H}_{\text{code}}^{(n) \otimes m_0 \otimes n}$ to $\mathcal{H}_{\text{code}}^{(n)}$. The parameter $r_s$ is assumed to be shared between the encoder and decoder but kept secret to all others, and $r_e$ is a private randomness of the encoder. Then, a quantum network code is defined as

$$C_n := \{(E^{(n)}_{r_s, r_e}(\rho), D^{(n)}_{r_s}(\sigma)) \mid (r_s, r_e) \in R_s \times R_e\}. \quad (7)$$

In order to evaluate the performance of a quantum network code $C_n$, we consider the averaged protocol $\Lambda[C_n, F^n, S_n][\rho]$:

$$\Lambda[C_n, F^n, S_n][\rho] := \frac{1}{|R_s \times R_e|} \sum_{(r_s, r_e)} D^{(n)}_{r_s} \otimes \Gamma[F^n, S_n] \circ E^{(n)}_{r_s, r_e}(\rho), \quad (8)$$

where the sum is taken in the set $R_s \times R_e$. If there is no confusion, we denote $\Lambda[C_n, F^n, S_n]$ by $\Lambda_n$. Then, the correctness and secrecy of the code is evaluated by the entanglement fidelity

$$F^{\text{ec}}(\rho_{\text{mix}}, \Lambda_n) := \langle \Phi | \Lambda_n \otimes \iota_R(\Phi) \langle \Phi | \rangle \quad (9)$$

of the completely mixed state $\rho_{\text{mix}}$ on $\mathcal{H}_{\text{code}}^{(n)}$ and the averaged protocol $\Lambda[C_n, F^n, S_n]$, where $|\Phi\rangle$ is the maximally entangled state and $\iota_R$ is the identity operator on the reference system.

Theorem III.1 (Quantum Network Code with Negligible Rate Secret Shared Randomness). Suppose that the sender and receiver can share any secret randomness of negligible size in comparison with the block-length. When $m_1 < m_0/2$, there exist a sequence $\{n_\ell\}^{\infty}_{\ell=1}$ with $n_\ell \to \infty$ as $\ell \to \infty$ and a sequence $\{C_m\}^{\infty}_{\ell=1}$ of quantum network codes of block-lengths $n_\ell$ such that

$$\lim_{\ell \to \infty} \frac{|R_s|}{n_\ell} = 0, \quad (10)$$

$$\lim_{\ell \to \infty} \frac{\log_2 \dim \mathcal{H}_{\text{code}}^{(n_\ell)}}{n_\ell} = m_0 - 2m_1. \quad (11)$$

Fig. 3. Protocol with negligible rate secret shared randomness. $S(\mathcal{H})$ denotes the set of density matrices on the Hilbert space $\mathcal{H}$. 
TABLE II

| Comparison of quantum codes for \( m_0 \) parallel channels |
|------------------------------------------------------------|
| Use of network | Quantum MDS code [19] | Our code |
| Error probability | zero-error | vanishing error |
| Range of \( m_1 \) | \( m_1 < m_0/4 \) | \( m_1 < m_0/2 \) |
| Rate | \( m_0 - 4m_1 \) | \( m_0 - 2m_1 \) |

\( m_0 \): number of parallel channels.
\( m_1 \): maximum number of corrupted channels.

\[
\lim_{\ell \to \infty} \max_{(F, S_{\ell n_1})} n_{\ell}(1 - F^2(\rho_{\text{mix}}, \Lambda_{n_\ell})) = 0, \tag{12}
\]

where \( \Lambda_{n_\ell} := \Lambda(C_{n_\ell}, F^{n_\ell}, S_{n_\ell}) \), and the maximum is taken with respect to \((F, S_{n_\ell})\) in \( \zeta_{n_\ell, m_1} \) which is defined in [6].

Notice that this code depends only on the rates \( m_0 \) and \( m_1 \), and does not depend on the detailed structure \( F \) of the network. Section [V] gives the code realizing the performance mentioned in Theorem III.1. Sections VII and VIII prove that the code in Section [V] satisfies the performance mentioned in Theorem III.1. Section [X] shows that the condition (12) implies the secrecy of the code, by using the result of [17].

Indeed, it is known that there exists a classical network code which transmits classical information securely when the number of attacked channels is less than a half of the transmission rate from the sender to the receiver [13]. Although Theorem III.1 requires secure transmission of classical information with negligible rate in order for shared randomness, the result (12) implies 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 VIII, the combination of the result [15] and Theorem III.1 yields the following theorem.

**Theorem III.2** (Quantum Network Code without Classical Communication). When \( m_1 < m_0/2 \), there exist a sequence \( \{n_\ell\}_{\ell=1}^\\infty \) with \( n_\ell \to \infty \) as \( \ell \to \infty \) and a sequence \( \{C_{n_\ell}\}_{\ell=1}^\\infty \) of quantum network codes of block-lengths \( n_\ell \) such that

\[
|R_\ell| = 0, \tag{13}
\]

\[
\frac{\log_q \dim F(n_{\ell})}{n_\ell} \to m_0 - 2m_1, \tag{14}
\]

\[
\lim_{\ell \to \infty} \max_{(F, S_{\ell n_1})} n_{\ell}(1 - F^2(\rho_{\text{mix}}, \Lambda_{n_\ell})) = 0, \tag{15}
\]

where \( \Lambda_{n_\ell} := \Lambda(C_{n_\ell}, F^{n_\ell}, S_{n_\ell}) \), and the maximum is taken with respect to \((F, S_{n_\ell})\) in \( \zeta_{n_\ell, m_1} \) which is defined in [6].

**C. Comparison our code with quantum error-correcting code and quantum secret sharing**

To compare with existing results, we consider the special case where the network consists of \( m_0 \) parallel channels. The quantum maximum distance separable (MDS) code [19] of length \( m_0 \) works in this network even for the one-shot setting which means one use of the network. When \( m_1 < m_0/4 \) and at most \( m_1 \) channels are corrupted, the code has the rate \( m_0 - 4m_1 \) and the error is zero. On the other hand, our code works with \( n \) uses of the same network, and the position of \( m_1 \) corrupted channels is assumed to be fixed over all network uses. Then, when \( m_1 < m_0/2 \) and at most \( m_1 \) channels are corrupted, our code has the rate \( m_0 - 2m_1 \) and the error goes to zero as the number \( n \) of network use goes to infinity.

On the other hand, our code has an advantage that it can be used in any networks defined in Section III without any modification of the code, whereas the quantum MDS code [19] works only in the network with \( m_0 \) parallel channels.

Our code applied for \( m_0 \) parallel channels can be thought of as an error-tolerant quantum secret sharing [18]. In error-tolerant quantum secret sharing, a sender encodes a secret to \( m_0 \) shares and distributes the shares to \( m_0 \) players, and all players send their shares to the receiver. If \( m_0 - m_1 \) players are honest, even if the other \( m_1 \) players send maliciously corrupted shares, the receiver can recover the secret and the secret is not leaked to the malicious players. Our code implements this task if the majority of players are honest, i.e., \( m_1 < m_0/2 \), which is the same for the error-tolerant quantum secret sharing scheme in [18].

**IV. PRELIMINARIES**

In this section, we prepare definitions and notations which are necessary for our code construction in Section V. In the remainder of this paper, we assume \( m_a \leq m_1 < m_0/2 \).

**A. Phase basis**

Let \( q = s^t \) for a prime number \( s \) and a positive integer \( t \). In the construction of our code, we will discuss operations on the phase basis \( \{|z\}_p \}_{z \in \mathbb{F}_q} \), which is defined as [20, Section 8.1.2]

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

for \( \omega := \exp(2\pi i/s) \) and \( tr(y) := Tr M_y \) (\( \forall y \in \mathbb{F}_q \)). Here, the matrix \( M_y \in \mathbb{F}_q^{s \times s} \) is the multiplication matrix \( x \in \mathbb{F}_q \mapsto yx \in \mathbb{F}_q \) where the finite field \( \mathbb{F}_q \) is identified with the vector space \( \mathbb{F}^s_q \).

