Converse bounds for private communication over quantum channels

Mark M. Wilde (LSU), Marco Tomamichel (Univ. Sydney), and Mario Berta (Caltech)

Based on arXiv:1602.08898 [WTB16]

QCrypt 2016, Washington DC, September 12, 2016
Given is a quantum channel $\mathcal{N}$ and a QKD protocol that uses it $n$ times:

Non-asymptotic private capacity: Maximum rate of $\varepsilon$-close secret key achievable using channel $n$ times and $N_S$ mean photons per channel use:

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

If no photon number constraint, then consider

$$\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon) = \sup_{N_S \geq 0} \hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, N_S, \varepsilon).$$
Main question

- Practical question: How to characterize $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, N_S, \varepsilon)$ for all $n \geq 1$, $N_S \geq 0$, and $\varepsilon \in (0, 1)$?

- 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 $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, N_S, \varepsilon)$ and $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon)$ can be used as benchmarks for quantum repeaters [TGW14].

- This talk discusses the tightest known upper bound on $\hat{P}_{\mathcal{N}}^{\leftrightarrow}(n, \varepsilon)$ for channels of practical interest and thus represents the best known benchmark for quantum repeaters [WTB16].
What was known before?

- Begin by reviewing what is known
- Let’s leap back to QCrypt 2014:

  - Takeoka presented results of [TGW14].
Most interested in the photon loss channel:

\[ \mathcal{L}_\eta : \hat{b} = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{\epsilon} \]

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

Practical question is tough, so consider limiting cases...

**[TGW14] bound:** Consider the limit as \( n \to \infty \) and then \( \varepsilon \to 0 \):

\[
\lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P} \xrightarrow{\mathcal{L}_\eta} (n, N_S, \varepsilon) \leq g((1 + \eta)N_S/2) - g((1 - \eta)N_S/2)
\]

where \( g(x) \equiv (x + 1) \log_2(x + 1) - x \log_2 x \)

is entropy of bosonic thermal state with mean photon number \( x \).

Based on the squashed entanglement measure [CW04].
[TGW14] bound without energy constraint

- Optimizing over energy gives the unconstrained [TGW14] bound:

\[
\lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}_{L, \eta}^\leftrightarrow(n, \varepsilon) \leq \log_2 \left( \frac{1 + \eta}{1 - \eta} \right).
\]

essentially because \( \sup_{N_S \geq 0} g((1 + \eta)N_S/2) - g((1 - \eta)N_S/2) = \log_2 \left( \frac{1 + \eta}{1 - \eta} \right) \).

- [TGW14] established existence of a fundamental rate-loss trade-off for any possible QKD protocol that uses a photon-loss channel.

- Bound is finite for all \( \eta \in [0, 1) \) and depends only on \( \eta \).

- Main drawback is that it is an asymptotic statement and thus has limited applicability in practice.

- (Original proof didn’t address issue with unbounded shield systems — now fixed in [W16])
Fundamental rate-loss trade-off from [TGW14]

Can translate x-axis to km by assuming fiber has 0.2 dB loss / km
By a different method, [PLOB15] established the upper bound:

\[
\lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}, \eta}(n, \varepsilon) \leq \log_2 \left( \frac{1}{1 - \eta} \right).
\]

\((\ast)\)

In fact, with an infinite number of channel uses, infinite energy, and perfect quantum computers for Alice and Bob, the bound is tight:

\[
\lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}, \eta}(n, \varepsilon) = \log_2 \left( \frac{1}{1 - \eta} \right).
\]

Drawbacks are the same: An asymptotic statement, and thus says little for practical protocols (called a weak converse bound)

Method used in [PLOB15] does not give any improved bound for protocols using finite energy (Finite-energy SE can be tighter [GEW16])

(Proof of \((\ast)\) in [PLOB15, Supp. Mat., Sec. III] does not address issue of unbounded shield systems, & thus their proof gives trivial upper bound of \(\infty\) for LHS of \((\ast)\) — this issue is addressed and fixed in [WTB16])
Upper bound for non-asymptotic private capacity [WTB16]

Bound on Non-Asymptotic Private Capacity

One consequence of the meta-converse approach in [WTB16]:

$$\hat{P}_{L_\eta}(n, \varepsilon) \leq \log_2 \left( \frac{1}{1 - \eta} \right) + \frac{C(\varepsilon)}{n},$$

where $C(\varepsilon) \equiv \log_2 6 + 2 \log_2 \left( \frac{1 + \varepsilon}{1 - \varepsilon} \right)$ (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.
- Remaining technical questions: Improve $C(\varepsilon)$ to $\log_2 \left( \frac{1}{1 - \varepsilon} \right)$? Finite-energy bound?
Meta-converse approach approach from [WTB16]

- Building on [Bla74, BDSW96, BK98, HW01, HHHO05, Che05, DJKR06, HHHO09, CKR09, PPV10, BD11, Li14, TH13, TT15, MLDS\(^+\)13, WWY14, TWW14, DPR15, TBR15, PLOB15]

- Meta-converse approach starts by using hypothesis testing relative entropy to compare the actual state resulting from the protocol to a separable state, the latter being useless for private comm.

