Entanglement Assisted Covert Communication via Qubit Depolarizing Channels

Elyakim Zlotnick

ECE, Technion

Supervisor: Uzi Pereg
Joint Work with Boulat Bash

Motivation

- Privacy and secrecy are critical in communication
- **Covert Communication**: Not only the transmitted information kept secret, but also the transmission itself.
- **Information Theory**: How many bits of information can be sent for n channel uses?
- Pre-shared entanglement resources can increase performance and throughput

Covert Communication - Background

- No-entanglement, $O(\sqrt{n})$ (SRL-square root law):
  - Classical communication [Bash et al. 2013, Bloch et al. 2016]
  - Discrete variable (classical-quatum) [Sheikholeslami et al. 2016]
  - Continuous variable (Gaussian bosonic) [Bash et al. 2015]
- Entanglement, $O(\sqrt{n}\log(n))$:
  - Continuous variable (Gaussian bosonic) [Gagatsos et al. 2020]
  - **Discrete variable?**

Covert Communication - Background

- No-entanglement, $O(\sqrt{n})$ (SRL-square root law):
  - Classical communication [Bash et al. 2013, Bloch et al. 2016]
  - Discrete variable (classical-quatum) [Sheikholeslami et al. 2016]
  - Continuous variable (Gaussian bosonic) [Bash et al. 2015]
- Entanglement, $O(\sqrt{n}\log(n))$:
  - Continuous variable (Gaussian bosonic) [Gagatsos et al. 2020]
  - **Discrete variable?** Yes!

TECHNION | Helen Diller Quantum Center

Main Contributions

- We consider covert communication over qubit depolarizing channels.
- Three scenarios:
  - Willie (adversary) has all environment
  - "half" the environment
  - the other "half"
- Logarithmic factor is not reserved for continuous variable
- Interpretation: energy-constrained capacities, decoding performance

Quantum Information: Pure States

A pure quantum state $|\psi\rangle$ is a normalized vector in the Hilbert space $\mathcal{H}_A$.

Qubit

For a quantum bit (qubit),

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum Information: Pure States

A pure quantum state $|\psi\rangle$ is a normalized vector in the Hilbert space $\mathcal{H}_A$.

Qubit

For a quantum bit (qubit),

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

α and β can be complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$

TECHNION | Helen Diller Quantum Center

Quantum Information: Pure States (Cont.)

A pure bi-partite state $|\psi_{AB}\rangle$ is a normalized vector in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Two qubits

For two qubits, $|\psi_{AB}\rangle = |i\rangle \otimes |j\rangle$, or

$$|\psi_{AB}\rangle = \sum_{i,j=0,1} \alpha_{ij} |i\rangle \otimes |j\rangle \ , \ \text{with} \sum |\alpha_{ij}|^2 = 1$$

TECHNION | Helen Diller Quantum Center

A pure bi-partite state $|\psi_{AB}\rangle$ is a normalized vector in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Two qubits

For two qubits, $|\psi_{AB}\rangle = |i\rangle \otimes |j\rangle$, or

$$|\psi_{AB}\rangle = \sum_{i,j=0,1} \alpha_{ij} |i\rangle \otimes |j\rangle \ , \ \text{with} \sum |\alpha_{ij}|^2 = 1$$

Entanglement

Systems A and B are entangled if $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$

For example, $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$.

Quantum Information: Mixed States

The (mixed) state ρ_A of a quantum system A is an Hermitian, positive semidefinite, unit-trace density matrix over $\mathcal{H}_A$.

- Mixed states reflecting uncertainty about a quantum system.
- For a joint state ρ_{AB}, the density matrix of the system A is the reduced matrix $\rho_A = \mathrm{Tr}_B(\rho_{AB})$.

TECHNION | Helen Diller Quantum Center

Quantum Information: Mixed States

The (mixed) state ρ_A of a quantum system A is an Hermitian, positive semidefinite, unit-trace density matrix over $\mathcal{H}_A$.

- Mixed states reflecting uncertainty about a quantum system.
- For a joint state ρ_{AB}, the density matrix of the system A is the reduced matrix $\rho_A = \mathrm{Tr}_B(\rho_{AB})$.

