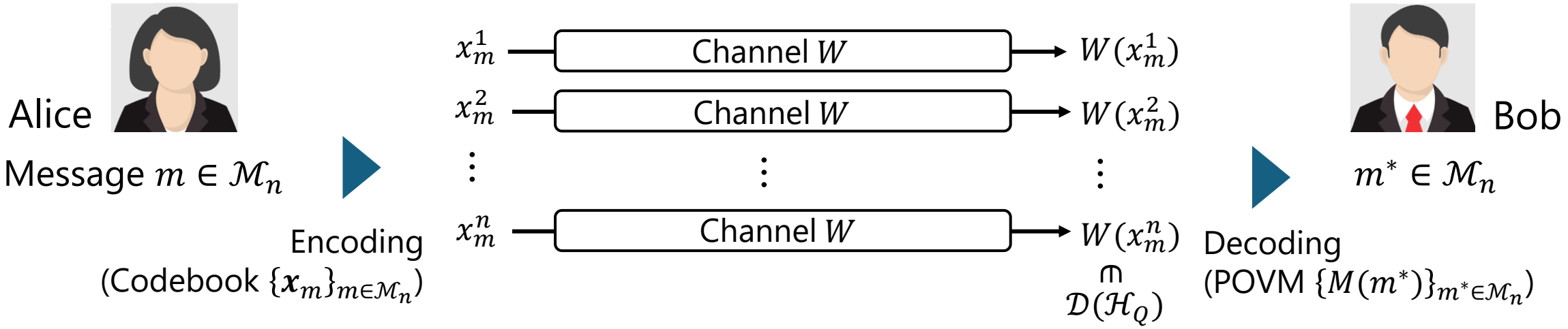
Universal classical-quantum channel resolvability and private channel coding

arXiv: 2510.02883

Takaya Matsuura[1], Masahito Hayashi[2,3,4], Min-Hsiu Hsieh[5]

[1] RIKEN Center for Quantum Computing (RQC)
[2] The Chinese University of Hong-Kong
[3] Shenzhen International Quantum Academy (SIQA)
[4] Nagoya University
[5] Hon Hai Research Institute

Classical-Quantum (CQ) Channel Coding



- Achievable transmission rate for a known $W: \mathcal{X} \to \mathcal{D}(\mathcal{H}_Q)$

$$\frac{\log|\mathcal{M}_n|}{n} \xrightarrow{(n\to\infty)} R < \max_P I(X:Q)_{W^P} \Rightarrow \Pr[m \neq m^*] \xrightarrow{(n\to\infty)} 0$$

Capacity — Decoding error

$$W_{XQ}^P = \sum_{x\in\mathcal{X}} P(x)\,|x\rangle\langle x|_X \otimes W(x)$$

→ Mutual information characterizes the ultimate limit of a reliable message transmission!

CQ Channel Resolvability Coding

Alice

Uniform randomness $\mathcal{K}_n \ni k$

Encoding (Codebook $\{\boldsymbol{x}_k\}_{k\in\mathcal{K}_n}$)

x_k^1 — Channel W

x_k^2 — Channel W

$\vdots$

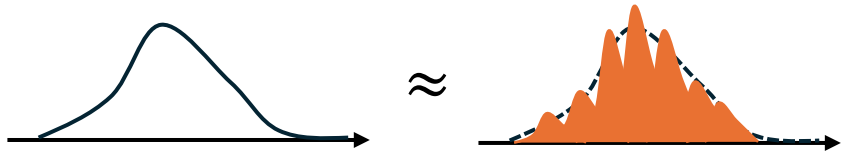
x_k^n — Channel W

$$\frac{1}{|\mathcal{K}_n|}\sum_{k\in\mathcal{K}_n} W^{\otimes n}(\boldsymbol{x}_k)$$

Target state

$$\approx \left(\sum_{x\in\mathcal{X}} P(x)W(x)\right)^{\otimes n} = \left(W_Q^P\right)^{\otimes n}$$

Conceptually…



- Randomness consumption rate for a known $W\colon \mathcal{X} \to \mathcal{D}(\mathcal{H}_Q)$

$$\frac{\log|\mathcal{K}_n|}{n} \xrightarrow{(n\to\infty)} R > I(X\colon Q)_{W^P} \Rightarrow \frac{1}{|\mathcal{K}_n|}\sum_{k\in\mathcal{K}_n} W^{\otimes n}(\boldsymbol{x}_k) \xrightarrow{(n\to\infty)} \left(W_Q^P\right)^{\otimes n}$$ (in the trace norm).

