11-1-2016

Squashed entanglement and approximate private states

Mark M. Wilde
Louisiana State University

Squashed entanglement and approximate private states

Mark M. Wilde*

January 9, 2018

Abstract

The squashed entanglement is a fundamental entanglement measure in quantum information theory, finding application as an upper bound on the distillable secret key or distillable entanglement of a quantum state or a quantum channel. This paper simplifies proofs that the squashed entanglement is an upper bound on distillable key for finite-dimensional quantum systems and solidifies such proofs for infinite-dimensional quantum systems. More specifically, this paper establishes that the logarithm of the dimension of the key system (call it $\log_2 K$) in an ε-approximate private state is bounded from above by the squashed entanglement of that state plus a term that depends only ε and $\log_2 K$. Importantly, the extra term does not depend on the dimension of the shield systems of the private state. The result holds for the bipartite squashed entanglement, and an extension of this result is established for two different flavors of the multipartite squashed entanglement.

1 Introduction

The squashed entanglement has become one of the most widely studied entanglement measures in quantum information theory, due in part to the fact that it satisfies many of the desirable properties that researchers have proposed should hold for an entanglement measure [HHHH09]. It was originally defined in [CW04] and shown there to satisfy monotonicity with respect to local operations and classical communication (LOCC), convexity, additivity, and reduction to the entanglement entropy for pure states. Independently, some discussions of a related definition appeared in [Tuc99, Tuc02]. Later, several different authors proved that squashed entanglement is asymptotically continuous [AF04], monogamous [KW04], and faithful [BCY11]. Multipartite generalizations of squashed entanglement were independently defined and explored in [AHS08] and [YHH$^+$09], a variety of other information measures related to squashed entanglement have been presented [YHW08, SBW15, SW15], and a detailed investigation of squashed entanglement in infinite-dimensional quantum systems appeared in [Shi16]. In spite of all of the properties that squashed entanglement possesses, it is not known whether the quantity is computable in the Turing sense.

One of the most valuable properties that squashed entanglement possesses is that it is an upper bound on the distillable entanglement of a bipartite state [CW04]. This result was later strengthened in [Chr06, CEH$^+$07, CSW12]: squashed entanglement is also an upper bound on the distillable secret key of a bipartite state. These results were further strengthened in [TGW14b],

*Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

where the squashed entanglement of a quantum communication channel was defined and shown to be an upper bound on the secret key agreement capacity of a quantum channel (i.e., the maximum rate at which secret key can be distilled by two parties connected by a quantum channel and free public classical communication links). Multipartite generalizations of these results are available in [YHH$^+$09, STW16].

The original proof that the squashed entanglement is an upper bound on the distillable key of a bipartite state ρ_{AB} contained a rather slight ambiguity [Chr06, Proposition 4.19], which was later clarified in [CEH$^+$07, CSW12]. At first glance, the issue might appear to be somewhat technical, but it is in fact critical for having a complete proof of this result. It is worthwhile to point out that no such issue exists in various proofs that the relative entropy of entanglement is an upper bound on distillable key [HHHO05, HHHO09, WTB17], due to the proof of [HHHO09, Theorem 9] and related bounds.

To spell out the issue in more detail, consider that the goal of any key distillation protocol is for two parties (Alice A and Bob B) to act on n independent copies of a shared bipartite state ρ_{AB} using LOCC in order to distill a so-called private state [HHHO05, HHHO09], which consists of two components: key systems and shield systems. Alice and Bob's distilled key is placed in the key systems, and the shield systems are extra systems inaccessible to any third eavesdropping party (Eve) who possesses a purifying system of $\rho_{AB}^{\otimes n}$ and can keep a local copy of all classical communication exchanged between Alice and Bob during the protocol. The shield systems are not in the possession of Eve, their purpose being to protect the key systems from Eve. However, in such a general protocol for key distillation, the dimension of the shield systems can be arbitrarily large. This aspect of the protocol is what led to a slight ambiguity in the proof from [Chr06, Proposition 4.19], wherein a parameter d is stated, but it is left unclear as to whether this is equal to the dimension of the key systems or the dimension of the key and shield systems combined. Interpreting the proof there, the only option seems to be that d is equal to the dimension of the combined key and shield systems, in which case the proof given in [Chr06, Proposition 4.19] does not generally establish that squashed entanglement bounds distillable key from above (i.e., there could exist a sequence of key distillation protocols resulting in shield systems with a dimension growing larger than an exponential in n, and in such a case the proof does not establish squashed entanglement as an upper bound on distillable key). This ambiguity was later resolved in [CEH$^+$07, CSW12] for finite-dimensional quantum states, by noting that all such sequences of protocols can be simulated by ones in which the shield systems are growing no larger than an exponential in n. This latter argument resolves the aforementioned problem for key distillation protocols operating on finite-dimensional quantum states, but there is still a gap left open for such protocols operating on infinite-dimensional quantum states, since the shield systems in this latter context are inherently infinite-dimensional. At the same time, it seems desirable at a fundamental level for the proof to hold regardless of the dimension of the shield systems (i.e., without the need for a simulation argument).

The present paper settles this issue, which has the simultaneous effect of 1) simplifying the proof that the squashed entanglement of a finite-dimensional state or channel is an upper bound on its distillable key and 2) solidifying the proof that the same is true for an infinite-dimensional state or channel. In particular, one of the main results of this paper is that the logarithm of the dimension of one key system (call it $\log_2 K$) of an ε-approximate private state is bounded from above by its squashed entanglement plus a term that depends only ε and $\log_2 K$. The important point here is that the upper bound has no dependence on the dimension of the shield systems of the ε-approximate private state. See Theorem 2 for a precise statement of the result. With this new result in hand, we provide a brief review of the proof that squashed entanglement is an upper bound on distillable key. This paper also delivers similar results for multipartite squashed entanglements (see Theorems 6 and 8 for precise statements). The upshot is a full justification of the original statements from [TGW14b, TGW14a, STW16] and the follow-up statements in [GEW16, AML16, AK17], regarding distillation of secret key using bosonic quantum Gaussian channels.

In the next section, we review some preliminary material needed to understand the main results of the paper. After that, we proceed to establishing proofs of the main results: Theorems 2, 6, and 8.

2 Preliminaries

Much of the background on quantum information theory reviewed here is available in [Wil16], with the exception of private states and squashed entanglement.

