Entanglement Assisted Covert Communication Over Qubit Depolarizing Channel

Elyakim Zlotnick[1], Boulat Bash[2], and **Uzi Pereg**[1]

[1]ECE Department, Technion

[2]ECE Department, University of Arizona

TECHNION | Helen Diller Quantum Center

Motivation

- Privacy and confidentiality are critical in communication.
- Traditional security requirement: Prevent an eavesdropper from recovering information.

Motivation

- Privacy and confidentiality are critical in communication.
- Traditional security requirement: Prevent an eavesdropper from recovering information.
- **Covert Communication**: Not only the transmitted information kept secret, but also the transmission itself.

Motivation

- Privacy and confidentiality are critical in communication.
- Traditional security requirement: Prevent an eavesdropper from recovering information.
- **Covert Communication**: Not only the transmitted information kept secret, but also the transmission itself.
  - Transmission rate is zero.

Motivation

- Privacy and confidentiality are critical in communication.
- Traditional security requirement: Prevent an eavesdropper from recovering information.
- **Covert Communication**: Not only the transmitted information kept secret, but also the transmission itself.
  - Transmission rate is zero.
  - Instead of sending a message of $n \cdot R$ bits, Alice sends a sublinear message of $f(n) \cdot L$ bits.

TECHNION | Helen Diller Quantum Center

Background: Covert Communication

- Without entanglement, # information bits is $O(\sqrt{n})$ (SRL-square root law):
  - classical communication [Bash et al. 2013, Bloch 2016]
  - continuous variable (bosonic channel) [Bash et al. 2015]
  - discrete variable (classical-quatum) [Sheikholeslami et al. 2016] [Bullock et al. 2023]

Background: Covert Communication

- Without entanglement, # information bits is $O(\sqrt{n})$ (SRL-square root law):
  - classical communication [Bash et al. 2013, Bloch 2016]
  - continuous variable (bosonic channel) [Bash et al. 2015]
  - discrete variable (classical-quatum) [Sheikholeslami et al. 2016] [Bullock et al. 2023]
- Given pre-shared entanglement, # information bits is $O(\sqrt{n}\log(n))$:
  - Continuous variable (bosonic channel) [Gagatsos et al. 2020]
  - **Discrete variable?**

TECHNION | Helen Diller Quantum Center

Background: Covert Communication

- Without entanglement, # information bits is $O(\sqrt{n})$ (SRL-square root law):
  - classical communication [Bash et al. 2013, Bloch 2016]
  - continuous variable (bosonic channel) [Bash et al. 2015]
  - discrete variable (classical-quatum) [Sheikholeslami et al. 2016] [Bullock et al. 2023]
- Given pre-shared entanglement, # information bits is $O(\sqrt{n}\log(n))$:
  - Continuous variable (bosonic channel) [Gagatsos et al. 2020]
  - **Discrete variable?** Yes!

TECHNION | Helen Diller Quantum Center

Main Contributions

We consider qubit depolarizing channels:

- Three scenarios
  1) adversary can access the entire environment
  2) "half" the environment
  3) other "half"
- Logarithmic factor is not reserved for continuous-variable channels
- Interpretation: Energy-constrained transmission

Outline

- Definitions and Related Work
- Main Results
- Discussion and Interpretation

Information Moments and Derivative

Information Moments

- First moment: Divergence

$$D(\rho||\sigma) = \mathrm{Tr}\left[\rho\left(\log(\rho) - \log(\sigma)\right)\right]$$

TECHNION | Helen Diller Quantum Center

Information Moments and Derivative

Information Moments

- First moment: Divergence

$$D(\rho||\sigma) = \mathrm{Tr}\left[\rho\left(\log(\rho) - \log(\sigma)\right)\right]$$

- Second moment:

$$V(\rho||\sigma) = \mathrm{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^2]$$

Information Moments and Derivative

Information Moments

- First moment: Divergence

$$D(\rho||\sigma) = \mathrm{Tr}\left[\rho\left(\log(\rho) - \log(\sigma)\right)\right]$$

- Second moment:

$$V(\rho||\sigma) = \mathrm{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^2]$$

- Fourth moment:

$$Q(\rho||\sigma) = \mathrm{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^4]$$

TECHNION | Helen Diller Quantum Center

Information Moments and Derivative (Cont.)