Entropy

Given ρ_A, define

$$H(A)_\rho \equiv -\mathrm{Tr}(\rho_A \log \rho_A)$$

For a **Pure** system A:

$$H(A)_\rho = 0$$

TECHNION | Helen Diller Quantum Center

Quantum Information: Definitions

Useful definitions:

- Divergence (Relative entropy):

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

(if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$; and $D(\rho||\sigma) = +\infty$, otherwise.)

TECHNION | Helen Diller Quantum Center

Quantum Information: Definitions

Useful definitions:

- Divergence (Relative entropy):

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

(if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$; and $D(\rho||\sigma) = +\infty$, otherwise.)

- Second moment:

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

Quantum Information: Definitions

Useful definitions:

- Divergence (Relative entropy):

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

(if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$; and $D(\rho||\sigma) = +\infty$, otherwise.)

- Second moment:

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

- Fourth moment:

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

Quantum Information: Definitions

Useful definitions:

- Divergence (Relative entropy):

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

(if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$; and $D(\rho||\sigma) = +\infty$, otherwise.)

- Second moment:

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

- Fourth moment:

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

- η-divergence: For a spectral decomposition $\sigma = \sum_i \lambda_i P_i$, let [Tahmasbi et al. 2021]:

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

TECHNION | Helen Diller Quantum Center

Quantum Information: Definitions (Cont.)

- Pauli Matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum Channel

Unitary Evolution - Pure State

- Evolution of a pure state is given by a unitary operator in Hilbert space $\mathcal{H}_A$:

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \qquad U^\dagger U = UU^\dagger = \mathbb{1}$$

Quantum Channel

Unitary Evolution - Pure State

- Evolution of a pure state is given by a unitary operator in Hilbert space $\mathcal{H}_A$:

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \qquad U^\dagger U = UU^\dagger = \mathbb{1}$$

Noisy Evolution - Density Matrix

- Evolution of a density matrix is given by a noisy channel $\mathcal{N}_{A\to B}$.
- A quantum noisy channel is defined as a completely-positive trace-preserving (CPTP) linear map.

$$\rho_A \xrightarrow{\mathcal{N}} \rho_B \equiv \mathrm{Tr}_E(V\rho_A V^\dagger) \qquad V \equiv V^{\mathcal{N}}_{A\to BE}$$

$$V^\dagger V = \mathbb{1}_A$$

- $V^{\mathcal{N}}_{A\to BE}$ is a linear opertor from $\mathcal{H}_A$ (Alice) to $\mathcal{H}_B \otimes \mathcal{H}_E$ (Bob and Enviroment).

Quantum Channel: Example 1

Example: "qubit flip" channel.

- Flips $|0\rangle$ into $|1\rangle$ and $|1\rangle$ into $|0\rangle$ with probability of q:

$$\mathcal{N}_{A\to B}(\rho) = (1-q)\rho + qX\rho X$$

Quantum Channel: Example 1

Example: "qubit flip" channel.

- Flips $|0\rangle$ into $|1\rangle$ and $|1\rangle$ into $|0\rangle$ with probability of q:

$$\mathcal{N}_{A\to B}(\rho) = (1-q)\rho + qX\rho X$$

- The "qubit flip" channel can be given by:

$$\mathcal{N}_{A\to B}(\rho) = \mathrm{Tr}_E(V\rho V^\dagger)$$

where $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ is an isometry defined by

$$V_{A\to BE} \equiv \sqrt{1-q}\mathbb{1} \otimes |1\rangle + \sqrt{q}X \otimes |2\rangle \ .$$

Quantum Channel: Example 2 (Study Case)

Example: qubit depolarizing channel.

- Bob receives Alice's qubit with probability $1-q$, and a completly mixed state with probability q:

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

Quantum Channel: Example 2 (Study Case)

Example: qubit depolarizing channel.