The following Lemma IV.1 describes the application of the unitaries \( L(A) \) and \( R(A) \), defined in [4], to the phase basis states, and is proved in Appendix A.

**Lemma IV.1.** For any \( Z \in \mathbb{F}^{m \times n}_q \) and any invertible matrices \( A \in \mathbb{F}^{n \times m}_q \) and \( B \in \mathbb{F}^{n \times n}_q \), we have

\[
L(A) |Z\rangle_p = |(A^T)^{-1}Z\rangle_p, \quad R(B) |Z\rangle_p = |Z(B^T)^{-1}\rangle_p. \tag{16}
\]

For convenience, we use notation \( [A]_p := (A^{-1})^T = (A^T)^{-1} \) for any invertible matrix \( A \).

**B. Block-lengths and extended quantum system in our code**

First, we define the sequence \( \{n_\ell\}_{\ell=1}^\infty \) of block-lengths. For any positive integer \( \ell \), define four parameters

\[
\alpha_\ell := \max\{5 \log_q \ell, 1\}, \quad n_\ell := \left\lceil \frac{\ell}{\alpha_\ell} \right\rceil, \quad n_\ell' := \alpha_\ell n_\ell, \quad q' := q^{\alpha_\ell}. \tag{17}
\]
Then, we have
\[
\lim_{\ell \to \infty} \frac{n_{\ell}}{(q')^{m_0 - m_1}} = 0,
\]
because
\[
\frac{n_{\ell}}{(q')^{m_0-m_1}} \leq \frac{\ell^1+m_0}{q'(\log_q \ell - 1)(m_0-m_1)} \leq \frac{\ell^{1.5}m_0}{q'^{m_1-m_0}} \to 0.
\]
In the following, we construct our code only for any sufficiently large \(\ell\) such that the condition
\[
n_{\ell} \geq 3m_0
\]
holds, which is enough to discuss the asymptotic performance of the code.

In our code, an extended quantum system \(\mathcal{H}^e := \mathcal{H}^q \otimes_{\mathbb{F}_q} \mathcal{H}^o\) is the unit quantum system for encoding and decoding operations. We identify the system \(\mathcal{H}^e\) with the system spanned by \(|\{x\}_{b}\rangle | x \in \mathbb{F}_q'\rangle\). Then, \(n_{\ell}\) uses of the network over \(\mathcal{H}\) can be regarded as \(n_{\ell}\) uses of the network over \(\mathcal{H}^e\). For invertible matrices \(A \in \mathbb{F}_q'^{m_0 \times m_0}\) and \(B \in \mathbb{F}_q'^{m \times n'\ell - m_0}\), two unitaries \(L'(A)\) and \(R'(B)\) are defined, similarly to \(L\) and \(R\), as
\[
L'(A) := \sum_{X \in \mathbb{F}_q'^{m' \times m}} |AX\rangle_{bb} |X\rangle, \quad R'(B) := \sum_{X \in \mathbb{F}_q'^{m' \times m}} |X B\rangle_{bb} |X\rangle,
\]
and similarly to Lemma \([\text{V}1]\) for any \(Z \in \mathbb{F}_q'^{m \times n}\), we have
\[
L'(A)|Z\rangle_p = (A^*)^{-1} |Z\rangle_p, \quad R'(B)|Z\rangle_p = |Z (B^*)^{-1}\rangle_p.
\]

**C. Notations for quantum systems and states**

In this subsection, we introduce several notations for quantum systems and states. For the quantum system \(\mathcal{H}^q\otimes_{\mathbb{F}_q} \mathcal{H}' = (\mathcal{H}^e)^{m_0 \times n'_{\ell}}\), which is transmitted by \(n_{\ell}\) uses of the network, we use the following notation:
\[
(\mathcal{H}^e)^{m_0 \times n'_{\ell}} = \mathcal{H}'_A \otimes \mathcal{H}'_B \otimes \mathcal{H}'_C
\]
\[
:= (\mathcal{H}^e)^{m_0 \times m_0} \otimes (\mathcal{H}^e)^{m_0 \times n'_{\ell}} \otimes (\mathcal{H}^e)^{n'_{\ell} \times 2m_0}.
\]
Moreover, for any \(X = \{A, B, C\}\) and \((m_A, m_B, m_C) := (m_0, n_0, n_{\ell}' - 2m_0)\), we denote
\[
\mathcal{H}'_X = \mathcal{H}'_{X1} \otimes \mathcal{H}'_{X2} \otimes \mathcal{H}'_{X3} := (\mathcal{H}^e)^{m_0 \times m_0} \otimes (\mathcal{H}^e)^{m_0 \times m_0} \otimes (\mathcal{H}^e)^{n_{\ell} \times m_0},
\]

The tensor product state of \(|\phi\rangle \in \mathcal{H}'_{X1}, |\psi\rangle \in \mathcal{H}'_{X2}\), and \(|\varphi\rangle \in \mathcal{H}'_{X3}\) is denoted as
\[
|\phi\rangle |\psi\rangle |\varphi\rangle := |\phi\rangle \otimes |\psi\rangle \otimes |\varphi\rangle \in \mathcal{H}'_X.
\]

For any block matrix \([X^T, Y^T, Z^T]^T \in \mathbb{F}_q'^{m_0 \times m_0} \times \mathbb{F}_q'^{m_0 \times m_0} \times \mathbb{F}_q'^{m_0 \times m_0}\), the bit and phase basis states of \([X^T, Y^T, Z^T]^T\) are denoted by
\[
\begin{bmatrix} |X\rangle \cr |Y\rangle \cr |Z\rangle \end{bmatrix}, \quad \begin{bmatrix} |X\rangle \cr |Y\rangle \cr |Z\rangle \end{bmatrix} := \begin{bmatrix} |X\rangle \cr |Y\rangle \cr |Z\rangle \end{bmatrix}_p.
\]
The \(k \times l\) zero matrix is denoted by \(0_{k,l}\), and \(|i, j\rangle := |i\rangle \otimes |j\rangle\).

**D. CSS code in our quantum network code**

In this subsection, we define a Calderbank–Steane–Shor (CSS) code \([21–23]\) which is used in the construction of our quantum network code in Section \([\text{V}]\). A CSS code is defined from two classical codes \(C_1\) and \(C_2\) satisfying \(C_1 \supset C_2\), where a classical code is defined as the set of codewords. Therefore, in order to define the CSS code used in our code, we define the following two classical codes: by identifying the set \(\mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\) of matrices with the vector space \(\mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\), the classical codes \(C_1, C_2 \subset \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\) are defined by
\[
C_1 := \left\{ \begin{bmatrix} 0_{m_1, n_{\ell}' - 2m_0} & Y & Z \end{bmatrix} \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)} \right\},
\]
\[
C_2 := \left\{ \begin{bmatrix} X & Y \end{bmatrix} \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)} \right\},
\]
\[
X \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}, \quad Y \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}.
\]

The classical codes \(C_1, C_2\) satisfy \(C_1 \supset C_2 = \{0_{m_1, n_{\ell}' - 2m_0} \otimes \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)} \cdot Z^T \}| \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\). For any coset \(M + C_2 \in C_1 / C_2\) containing \(M \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\), define a quantum state \(|M + C_2\rangle_b \in \mathcal{H}'_C\) by
\[
|M + C_2\rangle_b := \frac{1}{\sqrt{C_2}} \sum_{J \in C_2} \begin{bmatrix} 0_{m_1, n_{\ell}' - 2m_0} & J \end{bmatrix}_b \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}.
\]

Then, the CSS code is defined as \(\text{CSS}(C_1, C_2) := \{M + C_2\}_{b} \in \mathbb{F}_q'^{m_0 \times (n_{\ell}' - 2m_0)}\). That is, any state \(|\phi\rangle \in \mathcal{H}'_{\text{code}} := \mathcal{H}'_{C2} = (\mathcal{H}^e)^{m_0 \times (n_{\ell}' - 2m_0)}\) is encoded as
\[
\begin{bmatrix} 0_{m_1, n_{\ell}' - 2m_0} & |\phi\rangle \end{bmatrix}_b \in \text{span}(\text{CSS}(C_1, C_2)) \subset \mathcal{H}'_C.
\]
The above CSS code is used in our code construction.

