# A meta-converse 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, LA 70803, USA

Marco Tomamichel
School of Physics,
The University of Sydney,
Sydney, NSW 2006, Australia

Mario Berta
Institute for Quantum
Information and Matter,
California Institute of Technology,
Pasadena, CA 91125, USA

***Abstract*—We establish a converse bounds on the private transmission capabilities of a quantum channel. The main conceptual development builds firmly on the notion of a private state, which is a powerful, uniquely quantum method for simplifying the tripartite picture of privacy involving local operations and public classical communication to a bipartite picture of quantum privacy involving local operations and classical communication. This approach has previously led to some of the strongest upper bounds on secret key rates, including the squashed entanglement and the relative entropy of entanglement. Here we use this approach along with a "privacy test" to establish a general meta-converse bound for private communication.**

## I. Introduction

Ever since the discovery of quantum key distribution [3], researchers have been interested in exploiting quantum-mechanical effects in order to ensure the secrecy of communication. This has led to a large amount of research in many directions [21], both experimental and theoretical, and one of the recent challenges has been to connect both of these directions.

On the theoretical side, much progress has been made by generalizing several ideas developed in the context of classical information theory. For example, the wiretap channel is a simple model for private communication, and one can study its capacity for secure data transmission [33]. In this model, two honest parties, usually called Alice (the sender) and Bob (the receiver), are connected by a classical channel. At the same time, there is a classical channel connecting Alice to an eavesdropper or wiretapper, usually called Eve. The goal is to devise a communication scheme such that Alice can communicate to Bob with small error in such a way that Eve gets nearly zero information about the message communicated (with both the probability of error and information leakage vanishing in the limit of many channel uses). One can further generalize the model to allow for public classical communication and study capacities in this context [1], [17]. However, two major drawbacks of the wiretap model is that the honest parties need to assume that they have fully characterized both 1) their channel and 2) the channel to the eavesdropper, which may not be possible in practice. Nevertheless, techniques developed in the context of the wiretap channel have been foundational to our understanding of information-theoretically secure communication.

Quantum mechanics offers a route around one of the aforementioned problems with the classical model, via the notion of purification. Indeed, for any quantum channel connecting Alice to Bob, there is a purification (or isometric extension) of this channel that is unique up to unitary rotations. All the degrees of freedom that are not accessible to the receiver Bob are accessible to the environment of the channel, and in the spirit of being cautious, as is usually the case in cryptography, we assume that the eavesdropper has full access to the environmental system. For example, communication from Alice to Bob in free space can be modeled by an interaction at a beamsplitter [22], and in the wiretap model, we assume that all of the light that is lost along the way can be collected by the eavesdropper Eve [10]. Thus, in the quantum wiretap model, Alice and Bob can perform parameter estimation to characterize their channel, and once they have a complete characterization, they also have a model for the channel to the eavesdropper, circumventing one of the aforementioned problems with the classical model. If we allow for Alice and Bob to make use of public classical communication in addition to the quantum channel (see, e.g., [27], [28]), then this model is closely related to that which is used in some quantum key distribution protocols. In practice, one drawback of this model is that the channel from Alice to Bob might be changing with time or difficult to characterize, but nevertheless one can study the private capacities of this quantum wiretap channel model in an attempt to gain some understanding of what rates might be achievable in principle.

With this Shannon-theoretic viewpoint, the quantum wiretap model has been studied in much detail. The private capacity of a quantum wiretap channel was defined and characterized in [7], [8]. For the class of degradable quantum channels, there is a tractable formula for the private capacity [23]. Beyond such channels, little is known and recent evidence suggests that characterizing private capacity effectively is challenging [9], [16], [24].

