Converse bounds for private communication over quantum channels

Mark M. Wilde

Hearne Institute for Theoretical Physics,
Department of Physics and Astronomy,
Center for Computation and Technology,
Louisiana State University,
Baton Rouge, Louisiana, USA

mwilde@lsu.edu

Based on arXiv:1602.08898 (with Mario Berta and Marco Tomamichel)

SIPQNP, March 30-April 1, 2016, Waltham, MA

Main message

- We establish a general meta-converse bound for private communication protocols, by using the notion of a private state and a "privacy" test to determine whether a given state is a private state
- The meta-converse bound has a number of applications, including strong converse bounds and second-order characterizations of private communication
- The bounds are related to the relative entropy of entanglement and sharpen known upper bounds on rates of quantum key distribution protocols
- We establish the strong converse property for the two-way assisted private capacity of the pure-loss and quantum-limited amplifier channels. We also get strong converse rates for other quantum Gaussian channels.

Private states

Tripartite key state

A tripartite key state γ_{ABE} contains $\log K$ bits of secret key if there exists a state σ_E such that

$$\gamma_{ABE} = \frac{1}{K} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E.$$

Bipartite private state

A bipartite private state $\gamma_{ABA'B'}$ has the following form:

$$\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U^\dagger_{ABA'B'},$$

where $U_{ABA'B'}$ is a "twisting" unitary of the form $U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'}$, with each $U^{ij}_{A'B'}$ a unitary, and $\theta_{A'B'}$ a state.

Private states

- The systems A' and B' are called the "shield" systems because they, along with the twisting unitary, can help to protect the key in systems AB from any party possessing a purification of $\gamma_{ABA'B'}$.

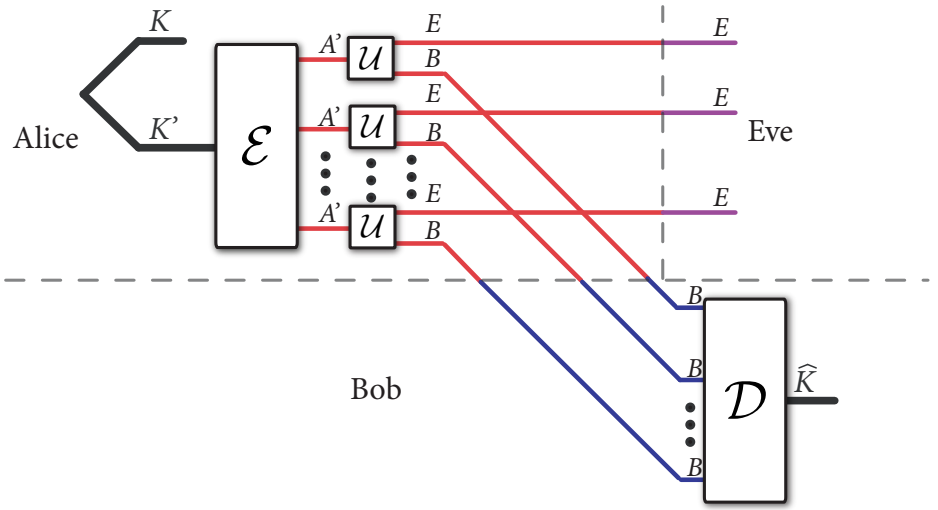
- Such bipartite private states are in one-to-one correspondence with tripartite key states. That is, for every tripartite key state γ_{ABE}, we can find a bipartite private state and vice versa.

- This correspondence takes on a more physical form: any tripartite protocol whose aim it is to extract tripartite key states is in 1-to-1 correspondence with a bipartite protocol whose aim it is to extract bipartite private states.

Private communication protocols

Unassisted private communication

- Given is a quantum channel $\mathcal{N}_{A' \to B}$. Let $U^{\mathcal{N}}_{A' \to BE}$ be an isometric extension of $\mathcal{N}_{A' \to B}$.
- A secret-key generation protocol for n channel uses consists of a triple $\{|K|, \mathcal{E}, \mathcal{D}\}$, where $|K|$ is the size of the secret key to be generated, $\mathcal{E}_{K' \to A'^n}$ is the encoder, and $\mathcal{D}_{B^n \to \hat{K}}$ is the decoder.



