Converse bounds for private communication over quantum channels

Mark M. Wilde (LSU)

joint work with Mario Berta (Caltech) and
Marco Tomamichel (|Univ. Sydney⟩ + |Univ. of Technology, Sydney⟩)

arXiv:1602.08898
accepted for publication in IEEE Trans. Inf. Theory
DOI: 10.1109/TIT.2017.2648825

QIP 2017 Seattle - January 20, 2017
Given a quantum channel $\mathcal{N}$ and a quantum key distribution (QKD) protocol that uses it $n$ times, how much key can be generated?

**Non-asymptotic private capacity**: maximum rate of $\varepsilon$-close secret key achievable using the channel $n$ times with two-way classical communication (LOCC) assistance

\[
\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon) := \sup \{ P : (n, P, \varepsilon) \text{ is achievable for } \mathcal{N} \text{ using LOCC} \}.
\]
Practical question: how to characterize $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon)$ for all $n \geq 1$ and $\varepsilon \in (0, 1)$? The answers give the fundamental limitations of QKD.

Upper bounds on $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon)$ can be used as benchmarks for quantum repeaters [Lütkenhaus].

Today, I will present the tightest known upper bound on $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon)$ for several channels of practical interest. Interesting special case: single-mode phase-insensitive bosonic Gaussian channels.
Overview

1. Main Results (Examples)

2. Proof Idea: Meta Converse

3. Conclusion
Main Result: Gaussian Channels I

- Converse bounds for single-mode phase-insensitive bosonic Gaussian channels, most importantly the photon loss channel

\[ \mathcal{L}_\eta : \hat{b} = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{e} \quad (2) \]

where transmissivity \( \eta \in [0, 1] \) and environment in vacuum state.

- Our approach gives a complete proof for the following weak converse bound, stated in [Pirandola et al. 2016]:

\[ P^{\leftrightarrow}(\mathcal{L}_\eta) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{N}_\eta}(n, \varepsilon) \leq \log\left(\frac{1}{1 - \eta}\right), \quad (3) \]

which is actually tight in the asymptotic limit, i.e., \( P^{\leftrightarrow}(\mathcal{N}_\eta) = \log\left(\frac{1}{1 - \eta}\right) \).

- Drawback: an asymptotic statement, and thus says little for practical protocols (called a weak converse bound).
Main Result: Gaussian Channels II

- We show the non-asymptotic converse bound

$$\hat{P}_{\mathbb{C}_n}(n, \varepsilon) \leq \log \left( \frac{1}{1 - \eta} \right) + \frac{C(\varepsilon)}{n},$$  \hspace{1cm} (4)

where $C(\varepsilon) := \log 6 + 2 \log \left( \frac{1 + \varepsilon}{1 - \varepsilon} \right)$ (other choices possible).

- Can be used to assess the performance of any practical quantum repeater which uses a loss channel $n$ times for desired security $\varepsilon$.

- Other variations of this bound are possible if $\eta$ is not the same for each channel use, if $\eta$ is chosen adversarially, etc.

- We give similar bounds for the quantum-limited amplifier channel (tight), thermalizing channels, amplifier channels, and additive noise channels.
Asymptotic result [Pirandola et al. 2016] for the qubit dephasing channel

\[ Z_\gamma : \rho \mapsto (1 - \gamma) \rho + \gamma Z \rho Z \]

with \( \gamma \in (0, 1) \) is

\[ P^{\leftrightarrow}(Z_{\gamma}) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{Z_{\gamma}}(n, \varepsilon) = 1 - h(\gamma), \]

(5)

with the binary entropy \( h(\gamma) := -\gamma \log \gamma - (1 - \gamma) \log(1 - \gamma) \).

By combining with [Tomamichel et al. 2016] we show the expansion

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

(6)

with \( \Phi \) the cumulative standard Gaussian distribution and the binary entropy variance \( v(\gamma) := \gamma (\log \gamma + h(\gamma))^2 + (1 - \gamma)(\log(1 - \gamma) + h(\gamma))^2 \).
For the dephasing parameter $\gamma = 0.1$ we get (figure from [Tomamichel et al. 2016]):

(c) Comparison of strict bounds with third order approximation for $\varepsilon = 5\%$. 

Proof Idea: Meta Converse I

- **Meta converse approach** from classical channel coding [Polyanskiy et al. 2010], uses connection to **hypothesis testing**. In the quantum regime, e.g., for classical communication [Tomamichel & Tan 2015] or quantum communication [Tomamichel et al. 2014 & 2016]. We extend this approach to **private communication**.