**E. Other Notations**

In correspondence with the notations in Section \([\text{V}C]\) for any positive integer \(k\) and any matrix \(X \in \mathbb{F}_q'^{m \times n}\), we denote
\[
X = [X^A, X^B, X^C] \in \mathbb{F}_q'^{m \times n} \times \mathbb{F}_q'^{m \times n} \times \mathbb{F}_q'^{m \times n}
\]
for any \(k \in m_0\), for any \(X = \{A, B, C\}\), we denote \(X^V = \left(\begin{bmatrix} X^A \end{bmatrix}, \begin{bmatrix} X^B \end{bmatrix}, \begin{bmatrix} X^C \end{bmatrix}\right)^T\), where \(X^A, X^B, X^C \in \mathbb{F}_q'^{m_0 \times m_0}\) and \(X^Y \in \mathbb{F}_q'^{m_0 \times (m_0 - 2m_1)}\).

\(\Pr_R[A(R)]\) denotes the probability that the random variable \(R\) satisfies the condition \(A\), and \(\Pr_R[A(R)|B(R)]\) denotes
the conditional probability that the variable $R$ satisfies the condition $A$ under the condition $B$.

V. CODE CONSTRUCTION WITH NEGligible RATE
SECRET SHARED RANDOMNESS

Now, we describe our quantum network code with the secret shared randomness of negligible rate by $\eta_t$ network uses.

In our code, the encoder and decoder are determined depending on secret randomizations. Let $R_{\ell}$ be the set of $m_0 \times m_0$ invertible matrices over $\mathbb{F}_q$, $R_1$ be the finite field $\mathbb{F}_q$, and $R_2$ be the set of $(m_0 - m_1) \times m_0$ matrices over $\mathbb{F}_q$ of rank $m_0 - m_1$. The private randomness $R_{\ell}$ of the encoder is uniformly chosen from $R_{\ell}$. The secret shared randomness $R_s := (S, R_2) := ((S_1, \ldots, S_{m_2}), (R_{2,b}, R_{2,p}))$ between the encoder and decoder is uniformly chosen from $R_s := R_1^{	imes m_0} \times R_2^2$. Note that the size of the shared secret randomness $R_s$ is less than $\log_q |\mathbb{F}_q^{	imes m_0} \times \mathbb{F}_q^{2(m_0 - m_1) \times m_0}| = \alpha_e(2m_0^2 + (4 - m_1)m_0)$ and therefore negligible with respect to $\eta_t$.

The code space is $\mathcal{H}_{code}^{(n_e)} := \mathcal{H}_{\ell}^{(n_e)} := \mathcal{H}_{\ell}^{(n_e)} \otimes \mathcal{H}_{\ell}^{(n_e)}$ which is the code space of the CSS code defined in Section V.D. The encoder $E_{R_{\ell}, R_s}^{(n_e)}$ is defined depending on $R_{\ell}$ and $R_s$ as an isometry quantum channel from $\mathcal{H}_{code}^{(n_e)}$ to $\mathcal{H}_{\ell}^{(n_e)} \otimes \mathcal{H}_{\ell}^{(n_e)}$, and the decoder $D_{R_s}^{(n_e)}$ is defined depending on $R_s$ as a TP-CP map from $\mathcal{H}_{\ell}^{(n_e)} \otimes \mathcal{H}_{\ell}^{(n_e)}$ to $\mathcal{H}_{code}^{(n_e)}$ in the following subsections, we give the details of the encoder $E_{R_{\ell}, R_s}^{(n_e)}$ and the decoder $D_{R_s}^{(n_e)}$.

A. Encoder $E_{R_{\ell}, R_s}^{(n_e)}$

For any input state $|\phi\rangle \in \mathcal{H}_{code}^{(n_e)}$, the encoder $E_{R_{\ell}, R_s}^{(n_e)}$ is described as follows.

Encode 1 (Check Bit Embedding) Encode the input state $|\phi\rangle$ by an isometry map $U_{R_2}^{(n_e)} : \mathcal{H}_{code}^{(n_e)} \rightarrow (\mathcal{H}_e^{\otimes m_0 \times n_e} = \mathcal{H}_e' \otimes \mathcal{H}_e \otimes \mathcal{H}_e')$ which defined as

$|\phi_1\rangle := U_{R_2}^{(n_e)}|\phi\rangle = \left[ \begin{array}{c} 0_{m_1, m_0} \end{array} \right] \otimes \left[ \begin{array}{c} R_{2,p} \\
R_{2,b} \\
0_{m_1, m_0} \end{array} \right] p \left[ \begin{array}{c} 0_{m_1, m_0} - 2m_0 \end{array} \right] p |\phi\rangle$.

Encode 2 (Vertical Mixing) Encode $|\phi_1\rangle$ as

$|\phi_2\rangle := L'(R_e)|\phi_1\rangle \in (\mathcal{H}_e')^{\otimes m_0 \times n_e'}$.

Encode 3 (Horizontal Mixing) From the shared randomness $S$, define matrices $Q_{2,1,i,j} := (S_{j})^i, Q_{2,2,i,j} := (S_{m_0 + j})^i$ for $1 \leq i \leq n_e - 2m_0, 1 \leq j \leq m_0$, and $Q_{3,1,i,j} := (S_{2m_0 + j})^i, Q_{3,2,i,j} := (S_{3m_0 + j})^i$ for $1 \leq i \leq m_0$ and $1 \leq j \leq m_0$, with these matrices, define a random matrix $R_{S_{1}} := \left[ \begin{array}{ccc} I_{m_0} & 0_{m_0, m_0} & 0_{m_0, n_e - 2m_0} \\
0_{n_e - 2m_0, m_0} & I_{m_0} & 0_{m_0, n_e - 2m_0} \\
0_{m_0, m_0} & 0_{m_0, m_0} & I_{m_0} \end{array} \right]$.

By the above three steps, the encoder $E_{R_{\ell}, R_s}^{(n_e)}$ is written as the isometry map $E_{R_{\ell}, R_s}^{(n_e)} : |\phi\rangle \rightarrow R'(R_{S_{1}})|\phi_2\rangle \in (\mathcal{H}_e')^{\otimes m_0 \times n_e'}$.

B. Decoder $D_{R_s}^{(n_e)}$

For any input state $|\psi\rangle \in (\mathcal{H}_e')^{\otimes m_0 \times n_e'}$, the decoder $D_{R_s}^{(n_e)}$ is described as follows.

Decide 1 (Decoding of Encode 3) The inverse of $R_{S_{1}}$ is derived from the shared randomness $S$ as

$(R_{S_{1}})^{-1} := \left[ \begin{array}{ccc} I_{m_0} & 0_{m_0, m_0} & 0_{m_0, n_e - 2m_0} \\
0_{m_0, m_0} & I_{m_0} & 0_{m_0, n_e - 2m_0} \\
0_{n_e - 2m_0, m_0} & 0_{n_e - 2m_0, m_0} & Q_{2}^{-1} \end{array} \right]$.