- Bob receives Alice's qubit with probability $1 - q$, and a completly mixed state with probability q:

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

- The qubit depolarizing channel can be given by:

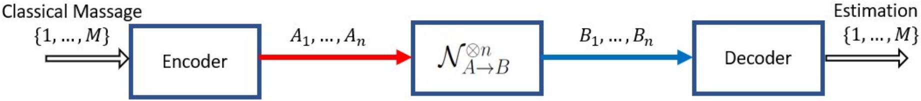
$$\mathcal{N}_{A\to B}(\rho) = \mathrm{Tr}_E(V\rho V^\dagger)$$

where $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ is an isometry defined by

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

TECHNION | Helen Diller Quantum Center

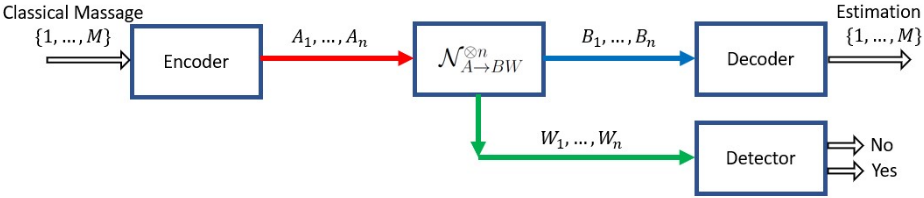
Without Covertness



- $\log(M)$ - #information bits, over n channel uses.
- Rate: $R = \frac{\log(M)}{n}$
- Example: 3-repetition code. $0 \to |000\rangle$, $1 \to |111\rangle$
  - $n = 3 \cdot \log(M)$, hence: $R = \frac{1}{3}$
  - #information bits: $\log(M) = \frac{1}{3} \cdot n = O(n)$
- In covert communication, $\log(M)$ is sub-linear

TECHNION | Helen Diller Quantum Center

Covert Communication



- **Reliability:** Bob's probability of error tends to zero

$$\lim_{n \to \infty} \Pr(\text{error}) = 0$$

- **Covertness:** Willie has a bad detection performance

$$\lim_{n \to \infty} D(\bar{\rho}_{W^n} || \omega_0^{\otimes n}) = 0$$

- **Covert "rate":**

$$L = \frac{\log(M)}{\log(n)\sqrt{nD(\bar{\rho}_{W^n} || \omega_0^{\otimes n})}}.$$

- **Covert capacity:** Supremum achievable rate as $n \to \infty$

TECHNION | Helen Diller Quantum Center

Discrete Vs. Continuous Channels

- The scale of $O(\sqrt{n}\log(n))$ has already been shown 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.
- There are communication settings, which 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].

Depolarizing Channel

- We study communication over the depolarizing channel.
- The qubit depolarizing channel can be given by:

$$\mathcal{N}_{A\to B}(\rho) = \mathrm{Tr}_{E_1E_2}(V\rho V^\dagger)$$

where $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2}$ is an isometry defined by

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

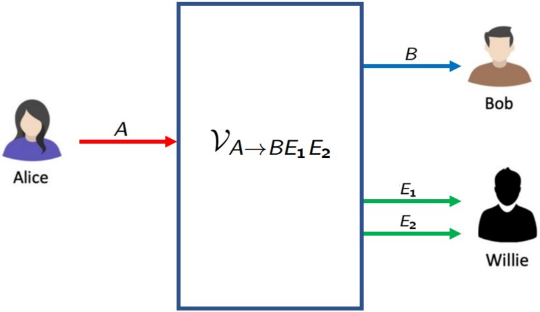
- Three qubits at the output of the channel
- 1st qubit belongs to Bob. 2nd and 3rd leak to the **environment**.
- Intuitively, (E_1, E_2) store a "flag" that indicates which Pauli error occurred.
- Willie's access is limited to the environment.
- No-Cloning Theorem: Willy's channel cannot be the same as Bob's

TECHNION | Helen Diller Quantum Center

Willie's Channel

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

- 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.

