

A meta-converse for private communication over quantum channels

Mario Berta

with Mark M. Wilde and Marco Tomamichel
IEEE Transactions on Information Theory, 63(3), 1792–1817 (2017)

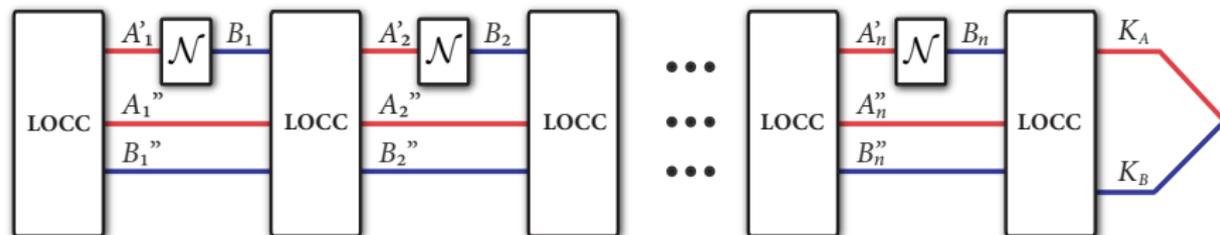
Beyond IID Singapore - July 17, 2017



Caltech

Setup I

- 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 ε -close secret key achievable using the channel n times with two-way public classical communication assistance (passive adversary)

$$\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon) := \sup \{ P : (n, P, \varepsilon) \text{ is achievable for } \mathcal{N} \text{ using LOCC} \}. \quad (1)$$

- 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 many channels of practical interest. Interesting special case: single-mode phase-insensitive bosonic Gaussian channels.

- Technical level: **quantum Shannon theory** with general $n \geq 1$ and $\varepsilon \geq 0$.

- 1 Main Results in 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.

- Previous asymptotic result from [Pirandola *et al.* 2017] in the infinite energy limit

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

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**

$$\frac{1}{n} \hat{P}_{\mathcal{L}_\eta}^{\leftrightarrow}(n, \varepsilon) \leq \log \left(\frac{1}{1 - \eta} \right) + \frac{C(\varepsilon)}{n}, \quad (4)$$

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 ε .
- Other variations of this bound are possible if η is not the same for each channel use, if η is chosen adversarially, etc.
- We give similar bounds for the quantum-limited amplifier channel (tight), thermalizing channels, amplifier channels, and additive noise channels.

Main Result: Dephasing Channels I

- Previous asymptotic result for the **qubit dephasing channel**

$\mathcal{Z}_\gamma : \rho \mapsto (1 - \gamma) \rho + \gamma Z \rho Z$ with $\gamma \in (0, 1)$ is [Bennett *et al.* 1996, Pirandola *et al.* 2017]

$$P^{\leftrightarrow}(\mathcal{Z}_\gamma) := \lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} \hat{P}_{\mathcal{Z}_\gamma}^{\leftrightarrow}(n, \varepsilon) = 1 - h(\gamma), \quad (5)$$

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

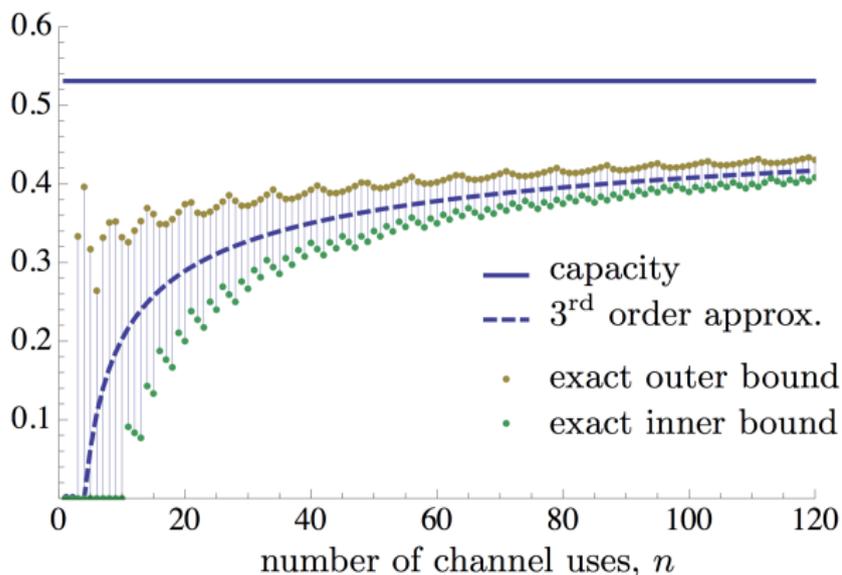
- By combining with [Tomamichel *et al.* 2016] we show the expansion

