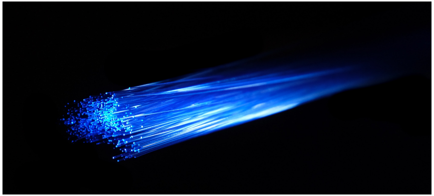
Secure Communication with Unreliable Entanglement Assistance

Meir Lederman, Uzi Pereg
ECE, Technion

International Symposium on Information Theory | July 9, 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

- 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: $\mathcal{N}_{A\to BE}$

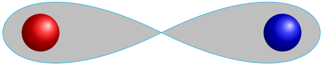
Motivation: Entanglement

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 [Bennett et al. 1999] [Hao et al. 2021]
- . . .

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



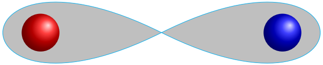
Motivation: Entanglement

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 [Bennett et al. 1999] [Hao et al. 2021]
- . . .

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

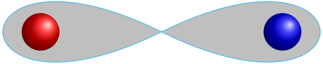


Motivation: Entanglement

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** [Bennett et al. 1999] [Hao et al. 2021]
- ...

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



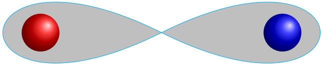
Motivation: Entanglement

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 [Bennett et al. 1999] [Hao et al. 2021]
- . . .

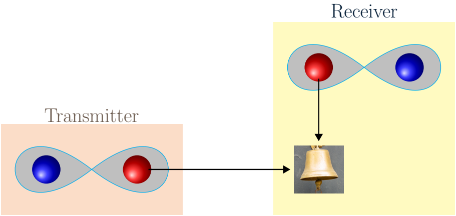
Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.



Motivation: Entanglement (Cont.)

TECHNION | Helen Diller Quantum Center

- 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, we 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, Deppe and Boche, 2023]
- **In our setting, assistance is unreliable as Eve may steal the entanglement resource intended for Bob.**

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, we 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, Deppe and Boche, 2023]

- In our setting, assistance is unreliable as Eve may steal the entanglement resource intended for Bob.

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, we 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, Deppe and Boche, 2023]
- **In our setting, assistance is unreliable as Eve may steal the entanglement resource intended for Bob.**

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) assisted 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) assisted capacity of a noiseless bit-pipe is

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

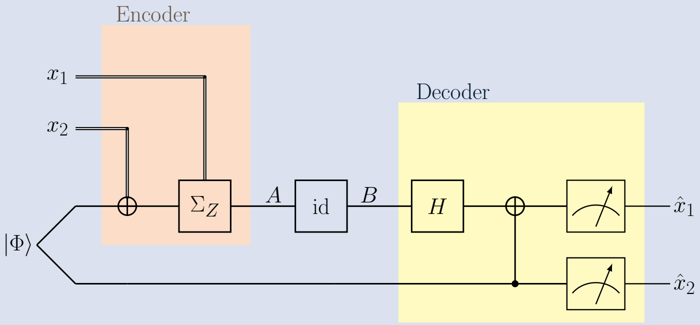
Theorem

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

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

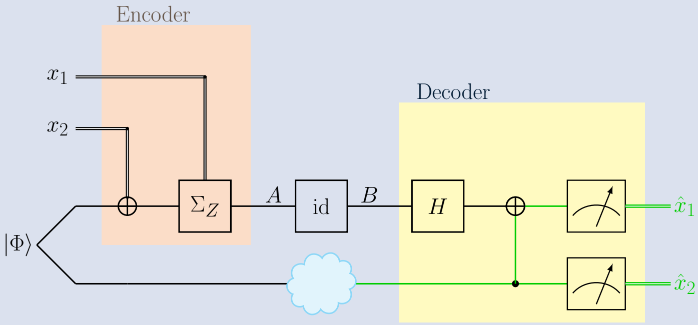
Fundamental Problem:
Noiseless Channel + EA

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.)

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.)

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.)

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.)

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.

Our Work

- In this work we deal with the case of a noisy channel **with secrecy**
- In this model, the entangled resource is unreliable since Eve may intercept it

Main Contributions

- An achievable secrecy rate region for general quantum wiretap channels.
- A multi-letter secrecy capacity formula for the special class of degraded channels.

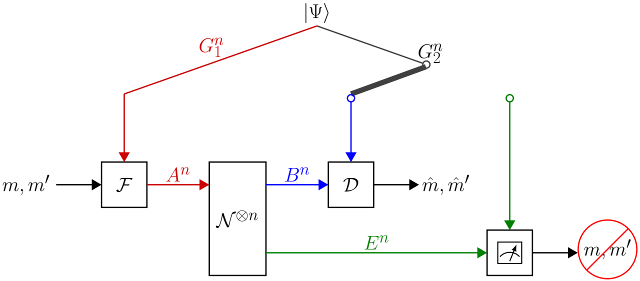
Main Contributions

- We observe that in general, time division is not necessarily possible under interception.
- For the Erasure Channel, classical randomization (mixture) achieves the time division region, and it is optimal.
- For the Amplitude Damping Channel, classical randomization is strictly sub-optimal.