Private communication protocols

Unassisted private communication

- A triple (n, P, ε) consists of the number n of channel uses, the rate P of secret-key generation, and the error $\varepsilon \in [0, 1]$.
- Such a triple is achievable on $\mathcal{N}_{A' \to B}$ if there exists a secret-key generation protocol $\{|K|, \mathcal{E}, \mathcal{D}\}$ and some state ω_{E^n} such that $\frac{1}{n} \log |K| \geq P$ and

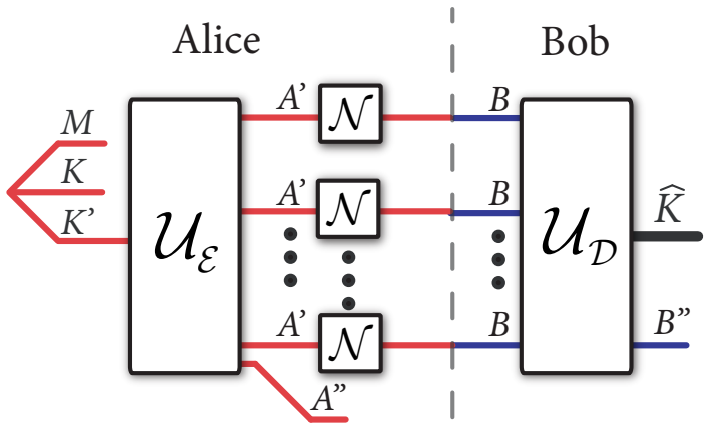
$$F(\overline{\Phi}_{K\hat{K}} \otimes \omega_{E^n}, \rho_{K\hat{K}E^n}) \geq 1 - \varepsilon,$$

where $\rho_{K\hat{K}E^n} \equiv (\mathcal{D}_{B^n \to \hat{K}} \circ (\mathcal{U}^{\mathcal{N}}_{A' \to BE})^{\otimes n} \circ \mathcal{E}_{K' \to A'^n})(\overline{\Phi}_{KK'})$ and

$$\overline{\Phi}_{KK'} \equiv \frac{1}{|K|} \sum_{i=0}^{|K|-1} |i\rangle\langle i|_K \otimes |i\rangle\langle i|_{K'}.$$

Equivalent bipartite protocol

Can reformulate such a protocol in the bipartite picture: perform every step coherently, with the goal to produce a bipartite private state



Due to equivalence between tripartite and bipartite pictures

$$F(\gamma_{K_A K_B S_A S_B}, \rho_{K\hat{K}MA''B''}) \geq 1 - \varepsilon,$$

for some private state $\gamma_{K_A K_B S_A S_B}$, where we identify $K_A \equiv K$, $K_B \equiv \hat{K}$, $S_A \equiv MA''$, and $S_B \equiv B''$, and

$$\rho_{K\hat{K}MA''B''} \equiv (\mathcal{U}^{\mathcal{D}}_{B^n \to \hat{K}B''} \circ (\mathcal{U}^{\mathcal{N}}_{A' \to BE})^{\otimes n} \circ \mathcal{U}^{\mathcal{E}}_{K' \to A'^n A''})(\Phi^{\mathrm{GHZ}}_{KK'M}).$$

Non-asymptotic achievable region

Non-asymptotic fundamental limits

Boundaries of the achievable regions:

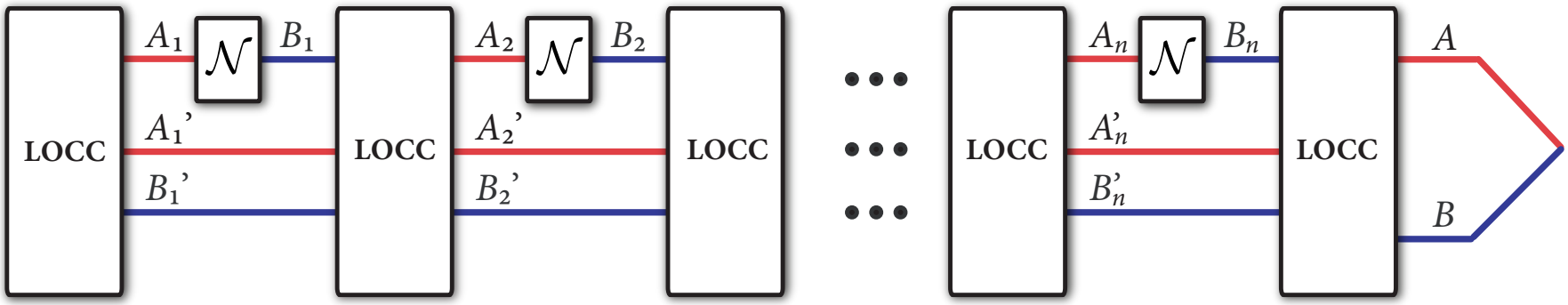
$$\hat{P}_{\mathcal{N}}(n,\varepsilon) \equiv \max\{P : (n,P,\varepsilon) \text{ is achievable for } \mathcal{N}\},$$
$$\hat{\varepsilon}_{\mathcal{N}}(n,P) \equiv \min\{\varepsilon : (n,P,\varepsilon) \text{ is achievable for } \mathcal{N}\}.$$

