A quantum secure direct communication & private dense coding framework

Speaker: Jiawei Wu

Tsinghua University

Collaborators: Guilu Long, Masahito Hayashi

Main points

- A framework of private classical communication using quantum state & quantum channel
- Application of quantum wiretap channel theory
- Improvement on finite-length secrecy bound
- Construct practical linear code for implementation

Power of entanglement: dense coding

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$$

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle)$$

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|1_A 0_B\rangle + |0_A 1_B\rangle)$$

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle)$$

- Transmit 2 bit classical information within 1 use of channel

$$|B_{10}\rangle = Z_A|B_{00}\rangle$$
$$|B_{01}\rangle = X_A|B_{00}\rangle$$
$$|B_{11}\rangle = Z_A X_A|B_{00}\rangle$$

Some variants

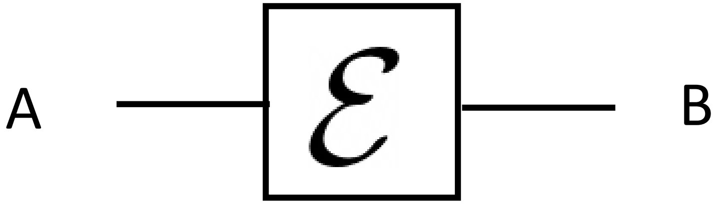
- Perfect entanglement + noisy channel: (Entanglement-assisted classical communication)

$$I(\mathcal{N}) \equiv \max_{\varphi_{AA'}} I(A;B)_\rho,$$

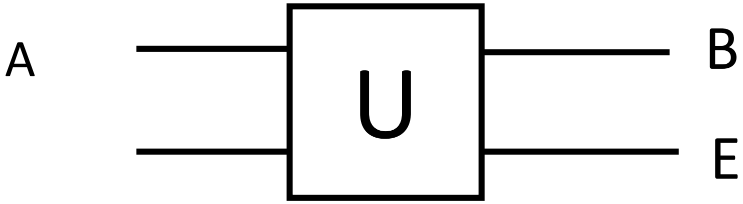
- Noisy entanglement + noiseless channel:

$$C = \log d - H(A|B)_{\rho_{AB}}$$

Power of quantum channel: secure communication



$$\Longleftrightarrow$$



$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$

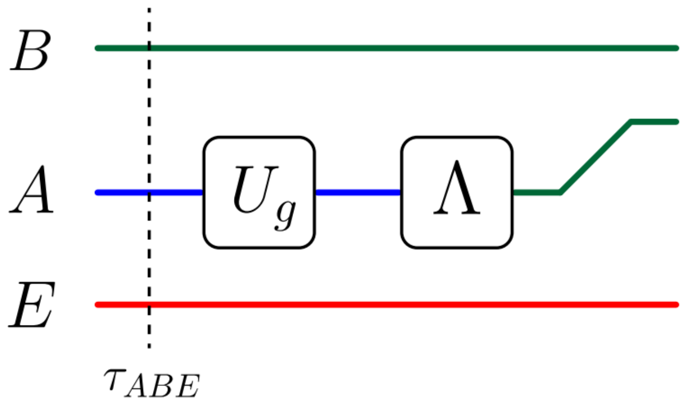
$$\rho_{BE} = U \rho_A \otimes |env\rangle\langle env| U^\dagger$$

E.g.

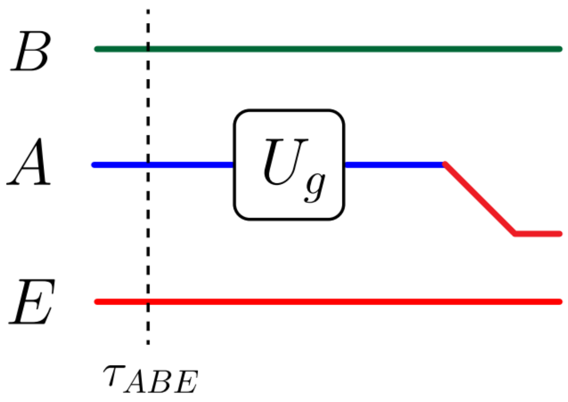
- Private capacity of noiseless channel + perfect entanglement = 2