→ Mutual information also characterizes the fundamental limit of channel resolvability!

Quantum Soft-covering Lemma

- With a random coding, drawn i.i.d. from P,

$$\mathbb{E}_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{|\mathcal{K}_n|}\sim P^n} \left\| \frac{1}{|\mathcal{K}_n|} \sum_{k\in\mathcal{K}_n} W^{\otimes n}(\boldsymbol{x}_k) - \left(W_Q^P\right)^{\otimes n} \right\|_1 \xrightarrow{(n\to\infty)} 0 \quad \text{if } R > I(X:Q)_{W^P} \qquad \text{(Achievability)}$$

$$\xrightarrow{(n\to\infty)} 1 \quad \text{if } R < I(X:Q)_{W^P} \qquad \text{(Converse)}$$

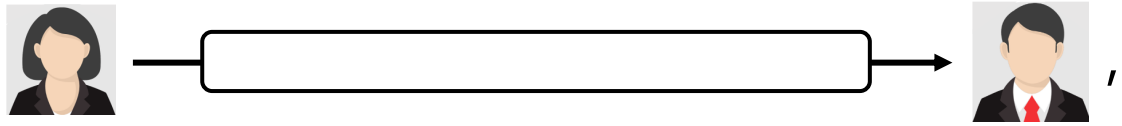
→ There exists a codebook $\{\boldsymbol{x}_k\}_{k\in\mathcal{K}_n}$ that realizes CQ channel resolvability.

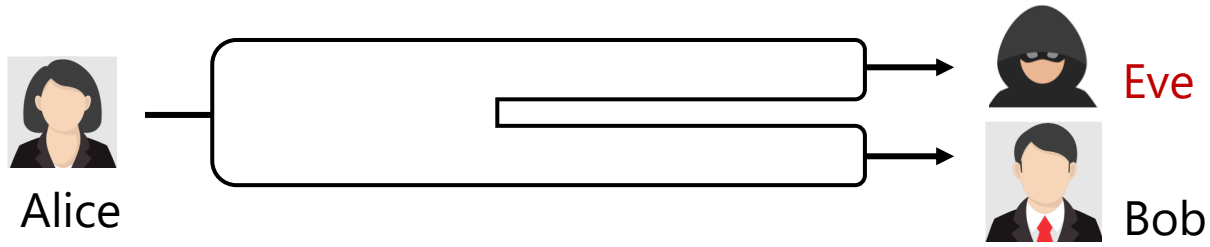
- Caution!

If $W_Q^{P'} = W_Q^P$ for some $P' \neq P$, then the resolvability coding may be more efficient, i.e., $R > \min\left\{I(X:Q)_{W^P}, I(X:Q)_{W^{P'}}\right\}$ is achievable.

In this talk, we do not consider such a degenerate case.

Private Channel Coding

- Instead of  ,

consider 

, i.e., information may be leaked.

- With $W: \mathcal{X} \to \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_E)$, can Alice send Bob a message that is secret to Eve?

  → **YES**, if Alice & Bob know W and $I(X:B)_{W^P} > I(X:E)_{W^P}$ for some P.

  → Transmission rate $\max_P I(X:B)_{W^P} - I(X:E)_{W^P}$ is achievable.

Information Theory 40, 318 (2004).
IEEE Trans. Inf. Theory 51, 44 (2005).

Strategy:

Encode a message $m \in \mathcal{M}_n$ with a random number $k \in \mathcal{K}_n$ into a codeword $\boldsymbol{x}_{m,k}$.