Interpretations

- 1st boundary $\hat{P}_{\mathcal{N}}(n,\varepsilon)$ identifies how rate can change as a function of n for fixed error ε, and 2nd-order coding rates can characterize it
- 2nd boundary $\hat{\varepsilon}_{\mathcal{N}}(n,P)$ identifies how error can change as a function of n for fixed rate R, and error exponents and strong converse exponents characterize it

LOCC-assisted private communication protocols

LOCC-assisted protocols are defined similarly, but allow for rounds of LOCC between channel uses (like in QKD)



Define boundaries of non-asymptotic achievable regions similarly as

$$\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon) \equiv \max\{P : (n,P,\varepsilon) \text{ is achievable for } \mathcal{N} \text{ using } \leftrightarrow\},$$
$$\hat{\varepsilon}^{\leftrightarrow}_{\mathcal{N}}(n,P) \equiv \min\{\varepsilon : (n,P,\varepsilon) \text{ is achievable for } \mathcal{N} \text{ using } \leftrightarrow\}.$$

Information measures

- Hypothesis testing relative entropy defined for a state ρ, positive semi-definite operator σ, and $\varepsilon \in [0,1]$ as

$$D_H^\varepsilon(\rho\|\sigma) \equiv -\log\left[\min\{\mathrm{Tr}\{\Lambda\sigma\} : 0 \leq \Lambda \leq I \wedge \mathrm{Tr}\{\Lambda\rho\} \geq 1-\varepsilon\}\right].$$

- Has a second-order expansion for i.i.d. states:

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

where
$$D(\rho\|\sigma) \equiv \mathrm{Tr}\{\rho[\log\rho - \log\sigma]\},$$
$$V(\rho\|\sigma) \equiv \mathrm{Tr}\{\rho[\log\rho - \log\sigma - D(\rho\|\sigma)]^2\}$$
$$\Phi(a) \equiv \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{a} dx\ \exp\left(-x^2/2\right)$$

Information measures

- Can use hypothesis testing relative entropy to define the ε-relative entropy of entanglement:

$$E_R^{\varepsilon}(A;B)_\rho \equiv \inf_{\sigma_{AB} \in \mathcal{S}(A:B)} D_H^{\varepsilon}(\rho_{AB} \| \sigma_{AB}).$$

  where $\mathcal{S}(A:B)$ is the set of separable states

- Can also define a channel's ε-relative entropy of entanglement:

$$E_R^{\varepsilon}(\mathcal{N}) \equiv \sup_{|\psi\rangle_{AA'} \in \mathcal{H}_{AA'}} E_R^{\varepsilon}(A;B)_\rho,$$

  where $\rho_{AB} \equiv \mathcal{N}_{A' \to B}(\psi_{AA'})$

- Standard relative entropies of entanglement defined by replacing D_H^{ε} with quantum relative entropy D

Privacy test

- Can test whether a given state is a γ-private state by "untwisting" and projecting onto the maximally entangled state:

$$\{\Pi_{ABA'B'}, I_{ABA'B'} - \Pi_{ABA'B'}\},$$

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}\left(\Phi_{AB} \otimes I_{A'B'}\right) U^{\dagger}_{ABA'B'}$.

- Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the γ-privacy test satisfies

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1 - \varepsilon,$$

- For a separable state $\sigma_{ABA'B'} \in \mathcal{S}(AA' : BB')$, the probability of passing any γ-privacy test is never larger than $1/K$:

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{ABA'B'}\} \leq \frac{1}{K},$$

where K is the number of values that the secret key can take.

Meta-converse bound for private communication

Theorem

For any fixed $\varepsilon \in (0,1)$, the achievable region satisfies

$$\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N}).$$

The same bound holds when allowing for a round of LOCC before and after the channel use.

Proof idea: use monotonicity of E_R^{ε} with respect to LOCC and use the bounds on the previous slide.