Our problem setting （Private dense coding）

- General shared states + noisy channel + unitary operations
- Use $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda)$ to denote this setting



Honest case



Worst case (common in QKD)

- Goal: explore the secure transmission rate

Requirements

- Soundness
  - reliability: If the protocol does not abort, Bob recovers the message with probability $\geq 1 - \epsilon_r$
  - secrecy: the information leakage $d(M; E) \leq \epsilon_s$ (measured by trace distance)
- Completeness: In honest case (without interception), the communication aborts with probability $\leq \epsilon_c$

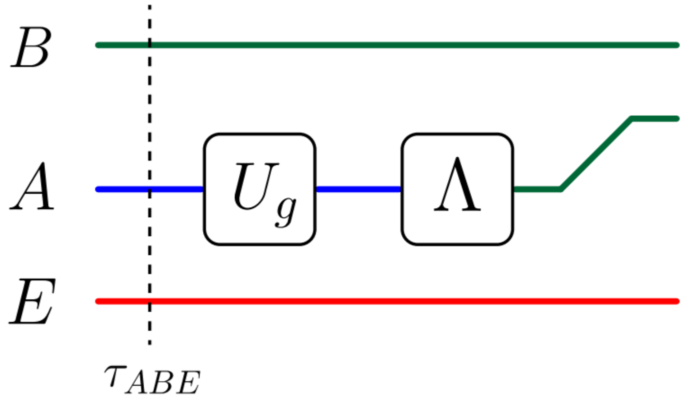
Secrecy criteria

$$
\begin{aligned}
d(M;EZ) &= \left\|\tau_{MEZ} - P_{\mathcal{M}} \otimes \tau_{EZ}\right\|_{\mathrm{tr}} \\
&= \mathbb{E}_Z \left\|\tau_{ME|Z} - P_{\mathcal{M}} \otimes \tau_{E|Z}\right\|_{\mathrm{tr}},
\end{aligned}
$$

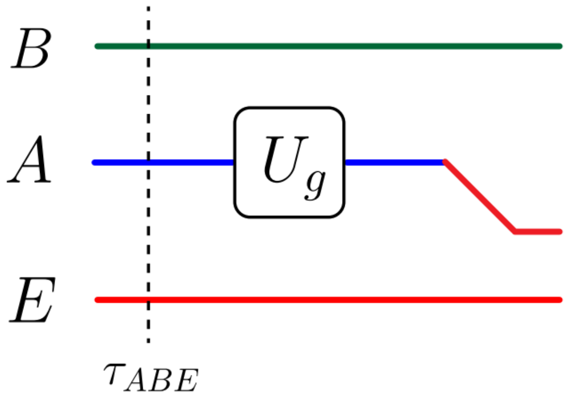
- τ_{MEZ} is the state after transmission
- Z is the publicly shared information, e.g., random seed for UHF

CQ wiretap channel for our setting

(Classical-quantum)