Communication with Interception

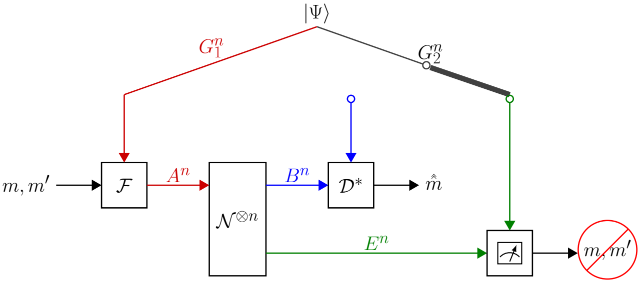
There are two scenarios:

- Bob receives the entanglement assistance



Communication with Interception (Cont.)

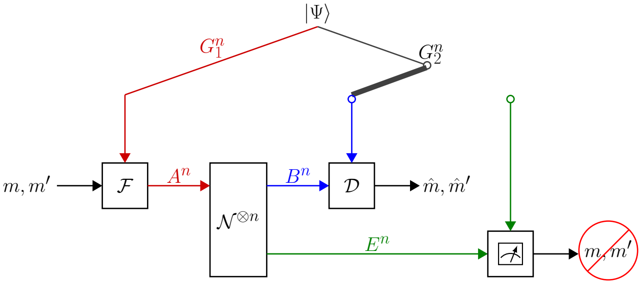
- Eve intercepts the entangled resource



Coding with Unreliable Assistance (Cont.)

Communication Scheme (1)

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

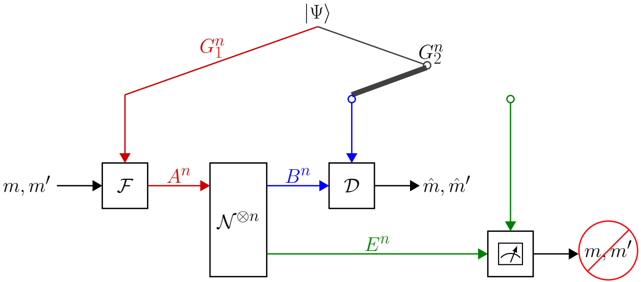


Coding with Unreliable Assistance (Cont.)

Communication Scheme (2)

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

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

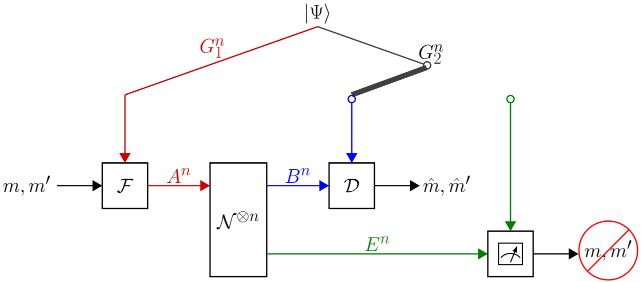


Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Decoding with Entanglement Assistance

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

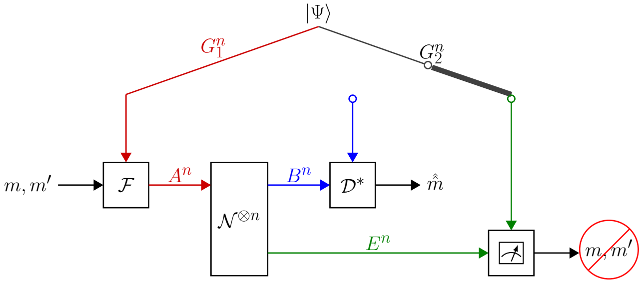


Coding with Unreliable Assistance (Cont.)

TECHNION | Helen Diller Quantum Center

Decoding without Assistance

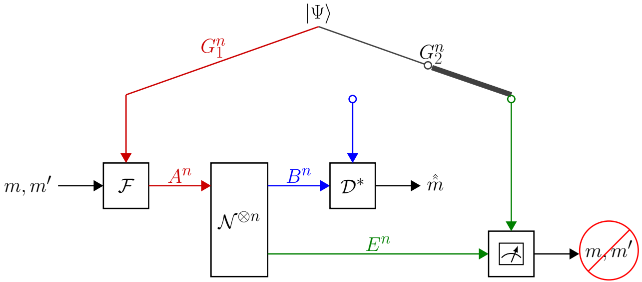
If Eve has sabotaged the entanglement assistance, Bob performs a measurement $\mathcal{D}^*$ to estimate *m* alone.



Coding with Unreliable Assistance (Cont.)

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.)