Information Derivative (η-divergence)

For a spectral decomposition $\sigma = \sum_i \lambda_i P_i$, let

$$\eta(\rho||\sigma) = \sum_{i \neq j} \frac{\log(\lambda_i) - \log(\lambda_j)}{\lambda_i - \lambda_j} \operatorname{Tr}[(\rho - \sigma)P_i(\rho - \sigma)P_j] + \sum_i \frac{1}{\lambda_i} \operatorname{Tr}[(\rho - \sigma)P_i(\rho - \sigma)P_i]$$

[Tahmasbi and Bloch 2021]

TECHNION | Helen Diller Quantum Center

Isometric Extension

Quantum Channel

A quantum channel $\mathcal{N}_{A\to B}$ is a completely-positive trace-preserving (CPTP) map.

TECHNION | Helen Diller Quantum Center

Isometric Extension

Quantum Channel

A quantum channel $\mathcal{N}_{A\to B}$ is a completely-positive trace-preserving (CPTP) map.

Stinespring Dilation

Every quantum channel has an isometric extension,

$$\mathcal{V}_{A\to BE}(\rho) = V\rho V^\dagger$$

where V is an isometry that maps from $\mathcal{H}_A$ to $\mathcal{H}_B \otimes \mathcal{H}_E$.

A, B and E are associated with Alice, Bob and the environment, respectively.

Study Case

Qubit Depolarizing Channel

Bob receives qubit state w.p. $1-q$, and a completely mixed state w.p. q,

$$\begin{aligned}\mathcal{N}_{A\to B}(\rho) &= (1-q)\rho + q\frac{\mathbb{1}}{2} \\ &= \left(1-\frac{3q}{4}\right)\rho + \frac{q}{4}\left(X\rho X + Y\rho Y + Z\rho Z\right)\end{aligned}$$

TECHNION | Helen Diller Quantum Center

Study Case

Qubit Depolarizing Channel

Bob receives qubit state w.p. $1-q$, and a completely mixed state w.p. q,

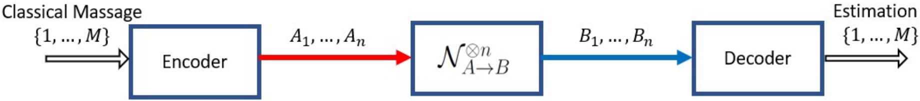
$$\mathcal{N}_{A\to B}(\rho) = (1-q)\rho + q\frac{\mathbb{1}}{2}$$
$$= \left(1 - \frac{3q}{4}\right)\rho + \frac{q}{4}\left(X\rho X + Y\rho Y + Z\rho Z\right)$$

Canonical Stinespring dilation

$$V \equiv \sqrt{1-\frac{3q}{4}}\,\mathbb{1}\otimes|1\rangle + \sqrt{\frac{q}{4}}X\otimes|2\rangle + \sqrt{\frac{q}{4}}Y\otimes|3\rangle + \sqrt{\frac{q}{4}}Z\otimes|4\rangle$$

TECHNION | Helen Diller Quantum Center

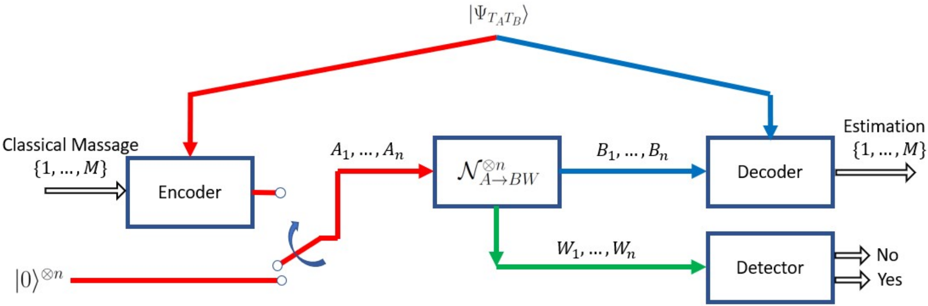
Coding for Covert Communication



- $\log(M)$ — #information bits, over n channel uses.
- In covert communication, $\log(M)$ is sub-linear
- Transmission rate: $R = \frac{\log(M)}{n} \to 0$

Coding for Covert Communication (Cont.)

