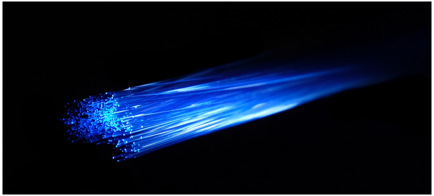
Secure Communication with Unreliable Entanglement Assistance: Interception and Loss

Meir Lederman, Uzi Pereg
ECE, Technion

Beyond IID in Information Theory 12 | August 1, 2024

Motivation

Quantum information technology will potentially boost future 6G systems from both communication and computing perspectives.



unsplash.com

Motivation: Secure Quantum Communication

TECHNION | Helen Diller Quantum Center

- Security poses a pivotal challenge in modern communication networks.
- Physical layer security leverages the inherent disturbance of the physical channel to ensure secure transmissions without relying on secret keys.
- Wiretap channel model: $\mathcal{N}_{A\to BE}$

Motivation: Secure Quantum Communication

- Security poses a pivotal challenge in modern communication networks.
- Physical layer security leverages the inherent disturbance of the physical channel to ensure secure transmissions without relying on secret keys.
- Wiretap channel model: $\mathcal{N}_{A\to BE}$

Motivation: Secure Quantum Communication

TECHNION | Helen Diller Quantum Center

- Security poses a pivotal challenge in modern communication networks.
- Physical layer security leverages the inherent disturbance of the physical channel to ensure secure transmissions without relying on secret keys.
- Wiretap channel model: $\mathcal{N}_{A \to BE}$

Motivation: Entanglement

TECHNION | Helen Diller Quantum Center

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- Communication rate
  - Without Security: Bennett et al. 1999
  - With Security: Qi et al. 2018
- . . .

Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.

Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- Communication rate
  - Without Security: Bennett et al. 1999
  - With Security: Qi et al. 2018
- . . .

Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.

Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- **Communication rate**
  - Without Security: Bennett et al. 1999
  - With Security: Qi et al. 2018
- . . .

Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.

Motivation: Entanglement

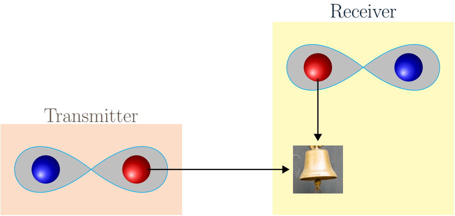
Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- Communication rate
  - Without Security: Bennett et al. 1999
  - With Security: Qi et al. 2018
- . . .

Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.

Motivation: Entanglement (Cont.)

- In order to generate (heralded) entanglement in an optical communication system, the transmitter may prepare an entangled pair of photons locally, and then send one of them to the receiver.
- Such generation protocols are not always successful, as photons are easily absorbed before reaching the destination.



Motivation: Entanglement (Cont.)

- In order to generate (heralded) entanglement in an optical communication system, the transmitter may prepare an entangled pair of photons locally, and then send one of them to the receiver.
- Such generation protocols are not always successful, as photons are easily absorbed before reaching the destination.

Motivation: Entanglement (Cont.)

- Therefore, practical systems require a back channel. In the case of failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources.

- In our previous work, Pereg et al. proposed a new principle of operation: The communication system operates on a rate that is adapted to the status of entanglement assistance. Hence, feedback and repetition are not required. [Pereg et al. 2023]

- **Here, we consider secure communication in two scenarios:**
  - **Eve might steal the assistance - Interception model**
  - **The assistance might get lost to the environment - Passive model**

Motivation: Entanglement (Cont.)

- Therefore, practical systems require a back channel. In the case of failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources.
- In our previous work, Pereg et al. proposed a new principle of operation: The communication system operates on a rate that is adapted to the status of entanglement assistance. Hence, feedback and repetition are not required. [Pereg et al. 2023]
- Here, we consider secure communication in two scenarios:
  - Eve might steal the assistance - Interception model
  - The assistance might get lost to the environment - Passive model

Motivation: Entanglement (Cont.)