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 the error probabilities and the leakage (with and without assistance) tend to zero as $n \to \infty$.
- The capacity region $\mathcal{C}_{\text{S-EA}^*}(\mathcal{N})$ 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 the error probabilities and the leakage (with and without assistance) tend to zero as $n \to \infty$.
- The capacity region $\mathcal{C}_{\text{S-EA}^*}(\mathcal{N})$ is the closure of the set of achievable rate pairs.

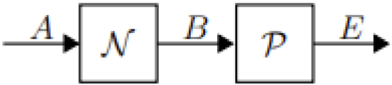
Degraded Channels

TECHNION | Helen Diller Quantum Center

Definition

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

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



Main Result

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

$$\mathcal{R}_{\text{S-EA}^*}(\mathcal{N}) \equiv \bigcup_{p_X, \varphi_{G_1 G_2}, \mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R, R') \ : \ R \leq & [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ R' \leq & [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\}$$

where the union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1 G_2}$, and quantum encoding channels $\mathcal{F}^{(x)}_{G_1\to A}$, with

$$\rho_{XG_2A} = \sum_{x\in\mathcal{X}} p_X(x)\, |x\rangle\langle x| \otimes (\text{id} \otimes \mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_1 G_2}),$$

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

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

Main Result

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

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

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 (Cont.)

Theorem

The region $\mathcal{R}_{\text{S-EA}^*}(\mathcal{N})$ is an achievable secrecy rate region with unreliable entanglement assistance. That is, the secrecy capacity region with unreliable entanglement assistance is bounded by

$$\mathcal{C}_{\text{S-EA}^*}(\mathcal{N}) \supseteq \mathcal{R}_{\text{S-EA}^*}(\mathcal{N})$$

Multi-Letter Formula

TECHNION | Helen Diller Quantum Center

Theorem

Let $\mathcal{N}_{A\to BE}$ be a **degraded** quantum wiretap channel. The unreliable entanglement assisted secrecy capacity region satisfies

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

- 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

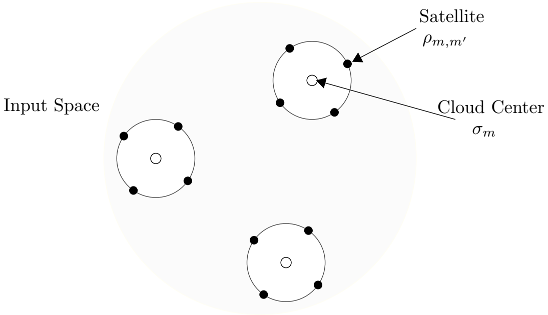
Let $\mathcal{N}_{A\to BE}$ be a **degraded** quantum wiretap channel. The unreliable entanglement assisted secrecy capacity region satisfies

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

- 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 $I(X;EG_2)$.

Achievability

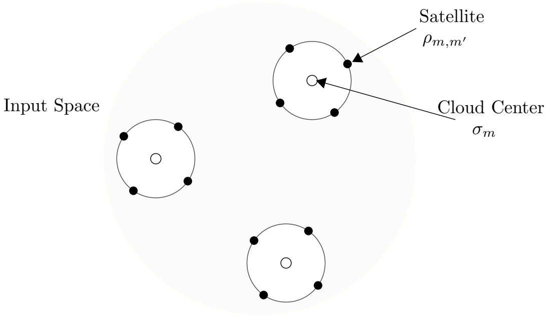
- based on a quantum version of “Superposition Coding":



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

Achievability

- 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

Example: Amplitude Damping Channel

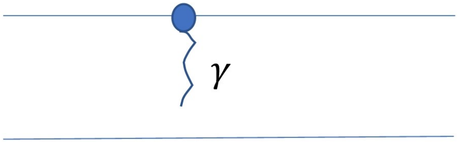
Technion | Helen Diller Quantum Center

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

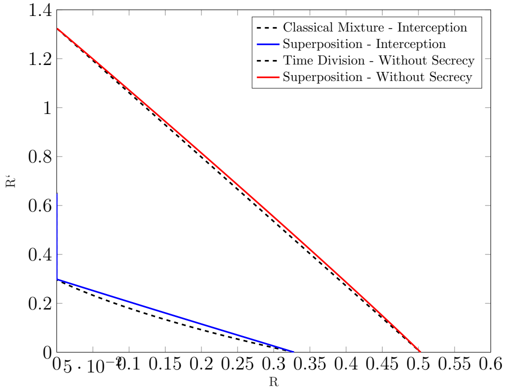
$$0 \leq \beta \leq p$$

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

- We considered secure communication with unreliable entanglement assistance where the adversary may intercept the entangled resource.
- 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 where the adversary may intercept the entangled resource.
- 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 where the adversary may intercept the entangled resource.
- 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

- Semantic Security and Maximal Error Criterion, Passive Model

Passive Model

A model where Eve is passive and cannot intercept the assistance. In this model, the assistance is unreliable because it may get lost to the environment.

[Lederman and Pereg, 2024]
`arXiv:2404.12880` **[quant-ph]** - submitted to ITW

Thank you