More recently there has been progress on characterizing the private capacity when public classical communication is available (for a given channel $\mathcal{N}$, let $P^{\leftrightarrow}(\mathcal{N})$ denote this quantity). The authors of [28] defined the squashed entanglement of a channel and showed that it is an upper bound on $P^{\leftrightarrow}(\mathcal{N})$ for any channel $\mathcal{N}$. This result thus established a strong limitation for quantum key distribution protocols as discussed in [27]. Following this development, by building on the notion of relative entropy of entanglement and the fact that this quantity is also an upper

bound on the distillable key of a bipartite state [13], [14], the authors of [20] defined a channel's relative entropy of entanglement and showed that it is an upper bound on $P^{\leftrightarrow}(\mathcal{N})$ for any channel $\mathcal{N}$ that has a "teleportation symmetry" identified in [4, Section V] and extended in [19], [20]. It is an open question to determine whether the relative entropy of entanglement is an upper bound on the two-way assisted private capacity of a general quantum channel.

Both of the aforementioned upper bounds on $P^{\leftrightarrow}(\mathcal{N})$ critically rely upon the notion of a private state [13], [14]. To motivate this notion, consider that the ultimate goal of a $P^{\leftrightarrow}$ protocol is to generate a secret-key state of the form

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K}\sum_{i=0}^{K-1} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E, \tag{1}$$

where the $A$ system is possessed by Alice, $B$ by Bob, and $E$ by the eavesdropper, $\gamma_{ABE}$ is some state on systems $ABE$, $\mathcal{M}(\cdot) = \sum_i |i\rangle\langle i|(\cdot)|i\rangle\langle i|$ is a projective measurement channel, and $\sigma_E$ is some state on system $E$. The state in (1) is such that the systems $A$ and $B$ are perfectly correlated (i.e., maximally classically correlated), and the value of the key is uniformly random and independent of Eve's system $E$. The main observation of [13], [14] is that, in principle, every step of a $P^{\leftrightarrow}$ protocol can be purified, and since these steps are conducted in the laboratories of Alice and Bob, these parties could possess purifying systems of $\gamma_{ABE}$ (call them $A'$ and $B'$), such that $\gamma_{ABA'B'E}$ is a pure state satisfying $\mathrm{Tr}_{A'B'}\{\gamma_{ABA'B'E}\} = \gamma_{ABE}$. By employing purification theorems of quantum information theory, the authors of [13], [14] showed that the reduced state of $\gamma_{ABA'B'E}$ on the systems $ABA'B'$ has the following form:

$$\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U^{\dagger}_{ABA'B'}, \tag{2}$$

where $\Phi_{AB}$ is a maximally entangled state, $U_{ABA'B'}$ is a special kind of unitary called a "twisting," and $\theta_{A'B'}$ is an arbitrary state (see Section II for more details). Such a state is now known as a bipartite private state and is fully equivalent to the state in (1) in the aforementioned sense. This observation thus allows for a perspective change which is helpful for analyzing private communication protocols: one can eliminate the eavesdropper from the analysis, revising the goal of such a protocol to be the production of states of the form in (2), and this allows for using the powerful tools of entanglement theory [15] to analyze secret-key rates.

Not only did the results of [13], [14] provide a conceptually different method for understanding privacy in the quantum setup, but they also showed how there are fundamental differences between entanglement distillation and secret-key distillation protocols. Indeed, the strongest demonstration of this difference was the realization that there exist quantum channels that have zero capacity to send quantum information and yet can generate private information at a non-zero rate [11], [12]. This in turn led to the discovery of the superactivation effect [25], [26]: two quantum channels each having zero quantum capacity can be used together to have a non-zero quantum capacity, by taking advantage of the intricate interplay between privacy and coherence.

In all of the above theoretical analyses, the statements made are asymptotic in nature, applying exclusively to the situation in which a large number of independent and identical channel uses are available. While these works have provided interesting bounds and are conceptually rich, they are somewhat removed from practical situations in which the number of channel uses is limited. However, some recent works have aimed to bridge this gap for the case of quantum communication [2], [6], [18], [29], [30], giving more refined bounds on what is possible and impossible for a limited number of channel uses. One goal of the present paper is to bridge the gap for private communication.

## II. Private States

We use standard notation and assume knowledge of basic concepts in quantum information theory. Private states [13], [14] are an essential ingredient of our development, and we review their basics here.