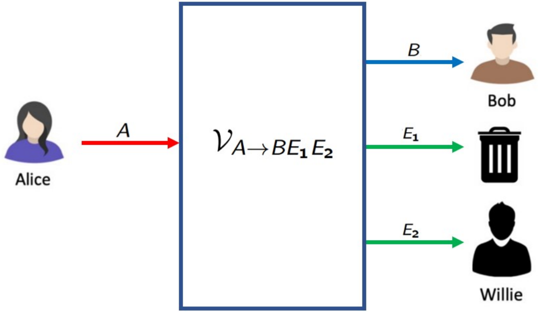


TECHNION | Helen Diller Quantum Center

Willie's Channel

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

- 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.

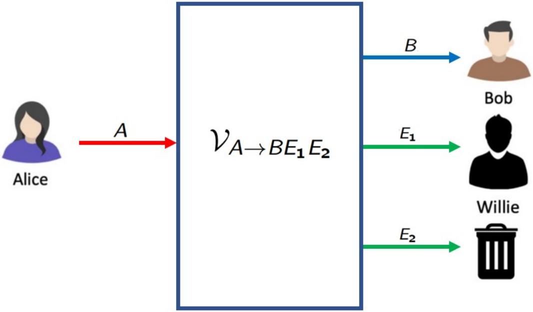


TECHNION | Helen Diller Quantum Center

Willie's Channel

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

- 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.

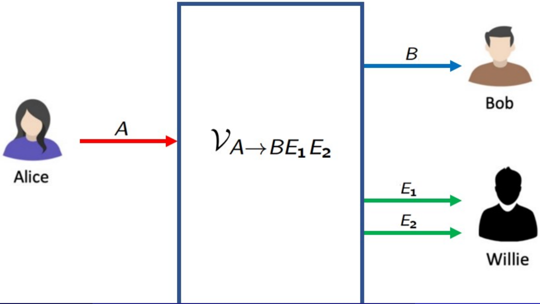


Willie's Channel: Scenario 1

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
- This is strong enough for him to detect any encoding operation.
- $\mathrm{supp}(\omega_1) \not\subseteq \mathrm{supp}(\omega_0)$, where $\omega_0 \equiv \widehat{\mathcal{N}}_{A\to W}(|0\rangle\langle 0|)$ and $\omega_1 \equiv \widehat{\mathcal{N}}_{A\to W}(|1\rangle\langle 1|)$
- Note: ω_1 and ω_0 depend on the channel parameter q.



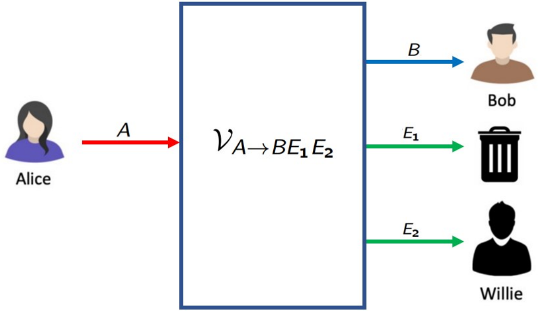
TECHNION | Helen Diller Quantum Center

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.

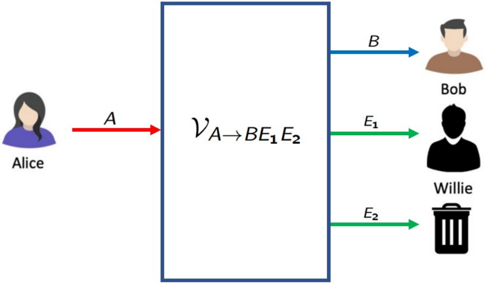
- Willie receives the second qubit.
- Willie cannot discern between the $|0\rangle$ and $|1\rangle$ inputs.
- $\omega_0 = \omega_1 = (1 - \frac{q}{2}) |0\rangle\langle 0| + \frac{q}{2} |1\rangle\langle 1|$



TECHNION | Helen Diller Quantum Center

Willie's Channel: Scenario 3

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



Main Result

Theorem

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

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

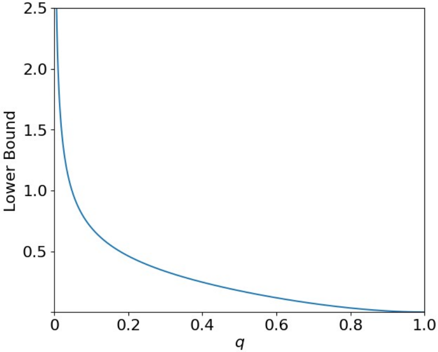
where $\omega_0 \equiv \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ *and* $\omega_1 \equiv \mathcal{N}_{A\to W}(|1\rangle\langle 1|)$.

