Secure Quantum Network Code

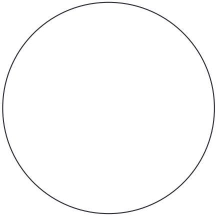
321701139 Song Seunghoan

アドバイザー**:** 林 正人 教授

修士論文発表会

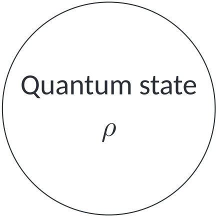
NAGOYA UNIVERSITY

Framework of Quantum Information Theory



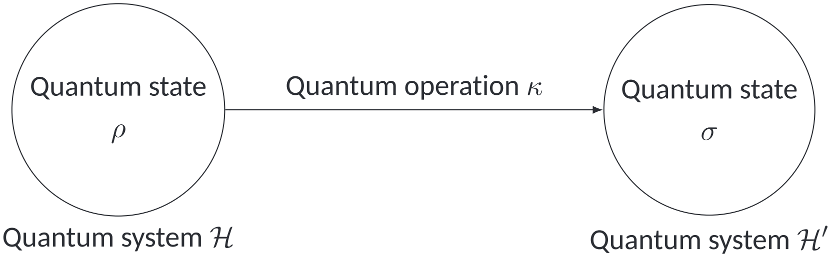
Quantum system $\mathcal{H}$

Framework of Quantum Information Theory

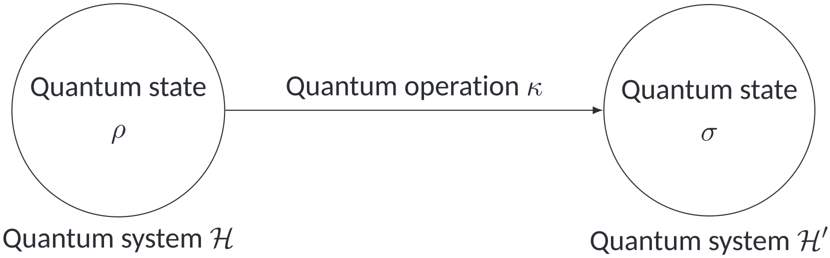


Quantum system $\mathcal{H}$

Framework of Quantum Information Theory



Framework of Quantum Information Theory



Quantum System and Quantum States

Postulate 1. Quantum system

Any quantum system is described by a *finite-dimensional Hilbert space* $\mathcal{H}$.

- Finite-dimensional Hilbert space: a complex vector space with the standard inner product $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$.
- The composite system of quantum systems is given by tensor products of the quantum systems.

Postulate 2. Quantum state

Any quantum state on a quantum system $\mathcal{H}$ is described by a *density matrix* on $\mathcal{H}$.

- A matrix ρ on $\mathcal{H}$ is called a *density matrix* on $\mathcal{H}$ if

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

- If a density matrix is a rank-one matrix $|x\rangle\langle x|$, it corresponds to the unit vector $|x\rangle \in \mathcal{H}_d$.
$\Longrightarrow$ the quantum state is represented by a unit vector.

Quantum Operations and Quantum Measurements

Postulate 3. Quantum Operation

Any quantum operation is described by a trace-preserving completely positive (TP-CP) linear map.

- *Positive map* is a map from positive semidefinite matrices to positive semidefinite matrices.
- A map κ is a *completely positive* if $\kappa \otimes \iota_{\mathbb{C}_n}$ is a positive map for all $n \in \mathbb{N}$.
  - $\iota_{\mathbb{C}_n}$ is identity map on $\mathbb{C}^n$.

Postulate 4. Measurement

Any measurement on a quantum system $\mathcal{H}$ is described by a positive operator-valued measurement (POVM).

