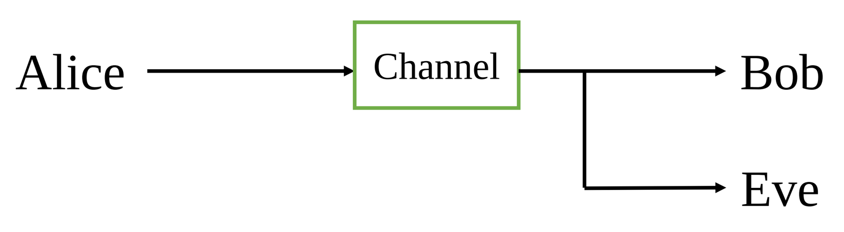
One-shot Inner Bounds for Sending Private Classical Information over a Quantum MAC

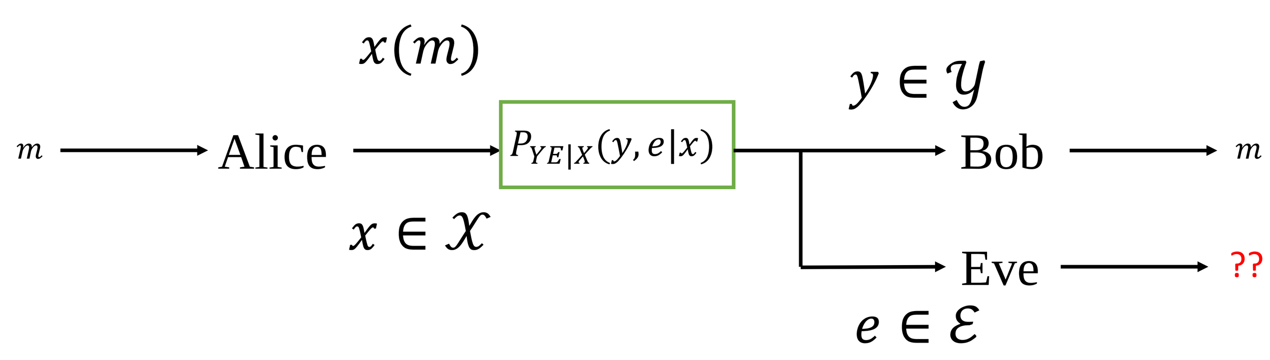
Sayantan Chakraborty, Aditya Nema and Pranab Sen

The Problem



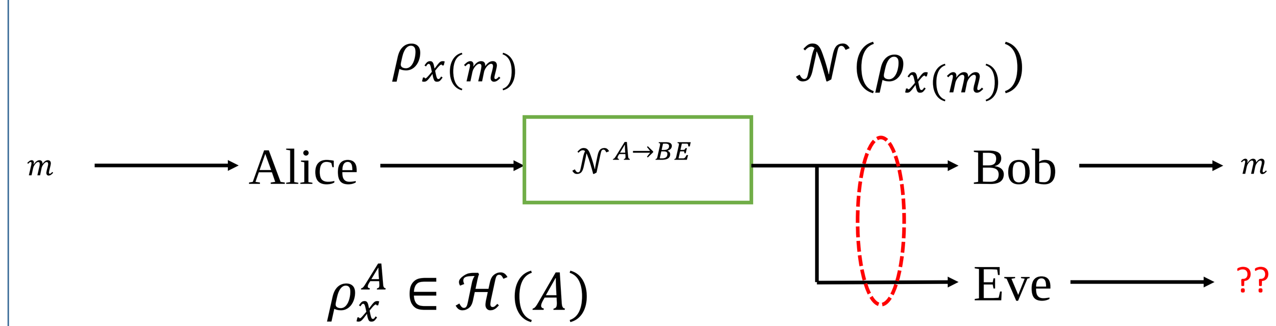
Can Alice send messages to Bob while hiding them from Eve?