**Definition 1.** *A tripartite key state $\gamma_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$ contains $\log K$ bits of secret key if there exists a state $\sigma_E \in \mathcal{D}(\mathcal{H}_E)$ and a projective measurement channels $\mathcal{M}_A$ and $\mathcal{M}_B$ such that (1) holds.*

That is, we see that the systems $A$ and $B$ are maximally classically correlated, and the key value is uniformly random and independent of the $E$ system. Physically, we can think of the $A$ system as being in Alice's laboratory, $B$ in Bob's, and $E$ in Eve's. We also think of Alice and Bob as two honest parties and Eve as a malicious eavesdropper whose system should ideally be independent of the key systems possessed by Alice and Bob.

Purifying such a state $\gamma_{ABE}$ with two systems $A'$ and $B'$, thinking of $A'$ as being available to Alice and $B'$ as being available to Bob (or alternatively as not being available to Eve), and tracing out the $E$ system then leads to the notion of a bipartite private state $\gamma_{ABA'B'}$ [13], [14]. As shown in [13], [14], any such state $\gamma_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ takes a canonical form:

**Definition 2.** *A bipartite private state $\gamma_{A''B''} \in \mathcal{D}(\mathcal{H}_{A''B''})$ contains $\log K$ bits of secret key if $\mathcal{H}_{A''} = \mathcal{H}_A \otimes \mathcal{H}_{A'}$ and $\mathcal{H}_{B''} = \mathcal{H}_B \otimes \mathcal{H}_{B'}$ such that $\gamma_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ has the form (2) where $U_{ABA'B'}$ is a "twisting" unitary of the form*

$$U_{ABA'B'} = \sum_{i,j=0}^{K-1} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'}, \tag{3}$$

*with each $U^{ij}_{A'B'}$ a unitary, and $\theta_{A'B'} \in \mathcal{D}(\mathcal{H}_{A'B'})$.*

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 $A$ and $B$ from any party possessing a purification of $\gamma_{ABA'B'}$. Such bipartite private states are in one-to-one correspondence with the tripartite key states given in (1) [13], [14]. That is, for every state $\gamma_{ABE}$ of the form in (1), we can find a state of the form in (2) and vice versa. We summarize this as the following proposition [13], [14]:

**Proposition 3.** *Bipartite private states and tripartite key states are equivalent. That is, for $\gamma_{ABA'B'}$ a bipartite private state, $\gamma_{ABE}$ is a tripartite key state for any purification $\gamma_{ABA'B'E}$ of $\gamma_{ABA'B'}$. Conversely, for any tripartite key state $\gamma_{ABE}$ and any purification $\gamma_{ABA'B'E}$ of it, $\gamma_{ABA'B'}$ is a bipartite private state.*

This correspondence takes on a more physical form (reviewed in Section III), which is that any tripartite protocol whose aim it is to extract tripartite key states of the form in (1) is in one-to-one correspondence with a bipartite protocol whose aim it is to extract bipartite private states of the form in (2) [13], [14].

**Definition 4.** *A state $\rho_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$ is an $\varepsilon$-approximate tripartite key state if there exists a tripartite key state $\gamma_{ABE}$ of the form in (1) such that*

$$F(\rho_{ABE}, \gamma_{ABE}) \geq 1 - \varepsilon, \tag{4}$$

*where $\varepsilon \in [0,1]$. Similarly, a state $\rho_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ is an $\varepsilon$-approximate bipartite private state if there exists a bipartite private state $\gamma_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ of the form in (2) such that*

$$F(\rho_{ABA'B'}, \gamma_{ABA'B'}) \geq 1 - \varepsilon. \tag{5}$$

Approximate tripartite key states are in one-to-one correspondence with approximate bipartite private states [14, Theorem 5], as summarized below:

**Proposition 5.** *If $\rho_{ABA'B'}$ is an $\varepsilon$-approximate bipartite key state with $K$ key values, then Alice and Bob hold an $\varepsilon$-approximate tripartite key state with $K$ key values. The converse statement is true as well.*

## III. Private classical communication over quantum channels

In this section, we define secret-key transmission codes and measures of their performance. We also review the identification from [13], [14], which shows how a tripartite key distillation protocol is in one-to-one correspondence with a bipartite private state distillation protocol.