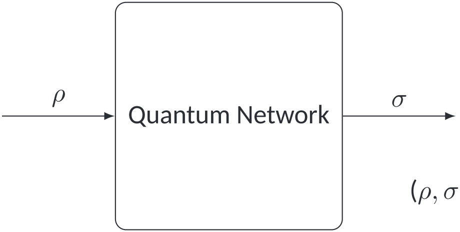
- A set of matrices $\mathbf{M}_\Omega := \{M_\omega : \omega \in \Omega\}$ is called a *POVM* on $\mathcal{H}$ if

$$\sum_\omega M_\omega = I_\mathcal{H} \quad \text{and} \quad M_\omega \geq 0 \quad \text{for any } \omega \in \Omega.$$

- The probability for obtaining ω is Tr ρM_ω. (c.f. $\sum_\omega$ Tr $\rho M_\omega = 1$)

Quantum Network Communication

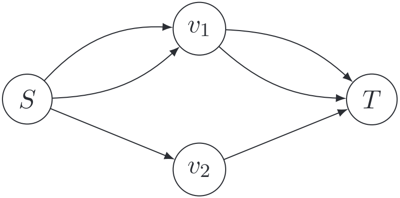
Quantum network communication is the transmission of quantum states over quantum network.



(ρ, σ: Quantum states)

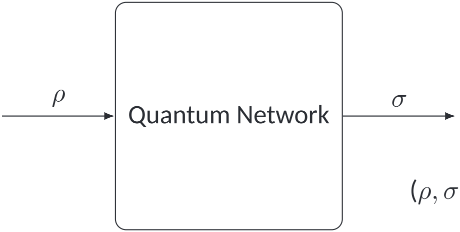
Quantum network consists of

- noiseless quantum channels
- sender/receiver nodes
- intermediate nodes
  - apply node operations (TP-CP maps).



Quantum Network Communication

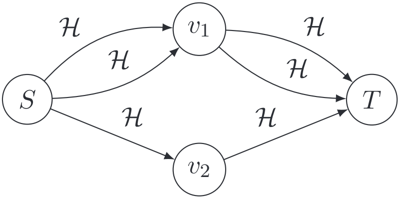
Quantum network communication is the transmission of quantum states over quantum network.



(ρ, σ: Quantum states)

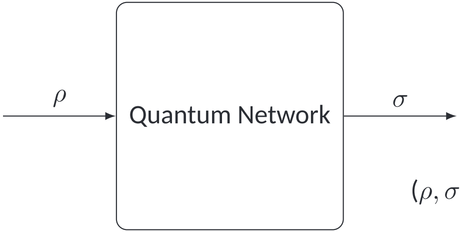
Quantum network consists of

- noiseless quantum channels
- sender/receiver nodes
- intermediate nodes
  - apply node operations (TP-CP maps).



Quantum Network Communication

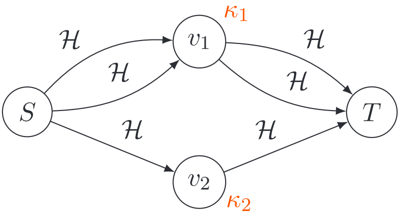
Quantum network communication is the transmission of quantum states over quantum network.



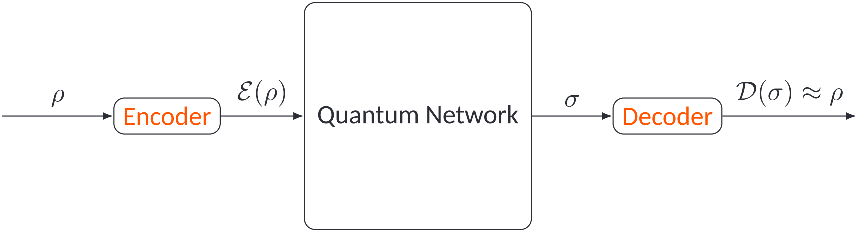
(ρ, σ: Quantum states)

Quantum network consists of

- noiseless quantum channels
- sender/receiver nodes
- intermediate nodes
  - apply node operations (TP-CP maps).