Honest case



Worst case

Channel 1：

$$g \mapsto \rho_{AB}$$

$$\rho_{AB} = \Lambda(U_g \tau_{AB} U_g^\dagger)$$

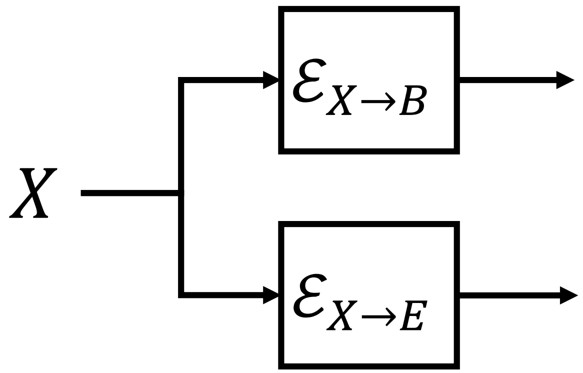
Channel 2：

$$g \mapsto \omega_{AE}$$

$$\omega_{AE} = U_g \tau_{AE} U_g^\dagger$$

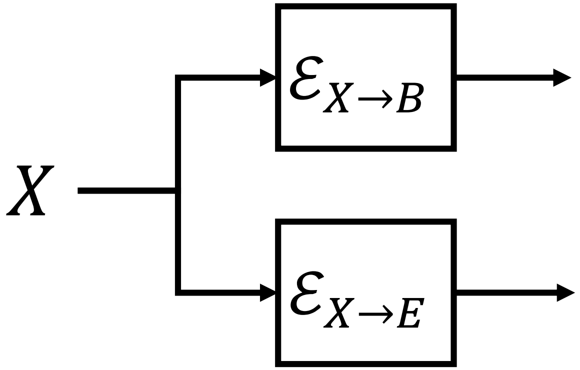
Tool: quantum wiretap channel

- Intuition: When $\mathrm{Ch}_{X\to B}$ is "stronger" than the channel $\mathrm{Ch}_{X\to E}$, reliable and secure communication is possible



- Achievable rate:
  - Exists a code s.t. $\overset{\text{Completeness}}{\boxed{error \to 0,}}\ \overset{\text{Secrecy}}{\boxed{d(M;E) \to 0}}\ as\ n \to \infty$
- Capacity: maximal achievable rate
  - $C \coloneqq \sup\{R: R \text{ is achievable}\}$

Capacity & Achievable rate of Q-wiretap



- Capacity of CQ wiretap channel (Devetak 2005)

$$C_s = \lim_{n\to\infty}\frac{1}{n}\max_{P_U,P_{X^n|U}}\left[I(U:B^n)-I(U:E^n)\right]$$

- A more simple but not tight achievable rate

$$R = I(X:B) - I(X:E)$$

General asymptotic result

- A simple application to $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda)$
- Achievable rate：

$$\mathcal{G}(\rho) := \sum_{g\in G} \frac{1}{|G|} U_g \rho U_g^\dagger$$

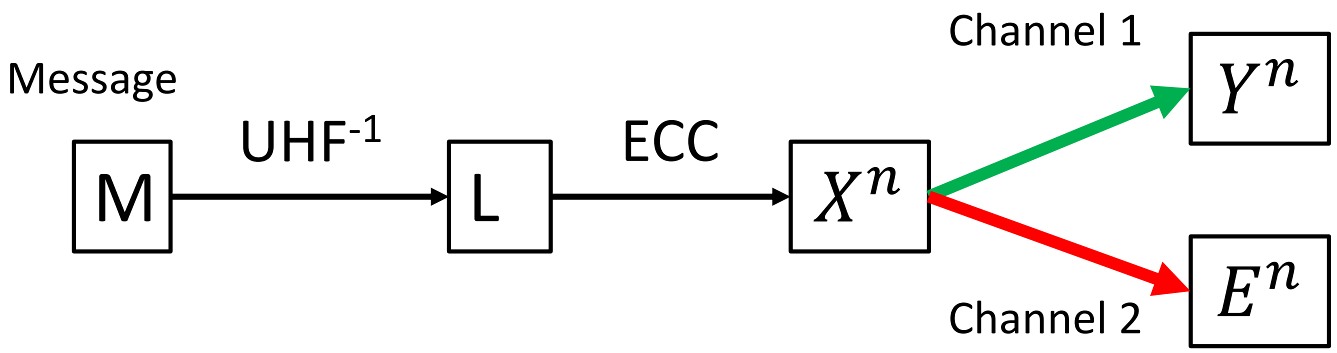
$$R_* = H(\mathcal{G}(\Lambda(\tau_{AB}))) - H(\Lambda(\tau_{AB})) - H(\mathcal{G}(\tau_{AE})) + H(\tau_{AE})$$