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

$$D_\varepsilon^H(\rho \| \sigma) := -\log \inf \{ \text{Tr}[\Lambda \sigma] : 0 \leq \Lambda \leq I \wedge \text{Tr}[\Lambda \rho] \geq 1 - \varepsilon \}.$$  \hfill (7)

- The $\varepsilon$-relative entropy of entanglement is defined as

$$E^\varepsilon_R(A; B)_\rho := \inf_{\sigma_{AB} \in S(A:B)} D_\varepsilon^H(\rho_{AB} \| \sigma_{AB}),$$  \hfill (8)

where $S(A : B)$ is the set of separable states (cf. relative entropy of entanglement). **Channel's $\varepsilon$-relative entropy of entanglement** is then given as

$$E^\varepsilon_R(\mathcal{N}) := \sup_{|\psi\rangle_{AA'}} E^\varepsilon_R(A; B)_\rho,$$  \hfill (9)

where $\rho_{AB} := \mathcal{N}_{A' \rightarrow B}(\psi_{AA'})$. 
Proof Idea: Meta Converse II

- Goal is the creation of \( \log K \) **bits of key**, i.e., states \( \gamma_{ABE} \) with

\[
(M_A \otimes M_B)(\gamma_{ABE}) = \frac{1}{K} \sum_i |i\rangle_A \langle i| \otimes |i\rangle_B \otimes \sigma_E
\]  

(10)

for some state \( \sigma_E \) and measurement channels \( M_A, M_B \).

- In **one-to-one correspondence** with pure states \( \gamma_{AA'BB'E} \) such that [Horodecki et al. 2005 & 2009]

\[
\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U_{ABA'B'}^\dagger
\]  

(11)

where \( \Phi_{AB} \) maximally entangled, \( U_{ABA'B'} = \sum_{i,j} |i\rangle_A \langle i| \otimes |j\rangle_B \otimes U^i_{A'B'} \) with each \( U^i_{A'B'} \) a unitary, and \( \theta_{A'B'} \) a state.

- Work in the latter, bipartite picture.
Proof Idea: Meta Converse III

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

\[
\text{Tr}\{\Pi_{ABA'B'} \rho_{ABA'B'}\} \geq 1 - \varepsilon,
\]

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB} \otimes I_{A'B'}) U_{ABA'B'}^\dagger$ is a projective "$\gamma$-privacy test."

- For separable states $\sigma_{AA'BB'}$ (useless for private communication) and a state $\gamma_{AA'BB'}$ with log $K$ bits of key we have [Horodecki et al. 2009]

\[
\text{Tr}\{\Pi_{ABA'B'} \sigma_{AA'BB'}\} \leq \frac{1}{K},
\]

- The monotonicity of the channel’s $\varepsilon$-relative entropy of entanglement $E^\varepsilon_R(\mathcal{N})$ with respect to LOCC together with (13) implies the meta converse

\[
\hat{P}_\mathcal{N}(1, \varepsilon) \leq E^\varepsilon_R(\mathcal{N}) \quad \text{(LOCC pre- and post-processing assistance).}
\]

For $n$ channel uses this gives $\hat{P}_\mathcal{N}(n, \varepsilon) \leq \frac{1}{n} E^\varepsilon_R(\mathcal{N}^\otimes n)$.

- Finite block-length version of relative entropy of entanglement upper bound [Horodecki et al. 2005 & 2009].

- One can then evaluate the meta converse for specific channels of interest.
Conclusion

- Our meta converse $\hat{P}_N(1, \varepsilon) \leq E^\varepsilon(N)$ gives bounds for the private transmission capabilities of quantum channels. These give the fundamental limitations of QKD and thus can be used as benchmarks for quantum repeaters.

- Can our bound be improved for the photon loss channel

$$\hat{P}_{L, \eta}(n, \varepsilon) \leq \log \left( \frac{1}{1 - \eta} \right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2 \log \left( \frac{1 + \varepsilon}{1 - \varepsilon} \right)$$

(15)

to $C'(\varepsilon) := \log \left( \frac{1}{1 - \varepsilon} \right)$?

- Corresponding matching achievability? (Tight analysis of random coding in infinite dimensions needed.)

- Tight finite-energy bounds for single-mode phase-insensitive bosonic Gaussian channels?

- Understand more channels, for example such with $P^{\leftrightarrow} > 0$ but zero quantum capacity [Horodecki et al. 2008]?
For **Gaussian channels** we need formulas for the relative entropy $D(\rho\|\sigma)$ and the relative entropy variance $V(\rho\|\sigma)$.

From [Chen 2005, Pirandola et al. 2015] and [Wilde et al. 2016], respectively: writing zero-mean Gaussian states in exponential form as

$$\rho = Z_\rho^{-1/2} \exp \left\{ -\frac{1}{2} \hat{x}^T G_\rho \hat{x} \right\} \quad \text{with}$$

$$Z_\rho := \det(V^\rho + i\Omega/2), \quad G_\rho := 2i\Omega \text{arcoth}(2V^\rho i\Omega),$$

and $V^\rho$ the Wigner function covariance matrix for $\rho$, we have

$$D(\rho\|\sigma) = \frac{1}{2} \left( \log \left( \frac{Z_\sigma}{Z_\rho} \right) - \text{Tr} [\Delta V^\rho] \right)$$

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

where $\Delta := G_\rho - G_\sigma$. 