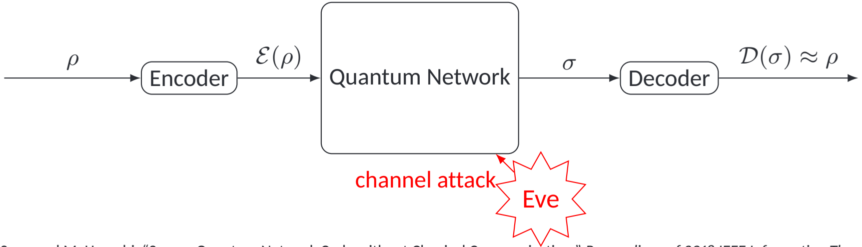
Quantum Network Code



- Network code: a pair of encoder $\mathcal{E}$ and decoder $\mathcal{D}$.

Main Results

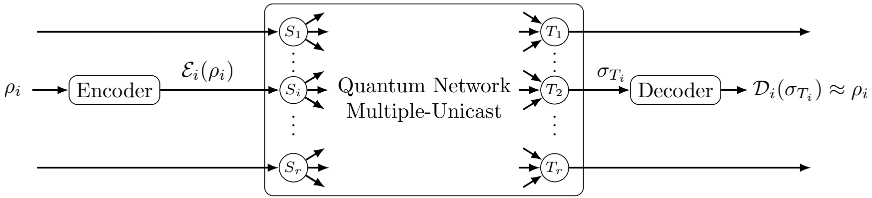
1. Secure Quantum Network Code



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

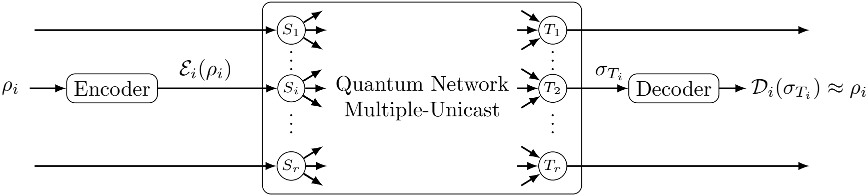
---

2. Quantum Network Code for Multiple-Unicast Network

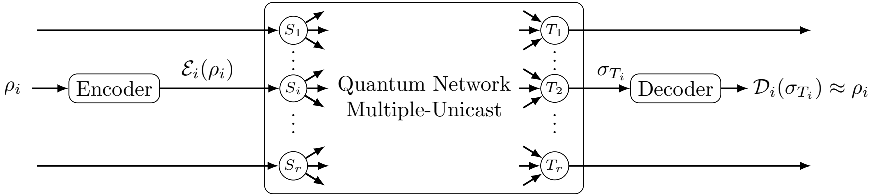


S. Song and M. Hayashi, "Quantum Network Code for Multiple-Unicast Network with Quantum Invertible Linear Operations," *Proceedings of 13th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2018)*, vol. 111, pp 10:1–10:20, 2018.

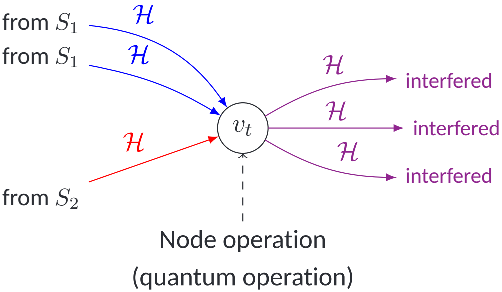
Quantum Network Code for Multiple-Unicast Network



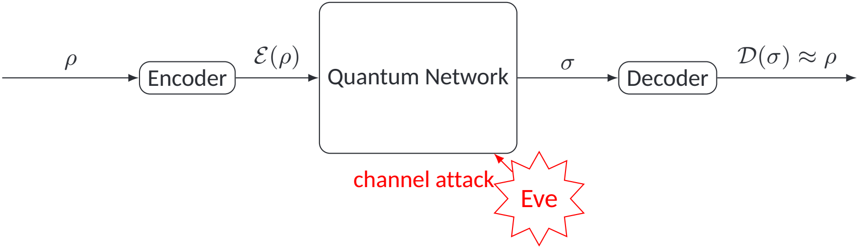
Quantum Network Code for Multiple-Unicast Network



Problem: coping with interference.