Decide 2 (Error Correction) Perform the bit basis measurement $|\langle O_{b, p} | O_{b} \in \mathbb{F}_{q}^{\otimes m_0 \times m_0}| \rangle$ on $H_{A}$ and the phase basis measurement $|\langle O_{p, p} | O_{p} \in \mathbb{F}_{q}^{\otimes m_0 \times m_0}| \rangle$ on $H_{B}$. The bit and phase measurement outcomes are denoted as $O_{b, p} \in \mathbb{F}_{q}^{\otimes m_0 \times m_0}$, respectively.

Next, find invertible matrices $D_{b, p} \in \mathbb{F}_{q}^{\otimes m_0 \times m_0}$ which satisfy

$P_{b}D_{b}O_{b} = \left[ \begin{array}{c} 0_{m_1, m_0} \\
R_{2,b} \\
0_{m_1, m_0} \end{array} \right],$ (20)

$P_{p}D_{p}O_{p} = \left[ \begin{array}{c} R_{2,p} \\
0_{m_1, m_0} \end{array} \right].$ (21)
Here, the maximally entangled state \( |\Phi_n\rangle = (1/\sqrt{m}) \sum_{x \in \mathbb{F}_q^m} |x, x\rangle \), for \( m := (m_0 - 2m_1)(n_1 - 2m_2) \), is written as the quantum network code con-
struction (10) in Theorem III.1. Thus, Theorem III.1 is proved.

The two terms in (24) are error probabilities with respect to the bit and phase bases, respectively, in the following sense. Define the bit error probability of \( \Lambda_{n_2} \) as the average probability that a bit basis state \(|x\rangle_b \in \mathcal{H}^{(n_2)} \) is the input state of \( \Lambda_{n_2} \) but the bit basis measurement outcome on the output state is not \( x \). Since the bit error probability is evaluated as

\[
1 - F^2_{\text{mix}}(\rho_{\text{mix}}, \Lambda_{n_2}) \leq (\text{bit error probability}) + (\text{phase error probability}).
\]

the bit error probability is equal to the first term of (24). Similarly, the second term \( \text{Tr} \Lambda_{n_2} \otimes \iota_R(\rho_{\text{mix}} | \Phi_n \rangle \langle \Phi_n | I) - P_2 \) of (24) is the phase error probability of \( \Lambda_{n_2} \) which is the average probability that a phase basis state is the input of \( \Lambda_{n_2} \) but the phase basis measurement outcome on output is incorrect. Therefore, we can bound the entanglement fidelity as

\[
1 - F^2_{\text{mix}}(\rho_{\text{mix}}, \Lambda_{n_2}) \leq \text{(bit error probability)} + \text{(phase error probability)}. \tag{25}
\]
VII. BIT AND PHASE ERROR PROBABILITIES

In this section, we prove Lemma VII.1 that is, we bound separately the bit and phase error probabilities of $A_{n_4}$.

A. Lemmas for derivation of bit and phase error probabilities

Before we prove Lemma VII.1, we prepare three lemmas. The first lemma is a variant of II.6 Lemma 5.

Lemma VII.1. Let $\mathcal{V}$ be a vector space, and $W_1$ and $W_2$ be subspaces of $\mathcal{V}$. Suppose the following two conditions (A) and (B) hold.

(A) $W_1 \cap W_2 = \{0\}$.

(B) $n_0$ vectors $v_1, v_2, \ldots, v_{n_0}$ in $W_1 \oplus W_2$ span the subspace $W_1 \oplus W_2$.

Then, the following two statements hold.

(C) Let $W_3$ be a subspace of $\mathcal{V}$ such that $\dim W_3 = \dim W_1$. For any bijective linear map $A$ from $W_1$ to $W_3$, there exists an invertible matrix $D$ on $\mathcal{V}$ such that

$$P_{W_3}D(u + v) = Au \quad (\forall i \in \{1, \ldots, n_0\}),$$

where $P_{W_3}$ is the projection to the subspace $W_3$.

(D) For any $u + v \in W_1 \oplus W_2$, any matrix $D$ satisfying (C) satisfies

$$P_{W_2}D(u + v) = Au.$$

Proof. From the condition (A), there exists an invertible matrix $D$ on $\mathcal{V}$ such that $Du = Au \in W_3$ and $Dv \in W_2$ for any $u \in W_1$ and $v \in W_2$. Then, the map $D$ satisfies (28), which implies the condition (C). Moreover, the condition (B) guarantees that the condition (C) implies the condition (D). \qed

In addition, we also prepare the following two lemmas.

Lemma VII.2. For any positive integers $n_0 \leq n_1 + n_2$, fix an $n_0$-dimensional vector space $\mathcal{V}$ over $\mathbb{F}_q$ and an $n_1$-dimensional subspace $W \subset \mathcal{V}$, and let $\mathfrak{R}$ be the set of $n_0$-dimensional subspaces of $\mathcal{V}$. When the choice of $\mathfrak{R} \in \mathfrak{R}$ follows the uniform distribution, we have

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

where the $\bigO$ notation is with respect to the prime power $q$ which goes to infinity.

Proof. The probability $\Pr[W \cap \mathfrak{R} = \{0\}]$ is the same as the probability to choose $n_2$ linearly independent vectors so that they do not intersect with $W$, which is done by the following method: choose $v_1$ from $W \setminus \mathcal{V}$, and for each $i \in \{1, \ldots, n_2 - 1\}$, choose $v_{i+1}$ from $W \setminus (W \oplus \text{span}\{v_1, \ldots, v_i\})$ by the mathematical inductions. Therefore, we have

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

Lemma VII.3. For any positive integer $n_4' > 3m_0$,

$$\max_{x \neq 0, n_1'} \Pr_S [x^T ((R^S_0)^{-1})^A = 0_{1,m_0}] \leq \left(\frac{n_4' - 2m_0}{q'}\right)^{m_0},$$

$$\max_{x \neq 0, n_1'} \Pr_S [x^T ([R^S_0]^T)^B = 0_{1,m_0}] \leq \left(\frac{n_4' - 2m_0}{q'}\right)^{m_0},$$

where the maximum is with respect to any nonzero vector $x \in \mathbb{F}_q^{n_4'}$, and the random variable $S = (S_1, \ldots, S_{m_0})$ and the matrix $R^S_0$ are defined in Section V.

The proof of Lemma VII.3 is given in Appendix C.

B. The analysis of protocol after bit basis measurement

Before we prove the upper bound (26) for the bit error probability, we analyze the protocol when any bit basis state $|M\rangle \in \mathcal{H}_{\text{code}}$ is the input state of the code. In the following, the parameter $(\mathcal{F}, S_{m_0}) \in \mathcal{C}(n_1, m_0)$ for the network operation is fixed but arbitrary.

In this case, the sender sends $E^{(n_1)}_{R_s} = \{M\} \otimes \{M\}$ over the network, and the receiver receives the state $\Gamma^{[\mathcal{F}, S_{m_0}] \otimes \mathcal{N}}\{M\}$ on $\mathcal{H}^{m_0 \times n_1} \otimes \mathcal{H}^{m_1 \times n_4'}$, where $\Gamma^{[\mathcal{F}, S_{m_0}] \otimes \mathcal{N}}$ is defined in [5]. The receiver applies the decoder $D^{(n_1)}$ and, finally, performs the bit basis measurement to the output state of the decoder.

Note that the bit basis measurement to the output state of the decoder commutes with the decoding operation $D^{(n_1)}$. That is, the process of applying the quantum decoder $D^{(n_1)}$ and then performing the bit basis measurement on $\mathcal{H}^{m_0 \times n_1}$ is equivalent to the process of performing the bit basis measurement on $\mathcal{H}^{m_0 \times n_1}$ and then applying the classical decoding which corresponds to the quantum decoder $D^{(n_1)}$. Therefore, we adopt the latter method to calculate the bit error probability.