- Entanglement assistance: Alice and Bob share $|\Psi_{T_A T_B}\rangle$ a priori.
- Detection: Willie performs hypothesis testing to determine whether Alice has transmitted information or not.



Coding for Covert Communication

An (M, n, ϵ, δ) code for covert communication with entanglement assistance satisfies two requirements.

1) **Low probability of error:** Bob decodes with

$$\Pr(\text{error}) \leq \epsilon$$

TECHNION | Helen Diller Quantum Center

Coding for Covert Communication

An (M, n, ϵ, δ) code for covert communication with entanglement assistance satisfies two requirements.

1) **Low probability of error:** Bob decodes with

$$\Pr(\text{error}) \leq \epsilon$$

2) **Covertness:** Willie has a bad detection performance

$$D(\rho_{W^n} || \omega_0^{\otimes n}) \leq \delta$$

where ρ_{W^n} is Willie's average state, and $\omega_0 \equiv \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$.
This guarantees $\Pr(\text{miss}) + \Pr(\text{False alarm}) \approx \frac{1}{2}$.

TECHNION | Helen Diller Quantum Center

Coding for Covert Communication (Cont.)

Covert Rate

The growth is characterized by the covert "rate",

$$L = \frac{\log(M)}{\sqrt{n\delta}\log(n)}.$$

A covert rate L is achievable if $\forall\ \epsilon, \delta > 0\ \exists\ n \geq n_0(L, \epsilon, \delta)$, there exists an $(M = 2^{L\sqrt{n\delta}\log(n)}, n, \epsilon, \delta)$ code for covert communication with entanglement assistance.

Covert Capacity

The entanglement-assisted **covert capacity** is the supremum of achievable rates.

TECHNION | Helen Diller Quantum Center

Discrete vs. Continuous-Variable Channels

- The scale of $O(\sqrt{n}\log(n))$ has already been observed in a continuous-variable model, i.e., the bosonic Gaussian channel [Gagatsos et al. 2020].

Discrete vs. Continuous-Variable Channels

- The scale of $O(\sqrt{n}\log(n))$ has already been observed in a continuous-variable model, i.e., the bosonic Gaussian channel [Gagatsos et al. 2020].
- Until now, it has remained unclear whether this performance boost can also be achieved in finite dimensions.

TECHNION | Helen Diller Quantum Center

Discrete vs. Continuous-Variable Channels

- The scale of $O(\sqrt{n}\log(n))$ has already been observed in a continuous-variable model, i.e., the bosonic Gaussian channel [Gagatsos et al. 2020].
- Until now, it has remained unclear whether this performance boost can also be achieved in finite dimensions.
- In some communication settings, the coding scale is larger for continuous-variable channels.

Discrete vs. Continuous-Variable Channels

- The scale of $O(\sqrt{n}\log(n))$ has already been observed in a continuous-variable model, i.e., the bosonic Gaussian channel [Gagatsos et al. 2020].
- Until now, it has remained unclear whether this performance boost can also be achieved in finite dimensions.
- In some communication settings, the coding scale is larger for continuous-variable channels.
- For example, in deterministic identification, the code size is super-exponential for Gaussian channels but limited to an exponential scale for finite-dimensional channels [Salariseddigh et al. 2021].