- Reminder - covert capacity is the supremum of $\frac{\log(M)}{\log(n)\sqrt{nD(\overline{\rho}_{W^n}||\omega_{\mathbf{0}}^{\otimes n})}}$
- Without entanglement, #information bits follows SRL, and here, the rate is defined according to the $\sqrt{n}\log(n)$ scale.
- Covert transmission of $O(\sqrt{n}\log n)$ information bits is achievable.
- Entanglement leads to a logarithmic performance boost.

TECHNION | Helen Diller Quantum Center

Main Results: Lower Bound

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



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

TECHNION | Helen Diller Quantum Center

Main Result: Analysis

Lemma (Wilde 2017, Gagatsos et al. 2020)

For an input state ψ_{A_1A}, and sufficiently large n, there exists a coding scheme that employs pre-shared entanglement resources to transmit $\log(M)$ bits over n uses of $\mathcal{N}_{A\to B}$ such that:

$$\log(M) \geq nD(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B) + \sqrt{nV(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)}\Phi^{-1}(\varepsilon) - C_n$$

with

$$\psi_{A_1B} = (\mathrm{id}_{A_1} \otimes \mathcal{N}_{A\to B})(\psi_{A_1A})$$

where,

$$C_n = \frac{\beta_{\text{B-E}}}{\sqrt{2\pi}} \frac{[Q(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)]^{\frac{3}{4}}}{V(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)} + \frac{V(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)}{\sqrt{2\pi}} + \log(4\varepsilon n)\,,$$

and Φ^{-1} is the inverse-Gaussian distribution function.

Main Result: Analysis

Lemma (Wilde 2017)

For an input state $\psi_{A_1 A}$*, and sufficiently large* n*, there exists a coding scheme that employs pre-shared entanglement resources to transmit* $\log(M)$ *bits over* n *uses of* $\mathcal{N}_{A\to B}$ *such that:*

$$\log(M) \geq nD(\psi_{A_1 B}||\psi_{A_1} \otimes \psi_B) + \sqrt{nV(\psi_{A_1 B}||\psi_{A_1} \otimes \psi_B)}\Phi^{-1}(\varepsilon) - C_n$$

with

$$\psi_{A_1 B} = (\mathrm{id}_{A_1} \otimes \mathcal{N}_{A\to B})(\psi_{A_1 A})$$

- The derivation is based on a *position-based* coding scheme.
- Each message is associated with n entangled pairs
- Bob uses sequential decoding on the output and the entanglement resources for each message consecutively

TECHNION | Helen Diller Quantum Center

Main Results: Analysis

- Unassisted communication: classical encoding [Sheikholeslami et al. 2016]
  - Alice selects **binary sequences** according to $\mathrm{Bernoulli}(\alpha_n)$, where $\alpha_n \sim \frac{1}{\sqrt{n}}$.
  - The average input state is $\psi_A = (1-\alpha_n)\,|0\rangle\langle 0| + \alpha_n\,|1\rangle\langle 1|$.

TECHNION | Helen Diller Quantum Center

Main Results: Analysis

- Unassisted communication: classical encoding [Sheikholeslami et al. 2016]
  - Alice selects **binary sequences** according to $\mathrm{Bernoulli}(\alpha_n)$, where $\alpha_n \sim \frac{1}{\sqrt{n}}$.
  - The average input state is $\psi_A = (1-\alpha_n)|0\rangle\langle 0| + \alpha_n |1\rangle\langle 1|$.
- Entanglement-assisted communication: In our scheme,
  - Alice encodes with the **superposition state**:

    $$|\psi_{A_1 A}\rangle = \sqrt{1-\alpha_n}\,|00\rangle + \sqrt{\alpha_n}\,|11\rangle \ ,$$

    where $\alpha_n \sim \frac{1}{\sqrt{n}}$.
  - A_1 is the pre-shared entanglement resource of Bob.
  - $|\psi_{A_1 A}\rangle$ can be considered as "very close" to the innocent state $|00\rangle$.
  - The channel input A is the reduced state $\psi_A = (1-\alpha_n)|0\rangle\langle 0| + \alpha_n |1\rangle\langle 1|$.