2.1 Quantum states

Let $\mathcal{L}(\mathcal{H})$ denote the algebra of bounded linear operators acting on a Hilbert space $\mathcal{H}$. Let $\mathcal{L}_+(\mathcal{H})$ denote the subset of positive semi-definite operators. An operator ρ is in the set $\mathcal{D}(\mathcal{H})$ of density operators (or states) if $\rho \in \mathcal{L}_+(\mathcal{H})$ and $\mathrm{Tr}\{\rho\} = 1$. The tensor product of two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is denoted by $\mathcal{H}_A \otimes \mathcal{H}_B$ or $\mathcal{H}_{AB}$. Given a multipartite density operator $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we unambiguously write $\rho_A = \mathrm{Tr}_B\{\rho_{AB}\}$ for the reduced density operator on system A. We use ρ_{AB}, σ_{AB}, τ_{AB}, ω_{AB}, etc. to denote general density operators in $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, while ψ_{AB}, φ_{AB}, ϕ_{AB}, etc. denote rank-one density operators (pure states) in $\mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (with it implicit, clear from the context, and the above convention implying that ψ_A, φ_A, ϕ_A may be mixed if ψ_{AB}, φ_{AB}, ϕ_{AB} are pure). A purification $|\phi^\rho\rangle_{RA} \in \mathcal{H}_R \otimes \mathcal{H}_A$ of a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ is such that $\rho_A = \mathrm{Tr}_R\{|\phi^\rho\rangle\langle\phi^\rho|_{RA}\}$. As is conventional, we often say that a unit vector $|\psi\rangle$ is a pure state or a pure-state vector (while also saying that $|\psi\rangle\langle\psi|$ is a pure state). An extension of a state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ is some state $\rho_{RA} \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_A)$ such that $\mathrm{Tr}_R\{\rho_{RA}\} = \rho_A$. Often, an identity operator is implicit if we do not write it explicitly (and it should be clear from the context).

Let $\{|i\rangle_A\}$ denote the standard, orthonormal basis for a Hilbert space $\mathcal{H}_A$, and let $\{|i\rangle_B\}$ be defined similarly for $\mathcal{H}_B$. If these spaces are finite-dimensional and their dimensions are equal $(\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = K)$, then we define the maximally entangled state $|\Phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ as

$$|\Phi\rangle_{AB} \equiv \frac{1}{\sqrt{K}} \sum_i |i\rangle_A \otimes |i\rangle_B. \tag{1}$$

2.2 Trace distance and fidelity

The trace distance between two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is equal to $\|\rho - \sigma\|_1$, where $\|C\|_1 \equiv \mathrm{Tr}\{\sqrt{C^\dagger C}\}$ for any operator C. It has a direct operational interpretation in terms of the distinguishability of these states. That is, if ρ or σ are prepared with equal probability and the task is to distinguish them via some quantum measurement, then the optimal success probability in doing so is equal to $(1 + \|\rho - \sigma\|_1 /2)/2$ [Hel69].

The fidelity is defined as $F(\rho,\sigma) \equiv \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$ [Uhl76]. Uhlmann's theorem states that [Uhl76]

$$F(\rho_A,\sigma_A) = \max_U |\langle\phi^\sigma|_{RA} U_R \otimes I_A |\phi^\rho\rangle_{RA}|^2, \tag{2}$$

where $|\phi^\rho\rangle_{RA}$ and $|\phi^\sigma\rangle_{RA}$ are fixed purifications of ρ_A and σ_A, respectively, and the optimization is with respect to all unitaries U_R. Uhlmann's theorem also implies that, for a given extension of ρ_{AB} of ρ_A, there exists an extension σ_{AB} of σ_A such that

$$F(\rho_A,\sigma_A) = F(\rho_{AB},\sigma_{AB}). \tag{3}$$

See, e.g., [Tom16, Corollary 3.1] for an explicit proof of the above equality. The following inequalities hold for trace distance and fidelity [FvdG98]:

$$1 - \sqrt{F(\rho,\sigma)} \le \frac{1}{2}\|\rho-\sigma\|_1 \le \sqrt{1-F(\rho,\sigma)}. \tag{4}$$

2.3 Private states

Let $\gamma_{ABA'B'} \in \mathcal{D}(\mathcal{H}_{AA'BB'})$ be a state shared between spatially separated parties Alice and Bob, such that $K \equiv \dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) < +\infty$, Alice possesses systems A and A', and Bob possesses systems B and B'. The state $\gamma_{ABA'B'}$ is called a private state [HHHO05, HHHO09] if Alice and Bob can extract a secret key from it by performing local measurements on A and B, which is product with any purifying system of $\gamma_{ABA'B'}$. That is, $\gamma_{ABA'B'}$ is a private state of $\log_2 K$ private bits if, for any purification $|\varphi^\gamma\rangle_{ABA'B'E}$ of $\gamma_{ABA'B'}$, the following holds:

$$(\mathcal{M}_A \otimes \mathcal{M}_B \otimes \mathrm{Tr}_{A'B'})\left(\varphi^\gamma_{ABA'B'E}\right) = \frac{1}{K}\sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E, \tag{5}$$

where $\mathcal{M}(\cdot) = \sum_i |i\rangle\langle i|(\cdot)|i\rangle\langle i|$ is a projective measurement channel and σ_E is some state on the purifying system E (which could depend on the particular purification). The systems A' and B' are known as "shield systems" because they aid in keeping the key secure from any party possessing the purifying system (part or all of which might belong to a malicious party). It is a non-trivial consequence of the above definition that a private state of $\log_2 K$ private bits can be written in the following form [HHHO05, HHHO09]:

$$\gamma_{ABA'B'} = U_{ABA'B'}\left(\Phi_{AB} \otimes \sigma_{A'B'}\right) U^\dagger_{ABA'B'}, \tag{6}$$

where Φ_{AB} is a maximally entangled state of Schmidt rank K

$$\Phi_{AB} \equiv \frac{1}{K}\sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B, \tag{7}$$

and

$$U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'} \tag{8}$$

is a controlled unitary known as a "twisting unitary," with each $U^{ij}_{A'B'}$ a unitary operator. Any extension $\gamma_{AA'BB'E} \in \mathcal{D}(\mathcal{H}_{AA'BB'E})$ of a private state $\gamma_{AA'BB'}$ necessarily has the following form:

$$\gamma_{AA'BB'E} = U_{AA'BB'}\left(\Phi_{AB} \otimes \sigma_{A'B'E}\right) U^\dagger_{AA'BB'}, \tag{9}$$

where $\sigma_{A'B'E}$ is an extension of $\sigma_{A'B'}$.