TECHNION | Helen Diller Quantum Center

- Therefore, practical systems require a back channel. In the case of failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources.
- In our previous work, Pereg et al. proposed a new principle of operation: The communication system operates on a rate that is adapted to the status of entanglement assistance. Hence, feedback and repetition are not required. [Pereg et al. 2023]
- **Here, we consider secure communication in two scenarios:**
  - **Eve might steal the assistance - Interception model**
  - **The assistance might get lost to the environment - Passive model**

Unreliable Resources

Reliability (very partial list):

- Unreliable channel
  - outage capacity [Ozarow, Shamai, and Wyner 1994]
  - automatic repeat request (ARQ) [Caire and Tuninetti 2001] [Steiner and Shamai 2008]
  - cognitive radio [Goldsmith et al. 2008]
  - Network connectivity [Simeone et al. 2012] [Sengupta and Tandon 2015]
- Unreliable cooperation - Dynamic links [Steinberg 2014]
  - cribbing encoders [Huleihel and Steinberg 2016]
  - conferencing decoders [Huleihel and Steinberg 2017] [Itzhak and Steinberg 2017] [Pereg and Steinberg 2020]

Related Work: Without Secrecy

Fundamental Problem: Noiseless Channel

Classical Bit-Pipe

The capacity of a classical noiseless bit channel is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

Holevo Bound

The classical capacity of a noiseless qubit channel is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

Fundamental Problem:
Noiseless Channel + Assistance

Theorem

The classical *common-randomness* (CR) capacity of a noiseless bit-pipe is

$$1 \; \frac{\text{classical bit}}{\text{transmission}}$$

Holevo Bound

The classical capacity of a noiseless qubit channel is

$$1 \; \frac{\text{classical bit}}{\text{transmission}}$$

Fundamental Problem: Noiseless Channel + Assistance

Theorem

The classical *common-randomness* (CR) capacity of a noiseless bit-pipe is

$$1 \frac{\text{classical bit}}{\text{transmission}}$$

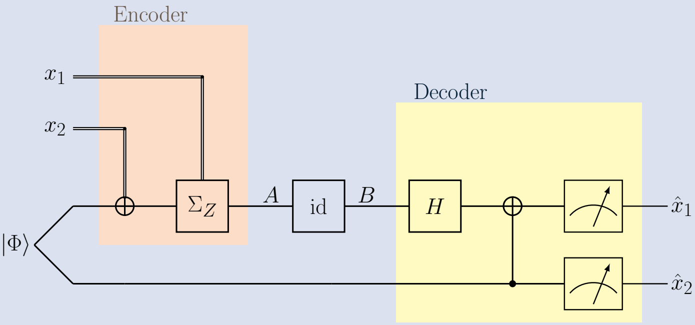
Theorem

The classical *entanglement-assisted* (EA) capacity of a noiseless qubit channel is

$$2 \frac{\text{classical bits}}{\textit{transmission}}$$

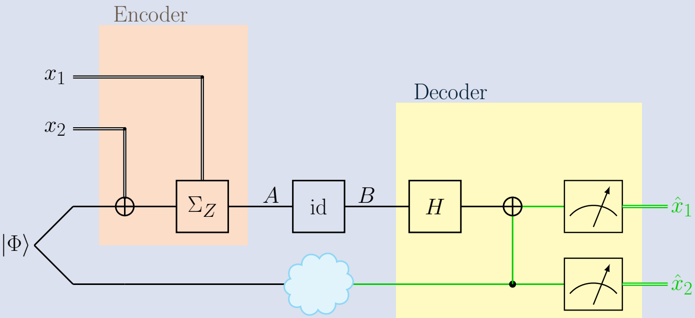
Fundamental Problem: Noiseless Channel + EA

Superdense Coding



Fundamental Problem: Noiseless Channel + EA (Cont.)

Superdense Coding



Fundamental Problem:
Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1) Uncoded communication
    - Guaranteed rate: $R = 1$
    - Excess rate: $R' = 0$

2) Alice: Employ superdense encoder.

    Bob: If EA is present, employ superdense decoder.

    If EA is absent, abort.
    - Guaranteed rate: $R = 0$
    - Excess rate: $R' = 2$

Fundamental Problem:
Noiseless Channel + EA (Cont.)

TECHNION | Helen Diller Quantum Center

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1) Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

2) Alice: Employ superdense encoder.

   Bob: If EA is **present**, employ superdense decoder.

   If EA is absent, abort.

   - Guaranteed rate: $R = 0$
   - Excess rate: $R' = 2$

Fundamental Problem: Noiseless Channel + EA (Cont.)

TECHNION | Helen Diller Quantum Center

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1) Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

2) Alice: Employ superdense encoder.

   Bob: If EA is present, employ superdense decoder.
   If EA is **absent**, abort.
   - Guaranteed rate: $R = 0$
   - Excess rate: $R' = 2$

Fundamental Problem:
Noiseless Channel + EA (Cont.)

TECHNION | Helen Diller Quantum Center

Time Division

- Guaranteed rate: $R = 1 - \lambda$
- Excess rate: $R' = 2\lambda$

⋆ Is this optimal?