TECHNION | Helen Diller Quantum Center

Alice encodes with the state:

$$|\psi_{A_1A}\rangle = \sqrt{1-\alpha_n}\,|00\rangle + \sqrt{\alpha_n}\,|11\rangle \ ,$$

using the mentioned lemma, and after some algebraic manipulation, we obtain

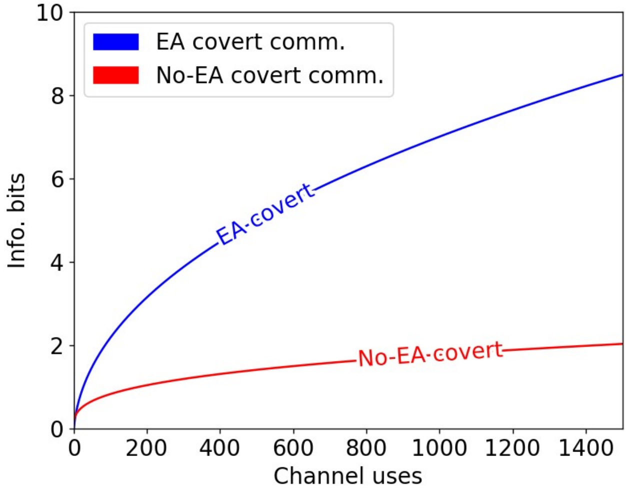
$$\log(M) \geq -2\frac{(1-q)^2}{2-q}\alpha_n \log(\alpha_n) + O(\alpha_n)\,,$$

and finally

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

Main Result: Info. Bits Graph

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



Interpretation: Energy Constraint

- The total energy of a state must not exceed a certain limit.
- A state ρ satisfies the energy constraint E, with the Hamiltonian $\hat{\mathrm{H}}$, if $\mathrm{Tr}(\hat{\mathrm{H}}\rho) \leq E$.
- For $E \ll 1$,
  - Unassisted energy-constrained capacity: $C_0 \sim E$
  - Entanglement assisted energy-constrained capacity: $C_{EA} \sim -E \log E$
- The ratio between the assisted and unassisted scales as $-\log(E)$
- For $E_n \sim \frac{1}{\sqrt{n}}$, the ratio scales as $\log(n)$
- Effectively, the covertness requirement imposes an energy constraint. with Hamiltonian $\hat{\mathrm{H}} = |1\rangle\langle 1|$ and the constraint $E_n \sim \frac{1}{\sqrt{n}}$

Interpretation: Bob's Decoding Performance

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 covert communication over depolarizing channels
  * main question: how can entanglement resources improve performance?
- We consider three scenarios: Willie has the entire environment, or, part of it.
- Our main contributions include:
  * Analysis of # information bits.
  * 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.

Future directions

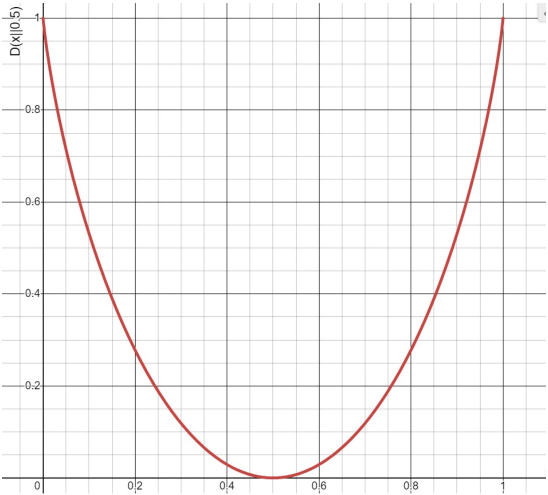
- Entanglement assisted covert communication over a general channel
- Quantum covert communication
- Converse - upper bound