A multipartite private state is a straightforward generalization of the bipartite definition [HA06]. Indeed, $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ is a state of $\log_2 K$ private bits if, for any purification $|\varphi^\gamma\rangle_{A_1\cdots A_m A'_1\cdots A'_m E}$ of $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$, the following holds:

$$\left(\mathcal{M}_{A_1}\otimes\cdots\otimes\mathcal{M}_{A_m}\otimes\mathrm{Tr}_{A'_1\cdots A'_m}\right)\left(\varphi^\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}\right)=\frac{1}{K}\sum_i |i\rangle\langle i|_{A_1}\otimes\cdots\otimes|i\rangle\langle i|_{A_m}\otimes\sigma_E, \quad (10)$$

where $\mathcal{M}$ and σ are as before, the key systems $A_1, \ldots, A_m$ all have the same dimension equal to K, and the shield systems $A'_1, \ldots, A'_m$ have arbitrary dimension. The above implies that an m-partite private state of $\log_2 K$ private bits is a quantum state $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ that can be written as

$$\gamma_{A_1\cdots A_m A'_1\cdots A'_m}=U_{A_1\cdots A_m A'_1\cdots A'_m}(\Phi_{A_1\cdots A_m}\otimes\sigma_{A'_1\cdots A'_m})U^\dagger_{A_1\cdots A_m A'_1\cdots A'_m}, \quad (11)$$

where $\Phi_{A_1\cdots A_m}$ is an m-qudit maximally entangled (GHZ) state

$$\Phi_{A_1\cdots A_m}\equiv\frac{1}{K}\sum_{i,j}|i\rangle\langle j|_{A_1}\otimes\cdots\otimes|i\rangle\langle j|_{A_m} \quad (12)$$

and

$$U_{A_1\cdots A_m A'_1\cdots A'_m}=\sum_{i_1,\ldots,i_m}|i_1,\ldots,i_m\rangle\langle i_1,\ldots,i_m|_{A_1\cdots A_m}\otimes U^{i_1,\ldots,i_m}_{A'_1\cdots A'_m} \quad (13)$$

is a twisting unitary, where each unitary $U^{i_1,\ldots,i_m}_{A'_1\cdots A'_m}$ depends on the values $i_1,\ldots,i_m$. Any extension $\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}$ of such a private state necessarily has the following form:

$$\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}=U_{A_1\cdots A_m A'_1\cdots A'_m}(\Phi_{A_1\cdots A_m}\otimes\sigma_{A'_1\cdots A'_m E})U^\dagger_{A_1\cdots A_m A'_1\cdots A'_m}, \quad (14)$$

where $\sigma_{A'_1\cdots A'_m E}$ is an extension of $\sigma_{A'_1\cdots A'_m}$.

2.4 Conditional quantum mutual and multipartite information

For a quantum state ρ_{ABE} shared between three parties (Alice, Bob, and Eve), the conditional quantum mutual information is defined as

$$I(A;B|E)_\rho\equiv H(AE)_\rho+H(BE)_\rho-H(E)_\rho-H(ABE)_\rho, \quad (15)$$

where $H(F)_\sigma\equiv-\mathrm{Tr}\{\sigma_F\log_2\sigma_F\}$ is the quantum entropy of a state σ_F on system F. The conditional quantum entropy is defined as

$$H(A|B)_\rho\equiv H(AB)_\rho-H(B)_\rho, \quad (16)$$

which allows us to write

$$I(A;B|E)_\rho=H(A|E)_\rho-H(A|BE)_\rho. \quad (17)$$

The conditional quantum mutual information is non-negative:

$$I(A;B|E)_\rho\geq 0, \quad (18)$$

which is an entropy inequality known as strong subadditivity [LR73b, LR73a]. The following uniform bound for the continuity of conditional quantum entropy was proven in [Win16], by building on [AF04]:

$$|H(A|B)_\rho - H(A|B)_\omega| \le 2\varepsilon \log_2 \dim(\mathcal{H}_A) + (1+\varepsilon) h_2(\varepsilon/[1+\varepsilon]), \tag{19}$$

for states $\rho_{AB}, \omega_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ such that

$$\frac{1}{2} \|\rho_{AB} - \omega_{AB}\|_1 \le \varepsilon \in [0,1] \tag{20}$$

and where the binary entropy $h_2(\varepsilon) \equiv -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$. The following uniform bound for continuity of conditional quantum mutual information holds as well [Shi17]:

$$|I(A;B|E)_\rho - I(A;B|E)_\omega| \le 2\varepsilon \log_2 \min\{\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)\} + 2(1+\varepsilon) h_2(\varepsilon/[1+\varepsilon])). \tag{21}$$

for states $\rho_{ABE}, \omega_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$ such that $\frac{1}{2}\|\rho_{ABE} - \omega_{ABE}\|_1 \le \varepsilon \in [0,1]$. Notice that this inequality is an improvement over what one would obtain merely by combining (17) and (19).

For an $m+1$-partite quantum state $\rho_{A_1 \cdots A_m E}$, there are at least two distinct ways to generalize the conditional mutual information:

$$I(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^m H(A_i|E) - H(A_1 \cdots A_m|E)_\rho, \tag{22}$$

$$\widetilde{I}(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^m H(A_{[m]\setminus\{i\}}|E)_\rho - (m-1)\, H(A_1 \cdots A_m|E)_\rho \tag{23}$$

$$= H(A_1 \cdots A_m|E)_\rho - \sum_{i=1}^m H(A_i|A_{[m]\setminus\{i\}}E)_\rho, \tag{24}$$

where the shorthand $A_{[m]\setminus\{i\}}$ indicates all systems $A_1 \cdots A_m$ except for system A_i. Both quantities are non-negative, due to strong subadditivity. The former is the conditional version of a quantity known as the total correlation [Wat60] and has been used in a variety of contexts [PHH08, YHW08, Wil14], while the latter is a conditional version of the dual total correlation [Han75, Han78], employed later on in [CMS02, YHH$^+$09, YHW08]. The above two quantities are generally incomparable, but related by the following formula [YHH$^+$09]:

$$I(A_1; \cdots; A_m|E)_\rho + \widetilde{I}(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^m I(A_i; A_{[m]\setminus\{i\}}|E)_\rho. \tag{25}$$

For a state $\rho_{BA_1A_2\cdots A_mE}$, the above conditional multipartite informations obey the following chain rules, respectively [YHH$^+$09, Section III]:

$$I(BA_1; \cdots; A_m|E)_\rho = I(A_1; \cdots; A_m|BE)_\rho + \sum_{i=2}^m I(B; A_i|E)_\rho, \tag{26}$$

$$\widetilde{I}(BA_1; A_2 \cdots; A_m|E)_\rho = \widetilde{I}(A_1; A_2; \cdots; A_m|BE)_\rho + I(B; A_2 \cdots A_m|E)_\rho. \tag{27}$$

2.5 Squashed entanglements

The squashed entanglement of a bipartite state ρ_{AB} is defined as

$$E_{\mathrm{sq}}(A;B)_\rho \equiv \frac{1}{2}\inf_{\omega_{ABE}}\left\{I(A;B|E)_\omega : \rho_{AB} = \mathrm{Tr}_E\left\{\omega_{ABE}\right\}\right\}, \tag{28}$$

where the infimum is with respect to all extensions ω_{ABE} of the state ρ_{AB} [CW04]. An interpretation of $E_{\mathrm{sq}}\left(A;B\right)_\rho$ is that it quantifies the correlations present between Alice and Bob after a third party (often associated to an environment or eavesdropper) attempts to "squash down" their correlations.