[Pereg et al. 2023]

- Time division is **optimal** for a noiseless channel
- Time division is **strictly sub-optimal** for depolarizing channels.

Fundamental Problem:
Noiseless Channel + EA (Cont.)

TECHNION | Helen Diller Quantum Center

Time Division

- Guaranteed rate: $R = 1 - \lambda$
- Excess rate: $R' = 2\lambda$

⋆ Is this optimal?

[Pereg et al. 2023]

- Time division is **optimal** for a noiseless channel
- Time division is **strictly sub-optimal** for depolarizing channels.

Main Contributions

We consider a quantum wiretap channel in two settings involving interception or loss.

1) Interception: Eve may “steal" Bob’s entanglement resource.
   - Inner bound (achievable rates)
   - Degraded channels: regularized capacity formula

2) Loss: The resource could get lost to the environment.
   - regularized capacity formula

- Both under semantic security and maximal error criterion

Main Contributions

We consider a quantum wiretap channel in two settings involving interception or loss.

1) Interception: Eve may “steal" Bob’s entanglement resource.
   - Inner bound (achievable rates)
   - Degraded channels: regularized capacity formula

2) Loss: The resource could get lost to the environment.
   - regularized capacity formula

- Both under semantic security and maximal error criterion

Main Contributions (Cont.)

- Observation: in the interception model, time division is not necessarily possible.
- Erasure channel: Time division is achievable and optimal in both models.
- Amplitude Damping Channel
  - Interception: Achievable region has discontinuous boundary.
  - Loss: Time division is achievable, but strictly sub-optimal.

Main Contributions (Cont.)

- Observation: in the interception model, time division is not necessarily possible.
- Erasure channel: Time division is achievable and optimal in both models.
- Amplitude Damping Channel
  - Interception: Achievable region has discontinuous boundary.
  - Loss: Time division is achievable, but strictly sub-optimal.

Main Contributions (Cont.)

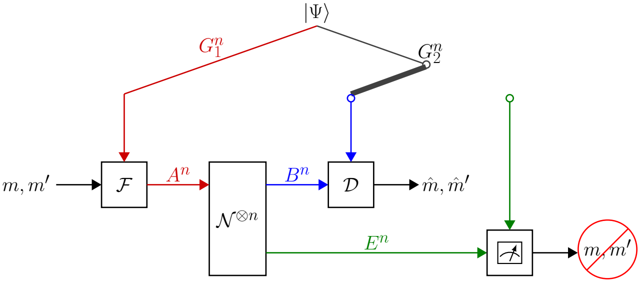
- Observation: in the interception model, time division is not necessarily possible.
- Erasure channel: Time division is achievable and optimal in both models.
- Amplitude Damping Channel
  - Interception: Achievable region has discontinuous boundary.
  - Loss: Time division is achievable, but strictly sub-optimal.

Interception Model: Definitions and Results

Communication with Interception

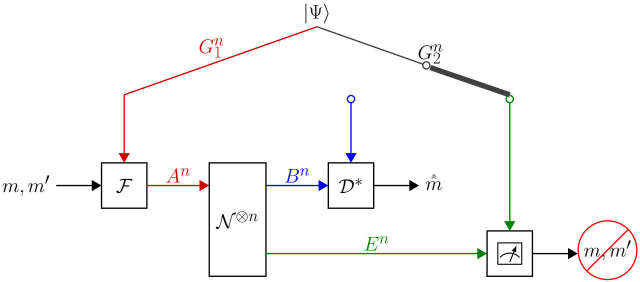
There are two scenarios:

- Bob receives the entanglement assistance



Communication with Interception (Cont.)

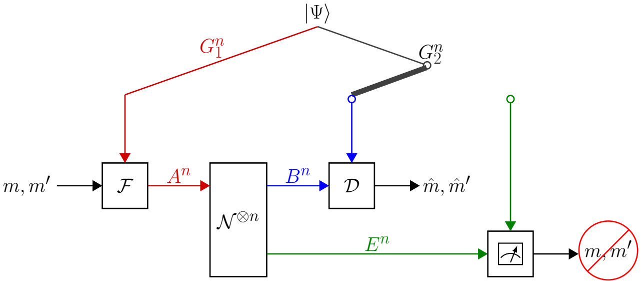
- Eve intercepts the entangled resource



Coding with Unreliable Assistance (Cont.)

Communication Scheme (1)

Alice chooses two messages, m and m', with rates R and R'.