- The approach extracts the relevant parameters of the protocol (\(n\), rate \(P\), and \(\varepsilon\)) and relates them via an information-like quantity.

- The meta-converse leads to various other bounds, including Renyi-entropic strong converse bounds and others in terms of relative entropy and relative entropy variance.

- Result: We get the tightest known upper bounds for non-asymptotic private capacity of many channels of practical interest.
Information measures

- Hypothesis testing relative entropy defined for a state $\rho$, positive semi-definite operator $\sigma$, and $\varepsilon \in [0, 1]$ as
  \[
  D_H^\varepsilon(\rho\|\sigma) \equiv -\log \left[ \min \{ \text{Tr}\{\Lambda \sigma\} : 0 \leq \Lambda \leq I \wedge \text{Tr}\{\Lambda \rho\} \geq 1 - \varepsilon \} \right].
  \]

- 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
\[
D(\rho\|\sigma) \equiv \text{Tr}\{\rho[\log \rho - \log \sigma]\},
\]
\[
V(\rho\|\sigma) \equiv \text{Tr}\{\rho[\log \rho - \log \sigma - D(\rho\|\sigma)]^2\}
\]
\[
\Phi(a) \equiv \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{a} dx \exp\left(-x^2/2\right)
\]
Example: Dephasing channel [TBR15, WTB16]

For the qubit dephasing channel

$$Z^\gamma : \rho \mapsto (1 - \gamma) \rho + \gamma Z \rho Z,$$

with $\gamma \in (0, 1)$, the non-asymptotic private capacity $\hat{P}^{\leftrightarrow}(n, \varepsilon)$ satisfies

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

where $\Phi$ 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: Dephasing channel [TBR15, WTB16]

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

$(\gamma = 0.1$, plot taken from [TBR15])
Example: Erasure channel [TBR15, WTB16]

For the qubit erasure channel

$$\mathcal{E}_{A' \to B}^p : \rho_{A'} \mapsto (1 - p)\rho_B + p|e\rangle\langle e|_B$$

with $p \in (0, 1)$, the non-asymptotic private capacity $\hat{P}_{\mathcal{E}^p}(n, \epsilon)$ satisfies

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

Moreover, the following expansion holds

$$\hat{P}_{\mathcal{E}^p}(n, \epsilon) = 1 - p + \sqrt{\frac{p(1-p)}{n}} \Phi^{-1}(\epsilon) + O\left(\frac{1}{n}\right).$$
Example: Erasure channel [TBR15, WTB16]

\( p = 0.25, \) plot taken from [TBR15]

(b) Comparison of exact bounds with third order approximation.
Second-order expansions of converse bounds [WTB16]

**Theorem**

If a finite-dim. quantum channel $\mathcal{N}_{A' \rightarrow B}$ is covariant, then

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

where $\rho_{AB} = \mathcal{N}_{A' \rightarrow B}(\Phi_{AA'})$, $E_R(A; B)_\rho$ is the relative entropy of entanglement,

and

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

with $\Pi_S \subseteq S(A:B)$ the set of states achieving minimum in $E_R(A; B)_\rho$. 
Application: Quantum Gaussian channels [WTB16]

Definitions of quantum Gaussian channels

- Thermal channel $\mathcal{L}_{\eta,N_B}$: $\hat{b} = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{e}$,

- Amplifier channel $\mathcal{A}_{G,N_B}$: $\hat{b} = \sqrt{G} \hat{a} + \sqrt{G - 1} \hat{e}^\dagger$,

- Additive-noise channel $\mathcal{W}_\xi$: $\hat{b} = \hat{a} + (x + ip) / \sqrt{2}$,

- 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 rel. entropies of entanglement [PLOB15]

- For the thermal channel $\mathcal{L}_{\eta,N_B}$, $E_R$ evaluates to
  $$-\log_2 \left( (1 - \eta) \eta^N_B \right) - g(N_B).$$

- For the amplifier channel $\mathcal{A}_{G,N_B}$, $E_R$ evaluates to
  $$\log_2 \left( \frac{G^{N_B+1}}{G - 1} \right) - g(N_B).$$