Meta-converse bound for private communication

Corollary

The following bound holds for n channel uses:

$$\hat{P}_{\mathcal{N}}(n,\varepsilon) \leq \frac{1}{n} E_R^{\varepsilon}(\mathcal{N}^{\otimes n}).$$

The same bound holds when allowing for rounds of LOCC before and after all n channel uses. The same bound holds for $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n,\varepsilon)$ *if the channel* $\mathcal{N}$ *is teleportation simulable.*

Application: Strong converse rate for private capacity

Theorem

For any channel $\mathcal{N}$, its relative entropy of entanglement is a strong converse rate for private communication:

$$P^{\dagger}(\mathcal{N}) \leq E_R(\mathcal{N}),$$

where $P^{\dagger}(\mathcal{N})$ is the strong converse private capacity of $\mathcal{N}$.

Proof idea: Use permutation symmetry of an i.i.d. channel, de Finetti theorem, and a Rényi version of the relative entropy of entanglement.

Theorem

If $\mathcal{N}$ is teleportation simulable, then its relative entropy of entanglement is an upper bound for the LOCC-assisted strong converse private capacity:

$$P^{\dagger}_{\leftrightarrow}(\mathcal{N}) \leq E_R(\mathcal{N}).$$

Application: Second-order expansions of converse bounds

Theorem

If a quantum channel $\mathcal{N}_{A'\to B}$ is covariant, then

$$\hat{P}_{\mathcal{N}}(n,\varepsilon) \leq E_R(A;B)_\rho + \sqrt{\frac{V^{\varepsilon}_{E_R}(A;B)_\rho}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right),$$

where $\rho_{AB} = \mathcal{N}_{A'\to B}(\Phi_{AA'})$. If a quantum channel $\mathcal{N}_{A'\to B}$ is teleportation-simulable with associated state ω_{AB}, then

$$\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon) \leq E_R(A;B)_\omega + \sqrt{\frac{V^{\varepsilon}_{E_R}(A;B)_\omega}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right).$$

where $$V^{\varepsilon}_{E_R}(A;B)_\rho \equiv \begin{cases} \max_{\sigma_{AB'}\in\Pi_{\mathcal{S}}} V(\rho_{AB}\|\sigma_{AB}) & \text{for } \varepsilon < 1/2 \\ \min_{\sigma_{AB}\in\Pi_{\mathcal{S}}} V(\rho_{AB}\|\sigma_{AB}) & \text{for } \varepsilon \geq 1/2 \end{cases},$$

with $\Pi_{\mathcal{S}} \subseteq \mathcal{S}(A\!:\!B)$ the set of states achieving minimum in $E_R(A;B)_\rho$

Example: Dephasing channel

Theorem

For the qubit dephasing channel $\mathcal{Z}^{\gamma} : \rho \mapsto (1-\gamma)\,\rho + \gamma Z \rho Z$, *with* $\gamma \in (0,1)$, *the boundary* $\hat{P}(n;\varepsilon)$ *satisfies*

$$\hat{P}(n,\varepsilon) = \hat{P}^{\leftrightarrow}(n,\varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}}\,\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right),$$

where Φ *is the cumulative standard Gaussian distribution,* $h(\gamma)$ *denotes the binary entropy and* $v(\gamma)$ *the corresponding variance, defined as*

$$h(\gamma) \equiv -\gamma \log \gamma - (1-\gamma)\log(1-\gamma),$$
$$v(\gamma) \equiv \gamma(\log\gamma + h(\gamma))^2 + (1-\gamma)(\log(1-\gamma) + h(\gamma))^2.$$

Example: Erasure channel

Theorem

For the qubit erasure channel $\mathcal{E}^p_{A'\to B} : \rho_{A'} \mapsto (1-p)\rho_B + p|e\rangle\langle e|_B$ *with* $p \in (0,1)$, *the boundary* $\hat{P}^{\leftrightarrow}_{\mathcal{E}^p}(n,\varepsilon)$ *satisfies*

$$\varepsilon = \sum_{l=n-k+1}^{n} \binom{n}{l} p^l (1-p)^{n-l} \left(1 - 2^{n\left(1-\hat{P}^{\leftrightarrow}_{\mathcal{E}^p}(n,\varepsilon)\right)-l}\right) .$$

Moreover, the following expansion holds

$$\hat{P}^{\leftrightarrow}_{\mathcal{E}^p}(n,\varepsilon) = 1 - p + \sqrt{\frac{p(1-p)}{n}}\Phi^{-1}(\varepsilon) + O\left(\frac{1}{n}\right) .$$

Application: Quantum Gaussian channels

Definitions of quantum Gaussian channels

$$\text{Thermal channel } \mathcal{L}_{\eta,N_B}: \quad \hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e},$$
$$\text{Amplifier channel } \mathcal{A}_{G,N_B}: \quad \hat{b} = \sqrt{G}\hat{a} + \sqrt{G-1}\hat{e}^\dagger,$$
$$\text{Additive-noise channel } \mathcal{W}_\xi: \quad \hat{b} = \hat{a} + (x+ip)/\sqrt{2},$$

- Thermal channel has transmissivity $\eta \in [0,1]$ and environment prepared in thermal state of mean photon number N_B.
- Amplifier channel has gain $G \in [1,\infty)$ and environment prepared in thermal state of mean photon number N_B. If $N_B = 0$, then channels are quantum-limited.
- Additive noise channel has x and p be zero-mean Gaussian random variables with variance $\xi \geq 0$.