Private Channel Coding (2)

Alice

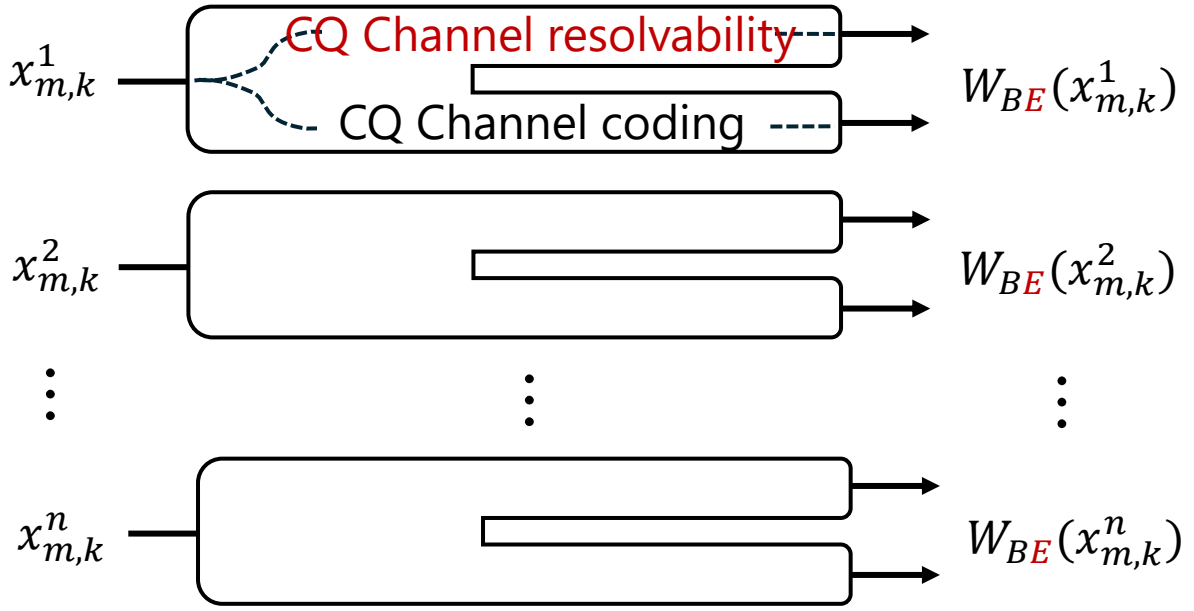
A pair (m, k) of a message $m \in \mathcal{M}_n$ and a randomness $k \in \mathcal{K}_n$

Encoding

$\|$

$m \in \mathcal{M}_n$

Stochastic encoding



Eve

Cannot distinguish the states for different m

Bob

Can decode (m, k)

$$\frac{\log|\mathcal{K}_n|}{n} \xrightarrow{(n\to\infty)} R_E > I(X:E)_{W^P}$$

$$\frac{\log|\mathcal{M}_n|}{n} \xrightarrow{(n\to\infty)} R < \max_P I(X:B)_{W^P} - I(X:E)_{W^P}$$

$$\Rightarrow$$

$$\sum_{k\in\mathcal{K}_n} W_E^{\otimes n}(\boldsymbol{x}_{m,k}) \approx \sum_{k\in\mathcal{K}_n} W_E^{\otimes n}(\boldsymbol{x}_{m',k})$$

$$\Pr[m \neq m^*] \xrightarrow{(n\to\infty)} 0$$

Constant-Composition Coding

- Recall the capacity $\max_P I(X:Q)_{WP}$ of CQ channel coding…

  What is the operational meaning of this?

  → A set of codewords generated i.i.d. according to P achieves the capacity.

  → It reflects the bias of the use of each symbol optimized for W.

- Type = Relative frequency of each symbol in a sequence

  E.g. The type of $\boldsymbol{x} = (a, a, c, b, c)$ is $({}^2/_5, {}^1/_5, {}^2/_5)$.

- Constant-composition coding

  → All the codewords have the same type.

  → For a fixed type P, $\max_P I(X:Q)_{WP}$ is achievable in CQ channel coding, and so is CQ channel resolvability coding.

  → Essential for universal coding.

The Challenge: Universality

What if we do not know the channel W?

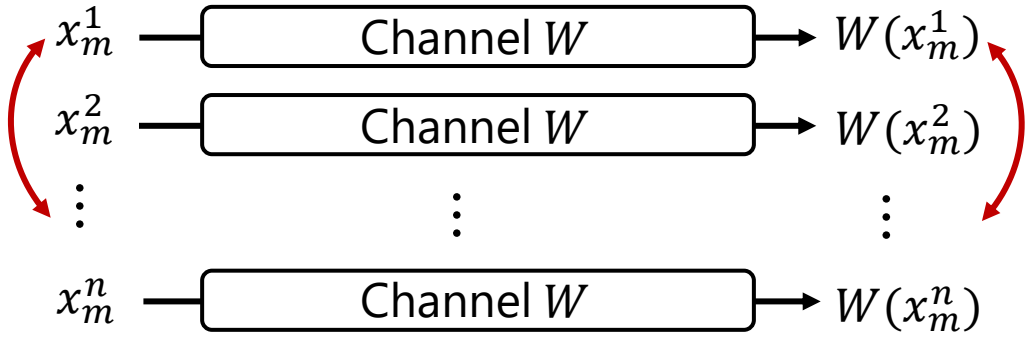
- Universal CQ channel coding
  [M. Hayashi, Commun. Math. Phys. 289, 1087 (2009)]