Let $Y \in \mathbb{F}_q^{m_0 \times n_1}$ be the outcome of the bit basis measurement on $(\mathcal{H}^{m_0 \times n_1})_\mathcal{A} \otimes \mathcal{H}^\mathcal{B} \otimes \mathcal{H}^\mathcal{C}$. From Eq. 3, the matrix $Y$ is written as

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

where $\tilde{K} \in \mathbb{F}_q^{m_0 \times m_0}$ and $\tilde{W} \in \mathbb{F}_q^{m_0 \times n_4'}$ are matrices equivalent to $K \in \mathbb{F}_q^{m_0 \times m_0}$ and $W \in \mathbb{F}_q^{m_0 \times n_4'}$ in field extension, respectively, and $X' := R^s_e X R^S_0$ is defined with some matrices $E_1 \in \mathbb{F}_q^{m_1 \times m_0}$, $E_2 \in \mathbb{F}_q^{m_1 \times n_4'}$, and $E_3 \in \mathbb{F}_q^{n_4' \times (n_4' - 2m_0)}$ by

$$X' := \begin{bmatrix} 0_{m_1, m_0} \\ R^S_{2, b} \end{bmatrix}, \quad \begin{bmatrix} E_1 \\ E_2 \\ E_3 \end{bmatrix} \begin{bmatrix} M \\ 0_{m_1, n_4' - 2m_0} \end{bmatrix}.$$

By Decode 1, the matrix $Y$ is decoded as

$$Y_1 := (R^S_0)^{-1} = (\tilde{K} R_e X + \tilde{W} ((R^S_0)^{-1})^A).$$

Since the bit measurement outcome $O_1$ in Decode 2 is

$$Y_1^A = (R^S_0)^{-1} A = Y ((R^S_0)^{-1})^A,$$

the equation (20) is written as

$$P_1 D_1 \left(\tilde{K} R_e \begin{bmatrix} 0_{m_1, m_0} \\ R^S_{2, b} \end{bmatrix} + \tilde{W} ((R^S_0)^{-1})^A \right) = \begin{bmatrix} 0_{m_1, m_0} \\ R^S_{2, b} \end{bmatrix}.$$
By Decode 2, the matrix \( Y_1 \) is decoded as
\[
Y_2 := \text{Db}Y_1 = \text{Db}(\bar{K}R_eX + \bar{W}(R_s^b)^{-1}).
\]

Though the decoding succeeds if \( Y_2R^c = M \), we evaluate instead the probability that \( P_bY_2^c = [0_{m_1,n_2'-2m_2},M^T,\bar{E}_3]^T \) holds. In other words, since \( P_bY_2^c \) is written as
\[
P_bY_2^c = P_bD_bY((R_s^b)^{-1}\ell)^c
\]
we evaluate the probability of
\[
P_bD_b(\bar{K}R_e[0_{m_1,n_2'-2m_2},M^T,\bar{E}_3]+\bar{W}((R_s^b)^{-1}\ell)^c) = [0_{m_1,n_2'-2m_2},M^T,\bar{E}_3].
\]
Then, the decoding success probability is lower bounded by the probability that \( \text{(35)} \) holds.

C. Upper bound of bit error probability

In this subsection, we derive the upper bound \( \text{(36)} \) for the bit error probability in Lemma VII.4.

Apply Lemma VII.2 to the following case:
\[
\mathcal{V} := \mathbb{F}_q^{m_0}, \quad \mathcal{W}_1 := \text{Im} \bar{K}R_e|_{W_b},
\]
\[
\mathcal{W}_2 := \text{Im} \bar{W}, \quad \mathcal{W}_3 := \mathcal{W}_b, \quad A := (\bar{K}R_e|_{W_b})^{-1}
\]
\[
[u_1 + v_1, \ldots, u_m + v_m] := \bar{K}R_e[0_{m_1,m_0},R_{2,b}^T]+\bar{W}((R_s^b)^{-1}\ell)^{-1},
\]
where \( \mathcal{W}_b \) is the image of the projection \( D_b \) defined in \( \text{(20)} \).

Let \( (A') \), \( (B') \), \( (C') \), and \( (D') \) be the conditions \( (A), (B), (C), \) and \( (D) \) of Lemma VII.2 for this allocation, respectively. If the conditions \( (A') \) and \( (B') \) hold, the condition \( (C') \) implies that the equation \( \text{(34)} \) has the solution \( D_b \). Moreover, it is clear from \( (D') \) that Eq. \( \text{(35)} \) holds, which implies there is no error in the protocol. Therefore, we have the inequality
\[
\text{Pr}_{R_eR_e}[\text{(A') \cap (B')} \leq 1 - \text{(bit error probability)}.
\]
where the probability of \( (A') \) depends on the random variable \( R_e \) and that of \( (B') \) depends on random variables \( R_e \) and \( R_s = (S,R_2) \). That is, the evaluation of the bit error probability is reduced to the evaluation of the probability that both conditions \( (A') \) and \( (B') \) hold.

In the remainder of this subsection, we will prove the following lemma.

**Lemma VII.4.** The following inequalities holds:
\[
\text{Pr}_{R_e}[\text{(A')} \geq 1 - O\left(\frac{1}{q}\right),
\]
\[
\text{Pr}_{R_eR_e}[\text{(B')|(A')} \geq 1 - O\left(\max \left\{\frac{1}{q'},\left(\frac{n'_i}{q'}\right)^{m_0-m_0}\right\}\right).
\]

Then, by combining the inequality \( \text{(38)} \) with Lemma VII.2, we obtain the desired upper bound \( \text{(36)} \) for the bit error probability.

1) **Proof of lower bound** \( \text{(39)} \) for \( \text{Pr}_{R_e}[\text{(A')}]: \) Apply Lemma VII.2 to the case \( \mathcal{V} := \mathbb{F}_q^{m_0}, \mathcal{W} := \text{Im} \bar{W}, \) and \( \mathcal{R} := \text{Im} \bar{K}R_e|_{W_b}. \) In this case, we have \( n_1 = \text{rank } W \leq \text{rank } W \leq m_0 \leq m_1 \) and \( n_2 = \text{rank } \bar{K}R_e|_{W_b} = m_0 - m_1. \) Therefore, Lemma VII.2 implies the desired inequality \( \text{(39)} \).

2) **Proof of lower bound** \( \text{(40)} \) for \( \text{Pr}_{R_eR_e}[\text{(B')|(A')}]: \) We derive the lower bound \( \text{(40)} \) for \( \text{Pr}_{R_eR_e}[\text{(B')|(A')} \), by three steps. In the following, we assume the condition \( (A') \).

**Step 1:** First, we give one necessary condition for \( (B') \) and calculate the probability that the necessary condition is satisfied. The condition \( (B') \) is equivalent to
\[
\text{rank } \bar{K}R_e[0_{m_1,m_0},R_{2,b}] + \bar{W}((R_s^b)^{-1}A) = \text{rank } R_{2,b} + \text{rank } \bar{W}.
\]
On the other hand, the following inequality holds from \( \text{rank } (A + B) \leq \text{rank } A + \text{rank } B \) and \( \text{rank } (AB) \leq \min \{\text{rank } A, \text{rank } B\} \) for any matrices \( A \) and \( B \):
\[
\text{rank } \bar{K}R_e[0_{m_1,m_0},R_{2,b}] + \bar{W}((R_s^b)^{-1}A) \leq \text{rank } R_{2,b} + \text{rank } \bar{W}.
\]
Therefore, the following condition is a necessary condition for \( (B') \):
\[
\text{rank } \bar{W}((R_s^b)^{-1}A) = \text{rank } \bar{W}.
\]
The condition \( \text{(45)} \) holds if and only if \( x^T \bar{W}((R_s^b)^{-1}A) \neq 0_{m_0}, \) holds for any \( x \in \mathbb{F}_q^{m_0} \) such that \( x^T \bar{W} \neq 0_{m_1,1} \). Apply Lemma VII.3 to all \( (q')^{\text{rank } \bar{W}} \) vectors in \( \{ x^T \bar{W} \neq 0_{m_1,1} \mid x \in \mathbb{F}_q^{m_0} \} \), and then we have
\[
\text{Pr}_{R_e}[\text{(45)}] \geq 1 - (q')^{\text{rank } \bar{W}} \left(\frac{n'_i - 2m_0}{q'}\right)^{m_0},
\]
\[
\geq 1 - (q')^{m_1} \left(\frac{n'_i - 2m_0}{q'}\right)^{m_0},
\]
\[
\geq 1 - \left(\frac{n'_i}{q'}\right)^{m_0}.
\]