Unconstrained relative entropy variances

Let $V_{\mathcal{L}_{\eta,N_B}}$, $V_{\mathcal{A}_{G,N_B}}$, and $V_{\mathcal{W}_\xi}$ be the unconstrained relative entropy variances of the thermalizing, amplifier, and additive-noise channels, respectively:

$$\begin{aligned} V_{\mathcal{L}_{\eta,N_B}} &\equiv N_B(N_B+1)\log^2(\eta\left[N_B+1\right]/N_B), \\ V_{\mathcal{A}_{G,N_B}} &\equiv N_B(N_B+1)\log^2(G^{-1}\left[N_B+1\right]/N_B), \\ V_{\mathcal{W}_\xi} &\equiv (1-\xi)^2/\ln^2 2. \end{aligned}$$

Application: Strong converse rates for Gaussian channels

Theorem

The following converse bounds hold for $\varepsilon \in (0,1)$*:*

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_{\eta,N_B}}(n,\varepsilon) \leq -\log\left((1-\eta)\,\eta^{N_B}\right) - g(N_B) + \sqrt{\frac{2V_{\mathcal{L}_{\eta,N_B}}}{n(1-\varepsilon)}} + O(1/n),$$

$$\hat{P}^{\leftrightarrow}_{\mathcal{A}_{G,N_B}}(n,\varepsilon) \leq \log\left(\frac{G^{N_B+1}}{G-1}\right) - g(N_B) + \sqrt{\frac{2V_{\mathcal{A}_{G,N_B}}}{n(1-\varepsilon)}} + O(1/n),$$

$$\hat{P}^{\leftrightarrow}_{\mathcal{W}_\xi}(n,\varepsilon) \leq \frac{\xi-1}{\ln 2} - \log\xi + \sqrt{\frac{2V_{\mathcal{W}_\xi}}{n(1-\varepsilon)}} + O(1/n).$$

Proof idea: Use a teleportation simulation argument, employ meta-converse theorem, apply Chebyshev inequality, a formula for the relative entropy variance of two Gaussian states, and take the infinite-energy limit

Application: Strong converse for quantum-limited channels

Corollary

For the pure-loss channel $\mathcal{L}_\eta$ and quantum-limited amplifier channel $\mathcal{A}_G$, the following bounds hold

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq -\log(1-\eta) + O\left(\frac{1}{n}\right),$$

$$\hat{P}^{\leftrightarrow}_{\mathcal{A}_G}(n,\varepsilon) \leq \log\left(\frac{G}{G-1}\right) + O\left(\frac{1}{n}\right).$$

Tool: Relative entropy variance for Gaussian states

Writing zero-mean Gaussian states in exponential form as

$$\rho = Z_\rho^{-1/2} \exp\left\{-\frac{1}{2}\hat{x}^T G_\rho \hat{x}\right\}, \qquad \sigma = Z_\sigma^{-1/2} \exp\left\{-\frac{1}{2}\hat{x}^T G_\sigma \hat{x}\right\},$$

where

$$Z_\rho \equiv \det(V^\rho + i\Omega/2), \qquad Z_\sigma \equiv \det(V^\sigma + i\Omega/2),$$
$$G_\rho \equiv 2i\Omega \operatorname{arcoth}(2V^\rho i\Omega), \qquad G_\sigma \equiv 2i\Omega \operatorname{arcoth}(2V^\sigma i\Omega),$$

and V^ρ and V^σ are Wigner function covariance matrices for ρ and σ.

Theorem

For zero-mean Gaussian states ρ and σ, the relative entropy variance is

$$V(\rho\|\sigma) = \frac{1}{2}\operatorname{Tr}\{\Delta V^\rho \Delta V^\rho\} + \frac{1}{8}\operatorname{Tr}\{\Delta\Omega\Delta\Omega\},$$

where $\Delta \equiv G_\rho - G_\sigma$.