- Under condition: $\Lambda(\tau_{AB})$ is maximally correlated, τ_{ABE} is pure

$$C_s = R_* = -2H(A|B)_{\Lambda(\tau)}$$

Modular code construction

- A modular constructive approach: (Hayashi 2010, Vardy 2015)



- Inverse Universal Hash function (UHF) + Any error correcting code

The finite-length bound

- Universal hash lemma (Dupuis 2021):

τ_{LE} is classical on L, $\{f_S\}$: $\mathcal{L} \to \mathcal{M}$ is a UHF family, then

$$\mathbb{E}_S \left\| f_S(\tau_{LE}) - P_{\mathcal{M}} \otimes \tau_E \right\|_1 \leq 2^{\frac{1-t}{1+t}} 2^{\frac{t}{1+t}(\log|\mathcal{M}| - \tilde{H}^{\uparrow}_{1+t}(L|E)_\tau)}$$

$\tilde{H}^{\uparrow}_{1+t}$ is the sandwiched Renyi conditional entropy

The one-shot secrecy bound

$$\text{leakage} \leq \min_{0 \leq t \leq 1} 2^{\frac{1-t}{1+t}} 2^{\frac{t}{1+t}(-\log \mathsf{L}_2 + \tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{L}}))}.$$

$\tilde{I}^{\downarrow}_{1+t}$ is the sandwiched Renyi mutual information

$\log L_2$ is the sacrificed length of UHF

Detailed definitions

$$D_{1+t}(\rho\|\sigma) := \frac{1}{t}\log \mathrm{Tr}\rho^{1+t}\sigma^{-t},$$

$$\tilde{D}_{1+t}(\rho\|\sigma) := \frac{1}{t}\log \mathrm{Tr}(\rho^{-t/2(1+t)}\sigma\rho^{-t/2(1+t)})^{1+t}.$$

$$H^{\downarrow}_{1+t}(A|B|\rho_{AB}) := -D_{1+t}(\rho_{AB}\|I_A \otimes \rho_B),$$

$$\tilde{H}^{\uparrow}_{1+t}(A|B|\rho_{AB}) := -\inf_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} \tilde{D}_{1+t}(\rho_{AB}\|I_A \otimes \sigma_B).$$

$$I^{\downarrow}_{1+t}(A;B|\rho_{AB}) := \inf_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} D_{1+t}(\rho_{AB}\|\rho_A \otimes \sigma_B),$$

$$\tilde{I}^{\downarrow}_{1+t}(A;B|\rho_{AB}) := \inf_{\sigma_B \in \mathcal{D}(\mathcal{H}_B)} \tilde{D}_{1+t}(\rho_{AB}\|\rho_A \otimes \sigma_B).$$

$\boldsymbol{n}$-fold i.i.d. case

- For n-fold symmetric channel, define the sacrificed rate $R_2 = \frac{\log \mathsf{L}_2}{n}$
- The symmetry condition reveals a connection

$$\tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{L}}) \quad \rightarrow \quad \tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{X}})$$

$$\text{leakage} \leq \min_{0\leq t\leq 1} 2^{\frac{1-t}{1+t}} 2^{\frac{t}{1+t} n(-R_2 + \tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{X}}))}$$

Improvement on exponent term

- Decreasing exponent

$$e_d(R_2|W_E) \geq \max_{0\leq t\leq 1} \boxed{\frac{t}{1+t}} (R_2 - \tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{X}}))$$

- Previous result

$$e_d(R_2|W_E) \geq \max_{0\leq t\leq 1} \boxed{\frac{t}{2}} (R_2 - I^{\downarrow}_{1+t}(X;E|W_E \times P_X))$$