There are at least two different multipartite generalizations of the squashed entanglement [YHH+09, AHS08]. For an m-partite quantum state $\rho_{A_1\cdots A_m}$, the squashed entanglement measures E_{sq} and $\widetilde{E}_{\mathrm{sq}}$ are defined as

$$E_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\omega_{A_1A_2\cdots A_mE}}\left\{I(A_1;\cdots;A_m|E)_\omega : \mathrm{Tr}_E\left\{\omega_{A_1\cdots A_mE}\right\} = \rho_{A_1\cdots A_m}\right\}, \tag{29}$$

$$\widetilde{E}_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\omega_{A_1A_2\cdots A_mE}}\left\{\widetilde{I}(A_1;\cdots;A_m|E)_\omega : \mathrm{Tr}_E\left\{\omega_{A_1\cdots A_mE}\right\} = \rho_{A_1\cdots A_m}\right\}, \tag{30}$$

where the infima are taken with respect to all possible extensions $\omega_{A_1\cdots A_mE}$ of $\rho_{A_1\cdots A_m}$, and I and $\widetilde{I}$ are the conditional quantum multipartite information quantities given in (22) and (23), respectively.

3 Bipartite squashed entanglement and approximate private states

This section establishes one of this paper's main results (Theorem 2), which is an upper bound on the logarithm of the dimension of a key system of an ε-approximate private state in terms of its squashed entanglement, plus another term depending only on ε and $\log_2 K$. We start with the following lemma, which applies to any extension of a bipartite private state:

Lemma 1 *Let $\gamma_{AA'BB'}$ be a bipartite private state and let $\gamma_{AA'BB'E}$ be an extension of it, as defined in Section 2.3. Then the following identity holds for any such extension:*

$$2\log_2 K = I(A;BB'|E)_\gamma + I(A';B|AB'E)_\gamma. \tag{31}$$

Proof. First consider that the following identity holds as a consequence of two applications of the chain rule for conditional quantum mutual information:

$$\begin{aligned} I(AA';BB'|E)_\gamma &= I(A;BB'|E)_\gamma + I(A';BB'|AE)_\gamma \\ &= I(A;BB'|E)_\gamma + I(A';B'|AE)_\gamma + I(A';B|B'AE)_\gamma. \end{aligned} \tag{32}$$

Combined with the following identity, which holds for an extension $\gamma_{AA'BB'E}$ of a private state $\gamma_{AA'BB'}$,

$$I(AA';BB'|E)_\gamma = 2\log_2 K + I(A';B'|AE)_\gamma, \tag{33}$$

we recover the statement in (31). So it remains to prove (33). This identity is a very slight rewriting of the last line in the proof of [Chr06, Proposition 4.19], and we recall the proof here. By definition, we have that

$$I(AA';BB'|E)_\gamma = H(AA'E)_\gamma + H(BB'E)_\gamma - H(E)_\gamma - H(AA'BB'E)_\gamma. \tag{34}$$

By applying (7)–(9), we can write $\gamma_{AA'BB'E}$ as follows:

$$\gamma_{AA'BB'E} = \frac{1}{K} \sum_{i,j} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B \otimes U^{ii}_{A'B'} \sigma_{A'B'E} (U^{jj}_{A'B'})^\dagger. \tag{35}$$

Tracing over system B leads to the following state:

$$\gamma_{AA'B'E} = \frac{1}{K} \sum_{i} |i\rangle\langle i|_A \otimes \gamma^i_{A'B'E}, \tag{36}$$

where

$$\gamma^i_{A'B'E} \equiv U^{ii}_{A'B'} \sigma_{A'B'E} (U^{ii}_{A'B'})^\dagger. \tag{37}$$

Similarly, tracing over system A of $\gamma_{AA'BB'E}$ leads to

$$\gamma_{BA'B'E} = \frac{1}{K} \sum_{i} |i\rangle\langle i|_B \otimes \gamma^i_{A'B'E}. \tag{38}$$

So these and the chain rule for conditional entropy imply that

$$H(AA'E)_\gamma = H(A)_\gamma + H(A'E|A)_\gamma = \log_2 K + H(A'E|A)_\gamma. \tag{39}$$

Similarly, we have that

$$H(BB'E)_\gamma = \log_2 K + H(B'E|B)_\gamma = \log_2 K + H(B'E|A)_\gamma, \tag{40}$$

where we have used the symmetries in (36)–(38). Since $\gamma_E = \gamma^i_E$ for all i, we find that

$$H(E)_\gamma = \frac{1}{K} \sum_i H(E)_{\gamma^i} = H(E|A)_\gamma. \tag{41}$$

Finally, we have that

$$H(AA'BB'E)_\gamma = H(ABA'B'E)_{\Phi\otimes\sigma} = H(AB)_\Phi + H(A'B'E)_\sigma \tag{42}$$

$$= \frac{1}{K} \sum_i H(A'B'E)_{\gamma^i} = H(A'B'E|A)_\gamma. \tag{43}$$

Combining the above, we recover (33). ■

We can now establish one of the main results of the paper:

Theorem 2 *Let $\gamma_{AA'BB'}$ be a private state and let $\omega_{AA'BB'}$ be an ε-approximate private state, in the sense that*

$$F(\gamma_{AA'BB'}, \omega_{AA'BB'}) \geq 1 - \varepsilon \tag{44}$$

for $\varepsilon \in [0,1]$. Then

$$\log_2 K \leq E_{\text{sq}}(AA';BB')_\omega + f_1(\sqrt{\varepsilon}, K), \tag{45}$$

where

$$f_1(\varepsilon, K) \equiv 2\varepsilon \log_2 K + 2(1+\varepsilon) h_2(\varepsilon/[1+\varepsilon]). \tag{46}$$

Proof. By (3) and (4), for a given extension $\omega_{AA'BB'E}$ of $\omega_{AA'BB'}$, there exists an extension $\gamma_{AA'BB'E}$ of $\gamma_{AA'BB'}$ such that

$$\frac{1}{2}\left\|\gamma_{AA'BB'E}-\omega_{AA'BB'E}\right\|_1 \leq \sqrt{\varepsilon}. \tag{47}$$