$$\frac{1}{n} \hat{P}_{\mathcal{Z}_\gamma}^{\leftrightarrow}(n, \varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}} \Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right), \quad (6)$$

with Φ the cumulative standard Gaussian distribution and the binary entropy variance $v(\gamma) := \gamma(\log \gamma + h(\gamma))^2 + (1 - \gamma)(\log(1 - \gamma) + h(\gamma))^2$.

Main Result: Dephasing Channels II

- For the dephasing parameter $\gamma = 0.1$ we get (figure from [Tomamichel *et al.* 2016]):



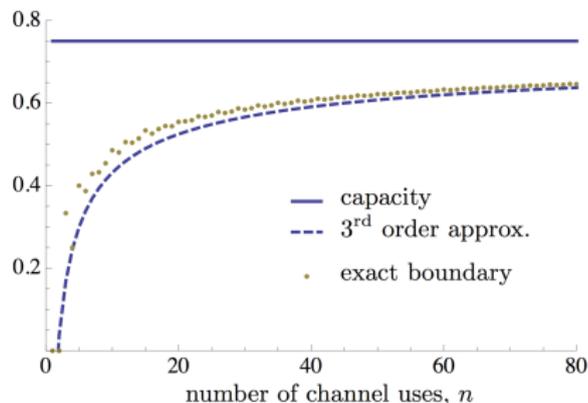
(c) Comparison of strict bounds with third order approximation for $\varepsilon = 5\%$.

Main Result: Erasure Channels

- For the **qubit erasure channel** $\mathcal{E}_p : \rho \mapsto (1-p)\rho + p|e\rangle\langle e|$ with $p \in (0, 1)$ we show by combining with [Tomamichel *et al.* 2016] the expansion

$$\frac{1}{n} \hat{P}_{\mathcal{E}_p}^{\leftrightarrow}(n, \varepsilon) = 1 - p + \sqrt{\frac{p(1-p)}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{1}{n}\right). \quad (7)$$

- For the erasure parameter $p = 0.25$ we get for $\varepsilon = 1\%$ (figure from [Tomamichel *et al.* 2016]):



(b) Comparison of exact bounds with third order approximation.

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 ρ , positive semi-definite operator σ , and $\varepsilon \in [0, 1]$ as

$$D_H^\varepsilon(\rho \parallel \sigma) := -\log \inf \{ \text{Tr}[\Lambda \sigma] : 0 \leq \Lambda \leq I \wedge \text{Tr}[\Lambda \rho] \geq 1 - \varepsilon \}. \quad (8)$$

- The ε -relative entropy of entanglement is defined as

$$E_R^\varepsilon(A; B)_\rho := \inf_{\sigma_{AB} \in \mathcal{S}(A:B)} D_H^\varepsilon(\rho_{AB} \parallel \sigma_{AB}), \quad (9)$$

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

$$E_R^\varepsilon(\mathcal{N}) := \sup_{|\psi\rangle_{AA'} \in \mathcal{H}_{AA'}} E_R^\varepsilon(A; B)_\rho, \quad (10)$$

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 γ_{ABE} with

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E \quad (11)$$

for some state σ_E and measurement channels $\mathcal{M}_A, \mathcal{M}_B$.

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

$$\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U_{ABA'B'}^\dagger, \quad (12)$$

where Φ_{AB} maximally entangled, $U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U_{A'B'}^{ij}$ with each $U_{A'B'}^{ij}$ a unitary, and $\theta_{A'B'}$ a state.