Secure Quantum Network Code



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

Existing Studies of Secure Network Code

Secure classical network code

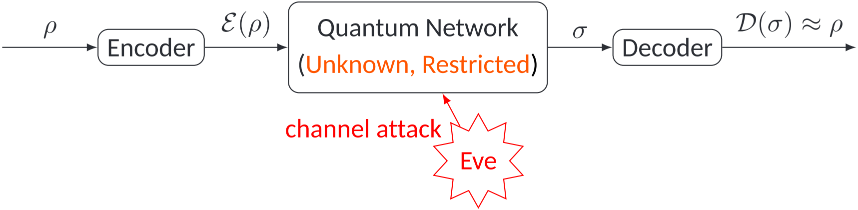
	Secrecy	Correct.	Controlled Op.	Asymp.	Universality
Cai and Yeung, 2002	✓		✓		
Matsumoto et al. , 2017	✓			✓	✓
Hayashi et al., 2017	✓	✓		✓	✓

Secure quantum network code

	Secrecy	Correct.	Controlled Op.	Asymp.	Universality
Kato et al., 2017	✓		✓		
Song and Hayashi, 2018	✓	✓		✓	✓

- *Secrecy* in that no information is leaked.
- *Correctability* in that original message is recovered from attack.
- *Controlled Operation* in that the code controls intermediate node operations.
- *Asymptotic* in that the code uses the network asymptotic number of times.
- *Universality* in that the code does not depend on the network structure.

Overview of Result: Secure Quantum Network Code



- Channel attack: measurements and/or TP-CP maps on attacking channels.
- Node operation: restricted to *quantum invertible linear operations*.

Main Theorem

Definitions of information quantities

m_0	The number of transmitted unit quantum systems $\mathcal{H}$ without attack
m_1	The maximum number of attacked channels

Main Theorem: Secure quantum network code

When $m_1 < m_0/2$, there exists a sequence of quantum codes $\kappa^{(n)}$ such that

- transmission rate is

$$\lim_{n\to\infty} \frac{1}{n} \log_q \dim \mathcal{H}_{\mathrm{code}}^{(n)} = m_0 - 2m_1,$$

- secrecy and correctability holds, i.e.,

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

Idea for code construction

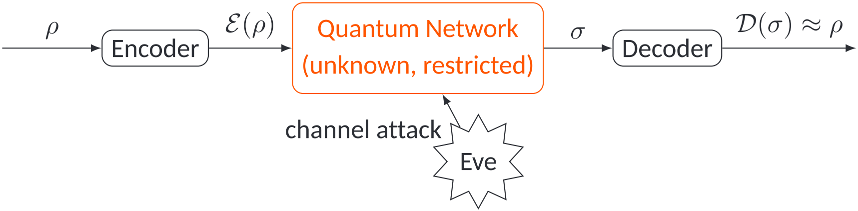
Idea for code construction

1. Node operations are restricted in the quantum network.
2. Two classical network is defined from quantum network.
   - The bit classical network.
   - The phase classical network.
3. If two classical network communications are correct, quantum network communication is also correct.
4. Quantum network code defined from classical network code.
5. Secrecy follows from correctability of quantum network code.

In the following, I will explain

1. Network Operation: Quantum Invertible Linear Operation.
2. Reduction to Classical Network Communication.
3. Quantum Network Code defined from Classical Network Code.

Network Operation:
Quantum Invertible Linear Operation



Network Transmission

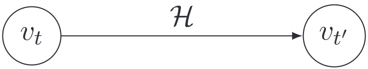
Unit quantum system $\mathcal{H}$ is a q-dimensional Hilbert space. (q: prime power)

- Bit basis $\{|x\rangle_b\}_{x \in \mathbb{F}_q}$, Phase basis $\{|x\rangle_p\}_{x \in \mathbb{F}_q}$.

$$|z\rangle_p := \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{F}_q} \omega^{xz} |x\rangle_b, \quad \omega := \exp\left(\frac{2\pi i}{q}\right). \tag{1}$$

By n uses of the network, $\mathcal{H}^{\otimes m_0 \times n}$ is transmitted.