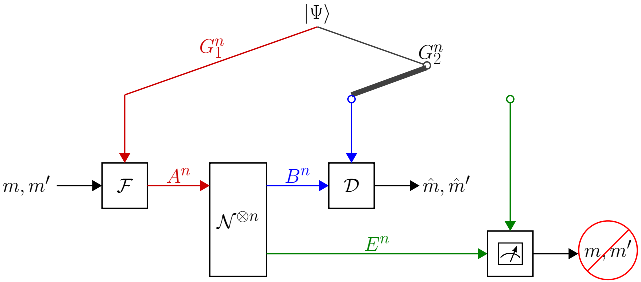
Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Communication Scheme (2)

Input: Alice prepares $\rho_{A^n}^{m,m'} = \mathcal{F}^{m,m'}(\Psi_{G_1})$, and transmits A^n.

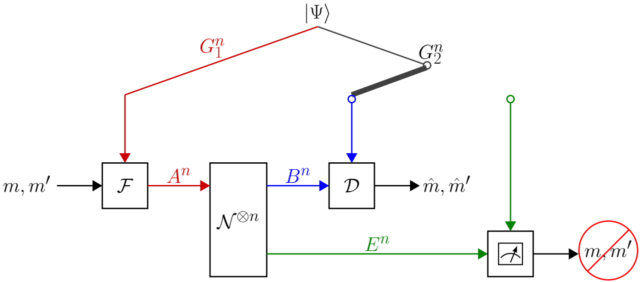
Output: Bob and Eve receive B^n, E^n respectively.



Coding with Unreliable Assistance (Cont.)

Decoding with Entanglement Assistance

If Bob has the EA, he performs a measurement $\mathcal{D}$ to estimate m, m'.

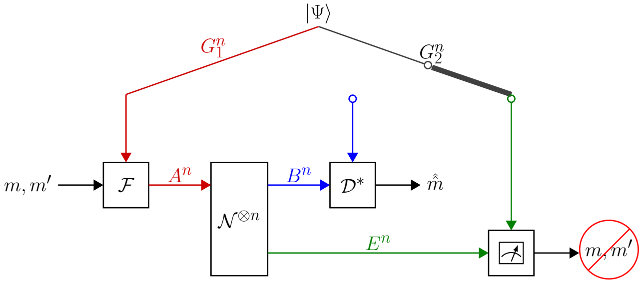


Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Decoding without Assistance

If Eve has sabotaged the entanglement assistance, Bob performs a measurement $\mathcal{D}^*$ to estimate *m* alone.

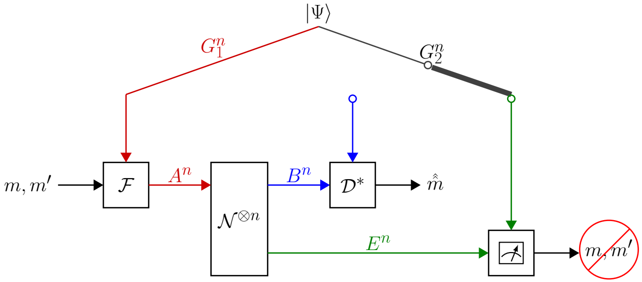


Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Decoding without Assistance

If Eve has sabotaged the entanglement assistance, Bob performs a measurement $\mathcal{D}^*$ to estimate m alone. **Nevertheless, secrecy needs to be maintained!**



Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Capacity Region

- (R, R') is achievable with unreliable entanglement assistance under interception if there exists a sequence of $(2^{nR}, 2^{nR'}, n)$ codes such that

$$\max_{m,m'} \Pr\left(\text{error}|m, m', \text{Scenario 1}\right), \Pr\left(\text{error}|m, m', \text{Scenario 2}\right) \to 0,$$

$$\max_{m,m'} \frac{1}{2}\left\|\rho^{m,m'}_{E^n G_2^n} - \theta_{E^n G_2^n}\right\|_1 \to 0$$

as $n \to \infty$.
Indistinguishability includes the entangled resource!

- The capacity region $\mathcal{C}_{\text{int}}(\mathcal{N})$ is the closure of the set of achievable rate pairs.

Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Capacity Region

- (R, R') is achievable with unreliable entanglement assistance under interception if there exists a sequence of $(2^{nR}, 2^{nR'}, n)$ codes such that

$$\max_{m,m'} \Pr\left(\text{error}|m, m', \text{Scenario 1}\right),\ \Pr\left(\text{error}|m, m', \text{Scenario 2}\right) \to 0\,,$$

$$\max_{m,m'} \frac{1}{2}\left\|\rho^{m,m'}_{E^n G_2^n} - \theta_{E^n G_2^n}\right\|_1 \to 0$$

as $n \to \infty$.
Indistinguishability includes the entangled resource!