We then find that

$$\begin{aligned} 2\log_2 K &= I(A;BB'|E)_\gamma + I(A';B|AB'E)_\gamma & (48)\\ &\leq I(A;BB'|E)_\omega + I(A';B|AB'E)_\omega + 2f_1(\sqrt{\varepsilon},K) & (49)\\ &\leq I(A;BB'|E)_\omega + I(A';B|AB'E)_\omega + I(A';B'|AE)_\omega + 2f_1(\sqrt{\varepsilon},K) & (50)\\ &= I(AA';BB'|E)_\omega + 2f_1(\sqrt{\varepsilon},K). & (51)\end{aligned}$$

The first equality follows from Lemma 1. The first inequality follows from two applications of (21). The second inequality follows because $I(A';B'|AE)_\omega \geq 0$ (this is strong subadditivity, recalled in (18)). The last equality is a consequence of the chain rule for conditional mutual information, as used in (32). Since the inequality

$$2\log_2 K \leq I(AA';BB'|E)_\omega + 2f_1(\sqrt{\varepsilon},K) \tag{52}$$

holds for any extension of ω, the statement of the theorem follows. ■

For completeness, we now provide an arguably simpler proof that squashed entanglement is an upper bound on distillable key. Before doing so, let us recall the definition of distillable key of a bipartite state ρ_{AB}. An (n,P,ε) key distillation protocol for ρ_{AB} consists of an LOCC channel $\mathcal{L}_{A^nB^n\to\hat{A}\hat{B}A'B'}$ such that

$$F(\omega_{\hat{A}\hat{B}A'B'},\gamma_{\hat{A}\hat{B}A'B'}) \geq 1-\varepsilon \in [0,1]\,, \tag{53}$$

where

$$\omega_{\hat{A}\hat{B}A'B'} \equiv \mathcal{L}_{A^nB^n\to\hat{A}\hat{B}A'B'}(\rho_{AB}^{\otimes n}), \tag{54}$$

$\gamma_{\hat{A}\hat{B}A'B'}$ is a private state, and $\left[\log_2\dim(\mathcal{H}_{\hat{A}})\right]/n = \left[\log_2\dim(\mathcal{H}_{\hat{B}})\right]/n \geq P$. A distillable key rate P is achievable for ρ_{AB} if for all $\varepsilon \in (0,1)$, $\delta > 0$, and sufficiently large n, there exists an $(n,P-\delta,\varepsilon)$ key distillation protocol for ρ_{AB}. The distillable key $P(\rho_{AB})$ is defined to be the supremum of all distillable key rates. We can then establish a slightly simpler proof of the following theorem from [Chr06, CEH+07, CSW12], by employing Theorem 2 in the first step of the proof:

Theorem 3 ([Chr06, CEH+07, CSW12]) *The distillable key $P(\rho_{AB})$ of a bipartite state ρ_{AB} is bounded from above by its squashed entanglement:*

$$P(\rho_{AB}) \leq E_{\text{sq}}(A;B)_\rho. \tag{55}$$

Proof. Consider an arbitrary (n,P,ε) key distillation protocol for ρ_{AB}. We then have that

$$\begin{aligned} \log_2\dim(\mathcal{H}_{\hat{A}}) &\leq E_{\text{sq}}(\hat{A}A';\hat{B}B')_\omega + f_1(\sqrt{\varepsilon},\log_2\dim(\mathcal{H}_{\hat{A}})) & (56)\\ &\leq E_{\text{sq}}(A^n;B^n)_{\rho^{\otimes n}} + f_1(\sqrt{\varepsilon},\log_2\dim(\mathcal{H}_{\hat{A}})) & (57)\\ &= nE_{\text{sq}}(A;B)_\rho + f_1(\sqrt{\varepsilon},\log_2\dim(\mathcal{H}_{\hat{A}})). & (58)\end{aligned}$$

The inequalities follow respectively from Theorem 2, LOCC monotonicity of squashed entanglement [CW04], and additivity of squashed entanglement with respect to tensor-product states [CW04]. We can then write the above explicitly as

$$P \leq \frac{1}{n}\log_2 \dim(\mathcal{H}_{\hat{A}}) \leq \frac{1}{1-2\sqrt{\varepsilon}} E_{\rm sq}(A;B)_\rho + \frac{2(1+\sqrt{\varepsilon})}{n(1-2\sqrt{\varepsilon})} h_2(\sqrt{\varepsilon}/\left[1+\sqrt{\varepsilon}\right]), \tag{59}$$

whenever $1-2\sqrt{\varepsilon} > 0$. Taking the limit as $n \to \infty$ and then as $\varepsilon \to 0$ establishes the result. ■

Remark 4 *An (n, P, ε) key distillation protocol which employs a quantum channel $\mathcal{N}$ is defined similarly, except one allows for n uses of a quantum channel, with each use interleaved by a round of LOCC (see [TGW14b] for a precise definition). One defines achievable rates similarly as above, and $P_2(\mathcal{N})$ is the LOCC-assisted private capacity of a quantum channel $\mathcal{N}$, equal to the supremum of all achievable rates. A similar argument as in the proof of Theorem 3, along with a particular subadditivity lemma for squashed entanglement from [TGW14b], can be used to establish the following bound for an (n, P, ε) key distillation protocol which employs a quantum channel $\mathcal{N}$:*

$$P \leq \frac{1}{1-2\sqrt{\varepsilon}} E_{\rm sq}(\mathcal{N}) + \frac{2(1+\sqrt{\varepsilon})}{n(1-2\sqrt{\varepsilon})} h_2(\sqrt{\varepsilon}/\left[1+\sqrt{\varepsilon}\right]), \tag{60}$$

whenever $1-2\sqrt{\varepsilon} > 0$. In the above, $E_{\rm sq}(\mathcal{N})$ is the squashed entanglement of a quantum channel $\mathcal{N}_{A'\to B}$, defined in [TGW14b] as

$$E_{\rm sq}(\mathcal{N}) \equiv \max_{\psi_{AA'}} E_{\rm sq}(A;B)_\omega, \tag{61}$$

$$\omega_{AB} \equiv \mathcal{N}_{A'\to B}(\psi_{AA'}), \tag{62}$$

where the optimization is with respect to all pure states $\psi_{AA'}$ with $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_{A'})$. The inequality in (60) implies that $P_2(\mathcal{N}) \leq E_{\rm sq}(\mathcal{N})$. See [TGW14b] for further details.

4 Multipartite squashed entanglements and approximate private states

We can handle the multipartite squashed entanglements in a similar way. The proof strategies are similar, with the main idea being to find particular representations for the following quantities:

$$I(A_1A_1';\cdots;A_mA_m'|E)_\gamma - I(A_1';\cdots;A_m'|EA_1)_\gamma, \tag{63}$$

$$\widetilde{I}(A_1A_1';\cdots;A_mA_m'|E)_\gamma - \widetilde{I}(A_1';\cdots;A_m'|EA_1)_\gamma, \tag{64}$$

each of which was previously shown to be equal to $m\log_2 K$ (see [YHH+09, Eqs. (78)–(80)] and [STW16, Eqs. (162)–(164)], respectively). These representations are in terms of information quantities which can be bounded from above by the dimensions of the key systems, so that we can employ uniform continuity estimates [Win16] for them in which the only dimension terms appearing are those of the key systems.