**Step 2:** In this step, we evaluate the conditional probability that \( (B') \) holds under the conditions \( (A') \) and \( \text{(45)} \), i.e., \( \text{Pr}_{R_eR_e}[\text{(B')|(A')} \]. Recall that the vectors \( u_k, v_k \in \mathbb{F}_q^{m_0} \) for \( k = 1, \ldots, m_0 \) are defined by \( \text{(37)} \) as
\[
[u_1, \ldots, u_m] = \bar{K}R_e[0_{m_1,m_0},R_{2,b}^T],
\]
\[
[v_1, \ldots, v_m] = \bar{W}((R_s^b)^{-1}A).
\]
Let \( m_2 := \text{rank } R_{2,b} + \text{rank } \bar{W} \). Define an injective function \( i : \{1, \ldots, m_0\} \rightarrow \{1, \ldots, m_0\} \) such that \( \text{rank } (v_{i(1)}, \ldots, v_{i(m_2)}) = \text{rank } \bar{W} \). Note that the condition \( (B') \) holds if the \( m_2 \) vectors \( u_{i(1)} + v_{i(1)}, \ldots, u_{i(m_2)} + v_{i(m_2)} \)
are linearly independent. Moreover, the condition (A') guarantees that the $m_2$ vectors $u_1(1) + v_1(1), \ldots, u_{m_2}(1) + v_{i}(m_2)$ are linearly independent if the following condition holds:

$$S_u^\perp \cap S_v^\perp = \{0_{m_2,1}\},$$

where

$$S_u^\perp := \{x \in \mathbb{F}_{q^2} : [u_i(1), \ldots, u_{i(m_2)}]x = 0_{m_0,1}\},$$

$$S_v^\perp := \{x \in \mathbb{F}_{q^2} : [v_i(1), \ldots, v_{i(m_2)}]x = 0_{m_0,1}\}.$$

Finally, combining the inequalities (48), (50), (51), and (52), we have

$$\Pr_{R_e,R_s}[B'](45) \cap (A') \geq \Pr_{R_e,R_s}[47,45] \cap (A').$$

This implies $\dim S_u^\perp + \dim S_v^\perp \geq m_2$, and therefore (47) holds only if

$$\dim S_u^\perp = \text{rank} \bar{W}.$$

We calculate the conditional probability that (47) holds by the following relation:

$$\Pr_{R_e,R_s}[\bar{W}'] = \Pr_{R_e,R_s}[47,49] \cap (A').$$

Applying Lemma VII.2 with $(n_0,W,R) := (m_2,S_v^\perp,S_u^\perp)$, we have

$$\Pr_{R_e,R_s}[47,49] \cap (A') = 1 - O\left(\frac{1}{q}\right).$$

Moreover, the following inequality is proved in Appendix D

$$\Pr_{R_e,R_s}[49] \cap (A') \geq 1 - O\left(\frac{1}{q}\right).$$

Finally, combining the inequalities (48), (50), (51), and (52), we have the inequality

$$\Pr_{R_e,R_s}[B'](45) \cap (A') \geq \Pr_{R_e,R_s}[47,45] \cap (A') \geq 1 - O\left(\frac{1}{q}\right).$$

Step 3: From the two inequalities (46) and (53), the probability $\Pr_{R_e,R_s}[B' \cap (A')]$ is evaluated as

$$\Pr_{R_e,R_s}[B'](A') = \Pr_{R_e,R_s}[B'](45)(A') \cdot \Pr_{R_e,R_s}[45](A') \geq 1 - O\left(\frac{1}{q}\right)(1 - \frac{n_i^{m_0}}{q^{m_0-m_1}}) = 1 - O\left(\max\left\{\frac{1}{q}, \frac{n_i^{m_0}}{q^{m_0-m_1}}\right\}\right).$$

Thus, we obtain the inequality (40).

D. Phase error probability

Since Lemma [VI.1] implies that coding and node operations are considered as classical linear operations even in the phase basis, we can apply similar analysis to the phase basis transmission as in Sections VII-B and VII-C.

Consider the situation that any phase basis state $|M\rangle_p \in \mathcal{H}_{\text{code}}$ is encoded and transmitted through the quantum network. In the same way as the bit basis states, we analyze the case that the receiver performs the phase basis measurement on $(H')^\otimes m_0 \times n'_1$ first, and then applies the decoding operations. After the phase basis measurement on $(H')^\otimes m_0 \times n'_1$, the measurement outcome $Y \in \mathbb{F}_{q^m} \times n'_1$ is written similarly to (32) as

$$Y := [\tilde{K}R_e]pZ[R'_1]_p + \tilde{W},$$

where $\tilde{W} \in \mathbb{F}_{q^m} \times n'_1$ is a matrix such that rank $\tilde{W} \leq m_1$ and

$$Z := \left[\begin{array}{c} \tilde{E}_1' \\ \tilde{E}_2' \\ \tilde{E}_3' \\ \tilde{E}_4' \\ M \\ 0_0 \end{array}\right] \in \mathbb{F}_{q^m} \times n'_1$$

for some matrices $\tilde{E}_1' \in \mathbb{F}_{q^m} \times m_0$, $\tilde{E}_2' \in \mathbb{F}_{q^m} \times n'_0 \times m_0$, and $\tilde{E}_4' \in \mathbb{F}_{q^m} \times (n'_0 - m_0)$. By the decoder, the matrix $Y$ is decoded as

$$Y_2 := [D_p]p[\tilde{K}R_e]pZ + \tilde{W}' [R'_0]^{-1}.$$

Consider applying Lemma VII.1 in the following case:

$$Y := [\tilde{K}R_e]pZ[R'_1]_p + \tilde{W},$$

$$W_1 := \text{Im}[\tilde{K}R_e]p|W_p\rangle,$$

$$W_2 := \text{Im}[\tilde{W}]_p, \quad W_3 := \text{Im}[W_p], \quad A = ([\tilde{K}R_e]p|W_p\rangle)^{-1}$$

where $W_3$ is the image of the projection $P$ defined in (20). Let $(A')^n, (B')^n, (C')^n,$ and $(D')^n$ be the conditions (A), (B), (C), and (D) of Lemma VII.1 for this allocation, respectively. From Lemma VII.1, if the conditions $(A')^n$ and $(B')^n$ hold, there is no error in the protocol after the phase basis measurement. That is, we have the relation

$$\Pr_{R_e,R_s}[A'(A') \cap (B')] \leq 1 - \text{phase error probability}.\ (55)$$

Moreover, by exactly the same way as in Sections VII-C and VII-C2, we have

$$\Pr_{R_e,R_s}[A'] \geq 1 - O\left(\frac{1}{q}\right),$$

$$\Pr_{R_e,R_s}[B'](A') \geq 1 - O\left(\max\left\{\frac{1}{q}, \frac{n_i^{m_0}}{q^{m_0-m_1}}\right\}\right).$$

Therefore, by combining inequalities (55), (56) and (57), we obtain the upper bound (27) of the phase error probability in Lemma VII.1.
We have provided a secure classical communication protocol for the classical network as Proposition VIII.1.