### A. Secret-key transmission codes

Given is a quantum channel $\mathcal{N}_{A'\to B}$. Let $\mathcal{N}^{\otimes n}_{A'\to B}$ denote the tensor-product channel, $U^{\mathcal{N}}_{A'\to BE}$ an isometric extension of $\mathcal{N}_{A'\to B}$, and $\mathcal{U}^{\mathcal{N}}_{A'\to BE}$ the associated isometric channel. A secret-key transmission 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 transmitted, $\mathcal{E}_{K'\to A'^n}$ is the encoder (a completely positive trace-preserving (CPTP) map), and $\mathcal{D}_{B^n\to\hat{K}}$ is the decoder (another CPTP map). The protocol begins with a third party preparing a maximally classically correlated state $\overline{\Phi}_{KK'}$ of the following form:

$$\overline{\Phi}_{KK'} \equiv \frac{1}{|K|} \sum_{i=0}^{|K|-1} |i\rangle\langle i|_K \otimes |i\rangle\langle i|_{K'}, \tag{6}$$

and then sending the $K'$ system to Alice. Alice then inputs the $K'$ system to an encoder $\mathcal{E}_{K'\to A'^n}$, transmits the $A'^n$ systems through the tensor-power channel $(\mathcal{U}^{\mathcal{N}}_{A'\to BE})^{\otimes n}$, and the receiver Bob applies the decoder $\mathcal{D}_{B^n\to\hat{K}}$ to the systems $B^n$. The state at the end of the protocol is

$$\rho_{K\hat{K}E^n} \equiv (\mathcal{D}_{B^n\to\hat{K}} \circ (\mathcal{U}^{\mathcal{N}}_{A'\to BE})^{\otimes n} \circ \mathcal{E}_{K'\to A'^n})(\overline{\Phi}_{KK'}). \tag{7}$$

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

$$F(\overline{\Phi}_{K\hat{K}} \otimes \omega_{E^n}, \rho_{K\hat{K}E^n}) \geq 1 - \varepsilon, \tag{8}$$

where

$$\rho_{K\hat{K}E^n} \equiv (\mathcal{D}_{B^n\to\hat{K}} \circ (\mathcal{U}^{\mathcal{N}}_{A'\to BE})^{\otimes n} \circ \mathcal{E}_{K'\to A'^n})(\overline{\Phi}_{KK'}). \tag{9}$$

Thus, the goal of such a secret-key transmission protocol is to realize an $\varepsilon$-approximate tripartite secret-key state as defined in (4). Note that this definition of secret-key transmission combines the error probability and the security parameter into a single parameter $\varepsilon$, in contrast to the other definitions in the literature. Doing so turns out to be beneficial for the developments in this paper. We compare different definitions in the full version [32].

As mentioned before Definition 4, it is possible to purify a secret-key transmission protocol [13], [14], such that every step is performed coherently and the ultimate goal is to produce a private bipartite state $\gamma_{K_AK_BS_AS_B}$, where we now denote the key systems by $K$ and the shield systems by $S$. In the class of protocols discussed above, this consists of replacing each step with the following:

1) A third party preparing a purification of the state $\overline{\Phi}_{KK'}$, which is a "GHZ state" that we denote by $|\Phi^{\text{GHZ}}\rangle_{KK'M} \equiv |K|^{-1/2}\sum_i |i\rangle_K \otimes |i\rangle_{K'} \otimes |i\rangle_M$, and giving the $K'$ system to Alice,
2) Alice performing an isometric extension of the encoder $\mathcal{E}_{K'\to A'^n}$, denoted by $\mathcal{U}^{\mathcal{E}}_{K'\to A'^nA''}$,
3) Bob performing an isometric extension of the decoder $\mathcal{D}_{B^n\to\hat{K}}$, denoted by $\mathcal{U}^{\mathcal{D}}_{B^n\to\hat{K}B''}$.