- For the additive noise channel $\mathcal{W}_\xi$, $E_R$ evaluates to
  $$\frac{\xi - 1}{\ln 2} - \log_2 \xi.$$
Let $V_{\mathcal{L},N_B}$, $V_{\mathcal{A},N_B}$, and $V_{\mathcal{W},\xi}$ be the unconstrained relative entropy variances of the thermalizing, amplifier, and additive-noise channels, respectively:

$$V_{\mathcal{L},N_B} \equiv N_B(N_B + 1) \log_2^2(\frac{\eta [N_B + 1]}{N_B}),$$
$$V_{\mathcal{A},N_B} \equiv N_B(N_B + 1) \log_2^2(\frac{G^{-1} [N_B + 1]}{N_B}),$$
$$V_{\mathcal{W},\xi} \equiv (1 - \xi)^2 / \ln^2 2.$$

Can compute these from a general formula for relative entropy variance of two Gaussian states [WTLB16].
The following strong converse bounds hold for $\varepsilon \in (0, 1)$:

1. $\hat{P}_{\mathcal{L}_{\eta},N_B}(n, \varepsilon) \leq -\log_2 \left( (1 - \eta) \eta^{N_B} \right) - g(N_B) + \sqrt{\frac{2V_{\mathcal{L}_{\eta},N_B}}{n(1 - \varepsilon)}} + C(\varepsilon)/n,$

2. $\hat{P}_{\mathcal{A}_G,N_B}(n, \varepsilon) \leq \log_2 \left( \frac{G^{N_B+1}}{G - 1} \right) - g(N_B) + \sqrt{\frac{2V_{\mathcal{A}_G,N_B}}{n(1 - \varepsilon)}} + C(\varepsilon)/n,$

3. $\hat{P}_{\mathcal{W}_\xi}(n, \varepsilon) \leq \frac{\xi - 1}{\ln 2} - \log_2 \xi + \sqrt{\frac{2V_{\mathcal{W}_\xi}}{n(1 - \varepsilon)}} + C(\varepsilon)/n.$
Corollary

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

$$\hat{P}_{\mathcal{L}_\eta}(n, \varepsilon) \leq \log_2 \left( \frac{1}{1 - \eta} \right) + \frac{C(\varepsilon)}{n},$$

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

- We have established bounds for QKD protocols conducted over quantum channels that are unassisted by quantum repeaters.
- Meta-converse has several 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 QKD 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.
- We have generalized these results to broadcast channels with a single sender and multiple receivers [TSW16].
- Squashed entanglement technique applied more generally in [GEW16].
Methods

- As said before, we build on a variety of techniques and approaches given in previous literature:
- Meta-converse approach for hypothesis testing [Li14, TH13, DPR15], classical communication [TT15], and quantum communication [TWW14, TBR15]
- Private states [HHHO05, HHHO09], a privacy test [HHH^+08b, HHH^+08a], and relative entropy of entanglement as an upper bound on distillable key [HHHO05, HHHO09]
- Gaussian states and channels [HW01] and formulas for relative entropy for Gaussian states [Che05, PLOB15]
- \(\varepsilon\)-relative entropy of entanglement [BD11] and sandwiched Renyi relative entropy [MLDS^+13, WWY14]
- Reduction of adaptive protocols to non-adaptive ones via simulation of channels by teleportation [BDSW96, PLOB15]
Private states

Tripartite key state

A tripartite key state $\gamma_{ABE}$ contains log $K$ bits of secret key if there exists a state $\sigma_E$ and measurement channels $\mathcal{M}_A$ and $\mathcal{M}_B$ such that

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

Bipartite private state

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

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

where $U_{ABA'B'}$ is a “twisting” unitary of the form

$$U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U_{A'B'}^{ij},$$

with each $U_{A'B'}^{ij}$ a unitary, and $\theta_{A'B'}$ a state.
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 $\gamma_{ABE}$, 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 $\mathcal{N}_{A'\rightarrow B}$. Let $U_{A'\rightarrow BE}^N$ be an isometric extension of $\mathcal{N}_{A'\rightarrow B}$.

- 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, $\mathcal{E}_{K'\rightarrow A'^n}$ is the encoder, and $\mathcal{D}_{B^n\rightarrow \hat{K}}$ is the decoder.
A triple \((n, P, \varepsilon)\) 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 \(\mathcal{N}_{A'\rightarrow B}\) if there exists a secret-key generation protocol \(\{|K|, \mathcal{E}, \mathcal{D}\}\) and some state \(\omega_{En}\) such that
\[
\frac{1}{n} \log |K| \geq P \quad \text{and} \\
F(\Phi_{KK'} \otimes \omega_{En}, \rho_{KK'En}) \geq 1 - \varepsilon,
\]
where \(\rho_{KK'En} \equiv (\mathcal{D}_{B^n \rightarrow \hat{K}} \circ (\mathcal{U}_{A'\rightarrow BE})^n \circ \mathcal{E}_{K'\rightarrow A'})(\Phi_{KK'})\) and
\[
\Phi_{KK'} = \frac{1}{|K|} \sum_{i=0}^{|K|-1} |i\rangle\langle i|_K \otimes |i\rangle\langle i|_{K'}.
\]
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

\[ K' \]

\[ A' \]

\[ A' \]

\[ B \]

\[ A'' \]

\[ B'' \]