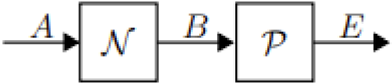
- The capacity region $\mathcal{C}_{\text{int}}(\mathcal{N})$ is the closure of the set of achievable rate pairs.

Degraded Channels

Definition

A quantum wiretap channel $\mathcal{N}_{A\to BE}$ is called **degraded** if there exists $\mathcal{P}_{B\to E}$ such that

$$\overline{\mathcal{N}}_{A\to E} = \mathcal{P}_{B\to E} \circ \mathcal{N}_{A\to B}$$



Main Result - Interception

TECHNION | Helen Diller Quantum Center

Let $\mathcal{N}_{A\to BE}$ be a wiretap quantum channel. Define

$$\mathcal{R}_{\text{int}}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : R \leq & [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ R' \leq & [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\}$$

where the union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1G_2}$, and quantum encoding channels $\mathcal{F}^{(x)}_{G_1\to A}$, with

$$\rho_{XG_2A} = \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes (\text{id}\otimes\mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_1G_2})\,,$$

$$\rho_{XG_2BE} = (\text{id}\otimes\mathcal{N}_{A\to BE})(\rho_{XG_2A})\,.$$

Note: The bound on the guaranteed rate includes the entanglement resource!

Main Result - Interception

Let $\mathcal{N}_{A\to BE}$ be a wiretap quantum channel. Define

$$\mathcal{R}_{\text{int}}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : R \leq & [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ R' \leq & [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\}$$

where the union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1G_2}$, and quantum encoding channels $\mathcal{F}^{(x)}_{G_1\to A}$, with

$$\rho_{XG_2A} = \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes (\text{id} \otimes \mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_1G_2}),$$

$$\rho_{XG_2BE} = (\text{id} \otimes \mathcal{N}_{A\to BE})(\rho_{XG_2A}).$$

Note: The bound on the guaranteed rate includes the entanglement resource!

Main Result - Interception (Cont.)

Theorem 1

The region $\mathcal{R}_{\text{int}}(\mathcal{N})$ is achievable with unreliable entanglement assistance and semantic security under *interception*. That is, the capacity region is bounded by

$$\mathcal{C}_{\text{int}}(\mathcal{N}) \supseteq \mathcal{R}_{\text{int}}(\mathcal{N})$$

Multi-Letter Formula

TECHNION | Helen Diller Quantum Center

Theorem 2

Let $\mathcal{N}_{A\to BE}$ be a **degraded** quantum wiretap channel. The capacity region with unreliable entanglement assistance and semantic security under interception satisfies

$$\mathcal{C}_{\text{int}}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{int}}(\mathcal{N}^{\otimes n})$$

- In the standard settings there is a single-letter formula for the degraded wiretap channels.
- Here, the analysis is more challenging, because of the term $I(X;EG_2)$.

Multi-Letter Formula

Theorem 2

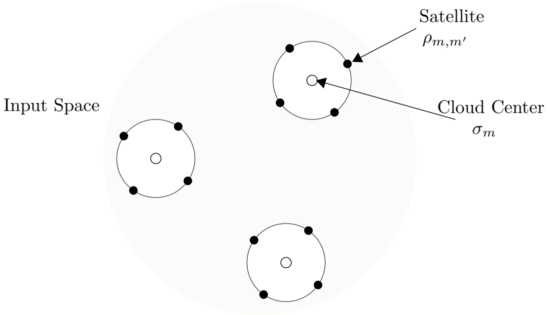
Let $\mathcal{N}_{A\to BE}$ be a **degraded** quantum wiretap channel. The capacity region with unreliable entanglement assistance and semantic security under interception satisfies

$$\mathcal{C}_{\text{int}}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{int}}(\mathcal{N}^{\otimes n})$$

- In the standard settings there is a single-letter formula for the degraded wiretap channels.
- Here, the analysis is more challenging, because of the term $I(X; E G_2)$.

Achievability

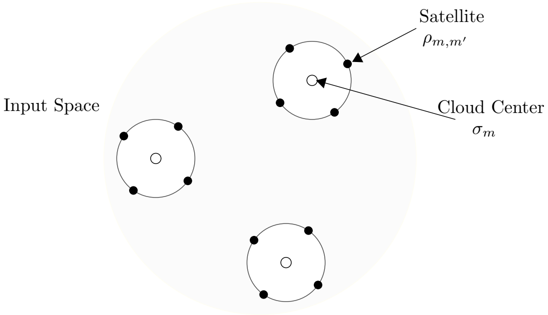
- The coding scheme is based on a quantum version of “Superposition Coding":



- To achieve secrecy, we insert local randomness elements in the encoding of each message in order to confuse Eve.