TECHNION | Helen Diller Quantum Center

Depolarizing Channel

The depolarizing channel has a Stinespring dilation $\mathcal{V}_{A\to BE_1E_2}(\rho_A) = V\rho_A V^\dagger$,

$$V \equiv \sqrt{1-\frac{3q}{4}}\mathbb{1}\otimes|00\rangle + \sqrt{\frac{q}{4}}X\otimes|01\rangle + \sqrt{\frac{q}{4}}Y\otimes|11\rangle + \sqrt{\frac{q}{4}}Z\otimes|10\rangle \ .$$

- Three qubits at the output of the channel. For example, given $|\phi_A\rangle = |+\rangle$,

$$\begin{aligned} |\psi_{BE_1E_2}\rangle &= V|+\rangle \\ &= \sqrt{1-\frac{3q}{4}}|+\rangle|00\rangle + \sqrt{\frac{q}{4}}|+\rangle|01\rangle \\ &\quad - i\sqrt{\frac{q}{4}}|-\rangle|11\rangle + \sqrt{\frac{q}{4}}|-\rangle|10\rangle \end{aligned}$$

TECHNION | Helen Diller Quantum Center

Depolarizing Channel

The depolarizing channel has a Stinespring dilation $\mathcal{V}_{A\to BE_1E_2}(\rho_A) = V\rho_A V^\dagger$,

$$V \equiv \sqrt{1-\frac{3q}{4}}\mathbb{1}\otimes|00\rangle + \sqrt{\frac{q}{4}}X\otimes|01\rangle + \sqrt{\frac{q}{4}}Y\otimes|11\rangle + \sqrt{\frac{q}{4}}Z\otimes|10\rangle \ .$$

- Three qubits at the output of the channel. For example, given $|\phi_A\rangle = |+\rangle$,

$$\begin{aligned} |\psi_{BE_1E_2}\rangle &= V|+\rangle \\ &= \sqrt{1-\frac{3q}{4}}|+\rangle|00\rangle + \sqrt{\frac{q}{4}}|+\rangle|01\rangle \\ &\quad - i\sqrt{\frac{q}{4}}|-\rangle|11\rangle + \sqrt{\frac{q}{4}}|-\rangle|10\rangle \end{aligned}$$

Intuitively, (E_1, E_2) store a "flag" that indicates which Pauli error occurred.

TECHNION | Helen Diller Quantum Center

Depolarizing Channel

The depolarizing channel has a Stinespring dilation $\mathcal{V}_{A\to BE_1E_2}(\rho_A) = V\rho_A V^\dagger$,

$$V \equiv \sqrt{1-\frac{3q}{4}}\mathbb{1}\otimes|00\rangle + \sqrt{\frac{q}{4}}X\otimes|01\rangle + \sqrt{\frac{q}{4}}Y\otimes|11\rangle + \sqrt{\frac{q}{4}}Z\otimes|10\rangle \ .$$

- Three qubits at the output of the channel. For example, given $|\phi_A\rangle = |+\rangle$,

$$\begin{aligned}|\psi_{BE_1E_2}\rangle &= V|+\rangle \\ &= \sqrt{1-\frac{3q}{4}}|+\rangle|00\rangle + \sqrt{\frac{q}{4}}|+\rangle|01\rangle \\ &\quad - i\sqrt{\frac{q}{4}}|-\rangle|11\rangle + \sqrt{\frac{q}{4}}|-\rangle|10\rangle\end{aligned}$$

  Intuitively, (E_1, E_2) store a "flag" that indicates which Pauli error occurred.

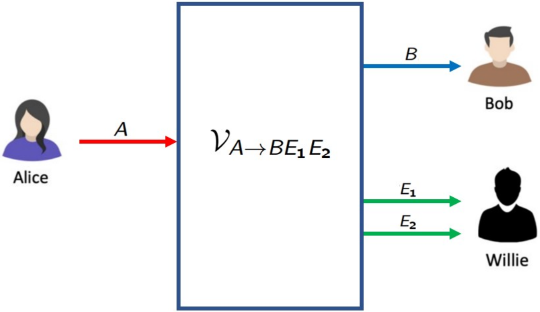
- 1st qubit belongs to Bob. 2nd and 3rd leak to the **environment**.