We begin by considering the first multipartite squashed entanglement in (29).

Lemma 5 *Let $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ be a multipartite private state and let $\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}$ be an extension of it, as defined in Section 2.3. Then the following identity holds for any such extension:*

$$m\log_2 K = \sum_{i=2}^{m} H(A_i|A'_iEA_1)_\gamma + \sum_{i=2}^{m} I(A_1;A_iA'_i|E)_\gamma - H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\gamma. \tag{65}$$

Proof. The following identity holds for multipartite private states [YHH+09, Eqs. (78)–(80)]:

$$I(A_1A'_1;\cdots;A_mA'_m|E)_\gamma = m\log_2 K + I(A'_1;\cdots;A'_m|EA_1)_\gamma. \tag{66}$$

Now, consider that

$$\begin{aligned}
&I(A_1A'_1;\cdots;A_mA'_m|E)_\gamma - I(A'_1;\cdots;A'_m|EA_1)_\gamma \\
&= I(A'_1;A_2A'_2;\cdots;A_mA'_m|EA_1)_\gamma + \sum_{i=2}^{m} I(A_1;A_iA'_i|E)_\gamma - I(A'_1;\cdots;A'_m|EA_1)_\gamma &(67)\\
&= H(A'_1|EA_1)_\gamma + \sum_{i=2}^{m} H(A_iA'_i|EA_1)_\gamma - H(A'_1A_2A'_2\cdots A_mA'_m|EA_1)_\gamma \\
&\qquad + \sum_{i=2}^{m} I(A_1;A_iA'_i|E)_\gamma - \left[H(A'_1|EA_1)_\gamma + \sum_{i=2}^{m} H(A'_i|EA_1)_\gamma - H(A'_1\cdots A'_m|EA_1)_\gamma\right] &(68)\\
&= \sum_{i=2}^{m} H(A_iA'_i|EA_1)_\gamma - H(A'_1A_2A'_2\cdots A_mA'_m|EA_1)_\gamma + \sum_{i=2}^{m} I(A_1;A_iA'_i|E)_\gamma \\
&\qquad - \sum_{i=2}^{m} H(A'_i|EA_1)_\gamma + H(A'_1\cdots A'_m|EA_1)_\gamma &(69)\\
&= \sum_{i=2}^{m} H(A_i|A'_iEA_1)_\gamma - H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\gamma + \sum_{i=2}^{m} I(A_1;A_iA'_i|E)_\gamma. &(70)
\end{aligned}$$

The first equality follows from (26). The second equality follows by expanding the multipartite information quantities using their definitions. The last equality follows because

$$H(A_iA'_i|EA_1)_\gamma - H(A'_i|EA_1)_\gamma = H(A_i|A'_iEA_1)_\gamma, \tag{71}$$

$$-H(A'_1A_2A'_2\cdots A_mA'_m|EA_1)_\gamma + H(A'_1\cdots A'_m|EA_1)_\gamma = -H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\gamma. \tag{72}$$

Putting (67)–(70) together with (66) gives the statement of the lemma. ■

Theorem 6 *Let $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ be a multipartite private state, as defined in Section 2.3, and let $\omega_{A_1\cdots A_m A'_1\cdots A'_m}$ be an ε-approximate private state, in the sense that*

$$F(\gamma_{A_1\cdots A_m A'_1\cdots A'_m}, \omega_{A_1\cdots A_m A'_1\cdots A'_m}) \geq 1-\varepsilon \tag{73}$$

for $\varepsilon \in [0,1]$. Then

$$\frac{m}{2}\log_2 K \leq E_{\rm sq}(A_1A'_1;\cdots;A_mA'_m)_\omega + f_2(\sqrt{\varepsilon},K), \tag{74}$$

where

$$f_2(\varepsilon,K,m) \equiv m\left[b_1\varepsilon\log_2 K + b_2(1+\varepsilon)h_2(\varepsilon/\left[1+\varepsilon\right])\right], \tag{75}$$

for some constants $b_1, b_2 \in \mathbb{Z}^+$.

Proof. By (3) and (4), for a given extension $\omega_{A_1\cdots A_m A'_1\cdots A'_m E}$ of $\omega_{A_1\cdots A_m A'_1\cdots A'_m}$, there exists an extension $\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}$ of $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ such that

$$\frac{1}{2}\left\|\gamma_{A_1\cdots A_m A'_1\cdots A'_m E} - \omega_{A_1\cdots A_m A'_1\cdots A'_m E}\right\|_1 \leq \sqrt{\varepsilon}. \tag{76}$$

We then find that

$$m\log_2 K = \sum_{i=2}^{m} H(A_i|A'_i E A_1)_\gamma + \sum_{i=2}^{m} I(A_1; A_i A'_i|E)_\gamma - H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\gamma \tag{77}$$

$$\leq \sum_{i=2}^{m} H(A_i|A'_i E A_1)_\omega + \sum_{i=2}^{m} I(A_1; A_i A'_i|E)_\omega - H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\omega + 2f_2(\sqrt{\varepsilon}, K, m) \tag{78}$$

$$\leq \sum_{i=2}^{m} H(A_i|A'_i E A_1)_\omega + \sum_{i=2}^{m} I(A_1; A_i A'_i|E)_\omega - H(A_2\cdots A_m|EA_1A'_1\cdots A'_m)_\omega + I(A'_1;\cdots;A'_m|EA_1)_\omega + 2f_2(\sqrt{\varepsilon}, K, m) \tag{79}$$

$$= I(A_1A'_1;\cdots;A_mA'_m|E)_\omega + 2f_2(\sqrt{\varepsilon}, K, m). \tag{80}$$

The first equality follows from Lemma 5. The first inequality follows from several applications of (19) and (21). The second inequality follows because $I(A'_1;\cdots;A'_m|EA_1)_\omega \geq 0$. The last equality is a consequence of (67)–(70), which clearly apply to an arbitrary state. Since the inequality

$$m\log_2 K \leq I(A_1A'_1;\cdots;A_mA'_m|E)_\omega + 2f_2(\sqrt{\varepsilon}, K, m) \tag{81}$$

holds for any extension of ω, the statement of the theorem follows. ■

We now handle the other multipartite squashed entanglement from (30).