  There exists a channel-independent sequence of constant-composition codebooks $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_{|\mathcal{M}_n|}\}_n$ with the type P and decoding POVMs $\{Y_n\}_n$ s.t.

  $$\frac{\log |\mathcal{M}_n|}{n} \xrightarrow{(n\to\infty)} R < I(X:Q)_{W^P} \Rightarrow \Pr[m \neq m^*] \xrightarrow{(n\to\infty)} 0.$$

  → Reliable message transmission with only knowledge of $I(X:Q)_{W^P}$.

  → Achievability of the capacity with additional knowledge of $\operatorname{argmax}_P I(X:Q)_{W^P}$.



- Exploits permutation-covariance.
- Appears to be too weak, but is sufficient in fact.

Tool:
Representation theory of permutation group, Schur-Weyl duality…

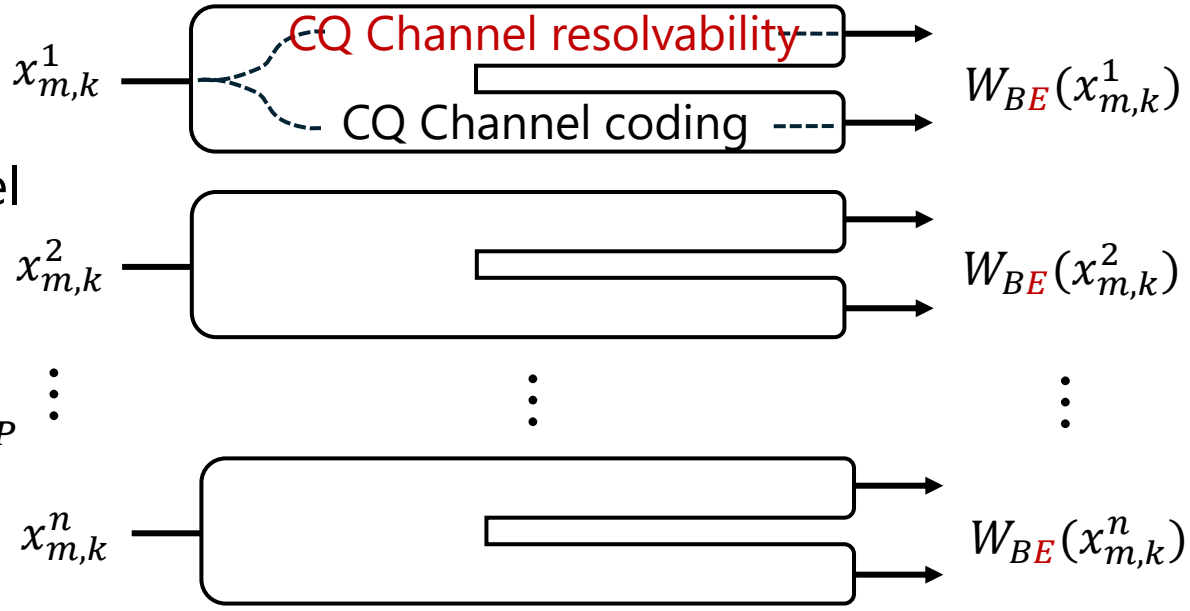
First Attempt: Randomized Construction

Combination of Universal CQ channel coding and randomized mixture

[Datta and Hsieh, J. Math. Phys. (2010)]

The randomization does not depend on the channel W. But, it is not a deterministic code.

→ Transmission rate $\max_P I(X:B)_{W^P} - I(X:E)_{W^P}$ is achievable.