Application to our framework

- Using the above modular code, the performance of our PDC protocol:

$$\epsilon_C(P(\varphi, n_2, n_3, q)) \le \epsilon(\varphi)$$

$$\epsilon_E(P(\varphi, n_2, n_3, q)) \le \min_{0 \le t \le 1} 2^{-\frac{1-t}{1+t}} 2^{\frac{tn}{1+t}(-\frac{n_1 - n_2 - n_3}{n} \log q + \log d_A - \tilde{H}^{\uparrow}_{1+t}(A|E|\tau_{AE}))}$$

$$\epsilon_B(P(\varphi, n_2, n_3, q)) \le q^{-n_3},$$

A typical example

- Generalized Pauli operator X, Z for dimension d
- Shared state is generated by Bell state + Pauli channel

$$\Lambda[P_{XZ}](\rho) = \sum_{(x,z)\in\mathbb{Z}_d^2} P_{XZ}(x,z)\mathbf{W}(x,z)\rho\mathbf{W}(x,z)^\dagger.$$

$$\rho[P_{XZ}] := \sum_{(x,z)\in\mathbb{Z}_d^2} P_{XZ}(x,z)\mathbf{W}(x,z)\boxed{|\Phi\rangle\langle\Phi|}\mathbf{W}(x,z)^\dagger.$$

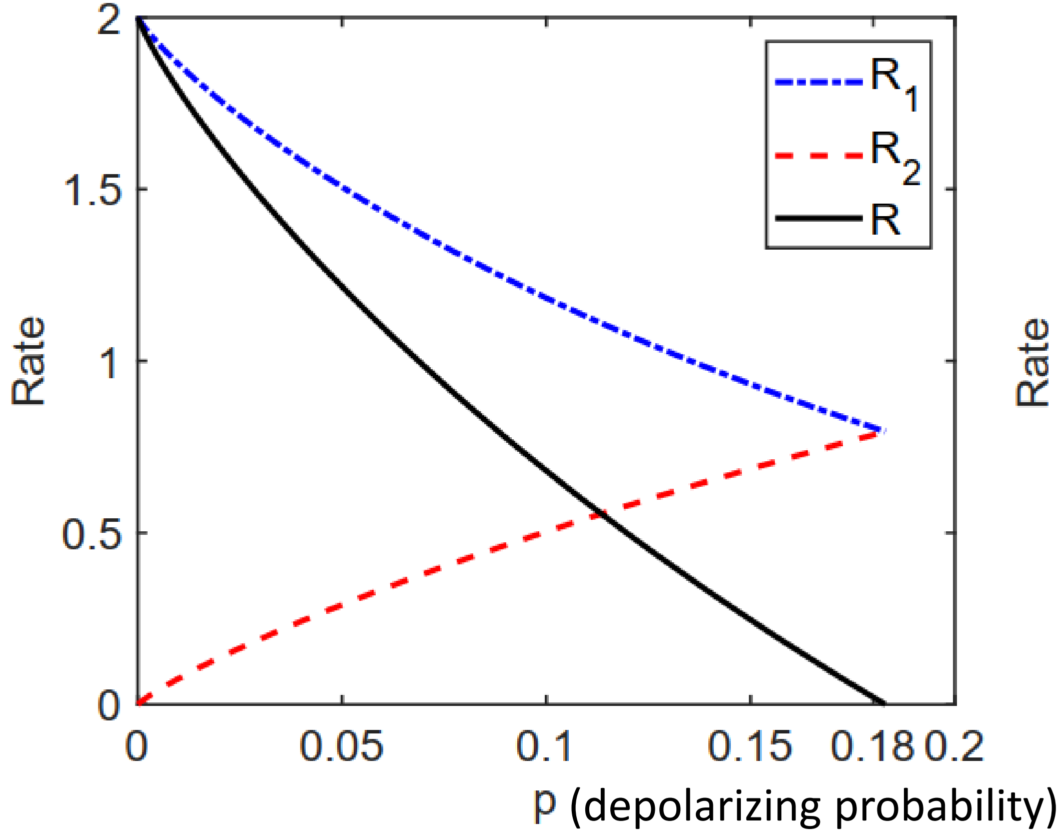
$$\mathbf{W}(x,z) = \mathbf{X}^x\mathbf{Z}^z$$