- Bit basis $\{|X\rangle_b\}_{X \in \mathbb{F}_q^{m_0 \times n}}$, Phase basis $\{|X\rangle_p\}_{X \in \mathbb{F}_q^{m_0 \times n}}$.



Network Transmission

Unit quantum system $\mathcal{H}$ is a q-dimensional Hilbert space. (q: prime power)

- Bit basis $\{|x\rangle_b\}_{x\in\mathbb{F}_q}$, Phase basis $\{|x\rangle_p\}_{x\in\mathbb{F}_q}$.

$$|z\rangle_p := \frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\omega^{xz}|x\rangle_b, \quad \omega := \exp\left(\frac{2\pi i}{q}\right). \tag{1}$$

By n uses of the network, $\mathcal{H}^{\otimes m_0\times n}$ is transmitted.

- Bit basis $\{|X\rangle_b\}_{X\in\mathbb{F}_q^{m_0\times n}}$, Phase basis $\{|X\rangle_p\}_{X\in\mathbb{F}_q^{m_0\times n}}$.

$$\mathcal{H}^{\otimes m_0} \longrightarrow \boxed{\text{Quantum Network}} \longrightarrow \mathcal{H}^{\otimes m_0}$$

Network Transmission

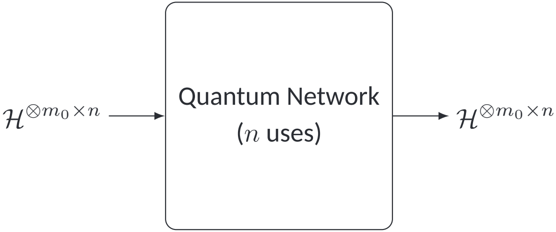
Unit quantum system $\mathcal{H}$ is a q-dimensional Hilbert space. (q: prime power)

- Bit basis $\{|x\rangle_b\}_{x\in\mathbb{F}_q}$, Phase basis $\{|x\rangle_p\}_{x\in\mathbb{F}_q}$.

$$|z\rangle_p := \frac{1}{\sqrt{q}}\sum_{x\in\mathbb{F}_q}\omega^{xz}|x\rangle_b, \quad \omega := \exp\left(\frac{2\pi i}{q}\right). \tag{1}$$

By n uses of the network, $\mathcal{H}^{\otimes m_0\times n}$ is transmitted.

- Bit basis $\{|X\rangle_b\}_{X\in\mathbb{F}_q^{m_0\times n}}$, Phase basis $\{|X\rangle_p\}_{X\in\mathbb{F}_q^{m_0\times n}}$.



Node Operation: Quantum Invertible Linear Operation

Restriction on node operations

- Every intermediate node v_t applies a unitary operation

$$\mathcal{L}(A_t) := \sum_{X \in \mathbb{F}_q^{m_0 \times n}} |A_t X\rangle_{bb}\langle X| \tag{2}$$

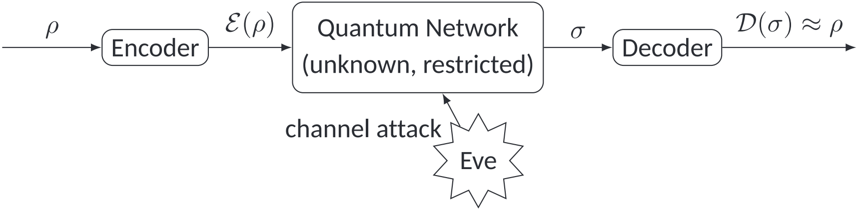
$$(A_t \in \mathbb{F}_q^{m_0 \times m_0} \text{ is an invertible matrix}).$$

The operation $\mathcal{L}(A_t)$ satisfies

$$\mathcal{L}(A_t)|X\rangle_b = |A_t X\rangle_b, \quad \mathcal{L}(A_t)|X\rangle_p = |(A_t^\top)^{-1} X\rangle_p. \tag{3}$$

- Entire network operation is $\mathcal{L}(K) := \mathcal{L}(A_c \cdots A_1) = \mathcal{L}(A_c) \cdots \mathcal{L}(A_1)$.