Second Attempt: Classical case

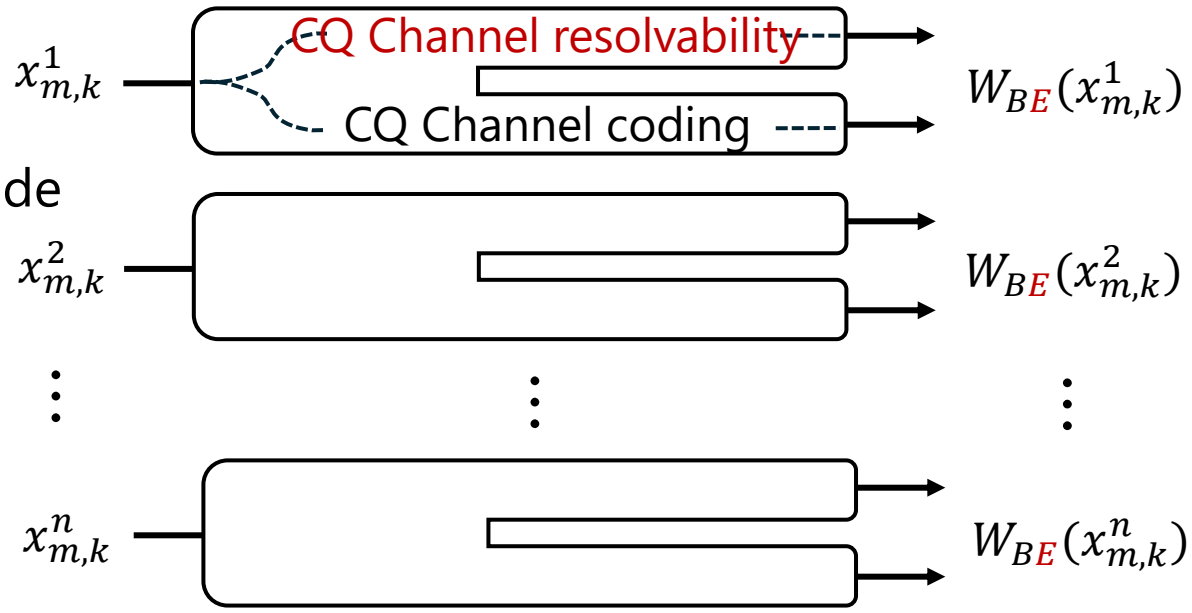
Classical channel can be written as a mixture of conditional types.

[Hayashi and R. Matsumoto, IEEE Transactions on IT (2016).]

It is sufficient to construct a deterministic secure code that works with a polynomial number of channel because the classical channel can be written as a convex combination of conditional types.
Since the averaged amount of information leakage goes to zero exponentially, this method works well.

→ Transmission rate $\max_P I(X:B)_{W^P} - I(X:E)_{W^P}$

is achievable.



TAKEAWAY: What We Have Solved

- Universal CQ channel resolvability coding? → **YES!**

  There is a sequence of channel-independent constant-composition codebooks $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_{|\mathcal{K}_n|}\}_n$ with the type P such that

  $$\frac{\log|\mathcal{K}_n|}{n} \xrightarrow{(n\to\infty)} R > I(X:Q)_{W^P} \implies \left\| \frac{1}{|\mathcal{K}_n|} \sum_{k\in\mathcal{K}_n} W^{\otimes n}(\boldsymbol{x}_k) - \bar{W}_P \right\|_1 \xrightarrow{(n\to\infty)} 0,$$

  where $\bar{W}_P = \frac{1}{|\mathcal{T}_P^n|} \sum_{\boldsymbol{x}\in\mathcal{T}_P^n} W^{\otimes n}(\boldsymbol{x})$, and $\mathcal{T}_P^n$ is the set of sequences with the type P.

  Key technique:
  De-randomization of quantum soft-covering lemma with an **expander graph**.

- (Fully) universal private channel coding? → **YES!**

  There is a sequence of channel-independent constant-composition codebooks $\{\{\boldsymbol{x}_{m,k}\}_{m\in\mathcal{M}_n, k\in\mathcal{K}_n}\}_n$ such that …

Universal construction for channel resolvability 1

S_n: Permutation group on {1,…,n}.