By employing [14, Theorem 5], we find that (8) implies

$$F(\gamma_{K_AK_BS_AS_B}, \rho_{K\hat{K}MA''B''}) \geq 1 - \varepsilon, \tag{10}$$

for some private state $\gamma_{K_AK_BS_AS_B}$, where we make the identifications $K_A \equiv K_B \equiv K$, $S_A \equiv MA''$, $S_B \equiv B''$, and

$$\rho_{K\hat{K}MA''B''} \equiv (\mathcal{U}^{\mathcal{D}}_{B^n\to\hat{K}B''} \circ (\mathcal{U}^{\mathcal{N}}_{A'\to BE})^{\otimes n} \circ \mathcal{U}^{\mathcal{E}}_{K'\to A'^nA''})(\Phi^{\text{GHZ}}_{KK'M}). \tag{11}$$

### B. Non-asymptotic achievable regions

The non-asymptotic private achievable region of a quantum channel is the union of all achievable triples $(n, P, \varepsilon)$, and we are interested in understanding its boundary:

$$\hat{P}_{\mathcal{N}}(n,\varepsilon) \equiv \max\{P : (n, P, \varepsilon) \text{ achievable on } \mathcal{N}\}. \tag{12}$$

This identifies how the rate can change as a function of $n$ for fixed error $\varepsilon$, and second-order coding rates can characterize this boundary for sufficiently large $n$.

## IV. META-CONVERSE BOUND

### A. Information measures

The general meta-converse bound in Section IV-B is given in terms of the following quantity, defined for $\rho \in \mathcal{D}(\mathcal{H})$, $\sigma \in \mathcal{L}_+(\mathcal{H})$, and $\varepsilon \in [0,1]$ as

$$D_H^\varepsilon(\rho\|\sigma) \equiv -\log\left[\min\{\mathrm{Tr}\{\Lambda\sigma\} : 0 \leq \Lambda \leq I \wedge \mathrm{Tr}\{\Lambda\rho\} \geq 1-\varepsilon\}\right]. \quad (13)$$

If $\sigma$ is a quantum state, $D_H^\varepsilon(\rho\|\sigma)$ has an interpretation as the optimal exponent of the Type II error in a hypothesis test to distinguish $\rho$ from $\sigma$, given the constraint that the Type I error should not exceed $\varepsilon$. It is monotone non-increasing with respect to quantum channels. From this quantity follows an information measure [5, Definition 4] closely related to the relative entropy of entanglement [31]:

$$E_R^\varepsilon(A;B)_\rho \equiv \inf_{\sigma_{AB}\in\mathcal{S}(A:B)} D_H^\varepsilon(\rho_{AB}\|\sigma_{AB}), \quad (14)$$

where $\mathcal{S}(A:B)$ denotes the set of separable states. This quantity is an LOCC (local operations and classical communication) monotone, meaning that

$$E_R^\varepsilon(A;B)_\rho \geq E_R^\varepsilon(A';B')_\omega, \quad (15)$$

for $\omega_{A'B'} \equiv \Lambda_{AB\to A'B'}(\rho_{AB})$, with $\Lambda_{AB\to A'B'}$ an LOCC channel. This follows because the underlying quantity $D_H^\varepsilon$ is monotone non-increasing with respect to quantum channels and the set of separable states is closed under LOCC channels. More generally, $E_R^\varepsilon(A;B)_\rho$ is monotone non-increasing with respect to separability-preserving channels for the same reasons. We can extend the definition in (14) to be a function of a quantum channel $\mathcal{N}_{A'\to B}$:

$$E_R^\varepsilon(\mathcal{N}) \equiv \sup_{|\psi\rangle_{AA'}\in\mathcal{H}_{AA'}} E_R^\varepsilon(A;B)_\rho, \quad (16)$$

where $\rho_{AB} \equiv \mathcal{N}_{A'\to B}(\psi_{AA'})$. Note that it suffices to perform the optimization with respect to pure states due to the fact that $D_H^\varepsilon$ satisfies the data processing inequality. The quantity $E_R^\varepsilon(\mathcal{N})$ will play an important role in establishing upper bounds on the private transmission capabilities of a quantum channel.