Reduction to Classical Network Communication



Reduction to Classical Network Communication

- Reduction to classical correctability from quantum correctability.

For any $M \in \mathbb{F}_q^{(m_0-2m_1)\times(n-2\alpha_n m_0)}$,

$$|M\rangle_b \longrightarrow \boxed{\text{Encoder}} \rightarrow \boxed{\text{Network}} \rightarrow \boxed{\text{Decoder}} \xrightarrow{\text{Bit basis measurement}} M$$

and

$$|M\rangle_p \longrightarrow \boxed{\text{Encoder}} \rightarrow \boxed{\text{Network}} \rightarrow \boxed{\text{Decoder}} \xrightarrow{\text{Phase basis measurement}} M$$

$$\Downarrow$$

Quantum network communication is correct.

Reduction to Classical Network Communication

- Reduction to classical correctability from quantum correctability.

For any $\rho \in \mathcal{S}(\mathcal{H}_{\mathrm{code}}^{(n)})$,

$$\underbrace{n(1 - F_e^2(\rho, \kappa^{(n)}))}_{\text{Correctability}} \leq n \cdot (\Pr[\text{bit error}] + \Pr[\text{phase error}]).$$

Reduction to Classical Network Communication

- Reduction to classical correctability from quantum correctability.

For any $M \in \mathbb{F}_q^{(m_0-2m_1)\times(n-2\alpha_n m_0)}$,

$$|M\rangle_b \longrightarrow \boxed{\text{Encoder}} \to \boxed{\text{Network}} \to \boxed{\text{Decoder}} \xrightarrow{\text{Bit basis measurement}} M$$

and

$$|M\rangle_p \longrightarrow \boxed{\text{Encoder}} \to \boxed{\text{Network}} \to \boxed{\text{Decoder}} \xrightarrow{\text{Phase basis measurement}} M$$

- Our quantum network is reduced to classical networks when bit or phase basis state is sent.

$$\mathcal{L}(A_t)|X\rangle_b = |A_t X\rangle_b, \quad \mathcal{L}(A_t)|X\rangle_p = |(A_t^\top)^{-1} X\rangle_p. \tag{4}$$

Reduction to Classical Network Communication

- Reduction to classical correctability from quantum correctability.

For any $M \in \mathbb{F}_q^{(m_0-2m_1)\times(n-2\alpha_n m_0)}$,

$$|M\rangle_b \longrightarrow \boxed{\text{Encoder}} \rightarrow \boxed{\text{Network}} \rightarrow \boxed{\text{Decoder}} \xrightarrow{\text{Bit basis measurement}} M$$

and

$$|M\rangle_p \longrightarrow \boxed{\text{Encoder}} \rightarrow \boxed{\text{Network}} \rightarrow \boxed{\text{Decoder}} \xrightarrow{\text{Phase basis measurement}} M$$

- Our quantum network is reduced to classical networks when bit or phase basis state is sent.

- Define quantum network code from classical network code.
  - Difficulty: One quantum network code should correct two classical network transmissions.