**Proposition VIII.1** ([15] Theorem 1). Consider a classical network where each channel transmits an element of the finite field \( \mathbb{F}_q \) and each node performs a linear operation. Let the inequality \( c_1 + c_2 < c_0 \) holds for the transmission rate \( c_0 \) from Alice to Bob, the rate \( c_1 \) of the noise injected by Eve, and the rate \( c_2 \) of the information leakage to Eve. For any positive integer \( \beta \), there exists a \( k \)-bit transmission protocol by \( n_2 := k\beta c_0(c_0 - c_2 + 1) \) uses of the network such that

\[
P_{\text{err}} \leq k \frac{c_0}{q^{n_2}} \quad \text{and} \quad I(M; E) = 0,
\]

where \( P_{\text{err}} \) 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 of Proposition VIII.1 as a quantum protocol, we can share the negligible rate randomness secretly as the following proof of Theorem III.2.

**Proof of Theorem III.2** Since the protocol of Proposition VIII.1 can be implemented with the quantum network by sending bit basis states instead of classical bits, the following code satisfies the conditions of Theorem III.2.

In the same way as (17), we choose \( \alpha_1 := \lceil 5 \log_q \beta \rceil \), \( n_{e,1} := \lfloor \alpha \ell \rfloor \), \( n_{e,1} := \alpha \ell \), \( n_{e,2} := q^{\alpha \ell} \) for any sufficiently large \( \ell \) such that \( \alpha_1 > 0 \) and \( n_{e,1} > 3n_0 \). For the implementation of the code given in Section V, we choose the block-length \( n_1, \ell \) and the extended field of size \( q' \), the sender and receiver need to share the secret randomness which consists of \( 4m_0 + 2m_0(m_0 - m_1) \) elements of \( \mathbb{F}_q \). Hence, using the protocol of Proposition VIII.1, the sender secretly sends \( k = \lceil (4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil \) bits to the receiver, which is called the preparation protocol.

To guarantee that the error of the preparation protocol goes to zero, we choose \( \beta := \lceil 2 \log_q \log_2 \beta \rceil \). Since \( k \) is evaluated as \( k = \lceil (4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil = \lceil (4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil \leq \lceil 5(4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil \leq \lceil 5(4m_0 + 2m_0(m_0 - m_1)) \log_2 q' \rceil \), we have \( P_{\text{err}} \leq O(\log_2 q'/\log_2 \beta) \rightarrow 0 \). Also, the preparation protocol requires \( n_{e,2} = k\beta m_0(m_0 - m_1) \) network uses. Finally, we apply the code given in Theorem III.1 with the block-length \( n_{e,1} \) and the above chosen \( \alpha_1 \) and \( q' \).

The block-length of this code is \( n_e = n_{e,1} + n_{e,2} \). Since \( n_{e,1} = \Theta(\ell) \) and

\[
n_{e,2} \leq m_0(m_0 - m_1 + 1)[5(4m_0 + 2m_0(m_0 - m_1)) \log_2 q' / 2 \log_2 \beta] = \Theta(\ell),
\]

we have \( n_{e,2}/n_e \rightarrow 0 \) and \( n_{e,1}/n_e \rightarrow 1 \). Therefore, Theorem III.1 guarantees the conditions \( 14 \) and \( 15 \), and this code do not assume any shared randomness, i.e., \( 13 \) is satisfied. Thus, this code realizes the required conditions.

**X. Conclusion**

We have presented an asymptotically secret and correctable quantum network code as a quantum extension of the classical network codes given in [14, 16]. To introduce our code, the network is constrained that the node operations are invertible linear operations to the basis states. When the transmission rate of a given network is \( m_0 \) without attack and the maximum number of attacked channels is \( m_1 \), by multiple uses of the network, our code achieves the rate \( m_0 - 2m_1 \) asymptotically without any classical communication. Our code needs a negligible rate secret shared randomness but it is implemented by attaching a known secure classical network communication protocol [15] to 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 code protocol. The correctability is derived analogously to the classical network codes [13, 16] but by evaluating the bit and phase error probabilities separately.

One remaining task is to show whether our code rate \( m_0 - 2m_1 \) is optimal or not. As a first step to discuss this problem, we may consider the quantum capacity when the network topology, node operations, and \( m_1 \) corrupted channels are fixed. This problem is remained as a future study.

**Acknowledgments**

SS is grateful to Yuuya Yoshida for helpful discussions and comments. 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 Advance-
APPENDIX A

PROOF OF LEMMA [V.I]

Proof of Lemma [V.I] For any \( x = (x_1, ..., x_m), y = (y_1, ..., y_m) \in \mathbb{F}_q^m \), define an inner product
\[
(x, y) := \sum_{i=1}^m x_i y_i = \sum_{i=1}^m x_i y_i,
\]
where \( \text{tr} \) is defined in Section [V.A]. Let \( T \) be a \( m \times m \) matrix on \( \mathbb{F}_q \). If \( x, y \) are considered as column vectors, it holds that \( (Tx, y) = (x, T^T y) \). On the other hand, if \( x, y \) are considered as row vectors, it holds that \( (xT, y) = (x, y T^T) \).

First, we show \( L(A) | Z \rangle_p = |(A^{-1})^T Z \rangle_p \) by considering \( \mathbb{F}_q^n \) as a column vector space. For \( L(A) := \sum_{x \in \mathbb{F}_q} |Ax \rangle \rangle \) and \( z \in \mathbb{F}_q^n \), we have
\[
L(A)(z)_p = \frac{1}{\sqrt{|q|^m}} \sum_{x \in \mathbb{F}_q} \omega^{-x \cdot z} |Ax \rangle b
\]
where \( \omega \) is defined in (59) for the proofs.

Since \( L(A) = (L(A))^{\otimes n} \), we have \( L(A) | Z \rangle_p = |(A^{-1})^T Z \rangle_p \).

Next, consider \( \mathbb{F}_q^n \) as an \( n \)-dimensional row vector space over \( \mathbb{F}_q \). For \( R(B) := \sum_{x \in \mathbb{F}_q} |xB \rangle b(x) \) and \( z \in \mathbb{F}_q^n \), we have
\[
R(B)(z)_p = \frac{1}{\sqrt{|q|^m}} \sum_{x \in \mathbb{F}_q} \omega^{-x \cdot z} |xB \rangle b
\]
where \( \omega \) is defined in (60) for the proofs.

Since \( R(B) = (R(B))^{\otimes m} \), we have \( R(B) | Z \rangle_p = |(B^{-1})^T \rangle_p \).

APPENDIX B

PROOF OF (23)

In this section, we show Lemmas [B.1] and [B.2] which shows the relationship between two maximally entangled states and projections \( P_1, P_2 \) defined by the bit and the phase bases.

Define the following maximally entangled states with respect to the bit and phase bases:
\[
|\Phi_1 \rangle := \frac{1}{\sqrt{q}} \sum_{i \in \mathbb{F}_q} |i, i \rangle_b, \quad |\Phi_2 \rangle := \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{F}_q} |i, z \rangle_b.
\]
We use the inner product \((\cdot, \cdot)\) defined in (59) for the proofs.

Lemma B.1. \( |\Phi_1 \rangle = |\Phi_2 \rangle \).