- Work in the latter, bipartite picture where the **adversary is removed**.

Proof Idea: Meta Converse III

- 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]

$$\mathrm{Tr}\{\gamma_{AA'BB'}\sigma_{AA'BB'}\} \leq \frac{1}{K}. \quad (13)$$

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

$$\hat{P}_{\mathcal{N}}(1, \varepsilon) \leq E_R^\varepsilon(\mathcal{N}) \quad (\text{LOCC pre- and post-processing assistance}). \quad (14)$$

For n channel uses this gives

$$\hat{P}_{\mathcal{N}}(n, \varepsilon) \leq E_R^\varepsilon(\mathcal{N}^{\otimes n}). \quad (15)$$

- Finite block-length version of **relative entropy of entanglement** upper bound [Horodecki *et al.* 2005 & 2009].
- The next step is to **evaluate** the meta converse for specific channels of interest.

Proof Idea: Meta Converse IV

- For **teleportation-simulable channels** $\mathcal{N}_{A' \rightarrow B}$ **with associated state** ω_{AB} [Bennett *et al.* 1996, Pirandola *et al.* 2017] the meta converse holds for **general LOCC assistance** and expands as

$$\frac{1}{n} \hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon) \leq E_R(A; B)_{\omega} + \sqrt{\frac{V_{E_R}^{\varepsilon}(A; B)_{\omega}}{n}} \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right), \quad (16)$$

$$\text{where } V_{E_R}^{\varepsilon}(A; B)_{\rho} \equiv \left\{ \begin{array}{ll} \max_{\sigma_{AB} \in \Pi_S} V(\rho_{AB} \| \sigma_{AB}) & \text{for } \varepsilon < 1/2 \\ \min_{\sigma_{AB} \in \Pi_S} V(\rho_{AB} \| \sigma_{AB}) & \text{for } \varepsilon \geq 1/2 \end{array} \right\} \quad (17)$$

with $\Pi_S \subseteq \mathcal{S}(A : B)$ the set of separable states achieving minimum in the relative entropy of entanglement

$$E_R(A; B)_{\rho} := \inf_{\sigma_{AB} \in \mathcal{S}(A : B)} D(\rho_{AB} \| \sigma_{AB}). \quad (18)$$

Here, we have the cumulative standard Gaussian distribution Φ , the relative entropy $D(\rho \| \sigma) := \text{Tr} [\rho (\log \rho - \log \sigma)]$, and the relative entropy variance $V(\rho \| \sigma) := \text{Tr} [\rho (\log \rho - \log \sigma - D(\rho \| \sigma))^2]$.

Extra: Gaussian Formulas

- 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.* 2017] and [Wilde *et al.* 2016], respectively: writing zero-mean Gaussian states in exponential form as

$$\rho = Z_\rho^{-1/2} \exp \left\{ -\frac{1}{2} \hat{x}^T G_\rho \hat{x} \right\} \quad \text{with} \quad (19)$$

$$Z_\rho := \det(V^\rho + i\Omega/2), \quad G_\rho := 2i\Omega \operatorname{arcoth}(2V^\rho i\Omega), \quad (20)$$

and V^ρ the Wigner function covariance matrix for ρ , we have

$$D(\rho||\sigma) = \frac{1}{2} \left(\log \left(\frac{Z_\sigma}{Z_\rho} \right) - \operatorname{Tr} [\Delta V^\rho] \right) \quad (21)$$

$$V(\rho||\sigma) = \frac{1}{2} \operatorname{Tr} \{ \Delta V^\rho \Delta V^\rho \} + \frac{1}{8} \operatorname{Tr} \{ \Delta \Omega \Delta \Omega \}, \quad (22)$$

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

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1, \varepsilon) \leq E_R^\varepsilon(\mathcal{N})$ 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**.
- Improve our bound for the **photon loss channel**

$$\frac{1}{n} \hat{P}_{\mathcal{L}_\eta}^{\leftrightarrow}(n, \varepsilon) \leq \log \left(\frac{1}{1-\eta} \right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2 \log \left(\frac{1+\varepsilon}{1-\varepsilon} \right) \quad (23)$$

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]?