### B. Privacy test

Here we define a "privacy test" as a method for testing whether a given bipartite state is private. In some sense, this notion is already implicit in the developments of [14, Eqns. (282)–(284)] and stated even more explicitly in [11], [12]. We state the notion here concretely for completeness.

**Definition 6** (Privacy test)**.** *Let $\gamma_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ be a bipartite private state as given in Definition 2. A privacy test corresponding to $\gamma_{ABA'B'}$ (a $\gamma$-privacy test) is defined as the following dichotomic measurement:*

$$\{\Pi_{ABA'B'}, I_{ABA'B'} - \Pi_{ABA'B'}\}, \quad (17)$$

*where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB}\otimes I_{A'B'})U^\dagger_{ABA'B'}$ and $U_{ABA'B'}$ is the unitary specified in (3).*

If one has access to the systems $ABA'B'$ of a bipartite state $\rho_{ABA'B'}$ and has a description of $\gamma_{ABA'B'}$ satisfying (5), then the $\gamma$-privacy test decides whether $\rho_{ABA'B'}$ is a private state with respect to $\gamma_{ABA'B'}$. The first outcome corresponds to the decision "yes, it is a $\gamma$-private state," and the second outcome corresponds to "no." Physically, this test is just untwisting the purported private state and projecting onto a maximally entangled state. The following lemma states that the probability for an $\varepsilon$-approximate bipartite private state to pass the $\gamma$-privacy test is high:

**Lemma 7.** *Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{ABA'B'})$ be an $\varepsilon$-approximate private state as given in Definition 4, with $\gamma_{ABA'B'}$ satisfying (5). The probability for $\rho_{ABA'B'}$ to pass the $\gamma$-privacy test is never smaller than $1-\varepsilon$:*

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1-\varepsilon, \quad (18)$$

*where $\Pi_{ABA'B'}$ is defined as above.*

*Proof.* See full version [32]. □

On the other hand, we have the following property of separable states [14, Eqns. (282)–(284)]:

**Lemma 8** ( [14, Eqn. (281)])**.** *For a separable state $\sigma_{ABA'B'} \in \mathcal{S}(AA':BB')$, the probability of passing any $\gamma$-privacy test is never larger than $1/K$:*

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{ABA'B'}\} \leq \frac{1}{K}, \quad (19)$$

*where $K$ is the number of values that the secret key can take (i.e., $K = \dim(\mathcal{H}_A) = \dim(\mathcal{H}_B)$).*

The bounds in (18) and (19) are the core ones underlying our meta-converse bound.

We now establish a general bound on the achievable region discussed in Section III-B.

**Theorem 9.** *Let $\mathcal{N}_{A'\to B}$ be a quantum channel. Then for any fixed $\varepsilon \in (0,1)$, the achievable region satisfies*

$$\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^\varepsilon(\mathcal{N}). \quad (20)$$

*Proof.* Consider any protocol which achieves a rate $\hat{P}_{\mathcal{N}}(1,\varepsilon) \equiv \hat{P}$, formulated in the bipartite picture as discussed in the previous section. Let $\omega_{A_0A'B_0} \in \mathcal{S}(A_0A':B_0)$ denote the separable state shared by Alice and Bob at the beginning of the protocol. The $A'$ system of this state gets sent through the channel $\mathcal{N}_{A'\to B}$, leading to the state

$$\theta_{A_0BB_0} \equiv \mathcal{N}_{A'\to B}(\omega_{A_0A'B_0}). \quad (21)$$

Alice and Bob apply a decoder $\mathcal{D}_{A_0BB_0\to K_AK_BS_AS_B}$, leading to the state

$$\omega_{K_AK_BS_AS_B} \equiv \mathcal{D}_{A_0BB_0\to K_AK_BS_AS_B}(\theta_{A_0BB_0}). \quad (22)$$