Achievability

- The coding scheme is based on a quantum version of “Superposition Coding":



- To achieve secrecy, we insert local randomness elements in the encoding of each message in order to confuse Eve.

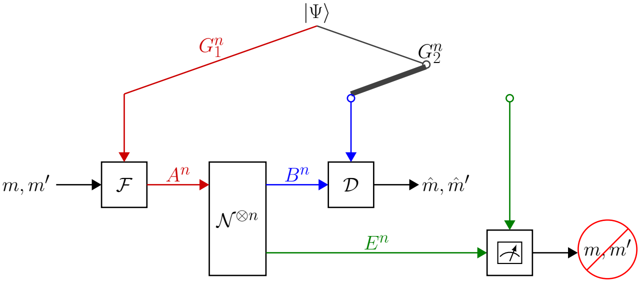
Passive Model:
Definitions and Results

Communication with Passive Eve

TECHNION | Helen Diller Quantum Center

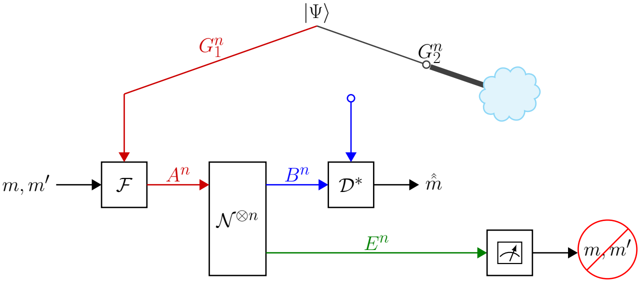
There are two scenarios:

- Optimistic Scenario: Bob receives the entanglement assistance



Communication with Passive Eve (Cont.)

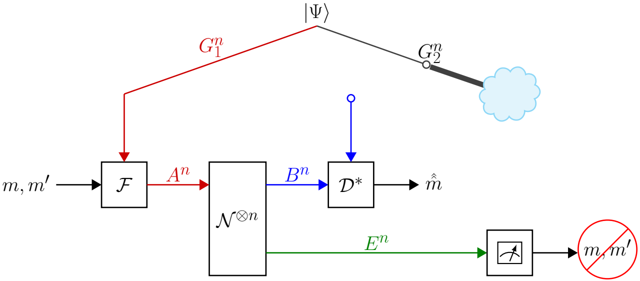
- Pessimistic Scenario: The assistance is lost to the environment.



- The coding scheme is similar to the one used in the interception model.

Communication with Passive Eve (Cont.)

- Pessimistic Scenario: The assistance is lost to the environment.



- The coding scheme is similar to the one used in the interception model.

Main Result - Passive Eve

Let $\mathcal{N}_{A\to BE}$ be a wiretap quantum channel. Define

$$\mathcal{R}_{\text{passive}}(\mathcal{N}) \equiv \bigcup_{p_X, \varphi_{G_1 G_2}, \mathcal{F}^{(x)}} \left\{ (R, R') \; : \; \begin{array}{rl} R \leq & [I(X;B)_\omega - I(X;E)_\omega]_+ \\ R' \leq & I(G_2; B|X)_\omega \end{array} \right\}$$

- Notice that as Eve is passive, the first bound no longer includes the entangled resource G_2.
- Since Eve cannot intercept the assistance, Alice and Bob can generate a secret key and use one-time padding. Therefore, security is assured, and the term for R' does not include Eve's system.

Main Result - Passive Eve

TECHNION | Helen Diller Quantum Center

Let $\mathcal{N}_{A\to BE}$ be a wiretap quantum channel. Define

$$\mathcal{R}_{\text{passive}}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ (R,R') \,:\, \begin{array}{rl} R \leq & [I(X;B)_\omega - I(X;E)_\omega]_+ \\ R' \leq & I(G_2;B|X)_\omega \end{array} \right\}$$

- Notice that as Eve is passive, the first bound no longer includes the entangled resource G_2.
- Since Eve cannot intercept the assistance, Alice and Bob can generate a secret key and use one-time padding. Therefore, security is assured, and the term for R' does not include Eve's system.

Main Result - Passive Eve (Cont.)