Due to equivalence between tripartite and bipartite pictures

\[ F(\gamma_{K_AK_BS_A}, \rho_{K\hat{K}MA''B''}) \geq 1 - \varepsilon, \]

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

\[ \rho_{K\hat{K}MA''B''} \equiv (\mathcal{U}_B^{\mathcal{D}} \circ \hat{K}_{B''} \circ (\mathcal{U}_A^{\mathcal{N}} \rightarrow BE) \otimes n \circ \mathcal{U}_B^{\mathcal{E}} \rightarrow A''A'')(\Phi_{KK'M}^{GHZ}). \]
Non-asymptotic achievable region

Non-asymptotic fundamental limit

Boundary of the achievable region:

\[ \hat{P}_N(n, \varepsilon) \equiv \max \{ P : (n, P, \varepsilon) \text{ is achievable for } N \} \]

Interpretation

- Boundary \( \hat{P}_N(n, \varepsilon) \) identifies how rate can change as a function of \( n \) for fixed error \( \varepsilon \), and 2nd-order coding rates can 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 boundary of non-asymptotic achievable region similarly as

\[ \hat{P}_{N}^{\leftrightarrow} (n, \varepsilon) \equiv \max \{ P : (n, P, \varepsilon) \text{ is achievable for } N \text{ using } \leftrightarrow \} . \]
Information measures

- Can use hypothesis testing relative entropy to define the \( \varepsilon \)-relative entropy of entanglement:

\[
E_R^\varepsilon(A; B)_\rho \equiv \inf_{\sigma_{AB} \in S(A:B)} D_H^\varepsilon(\rho_{AB} \parallel \sigma_{AB}).
\]

where \( S(A:B) \) is the set of separable states

- Can also define a channel’s \( \varepsilon \)-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 \( \rho_{AB} \equiv \mathcal{N}_{A' \rightarrow B}(|\psi_{AA'}\rangle) \)

- Standard relative entropies of entanglement defined by replacing \( D_H^\varepsilon \) with quantum relative entropy \( D \)
Privacy test

- Can test whether a given state is a $\gamma$-private state by “untwisting” and projecting onto the maximally entangled state:

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

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

- 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

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

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

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

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

$$\hat{P}_N(1, \varepsilon) \leq E^\varepsilon_R(N).$$

“One-shot $\varepsilon$-private capacity $\leq$ channel’s $\varepsilon$-relative entropy of entanglement.”

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

Proof idea: use monotonicity of $E^\varepsilon_R$ with respect to LOCC and use the bounds on the previous slide.
Corollary

The following bound holds for $n$ channel uses:

$$\hat{P}_N(n, \varepsilon) \leq \frac{1}{n} E^\varepsilon(N^\otimes n).$$

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

The previous theorem and this corollary then imply all of our previous results, with some extra work needed to establish a formula for the relative entropy variance of Gaussian states.
Theorem

If a quantum channel $N_{A' \rightarrow B}$ is teleportation-simulable with associated state $\omega_{AB}$, then

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

where

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

with $\Pi_S \subseteq S(A:B)$ the set of states achieving minimum in $E_R(A; B)_\rho$. 
Writing zero-mean Gaussian states in exponential form as

\[
\rho = Z^\rho \exp\left\{-\frac{1}{2} \hat{x}^T G^\rho \hat{x}\right\}, \quad \sigma = Z^\sigma \exp\left\{-\frac{1}{2} \hat{x}^T G^\sigma \hat{x}\right\},
\]

where

\[
Z^\rho \equiv \det(V^\rho + i\Omega/2), \quad Z^\sigma \equiv \det(V^\sigma + i\Omega/2),
\]
\[
G^\rho \equiv 2i\Omega \text{arcoth}(2V^\rho i\Omega), \quad G^\sigma \equiv 2i\Omega \text{arcoth}(2V^\sigma i\Omega),
\]

and \( V^\rho \) and \( V^\sigma \) are Wigner function covariance matrices for \( \rho \) and \( \sigma \).

**Theorem**

For zero-mean Gaussian states \( \rho \) and \( \sigma \), the relative entropy variance is

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

where \( \Delta \equiv G^\rho - G^\sigma \).