TECHNION | Helen Diller Quantum Center

Thank you

TECHNION | Helen Diller Quantum Center

Appendix A - Divergence of two Bernoulli's



- Divergence between Bernoulli(x) and (0.5)
- $D(x||0.5) = x\log\left(\frac{x}{0.5}\right) + (1-x)\log\left(\frac{1-x}{0.5}\right)$

TECHNION | Helen Diller Quantum Center

Appendix B - explicit expression of ω_0 and ω_1 - scenario 1

$$\omega_0(q) = \begin{pmatrix} 1-\frac{3q}{4} & 0 & 0 & \sqrt{\frac{q}{4}(1-\frac{3q}{4})} \\ 0 & \frac{q}{4} & -i\frac{q}{4} & 0 \\ 0 & i\frac{q}{4} & \frac{q}{4} & 0 \\ \sqrt{\frac{q}{4}(1-\frac{3q}{4})} & 0 & 0 & \frac{q}{4} \end{pmatrix} \tag{1}$$

$$\omega_1(q) = \begin{pmatrix} 1-\frac{3q}{4} & 0 & 0 & -\sqrt{\frac{q}{4}(1-\frac{3q}{4})} \\ 0 & \frac{q}{4} & i\frac{q}{4} & 0 \\ 0 & -i\frac{q}{4} & \frac{q}{4} & 0 \\ -\sqrt{\frac{q}{4}(1-\frac{3q}{4})} & 0 & 0 & \frac{q}{4} \end{pmatrix} \tag{2}$$

TECHNION | Helen Diller Quantum Center

Appendix C - explicit expression of $\mathcal{N}_{A\to W}(\rho)$ - scenario 2

$$\mathcal{N}_{A\to W}(\rho) = \left(1 - \frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}|1\rangle\langle 1|$$
$$+ 2\,\mathrm{Re}\{b\}\left(\left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} + i\frac{q}{4}\right)|0\rangle\langle 1| + \left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} - i\frac{q}{4}\right)|1\rangle\langle 0|\right) \tag{3}$$

Appendix D - Coding in Shannon theory

- **Random codebook generation:** Randomly and independently generate $2^{\log(M)}$ sequences (codewords) $x^n(m)$, $m \in [1:M]$

$$x^n(m) \sim \prod_{i=1}^{n} p_X(x_i) \tag{4}$$

- **Encoding:** To send message $m \in [1:M]$, use $x^n(m)$.
- **Decoding**: Given a received sequence y^n, the decoder searches for a codeword x^n in the set of possible transmitted codewords such that (x^n, y^n) are jointly typical. (vary close to the expected probability given by P_{XY}).
- Why does it work? **Law of large numbers**.

Appendix E - Hypothesis testing relative entropy

- The hypothesis testing relative entropy is defined for $\varepsilon \in [0,1]$ as :

$$D_H^{\varepsilon}(\rho||\sigma) = -\log \inf_{\Lambda} \{\mathrm{Tr}\{\Lambda\sigma\} : \mathrm{Tr}\{\Lambda\rho\} \geq 1-\varepsilon \wedge 0 \leq \Lambda \leq I\}. \quad (5)$$

- The following expansion holds for a sufficiently large positive integer n:

$$D_H^{\varepsilon}(\rho^{\otimes}||\sigma^{\otimes}) = nD(\rho||\sigma) + \sqrt{nV(\rho||\sigma)}\Phi^{-1}(\varepsilon) + O(\log n) \quad (6)$$

- where:

$$\Phi^{-1}(\varepsilon) = \sup\{\varepsilon \in \mathbb{R} | \Phi(\varepsilon) \leq \varepsilon\} \qquad \Phi(\varepsilon) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\varepsilon} dx \exp\left(-x^2/2\right) \quad (7)$$

- $\Phi(\varepsilon)$ comes from Berry–Esseen theorem - a variation of the central limit theorem.

TECHNION | Helen Diller Quantum Center