TECHNION | Helen Diller Quantum Center

Willie's Channel

Willie has access to (part of) the environment.
We consider three scenarios:

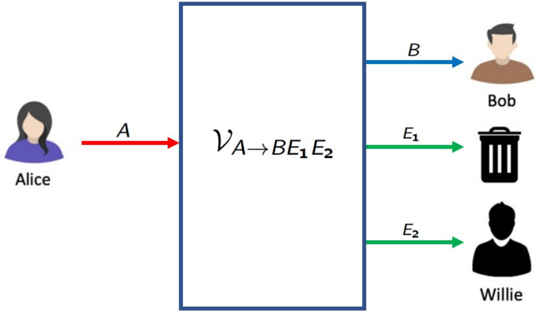
- Scenario 1: Willie receives both qubits, E_1 and E_2.
- Scenario 2: Willie receives last qubit, E_2.
- Scenario 3: Willie receives the qubit E_1.



TECHNION | Helen Diller Quantum Center

Willie has access to (part of) the environment.
We consider three scenarios:

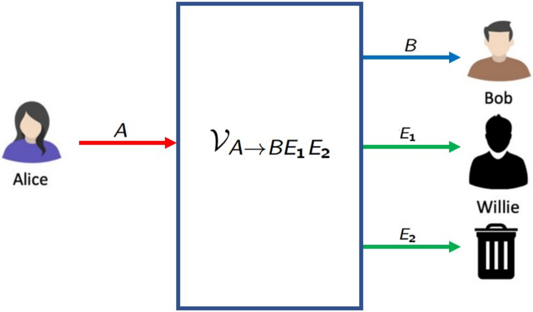
- Scenario 1: Willie receives both qubits, E_1 and E_2.
- Scenario 2: Willie receives last qubit, E_2.
- Scenario 3: Willie receives the qubit E_1.



Willie's Channel

Willie has access to (part of) the environment.
We consider three scenarios:

- Scenario 1: Willie receives both qubits, E_1 and E_2.
- Scenario 2: Willie receives last qubit, E_2.
- Scenario 3: Willie receives the qubit E_1.



TECHNION | Helen Diller Quantum Center

Outline

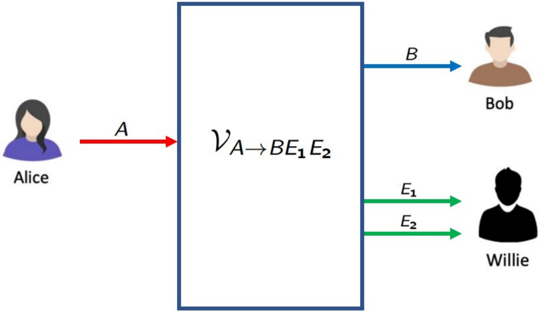
- Definitions and Related Work
- Main Results
- Discussion and Interpretation

Willie's Channel: Scenario 1

Theorem

Covert communication is impossible in Scenario 1. Hence, if $W = (E_1, E_2)$, then $C_{cov\text{-}EA}(\mathcal{N}) = 0$.

- Willie receives the entire environment
- Willie can then detect any encoding operation, because $\text{supp}(\omega_1) \not\subseteq \text{supp}(\omega_0)$, where $\omega_0 \equiv \widehat{\mathcal{N}}_{A\to W}(|0\rangle\langle 0|)$ and $\omega_1 \equiv \widehat{\mathcal{N}}_{A\to W}(|1\rangle\langle 1|)$



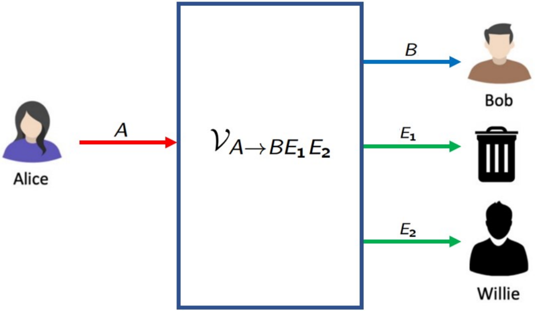
TECHNION | Helen Diller Quantum Center

Willie's Channel: Scenario 2

Theorem

Covert communication is trivial in Scenario 2. That is, Alice can communicate information as without the covertness requirement, and send $O(n)$ bits.