The Problem : Variants



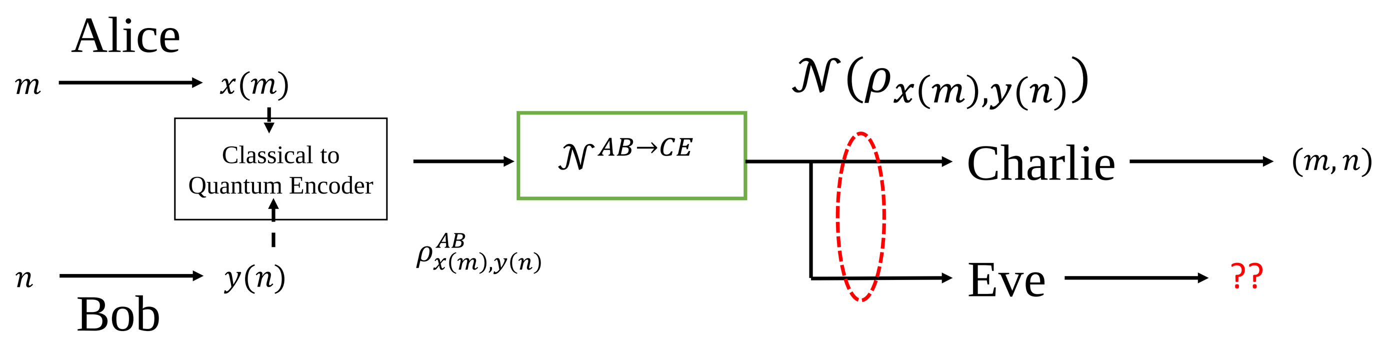
Classical Input Classical Output

The Problem : Variants



Classical Input Quantum Output

The Problem : Variants



Classical Quantum Multiple Access Channel

This Paper

Formal Problem Statement :The Point to Point Channel

Given a quantum channel $\mathcal{N}^{A\to BE}$, where A belongs the sender Alice, B belongs to the legitimate receiver Bob and E belongs to the eavesdropper Eve, does there exist a classical to quantum encoding map $\mathcal{F}^{[M]\to A}$ and a quantum classical decoding map $\mathcal{D}^{B\to[M]}$ such that the following conditions are met :

- **Reliability :** For all $m \in [M]$ Bob should be able to recover the transmitted message with probability of error at most some small constant $\epsilon > 0$ **.**
- **Privacy :** For all $m \in [m]$**,** the state on Eve's system E should be close to a constant independent of m**.**

Strategy for the Point to Point Channel

- Alice creates a random code $\{x(m,k)\}$ from a fixed distribution P_X, for each index (m,k).
- She divides the codebook into blocks of size k, where each block corresponds to some message m. Here, $k \in [K], m \in [M]$.
- This operation corresponds to the encoding map $\mathcal{F}^{[M]\to A}$.
- To send the message m, Alice randomly chooses an index $k \in [K]$ at random and encodes the corresponding symbol $x(m,k)$ into the input state $\rho_{x(m,k)}$.
- $\rho_{x(m,k)}$ is input to the channel.

Strategy for the Point to Point Channel

- **Reliability :** Existence of $\mathcal{D}$ guaranteed by
  - the HSW theorem in the asymptotic iid regime, whenever $M < I(X:B)$
  - by Sen's sequential decoder in the One-shot regime, whenever $M < I_H^\epsilon(X:B)$
- **Privacy :** Guaranteed by the covering lemma and the random choice of k at the encoder (both iid and one-shot) :

$$\left\| \frac{1}{K}\sum_k \rho^E_{x(m,k)} - \rho^E \right\| \leq \epsilon$$

  - Whenever $K > I(X:E)$ in the asymptotic iid regime
  - Whenever $K > I^\epsilon_{\max}(X:E)$ in the one-shot regime.

The Classical-Quantum MAC

Reliability :
- Successive Cancellation + Time Sharing in asymptotic iid
- Sen's Simultaneous decoder in the one-shot regime

ISSUE : Need a multiterminal version of the covering lemma to guarantee joint secrecy of Alice and Bob.