Lemma 7 *Let $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ be a multipartite private state, and let $\gamma_{A_1\cdots A_m A'_1\cdots A'_m E}$ be an extension of it, as defined in Section 2.3. Then the following identity holds for any such extension:*

$$m\log_2 K = H(A_2\cdots A_m|EA_1A'_2\cdots A'_m)_\gamma - \sum_{i=2}^{m} H(A_i|EA_1A'_{[m]})_\gamma + \sum_{i=2}^{m} I(A_iA'_i; A_{[m]\setminus\{i,1\}}|EA_1A'_{[m]\setminus\{i\}})_\gamma + I(A_1; A_2A'_2\cdots A_mA'_m|E)_\gamma. \tag{82}$$

Proof. The following identity holds for an extension of a private state [STW16, Eqs. (162)–(164)]:

$$\widetilde{I}(A_1A'_1;\cdots;A_mA'_m|E)_\gamma = m\log_2 K + \widetilde{I}(A'_1;\cdots;A'_m|EA_1)_\gamma. \tag{83}$$

At the same time, we have that

$$
\begin{aligned}
&\widetilde{I}(A_1A_1';\cdots;A_mA_m'|E)_\gamma - \widetilde{I}(A_1';\cdots;A_m'|EA_1)_\gamma \\
&= \widetilde{I}(A_1';A_2A_2';\cdots;A_mA_m'|EA_1)_\gamma + I(A_1;A_2A_2'\cdots A_mA_m'|E)_\gamma - \widetilde{I}(A_1';\cdots;A_m'|EA_1)_\gamma \qquad (84)\\
&= H(A_1'A_2A_2'\cdots A_mA_m'|EA_1)_\gamma - H(A_1'|EA_1A_2A_2'\cdots A_mA_m')_\gamma \\
&\quad - \sum_{i=2}^m H(A_iA_i'|EA_1A_{[m]\setminus\{i,1\}}A'_{[m]\setminus\{i\}})_\gamma + I(A_1;A_2A_2'\cdots A_mA_m'|E)_\gamma \\
&\quad - \left[H(A_1'\cdots A_m'|EA_1)_\gamma - H(A_1'|EA_1A_2'\cdots A_m')_\gamma - \sum_{i=2}^m H(A_i'|EA_1A'_{[m]\setminus\{i\}})_\gamma\right] \qquad (85)\\
&= H(A_2\cdots A_m|EA_1A_1'\cdots A_m')_\gamma + I(A_1';A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma \\
&\quad - \sum_{i=2}^m H(A_iA_i'|EA_1A_{[m]\setminus\{i,1\}}A'_{[m]\setminus\{i\}})_\gamma + I(A_1;A_2A_2'\cdots A_mA_m'|E)_\gamma \\
&\quad + \sum_{i=2}^m H(A_i'|EA_1A'_{[m]\setminus\{i\}})_\gamma \qquad (86)
\end{aligned}
$$

The first equality follows from (27). The second equality follows by expanding using (24). The third equality follows because

$$
\begin{aligned}
H(A_1'A_2A_2'\cdots A_mA_m'|EA_1)_\gamma - H(A_1'\cdots A_m'|EA_1)_\gamma &= H(A_2\cdots A_m|EA_1A_1'\cdots A_m')_\gamma, \qquad (87)\\
-H(A_1'|EA_1A_2A_2'\cdots A_mA_m')_\gamma + H(A_1'|EA_1A_2'\cdots A_m')_\gamma &= I(A_1';A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma. \qquad (88)
\end{aligned}
$$

Continuing,

$$
\begin{aligned}
(86) &= H(A_2\cdots A_m|EA_1A_1'\cdots A_m')_\gamma + I(A_1';A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma \\
&\quad - \sum_{i=2}^m H(A_iA_i'|EA_1A'_{[m]\setminus\{i\}})_\gamma + \sum_{i=2}^m I(A_iA_i';A_{[m]\setminus\{i,1\}}|EA_1A'_{[m]\setminus\{i\}})_\gamma \\
&\quad + I(A_1;A_2A_2'\cdots A_mA_m'|E)_\gamma + \sum_{i=2}^m H(A_i'|EA_1A'_{[m]\setminus\{i\}})_\gamma \qquad (89)\\
&= H(A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma - \sum_{i=2}^m H(A_i|EA_1A'_{[m]})_\gamma \\
&\quad + \sum_{i=2}^m I(A_iA_i';A_{[m]\setminus\{i,1\}}|EA_1A'_{[m]\setminus\{i\}})_\gamma + I(A_1;A_2A_2'\cdots A_mA_m'|E)_\gamma. \qquad (90)
\end{aligned}
$$

The first equality follows because

$$
\begin{aligned}
-\sum_{i=2}^m H(A_iA_i'|EA_1A_{[m]\setminus\{i,1\}}A'_{[m]\setminus\{i\}})_\gamma &= -\sum_{i=2}^m H(A_iA_i'|EA_1A'_{[m]\setminus\{i\}})_\gamma \\
&\quad + \sum_{i=2}^m I(A_iA_i';A_{[m]\setminus\{i,1\}}|EA_1A'_{[m]\setminus\{i\}})_\gamma, \qquad (91)
\end{aligned}
$$

and the second because

$$H(A_2\cdots A_m|EA_1A_1'\cdots A_m')_\gamma + I(A_1';A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma \\ = H(A_2\cdots A_m|EA_1A_2'\cdots A_m')_\gamma, \quad (92)$$

$$-\sum_{i=2}^{m} H(A_iA_i'|EA_1A_{[m]\setminus\{i\}}')_\gamma + \sum_{i=2}^{m} H(A_i'|EA_1A_{[m]\setminus\{i\}}')_\gamma = -\sum_{i=2}^{m} H(A_i|EA_1A_{[m]}')_\gamma. \quad (93)$$

This concludes the proof. ■

We state a final theorem without proof, as it goes similarly to the proof of Theorem 6.

Theorem 8 *Let $\gamma_{A_1\cdots A_mA_1'\cdots A_m'}$ be a private state and let $\omega_{A_1\cdots A_mA_1'\cdots A_m'}$ be an ε-approximate private state, in the sense that*

$$F(\gamma_{A_1\cdots A_mA_1'\cdots A_m'}, \omega_{A_1\cdots A_mA_1'\cdots A_m'}) \geq 1-\varepsilon \quad (94)$$

for $\varepsilon \in [0,1]$. Then

$$\frac{m}{2}\log_2 K \leq \widetilde{E}_{\text{sq}}(A_1A_1';\cdots;A_mA_m')_\omega + f_3(\sqrt{\varepsilon}, K), \quad (95)$$

where

$$f_3(\varepsilon, K, m) \equiv m\left[c_1\varepsilon\log_2 K + c_2(1+\varepsilon)h_2(\varepsilon/\left[1+\varepsilon\right])\right], \quad (96)$$

for some constants $c_1, c_2 \in \mathbb{Z}^+$.