TECHNION | Helen Diller Quantum Center

Theorem 3

Let $\mathcal{N}_{A\to BE}$ be a general quantum wiretap channel. the capacity region with unreliable entanglement assistance and a passive eavesdropper satisfies

$$\mathcal{C}_{\text{passive}}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{passive}}(\mathcal{N}^{\otimes n})$$

Proof Outline

Achievability Proof Outline

- Generate $2^{n(R+R_0)}$ independent sequences $x^n(m,k)$, i.i.d. $\sim p_X$, for $m \in \{1,...,2^{nR}\}$, $k \in \{1,...,2^{nR_0}\}$.
- Set the 'superdense coding unitary' $U(\gamma|x^n)$, using $2^{n(R'+R_0')}$ conditionally independent sequences,

$$\{\gamma(m',k'|x^n(m,k)\}_{m'\in[1:2^{nR'}],\,k'\in[1:2^{nR_0'}]}$$

Achievability Proof Outline (Cont.)

- Suppose that Alice and Bob would like to share $|\phi_{G_1 G_2}\rangle^{\otimes n}$.
- Alice would like to send the message pair (m, m').
- The encoder generates local randomness elements, k and k', uniformly at random.
- Apply $F^{(x^n)}_{G_1^n \to A^n}$ and $U(\gamma)$, with $x^n = x^n(m,k)$ and $\gamma \equiv \gamma(m', k' | x^n)$ on G_1^n (Alice's resource).

⋆ Message-average analyses are based on the quantum packing lemma (error) and covering lemma (security).

Achievability Proof Outline (Cont.)

To show the maximal error/security criteria, we modify the technique of [Cai, 2004] (originally applied to classical MAC's):

- ⋆ Guaranteed message: Expurgate the worst λ fraction of messages, to get a rate of $R - \frac{1}{n}\log\left((1-\lambda)^{-1}\right)$, which tends to R as $n \to \infty$.
- ⋆ Excess message:
  - Selects a uniform "key" $L \in [1:n^2]$.
  - Choose a permutation π_L on the message set $[1:2^{nR'}]$, and encode the message pair $(m_0, m_0') = (m, \pi_L(m'))$ using the codebook $\mathscr{C}$.
  - Bob obtains an estimate, $\hat{L}$ and $(\hat{m}_0, \hat{m}_0')$, and then declares his estimation for the original messages as $\hat{m} = \hat{m}_0$ and $\hat{m}' = \pi_{\hat{L}}^{-1}(\hat{m}_0')$.

Achievability Proof Outline (Cont.)

TECHNION | Helen Diller Quantum Center

To show the maximal error/security criteria, we modify the technique of [Cai, 2004] (originally applied to classical MAC's):

- ⋆ Guaranteed message: Expurgate the worst λ fraction of messages, to get a rate of $R - \frac{1}{n}\log\left((1-\lambda)^{-1}\right)$, which tends to R as $n \to \infty$.
- ⋆ Excess message:
  - Selects a uniform “key" $L \in [1:n^2]$.
  - Choose a permutation π_L on the message set $[1:2^{nR'}]$, and encode the message pair $(m_0, m_0') = (m, \pi_L(m'))$ using the codebook $\mathscr{C}$.
  - Bob obtains an estimate, $\hat{L}$ and $(\hat{m}_0, \hat{m}_0')$, and then declares his estimation for the original messages as $\hat{m} = \hat{m}_0$ and $\hat{m}' = \pi_{\hat{L}}^{-1}(\hat{m}_0')$.

Achievability Proof Outline (Cont.)

TECHNION | Helen Diller Quantum Center

Error Analysis:

$$\mathbb{E}\left[P_e^{(n)}(\Pi(\mathscr{C})|m,m')\right] = \sum_{\bar{m}'} \Pr\left(\Pi_{\ell'}(m') = \bar{m}'\right) P_e^{(n)}(\mathscr{C}|m,\bar{m}')$$
$$= \frac{1}{2^{nR'}} \sum_{\bar{m}'} P_e^{(n)}(\mathscr{C}|m,\bar{m}') \leq \lambda$$

Then, by the Chernoff bound,

$$\Pr\left(\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m.m') > 4\lambda\right) < e^{-\lambda n^2}$$

Since the bound is super-exponential, the maximal error probability vanishes.

Achievability Proof Outline (Cont.)

Error Analysis:

$$\mathbb{E}\left[P_e^{(n)}(\Pi(\mathscr{C})|m,m')\right] = \sum_{\bar{m}'} \Pr\left(\Pi_{\ell'}(m') = \bar{m}'\right) P_e^{(n)}(\mathscr{C}|m,\bar{m}')$$

$$= \frac{1}{2^{nR'}} \sum_{\bar{m}'} P_e^{(n)}(\mathscr{C}|m,\bar{m}') \leq \lambda$$

Then, by the Chernoff bound,

$$\Pr\left(\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m.m') > 4\lambda\right) < e^{-\lambda n^2}$$

Since the bound is super-exponential, the maximal error probability vanishes.