Proof. The lemma is proved as follows:
\[
|\Phi_2 \rangle = \frac{1}{\sqrt{q^m}} \left( \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \omega^{x \cdot (z, j)} |y \rangle b \right) \left( \sum_{l \in \mathbb{F}_q} \sum_{m \in \mathbb{F}_q} \omega^{y \cdot (l, j)} |l \rangle b \right)
\]
\[
= \frac{1}{\sqrt{q^m}} \left( \sum_{y \in \mathbb{F}_q} \omega^{x \cdot (z, j)} |y \rangle b \right) \left( \sum_{l \in \mathbb{F}_q} \sum_{m \in \mathbb{F}_q} \omega^{y \cdot (l, j)} |l \rangle b \right)
\]
\[
= \frac{1}{\sqrt{q^m}} \left( \sum_{y \in \mathbb{F}_q} \sum_{l \in \mathbb{F}_q} \omega^{x \cdot (z, j)} |y \rangle b \right) \left( \sum_{l \in \mathbb{F}_q} \sum_{m \in \mathbb{F}_q} \omega^{y \cdot (l, j)} |l \rangle b \right)
\]
\[
= |\Phi_1 \rangle,
\]
where the first equality in (60) holds because
\[
\sum_{z \in \mathbb{F}_q} \omega^{-x \cdot (j, l)} = \begin{cases} 0 & \text{if } j \neq l, \\ 1 & \text{otherwise.} \end{cases}
\]

From the above lemma, we denote \( |\Phi \rangle := |\Phi_1 \rangle = |\Phi_2 \rangle \).

Eq. (23) is proved by the following lemma.

Lemma B.2. \( P_1 P_2 = P_2 P_1 = |\Phi \rangle \langle \Phi | \).

Proof. The lemma is proved as follows:
\[
P_1 P_2 = \sum_{i, z \in \mathbb{F}_q} \langle i, i | z, z \rangle_p |i, i \rangle_b \langle z, z | b(i, i)_{P_1} |z, z \rangle \]
\[
= \sum_{i, z \in \mathbb{F}_q} \sum_{j \in \mathbb{F}_q} \sum_{l \in \mathbb{F}_q} \omega^{x \cdot (z, i)} \omega^{y \cdot (i, j)} |i, i \rangle b(j, l)
\]
\[
= \sum_{j, l \in \mathbb{F}_q} |i, i \rangle b(j, l)
\]
\[
= \frac{1}{q^m} \sum_{j, l \in \mathbb{F}_q} |i, i \rangle b(j, l) = |\Phi \rangle \langle \Phi |.
\]

APPENDIX C

PROOF OF LEMMA VII.3

We use the following lemma [13] Claim 5] to prove Lemma VII.3

Lemma C.1 ( [13] Claim 5]). Suppose independent \( m \) random variables \( S_1, ..., S_m \in \mathbb{F}_q \) are uniformly chosen in \( \mathbb{F}_q \) and define the random matrix \( Q \in \mathbb{F}_q^{n \times m} \) as \( Q_{i,j} := (S_j)^i \). For any row vectors \( x \in \mathbb{F}_q^n \) and \( y \in \mathbb{F}_q^m \) \((l \geq m)\), we have
\[
Pr_{S} [x = yQ] \leq \left( \frac{1}{q} \right)^m.
\]

Now, we prove Lemma VII.3

Proof of Lemma VII.3 Let \( x = (x^A, x^B, x^C) \in \mathbb{F}_q^{m_1} \times \mathbb{F}_q^{m_2} \times \mathbb{F}_q^{n_1 - 2m_1} \) be a nonzero row vector. From the definition of \( R_{1,1}^1 \), we have the relations
\[
x((R_{1,1}^1)^{-1} A) = x^A - x^B (Q_3^T + Q_4) - x^C Q_1,
\]
\[
x((R_{1,1}^1)^{-1} B) = x^B + x^A (Q_4 + Q_3 + Q_1) + x^C Q_2.
\]

The inequality (61) is proved as follows. The relation (62) implies that the condition \( x((R_{1,1}^1)^{-1} A) = 0_{1, m_1} \) holds
in the following cases. In each case, the probability for $x((R_S^q)^{-1}) = 0_{1,m_0}$ is calculated by Lemma A.1 as follows.

1) If $x^C \neq 0_{1,n'_q-2m_0}$, the inequality (61) for $Q := Q_1$ implies

$$\Pr_{S}[x^A - x^B (Q_3^q + Q_4)] = x^C Q_2 \leq \left( \frac{n'_q - 2m_0}{q} \right)^{m_0}.$$  (64)

2) If $x^B \neq 0_{1,m_0}$ and $x^C = 0_{1,n'_q-2m_0}$, the inequality (61) for $Q := Q_2$ implies

$$\Pr_{S}[x^A - x^B Q_3^q + x^B Q_4] \leq \left( \frac{m_0}{q} \right)^{m_0}.$$  (65)

Therefore, from the inequality (61) in Lemma VII.3, we obtain the inequality (65) for $Q := Q_2$.

Since $n'_q > 3m_0$ holds from (19), we have

$$\left( \frac{m_0}{q} \right)^{m_0} \leq \left( \frac{n'_q - 2m_0}{q} \right)^{m_0}.$$  (64)

Therefore, we obtain the inequality (65) in Lemma VII.3.

Next, we show the inequality (61) as follows. The relation (65) implies that the condition $x((R_S^q)^{-1}) = 0_{1,m_0}$ holds in the following cases. In each case, the probability for $x((R_S^q)^{-1}) = 0_{1,m_0}$ is calculated by Lemma A.1 as follows.

1) If $x^C \neq 0_{1,n'_q-2m_0}$, the inequality (61) for $Q := Q_2$ implies

$$\Pr_{S}[x^B + x^A (Q_3^q + Q_4)] = x^C Q_2 \leq \left( \frac{n'_q - 2m_0}{q} \right)^{m_0}.$$  (66)

2) If $x^A \neq 0_{1,m_0}$, $x^C = 0_{1,n'_q-2m_0}$, the probability $Q := Q_3$ implies

$$\Pr_{S}[x^B + x^A (Q_3^q + Q_4)] = x^C Q_2 \leq \left( \frac{m_0}{q} \right)^{m_0}.$$  (67)

3) If $x^A = 0_{1,m_0}$, $x^B \neq 0_{1,m_0}$, and $x^C = 0_{1,n'_q-2m_0}$, the probability $Q := Q_3$ is zero.

Therefore, from the inequality (64) in Lemma VII.3, we obtain the inequality (61) in Lemma VII.3.

**APPENDIX D**

**PROOF OF (65)**

From dim $S_a^q = m_2 = \text{rank}[u_1, \ldots, u_{m_2}]$, we have

$$\Pr[\text{dim } S_a^q = \text{rank } W] = \Pr[\text{rank } [u_1, \ldots, u_{m_2}] = \text{rank } R_{2,b}].$$

Since $R_{2,b} = [u_1, \ldots, u_{m_2}]$ is a random matrix with rank $R_{2,b} = m_0 - m_1$, this probability is equivalent to

$$\Pr[\text{rank } [u_1, \ldots, u_{m_2}] = m_0 - m_1] \geq \Pr[\text{rank } [u_1, \ldots, u_{m_0}] = m_0 - m_1 | v_k \in \mathbb{F}_{q^{m_0-m_1}}].$$

Therefore, it holds that

$$\Pr[\text{rank } [u_1, \ldots, u_{m_0}] = m_0 - m_1 | v_k \in \mathbb{F}_{q^{m_0-m_1}}].$$
[17] B. Schumacher, “Sending quantum entanglement through noisy channels,” *Phys. Rev. A*, 54, 2614–2628 (1996).
[18] 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.
[19] E.M. Rains, “Nonbinary quantum codes,” IEEE Transactions Information Theory, vol. 45, no. 1827–1832, 1999.
[20] M. Hayashi, Group Representation for Quantum Theory. Cham, Switzerland: Springer, 2017.
[21] A. M. Steane, “Error correcting codes in quantum theory,” *Phys. Rev. Lett.*, vol. 77, pp. 793-767, July 1996.
[22] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098-1105, Aug. 1996.
[23] A. M. Steane, “Multiple particle interference and quantum error correction,” *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551-2577, Nov. 1996.