Remark 9 *Theorems 6 and 8 can be used to establish upper bounds on multipartite distillable key of multipartite states and broadcast channels, in a way similar to Theorem 3 and Remark 4. See [YHH+09] and [STW16] for details.*

Acknowledgements. I am grateful to Koji Azuma and Stefan Baeuml for pointing out the main issue discussed in this paper. I am as well thankful to Koji Azuma, Stefan Baeuml, Saikat Guha, Ryan Gregory James, Masahiro Takeoka, and Stephanie Wehner for discussions related to the topic of this paper. I thank the anonymous referees for helpful comments that improved the readability of the paper. I acknowledge support from the NSF under Award No. CCF-1350397 and thank Stefano Mancini for hosting me at University of Camerino during late June 2016, where this result was developed.

References

[AF04] Robert Alicki and Mark Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, February 2004. arXiv:quant-ph/0312081.

[AHS08] David Avis, Patrick Hayden, and Ivan Savov. Distributed compression and multiparty squashed entanglement. *Journal of Physics A: Mathematical and Theoretical*, 41(11):115301, March 2008. arXiv:0707.2792.

[AK17] Koji Azuma and Go Kato. Aggregating quantum repeaters for the quantum internet. *Physical Review A*, 96(3):032332, September 2017. arXiv:1606.00135.

[AML16] Koji Azuma, Akihiro Mizutani, and Hoi-Kwong Lo. Fundamental rate-loss trade-off for the quantum internet. *Nature Communications*, 7:13523, November 2016. arXiv:1601.02933.

[BCY11] Fernando G. S. L. Brandao, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750.

[CEH$^+$07] Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner. Unifying classical and quantum key distillation. *Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science*, 4392:456–478, February 2007. arXiv:quant-ph/0608199.

[Chr06] Matthias Christandl. *The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography*. PhD thesis, University of Cambridge, April 2006. arXiv:quant-ph/0604183.

[CMS02] Nicolas J. Cerf, Serge Massar, and Sara Schneider. Multipartite classical and quantum secrecy monotones. *Physical Review A*, 66(4):042309, October 2002. arXiv:quant-ph/0202103.

[CSW12] Matthias Christandl, Norbert Schuch, and Andreas Winter. Entanglement of the antisymmetric state. *Communications in Mathematical Physics*, 311(2):397–422, April 2012. arXiv:0910.4151.

[CW04] Matthias Christandl and Andreas Winter. Squashed entanglement: An additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, March 2004. arXiv:quant-ph/0308088.

[FvdG98] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, May 1998. arXiv:quant-ph/9712042.

[GEW16] Kenneth Goodenough, David Elkouss, and Stephanie Wehner. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New Journal of Physics*, 18(6):063005, June 2016. arXiv:1511.08710.

[HA06] Paweł Horodecki and Remigiusz Augusiak. Quantum states representing perfectly secure bits are always distillable. *Physical Review A*, 74(1):010302, July 2006. arXiv:quant-ph/0602176.

[Han75] Te Sun Han. Linear dependence structure of the entropy space. *Information and Control*, 29(4):337–368, December 1975.

[Han78] Te Sun Han. Nonnegative entropy measures of multivariate symmetric correlations. *Information and Control*, 36(2):133–156, February 1978.

[Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1:231–252, 1969.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225v2.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. arXiv:quant-ph/0309110.

[HHHO09] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189.

[KW04] Masato Koashi and Andreas Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69(2):022309, February 2004. arXiv:quant-ph/0310037.

[LR73a] Elliott H. Lieb and Mary Beth Ruskai. A fundamental property of quantum-mechanical entropy. *Physical Review Letters*, 30(10):434–436, March 1973.

[LR73b] Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *Journal of Mathematical Physics*, 14(12):1938–1941, December 1973.

[PHH08] Marco Piani, Pawel Horodecki, and Ryszard Horodecki. No-local-broadcasting theorem for multipartite quantum correlations. *Physical Review Letters*, 100(9):090502, March 2008. arXiv:0707.0848.

[SBW15] Kaushik P. Seshadreesan, Mario Berta, and Mark M. Wilde. Rényi squashed entanglement, discord, and relative entropy differences. *Journal of Physics A: Mathematical and Theoretical*, 48(39):395303, September 2015. arXiv:1410.1443.

[Shi16] Maksim E. Shirokov. Squashed entanglement in infinite dimensions. *Journal of Mathematical Physics*, 57(3):032203, March 2016. arXiv:1507.08964.

[Shi17] Maksim E. Shirokov. Tight continuity bounds for the quantum conditional mutual information, for the Holevo quantity and for capacities of a channel. *Journal of Mathematical Physics*, 58(10):102202, October 2017. arXiv:1512.09047.

[STW16] Kaushik P. Seshadreesan, Masahiro Takeoka, and Mark M. Wilde. Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. *IEEE Transactions on Information Theory*, 62(5):2849–2866, May 2016. arXiv:1503.08139.

[SW15] Kaushik P. Seshadreesan and Mark M. Wilde. Fidelity of recovery, squashed entanglement, and measurement recoverability. *Physical Review A*, 92(4):042321, October 2015. arXiv:1410.1441.

[TGW14a] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5:5235, October 2014. arXiv:1504.06390.

[TGW14b] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, August 2014. arXiv:1310.0129.

[Tom16] Marco Tomamichel. *Quantum Information Processing with Finite Resources — Mathematical Foundations*, volume 5 of *SpringerBriefs in Mathematical Physics*. Springer, 2016. arXiv:1504.00233.

[Tuc99] Robert R. Tucci. Quantum entanglement and conditional information transmission, 1999. arXiv:quant-ph/9909041v2.

[Tuc02] Robert R. Tucci. Entanglement of distillation and conditional mutual information. 2002. arXiv:quant-ph/0202144.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[Wat60] Satosi Watanabe. Information theoretical analysis of multivariate correlation. *IBM Journal of Research and Development*, 4(1):66–82, January 1960.

[Wil14] Mark M. Wilde. Multipartite quantum correlations and local recoverability. *Proceedings of the Royal Society A*, 471:20140941, March 2014. arXiv:1412.0333.

[Wil16] Mark M. Wilde. *From Classical to Quantum Shannon Theory.* March 2016. arXiv:1106.1445v7.

[Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, October 2016. arXiv:1507.07775.

[WTB17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, March 2017. arXiv:1602.08898.

[YHH+09] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. *IEEE Transactions on Information Theory*, 55(7):3375–3387, July 2009. arXiv:0704.2236.

[YHW08] Dong Yang, Michal Horodecki, and Z. D. Wang. An additive and operational entanglement measure: Conditional entanglement of mutual information. *Physical Review Letters*, 101(14):140501, September 2008. arXiv:0804.3683.