Example: Erasure Channel

TECHNION | Helen Diller Quantum Center

Qubit Erasure channel

$$\mathcal{N}(\rho) = (1-\epsilon)\rho + \epsilon\,|e\rangle\langle e|$$

with $\epsilon \in [0,1]$

and $|e\rangle$ is an erasure symbol orthogonal to the input space of the channel.

Theorem 4

Time division is optimal for the qubit erasure channel, for both models.

Example: Erasure Channel

Qubit Erasure channel

$$\mathcal{N}(\rho) = (1-\epsilon)\rho + \epsilon\,|e\rangle\langle e|$$

with $\epsilon \in [0,1]$

and $|e\rangle$ is an erasure symbol orthogonal to the input space of the channel.

Theorem 4

Time division is optimal for the qubit erasure channel, for both models.

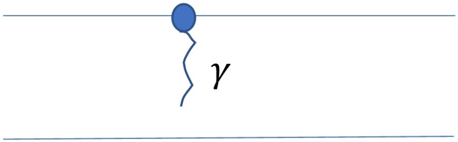
Example: Amplitude Damping Channel

Qubit Amplitude Damping channel

$$\mathcal{N}(\rho) = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger$$

with

$$K_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|\,, K_1 = \sqrt{\gamma}\,|0\rangle\langle 1| \quad , \quad \gamma \in [0,1]$$



Example: Amplitude Damping Channel (Cont.)

TECHNION | Helen Diller Quantum Center

Achievability: Quantum Superposition State

Set

$$|u_\beta\rangle \equiv \sqrt{1-\beta}\,|0\rangle \otimes |0\rangle + \sqrt{\beta}\,|1\rangle \otimes |1\rangle$$

with

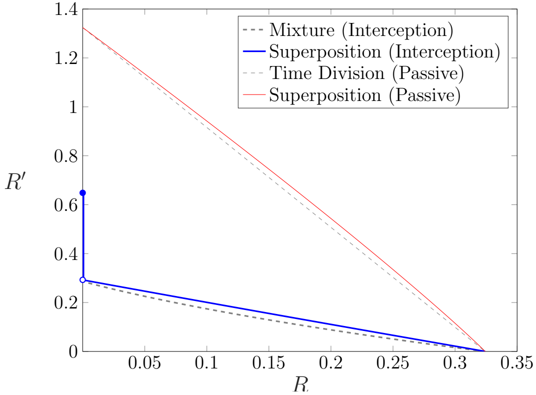
$$0 \le \beta \le p$$

and the encoding scheme:

$$p_X = (1-q, q) \quad , \quad \mathcal{F}^{(x)}(\rho) \equiv \Sigma_X^x \rho \Sigma_X^x \quad , \quad x \in \{0, 1\}$$

Example: Amplitude Damping Channel (Cont.)

Figure: Achievable region for $\gamma = 0.3$.



Summary and Concluding Remarks

TECHNION | Helen Diller Quantum Center

- We considered secure communication with unreliable entanglement assistance, in two models of unreliable assistance: Interception and Loss.
- Our model considers two extreme scenarios, i.e., the entanglement resources are either entirely available to Bob or not at all.
- While the setting resembles layered secrecy broadcast models, the analysis is much more involved, and the formulas have a different form.

Summary and Concluding Remarks

- We considered secure communication with unreliable entanglement assistance, in two models of unreliable assistance: Interception and Loss.
- Our model considers two extreme scenarios, i.e., the entanglement resources are either entirely available to Bob or not at all.
- While the setting resembles layered secrecy broadcast models, the analysis is much more involved, and the formulas have a different form.

Summary and Concluding Remarks

- We considered secure communication with unreliable entanglement assistance, in two models of unreliable assistance: Interception and Loss.
- Our model considers two extreme scenarios, i.e., the entanglement resources are either entirely available to Bob or not at all.
- While the setting resembles layered secrecy broadcast models, the analysis is much more involved, and the formulas have a different form.

Summary and Concluding Remarks (Cont.)

TECHNION | Helen Diller Quantum Center

[Lederman and Pereg, 2024] `arXiv:2401.12861` **[quant-ph]** - Interception Model

[Lederman and Pereg, 2024] `arXiv:2404.12880` **[quant-ph]** - Passive Model

Thank you