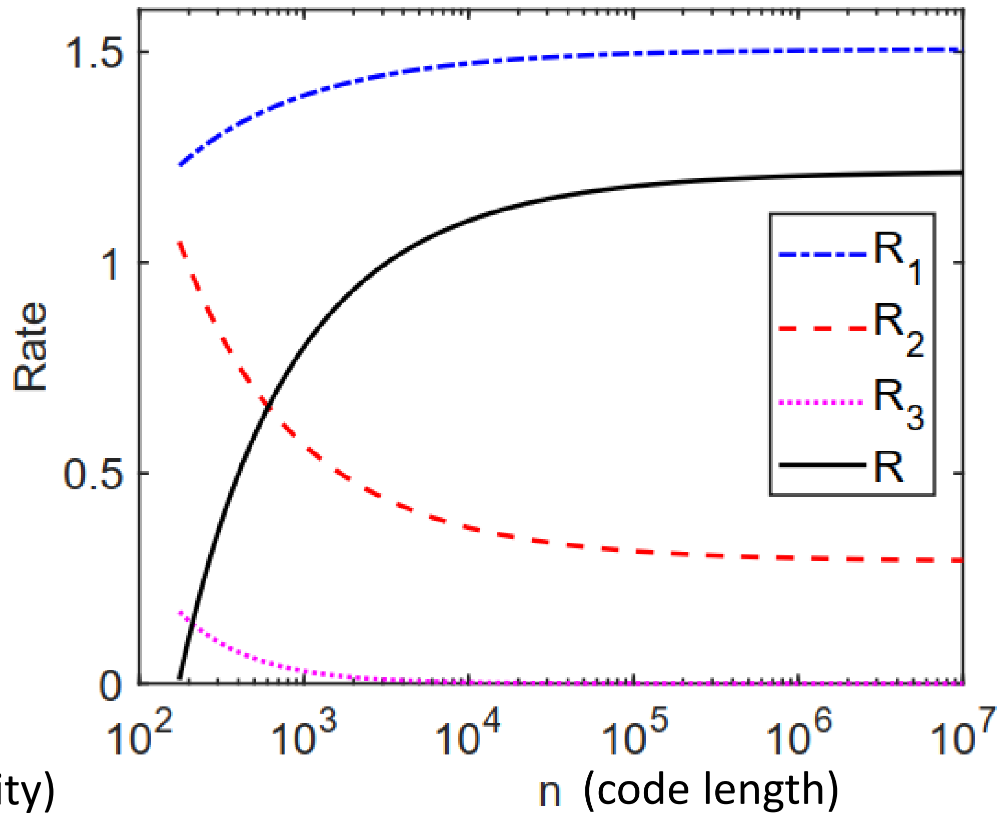
$$\mathbf{X} = \sum_{j\in\mathbb{F}_p} |j+1\rangle\langle j|,$$

$$\mathbf{Z} = \sum_{j\in\mathbb{F}_p} \omega^j |j\rangle\langle j|,$$

- Eve is the environment

- Asymptotic (left) and finite-length (right) rate in a depolarizing channel





R : final rate, R_1: error correcting rate
R_2: sacrificed rate in coding, R_3: sacrificed rate in error verification

Practical linear code

- "Practical" requires:
  - Easily encoded and decoded
  - Bob's measurement is simple
- Conditions

(B1) The group G forms a vector space over a finite field $\mathbb{F}_q$.

(B2) The states $\{U_g \Lambda(\tau_{AB}) U_g^\dagger\}_{g \in G}$ are commutative with each other.

Parameter estimation for unknown state

- Need to perform test and estimate key parameters
- Apply discrete twirling operation

$$T(\tau_{AB}) := \frac{1}{d^2} \sum_{x,z} (\mathbf{W}(x,z)_A \otimes \overline{\mathbf{W}(x,z)}_B) \tau_{AB} (\mathbf{W}(x,z)_A \otimes \overline{\mathbf{W}(x,z)}_B)^\dagger,$$

- Simplify the estimation

Summary

- A general private dense coding framework
- Improved finite-length secrecy bound
- Practical linear code implementation
- Parameter estimation method for high-dimensional unkown state