Reduction to Classical Network Communication

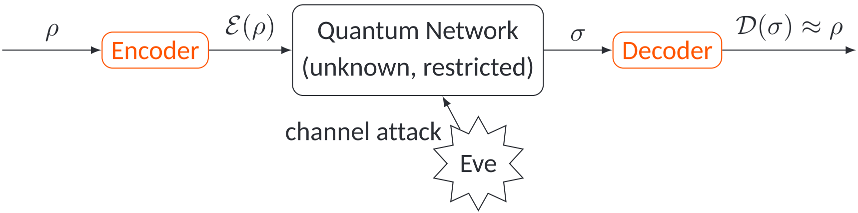
For any $\rho \in \mathcal{S}(\mathcal{H}_{\text{code}}^{(n)})$,

$$n(1 - F_e^2(\rho, \kappa^{(n)})) \leq n \cdot (\Pr[\text{bit error}] + \Pr[\text{phase error}]) \tag{4}$$

$$\leq n \cdot O\left(\max\left\{\frac{1}{q^{\alpha_n}}, \frac{(n/\alpha_n)^{m_0}}{q^{\alpha_n(m_0-m_1)}}\right\}\right) \to 0. \tag{5}$$

Quantum Network Code

defined from Classical Network Code



The encoder and decoder depends only on m_0 and m_1.

Classical Network Code (Modified from Hayashi et al.)

Encoding (Orange: Shared Randomness // $\mathrm{rank}\, R_{2,b} = m_0 - m_1$)

$$M \in \mathbb{F}_q^{(m_0-m_1)\times(n-m_0)} \longrightarrow R_0 \left[\begin{array}{c:c} \mathbf{0} & \mathbf{0} \\ \hdashline R_{2,b} & M \end{array}\right] R_1^V =: X \in \mathbb{F}_q^{m_0 \times n}$$

Decoding

$$Y = KX + Z \qquad \Big(K\text{: Network Operation, } Z\text{: Malicious Attack} \Big)$$

$$\longrightarrow Y' := Y(R_1^V)^{-1} = K R_0 \left[\begin{array}{c:c} \mathbf{0} & \mathbf{0} \\ \hdashline R_{2,b} & M \end{array}\right] + Z(R_1^V)^{-1}$$

$\longrightarrow$ Find invertible matrix D s.t. $D\Big(Y'\Big)_{\text{left block}} = \left[\begin{array}{c} ? \\ \hdashline R_{2,b} \end{array}\right]$,

and apply D to the right block: $D\Big(Y'\Big)_{\text{right block}} \underset{\uparrow}{=} \left[\begin{array}{c} ? \\ \hdashline M \end{array}\right] \longrightarrow M$

(with high probab.)

Classical Code to Quantum Code

- In the decoding of classical code,

$$\text{Find invertible matrix } D \text{ s.t. } D\Big(Y'\Big)_{\text{left block}} = \left[\begin{array}{c} ? \\ \hdashline R_{2,b} \end{array}\right],$$

$$\text{and apply } D \text{ to the right block: } D\Big(Y'\Big)_{\text{right block}} = \left[\begin{array}{c} ? \\ \hdashline M \end{array}\right] \longrightarrow M$$

Quantum code 1. performs measurement to the left block,
2. finds $D \in \mathbb{F}_q^{m_0 \times m_0}$ and 3. applies $\mathcal{L}(D)$ to the right block.

$$\begin{array}{r} m_1 \{ \\ m_0 - 2m_1 \{ \\ m_1 \{ \end{array} \left[\begin{array}{c:c:c} \mathcal{H}_{\mathcal{A}1} & \mathcal{H}_{\mathcal{B}1} & \mathcal{H}_{\mathcal{C}1} \\ \hdashline \mathcal{H}_{\mathcal{A}2} & \mathcal{H}_{\mathcal{B}2} & \mathcal{H}_{\text{code}}^{(n)} \\ \hdashline \mathcal{H}_{\mathcal{A}3} & \mathcal{H}_{\mathcal{B}3} & \mathcal{H}_{\mathcal{C}3} \end{array}\right] = \mathcal{H}^{\otimes m_0 \times n}$$

$$\underbrace{\qquad}_{\text{left bit}} \quad \underbrace{\qquad}_{\text{left phase}} \quad \underbrace{\qquad}_{\text{right}}$$

Conclusion

We have constructed a secure quantum network code.

- Security (secrecy & correctability) is from malicious channel attacks.
- Our code is a quantum generalization of the classical network code.
- Multiple-unicast extension can be constructed by considering interference as channel attack.