By assumption we have that

$$F(\gamma_{K_AK_BS_AS_B}, \omega_{K_AK_BS_AS_B}) \geq 1-\varepsilon, \quad (23)$$

for some private state $\gamma_{K_AK_BS_AS_B}$. By Lemma 7, there is a projector $\Pi_{K_AK_BS_AS_B}$ corresponding to a privacy test of the form in Definition 6, such that

$$\mathrm{Tr}\{\Pi_{K_AK_BS_AS_B}\omega_{K_AK_BS_AS_B}\} \geq 1-\varepsilon. \quad (24)$$

From Lemma 8, we have that

$$\mathrm{Tr}\{\Pi_{K_AK_BS_AS_B}\sigma_{K_AK_BS_AS_B}\} \leq 2^{-\hat{P}}, \quad (25)$$

for any separable state $\sigma_{K_AK_BS_AS_B} \in \mathcal{S}(K_AS_A:K_BS_B)$. Thus, this test is feasible for $D_H^\varepsilon(\omega\|\sigma)$ and we find that

$$\hat{P} \leq D_H^\varepsilon(\omega_{K_AK_BS_AS_B}\|\sigma_{K_AK_BS_AS_B}) \quad (26)$$

for any separable state $\sigma_{K_A K_B S_A S_B} \in \mathcal{S}(K_A S_A : K_B S_B)$. Let $\tau_{A_0 B} \in \mathcal{S}(A_0 : B)$. From the quasi-convexity of $D_H^\varepsilon$ we find that there exist pure states $\psi_{A_0 A'}$ and $\varphi_{B_0}$ such that

$$\begin{aligned} & D_H^\varepsilon(\mathcal{N}_{A' \to B}(\psi_{A_0 A'}) \| \tau_{A_0 B}) \\ & \quad = D_H^\varepsilon(\mathcal{N}_{A' \to B}(\psi_{A_0 A'}) \otimes \varphi_{B_0} \| \tau_{A_0 B} \otimes \varphi_{B_0}) \quad (27) \\ & \quad \geq D_H^\varepsilon(\mathcal{N}_{A' \to B}(\omega_{A_0 A' B_0}) \| \tau_{A_0 B} \otimes \varphi_{B_0}) \quad (28) \\ & \quad \geq D_H^\varepsilon(\omega_{K_A K_B S_A S_B} \| \sigma_{K_A K_B S_A S_B}) \geq \hat{P}, \quad (29) \end{aligned}$$

where $\sigma_{K_A K_B S_A S_B} = \mathcal{D}_{A_0 B B_0 \to K_A K_B S_A S_B}(\tau_{A_0 B} \otimes \varphi_{B_0})$. The first equality follows because $D_H^\varepsilon$ is invariant with respect to tensoring in the same state on an extra system (doing so does not change the constrained Type II error in a quantum hypothesis test). The first inequality follows from quasi-convexity of $D_H^\varepsilon$. The second inequality follows from the monotonicity of $D_H^\varepsilon$ with respect to quantum channels. Since the decoder $\mathcal{D}_{A_0 B B_0 \to K_A K_B S_A S_B}$ is an LOCC channel, we can conclude that $\sigma_{K_A K_B S_A S_B} \in \mathcal{S}(K_A S_A : K_B S_B)$. The final inequality follows from (26). Since the inequality holds for any choice $\tau_{A_0 B} \in \mathcal{S}(A_0 : B)$, we conclude that

$$E_R^\varepsilon(\mathcal{N}_{A' \to B}(\psi_{A_0 A'})) \geq \hat{P}. \quad (30)$$

Optimizing over all input states $\psi_{A_0 A'}$, we can conclude the statement of the proposition. □

The above theorem immediately leads to the following bound for any quantum channel $\mathcal{N}$:

$$\hat{P}_{\mathcal{N}}(n, \varepsilon) \leq \frac{1}{n} E_R^\varepsilon(\mathcal{N}^{\otimes n}). \quad (31)$$

In the full version [32] we use the meta-converse and prior developments in [30] to prove that a channel's relative entropy of entanglement is a strong converse rate for private communication. This strengthens [20], which asserts that the channel's relative entropy of entanglement is an upper bound on the private capacity. We also establish strong converse rates for all phase-insensitive bosonic channels and find that the pure-loss and quantum-limited amplifier channels satisfy the strong converse property. Finally, we derive tight second-order converse bounds from this expression for channels with sufficient symmetry.