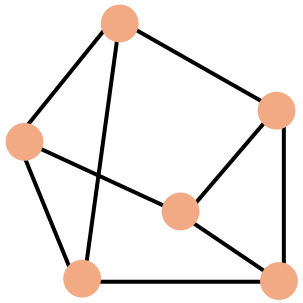
$S_x := \{g \in S_n \mid gx = x\}, x \in X^n$

$S \subseteq S_n$: Subset such that $g \in S \Longrightarrow g^{-1} \in S$

- Schreier graph $\Gamma(S_n/\ S_x, S)$

$S_n/\ S_x$:verteces,

$\{([g].[g'g])\}_{g \in S_n, g' \in S}$:edges



$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{|S_n/\ S_x|}$:
Eigen values of (Probability)
Transition Matrix of the graph
$\Gamma(S_n/\ S_x, S)$

$$\lambda(\Gamma(S_n/\ S_x, S)) := \max(\lambda_2, -\lambda_{|S_n/\ S_x|})$$

Universal construction for channel resolvability 2

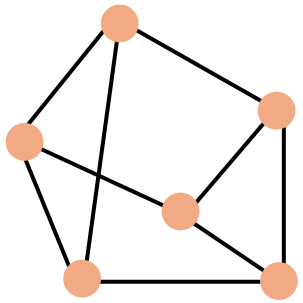
((P,R, δ)-radical spectral expander

Codebook $\mathcal{M}_n = \{g(x)\}_{g\in S}$ such that

$|\mathcal{M}_n| = |S|$=exp[nR+δ]

Schreier graph $\Gamma(S_n/\ S_x, S)$ satisfies

$\lambda(\Gamma(S_n/\ S_x, S))\ \leq$exp(-nR/2)



$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{|S_n/\ S_x|}$:

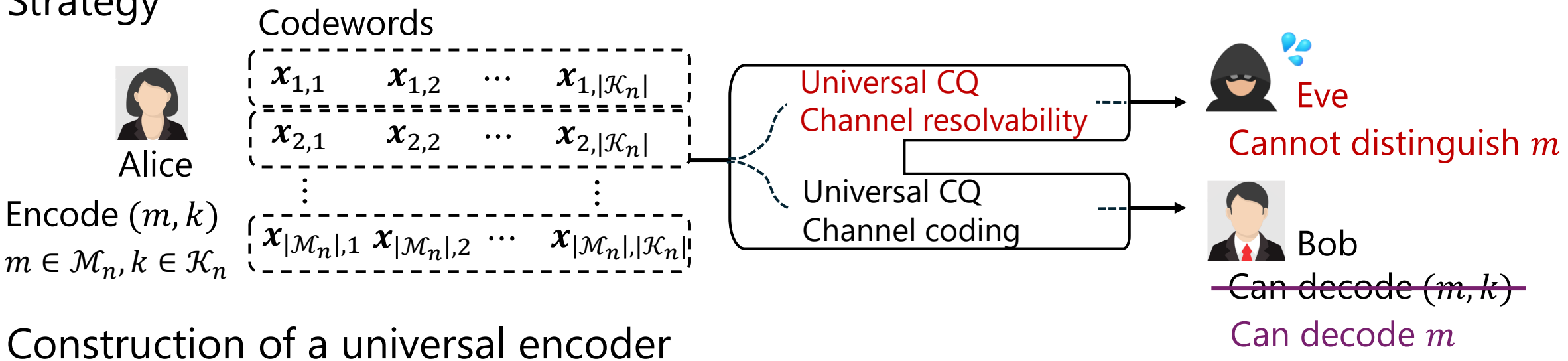
Eigen values of (Probability) Transition Matrix of the graph $\Gamma(S_n/\ S_x, S)$

$\lambda(\Gamma(S_n/\ S_x, S))\ :=\ \max(\lambda_2, -\lambda_{|S_n/\ S_x|})$

This codebook satisfies the condition for channel resolvability, and its construction does not depend on the form of channel.

Universal Private Channel Coding

- Strategy



- Construction of a universal encoder

Codewords s.t. universal CQ channel coding works

Codewords s.t. universal CQ channel resolvability coding works for all $|\mathcal{M}_n|$ blocks

Conclusion and Outlook

Conclusion

- We have constructed a universal CQ channel resolvability coding and a universal private channel coding.
- Quantum soft-covering lemma for constant composition can be de-randomized by a codebook constructed from the Schreier graph with the expander property.

Future directions

- Expander graph also plays important roles in quantum error correction (QEC).
  Is there a duality relation?
- Other quantum-information tasks can be de-randomized by an expander graph?

Thank you for your attention!

arXiv: 2510.02883