The Simultaneous Smoothing Conjecture

Ideal Multiterminal Covering Lemma : For senders Alice and Bob, given the encoding distributions P_X and P_Y , the classical to quantum channel $\mathcal{N}^{AB\to CE}$ and the resulting control state

$$\sum_{x,y} P_X(x)P_Y(y)\,|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho^{CE}_{x,y}$$

for K and L random samples $\{x(k) \mid k \in [K]\}$ and $\{y(\ell) \mid \ell \in [L]\}$ picked independently form P_X and P_Y , we have

$$\mathbb{E}\left\| \frac{1}{KL}\sum_{k,\ell} \rho^E_{x(k),y(\ell)} - \rho^E \right\| \leq \epsilon$$

whenever

$$K > I^\epsilon_{\max}(X:C)$$
$$L > I^\epsilon_{\max}(Y:C)$$
$$K + L > I^\epsilon_{\max}(XY:C)$$

THIS IS OPEN!

The Solution : A Successive Cancellation Covering Lemma

Under the same setup as the ideal lemma, the secrecy condition

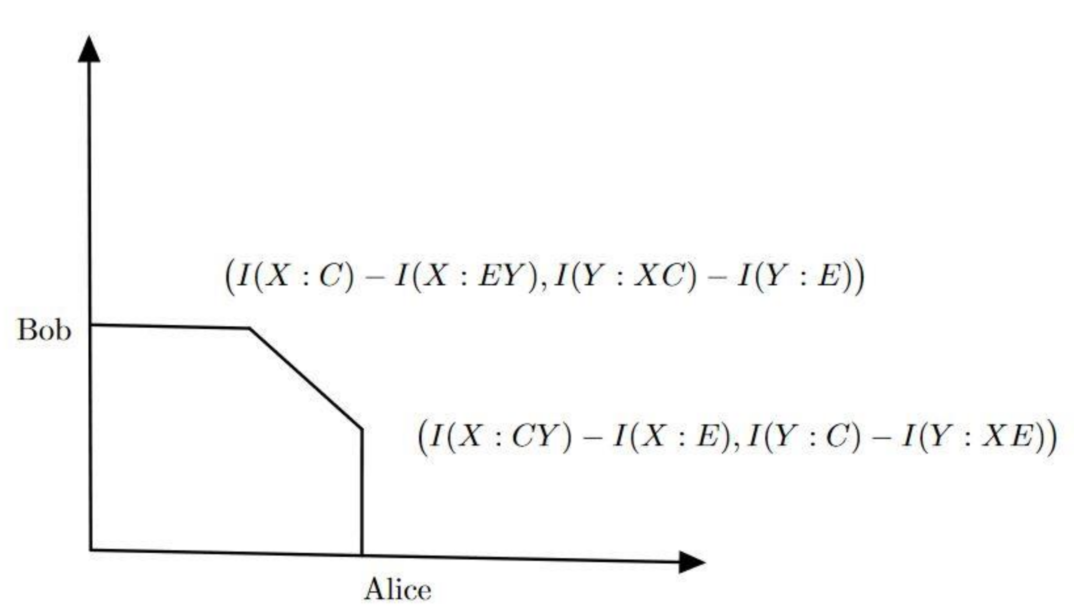
$$\mathbb{E}\left\| \frac{1}{KL}\sum_{k,\ell} \rho^E_{x(k),y(\ell)} - \rho^E \right\| \leq \epsilon$$

holds whenever

$$K > I^\epsilon_{\max}(X:EY) \qquad K > I^\epsilon_{\max}(X:E)$$
$$L > I^\epsilon_{\max}(Y:E) \quad \text{or} \quad L > I^\epsilon_{\max}(Y:XE)$$

Consequences : The Private Classical Capacity of the Quantum MAC

Asymptotic IID : Joint secrecy for points on the dominant face (other than the corner points) guaranteed by time sharing.



Consequences : The Private Classical Capacity of the Quantum MAC

One-Shot : Issue – Time sharing can no longer be done.

Solution – Use rate splitting and the successive cancellation covering lemma to guarantee joint secrecy for more points other than the corner points.