## References


[1] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[2] S. Beigi, N. Datta, and F. Leditzky. Decoding quantum information via the Petz recovery map. *Journal of Mathematical Physics*, 57(8):082203, 2016. arXiv:1504.04449.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, 1996. arXiv:quant-ph/9604024.

[5] F. G. S. L. Brandao and N. Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57(3):1754–1760, 2011. arXiv:0905.2673.

[6] F. Buscemi and N. Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, 2010. arXiv:0902.0158.

[7] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004.

[8] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005. arXiv:quant-ph/0304127.

[9] D. Elkouss and S. Strelchuk. Superadditivity of private information for any number of uses of the channel. *Physical Review Letters*, 115(4):040501, 2015. arXiv:1502.05326.

[10] S. Guha, J. H. Shapiro, and B. I. Erkmen. Capacity of the bosonic wiretap channel and the entropy photon-number inequality. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 91–95, Toronto, Ontario, Canada, 2008. arXiv:0801.0841.

[11] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity. *IEEE Transactions on Information Theory*, 54(6):2604–2620, 2008. arXiv:quant-ph/0608195.

[12] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. Unconditional privacy over channels which cannot convey quantum information. *Physical Review Letters*, 100(11):110502, 2008. arXiv:quant-ph/0702077.

[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, 2005. arXiv:quant-ph/0309110.

[14] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009. arXiv:quant-ph/0506189.

[15] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009. arXiv:quant-ph/0702225.

[16] K. Li, A. Winter, X. Zou, and G.-C. Guo. Private capacity of quantum channels is not additive. *Physical Review Letters*, 103(12):120501, 2009. arXiv:0903.4308.

[17] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[18] C. Morgan and A. Winter. "Pretty strong" converse for the quantum capacity of degradable channels. *IEEE Transactions on Information Theory*, 60(1):317–333, 2014. arXiv:1301.4927.

[19] J. Niset, J. Fiurasek, and N. J. Cerf. No-go theorem for Gaussian quantum error correction. *Physical Review Letters*, 102(12):120501, 2009. arXiv:0811.3128.

[20] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. 2016. arXiv:1510.08863. arXiv:1510.08863v6.

[21] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009. arXiv:0802.4155.

[22] J. H. Shapiro. The quantum theory of optical communications. *IEEE Journal of Selected Topics in Quantum Electronics*, 15(6):1547–1569, 2009.

[23] G. Smith. Private classical capacity with a symmetric side channel and its application to quantum cryptography. *Physical Review A*, 78(2):022306, 2008. arXiv:0705.3838.

[24] G. Smith, J. M. Renes, and J. A. Smolin. Structured codes improve the Bennett-Brassard-84 quantum key rate. *Physical Review Letters*, 100(17):170502, 2008. arXiv:quant-ph/0607018.

[25] G. Smith, J. A. Smolin, and J. Yard. Quantum communication with Gaussian channels of zero quantum capacity. *Nature Photonics*, 5:624–627, 2011. arXiv:1102.4580.

[26] G. Smith and J. Yard. Quantum communication with zero-capacity channels. *Science*, 321(5897):1812–1815, 2008. arXiv:0807.4935.

[27] M. Takeoka, S. Guha, and M. M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5:5235, 2014. arXiv:1504.06390.

[28] M. Takeoka, S. Guha, and M. M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, 2014. arXiv:1310.0129.

[29] M. Tomamichel, M. Berta, and J. M. Renes. Quantum coding with finite resources. *Nature Communications*, 7:11419, 2016. arXiv:1504.04617.

[30] M. Tomamichel, M. M. Wilde, and A. Winter. Strong converse rates for quantum communication. *IEEE Transactions on Information Theory*, 63(1):715–727, 2017. arXiv:1406.2946.

[31] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619–1633, 1998. arXiv:quant-ph/9707035.

[32] M. M. Wilde, M. Tomamichel, and M. Berta. Converse bounds for private communication over quantum channels. 2016. arXiv:1602.08898.
[33] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.