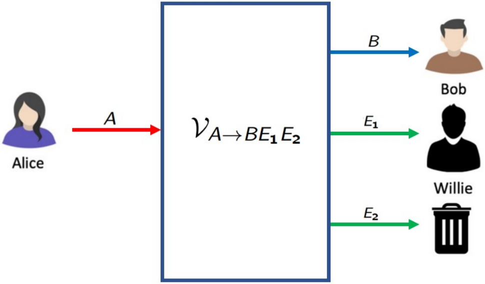
- Willie receives the second qubit.
- Willie cannot discern between the $|0\rangle$ and $|1\rangle$ inputs, as $\omega_0 = \omega_1 = (1 - \frac{q}{2})\,|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1|$



TECHNION | Helen Diller Quantum Center

Willie's Channel: Scenario 3

- Willie receives the first qubit.
- Covert communication is possible, yet not trivial.
  ($\text{supp}(\omega_1) \subseteq \text{supp}(\omega_0)$ and $\omega_0 \neq \omega_1$)



TECHNION | Helen Diller Quantum Center

Main Result

Theorem

Consider a qubit depolarizing channel as in scenario 3. The entanglement-assisted covert capacity is bounded as

$$C_{cov\text{-}EA}(\mathcal{N}) \geq \frac{4\sqrt{2}}{3} \frac{(1-q)^2}{(2-q)\sqrt{\eta(\omega_1||\omega_0)}}$$

where $\omega_0 \equiv \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ *and* $\omega_1 \equiv \mathcal{N}_{A\to W}(|1\rangle\langle 1|)$.

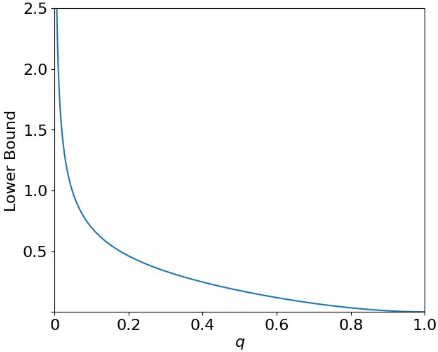
- Recall that the covert rate is defined as $L \equiv \frac{\log(M)}{\log(n)\sqrt{n\delta}}$
- Without entanglement, #information bits follows SRL, and here, the rate is defined according to the $\sqrt{n}\log(n)$ scale.

$\Rightarrow$ Covert transmission of $O(\sqrt{n}\log n)$ information bits is achievable.

TECHNION | Helen Diller Quantum Center

Main Results: Lower Bound

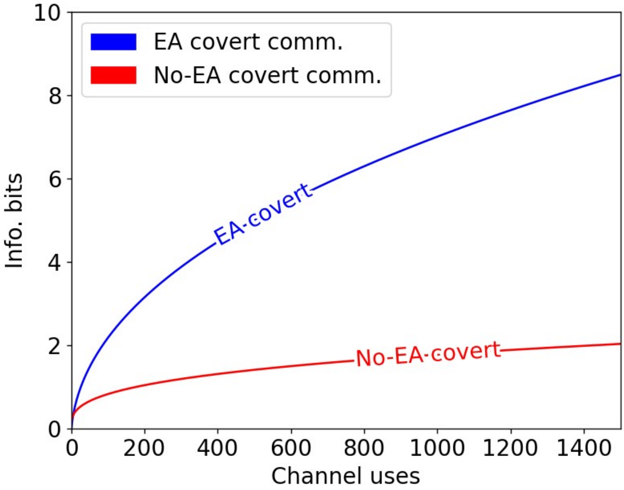
Lower bound of the covert rate $C_{\text{cov-EA}}$ as function of the noise paramtere q:



- $q \to 0$: No noise, covert communication is trivial.
- $q \to 1$: Completely noise, communication is impossible.

Main Result: Info. Bits Graph

Number of information bits for noise parameter $q = \frac{1}{2}$, and $D(\bar{\rho}_{W^n} || \omega_0^{\otimes n}) \leq 0.1$:



Outline

Interpretation: Energy Constraint

Energy Constraint

Suppose that the total energy of the input state is constrained.

- A state ρ satisfies an energy constraint E w.r.t. the Hamiltonian $\hat{\mathrm{H}} = |1\rangle\langle 1|$, if

$$\mathrm{Tr}(\hat{\mathrm{H}}\rho) \leq E$$

- The capacities with and without entanglement assistance, are given by

$$C_0(\mathcal{N}, E) = H_2\left(E * \frac{q}{2}\right) - H_2(E)$$
$$C_{\mathrm{EA}}(\mathcal{N}, E) = H_2(E) + H_2\left(E * \frac{q}{2}\right) - H(\psi_{A_1 B})$$

where $H_2(x)$ is the binary entropy function, $a * b = (1-a)b + a(1-b)$, and

$$\psi_{A_1 B} = (\mathrm{id}_{A_1} \otimes \mathcal{N}_{A\to B})\left(\sqrt{1-E}\,|00\rangle + \sqrt{E}\,|11\rangle\right)$$

Interpretation: Energy Constraint (Cont.)

For $E \ll 1$,

- Unassisted energy-constrained capacity: $C_0(\mathcal{N}, E) \sim E$
- Entanglement-assisted energy-constrained capacity: $C_{EA}(\mathcal{N}, E) \sim -E \log E$

Interpretation: Energy Constraint (Cont.)

For $E \ll 1$,

- Unassisted energy-constrained capacity: $C_0(\mathcal{N}, E) \sim E$
- Entanglement-assisted energy-constrained capacity: $C_{EA}(\mathcal{N}, E) \sim -E \log E$

The ratio between the assisted and unassisted capacities scales as

$$\frac{C_{EA}(\mathcal{N}, E)}{C_0(\mathcal{N}, E)} \sim -\log(E)$$

Interpretation: Energy Constraint (Cont.)

For $E \ll 1$,

- Unassisted energy-constrained capacity: $C_0(\mathcal{N}, E) \sim E$
- Entanglement-assisted energy-constrained capacity: $C_{EA}(\mathcal{N}, E) \sim -E \log E$

The ratio between the assisted and unassisted capacities scales as

$$\frac{C_{EA}(\mathcal{N}, E)}{C_0(\mathcal{N}, E)} \sim -\log(E)$$

Effectively, the covertness requirement imposes an energy constraint
$\Rightarrow$ Taking $E_n \sim \frac{1}{\sqrt{n}}$, the ratio becomes $O(\log(n))$.

- A similar behavior has been observed for bosonic channels with a mean photon number constraint [Guha et al. 2020] [Shi et al. 2020].

TECHNION | Helen Diller Quantum Center

Interpretation: Unfair Detection Capability

Bob's Detection Capability

The "unfair channel setting": Bob can determine that some outputs are associated with a non-zero input, while Willie cannot. Hence, Bob has an unfair advantage over Willie.

- Examples: erasure channel, amplitude-damping channel.
- Even without assistance, # information bits scales as $\sqrt{n}\log(n)$ [Bloch et al. 2016, Sheikholeslami et al. 2016]

The depolarizing channel is fair in this sense, yet entanglement assistance has a similar effect as granting Bob the capability of identifying a non-zero transmission with certainty.

TECHNION | Helen Diller Quantum Center

Conclusion

We address entanglement-assited and covert communication over depolarizing channels

- We consider different scenarios, where Willie has the entire environment, or, part of it.

TECHNION | Helen Diller Quantum Center

Conclusion

We address entanglement-assited and covert communication over depolarizing channels

- We consider different scenarios, where Willie has the entire environment, or, part of it.
- Our main contributions include:
  - ∗ Analysis of # information bits per channel uses.
  - ∗ Demonstrating that the logarithmic factor is not exclusive to continuous variable systems.
  - ∗ Interpretation of covert communication rates as energy-constrained capacities for the qubit depolarizing channel.

TECHNION | Helen Diller Quantum Center

Thank You

TECHNION | Helen Diller Quantum Center