5-1-2016

Bounds on entanglement distillation and secret key agreement for quantum broadcast channels

Kaushik P. Seshadreesan
Louisiana State University

Masahiro Takeoka
Japan National Institute of Information and Communications Technology

Mark M. Wilde
Louisiana State University

Recommended Citation

Seshadreesan, K., Takeoka, M., & Wilde, M. (2016). Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. *IEEE Transactions on Information Theory, 62* (5), 2849-2866. https://doi.org/10.1109/TIT.2016.2544803

Bounds on entanglement distillation and secret key agreement for quantum broadcast channels

Kaushik P. Seshadreesan* Masahiro Takeoka† Mark M. Wilde*‡

September 5, 2018

Abstract

The squashed entanglement of a quantum channel is an additive function of quantum channels, which finds application as an upper bound on the rate at which secret key and entanglement can be generated when using a quantum channel a large number of times in addition to unlimited classical communication. This quantity has led to an upper bound of $\log((1+\eta)/(1-\eta))$ on the capacity of a pure-loss bosonic channel for such a task, where η is the average fraction of photons that make it from the input to the output of the channel. The purpose of the present paper is to extend these results beyond the single-sender single-receiver setting to the more general case of a single sender and multiple receivers (a quantum broadcast channel). We employ multipartite generalizations of the squashed entanglement to constrain the rates at which secret key and entanglement can be generated between any subset of the users of such a channel, along the way developing several new properties of these measures. We apply our results to the case of a pure-loss broadcast channel with one sender and two receivers.

1 Introduction

Quantum key distribution (QKD) refers to the quantum communication task of generating a shared secret key between two or more cooperating parties that is information-theoretically secure against an all-powerful eavesdropper [4, 40]. The security of QKD is based on physical principles, guaranteed by the laws of quantum mechanics. QKD protocols such as BB84 [4], Ekert91 [18] and CVGG02 [22] have been studied both theoretically and experimentally over many years since the original BB84 proposal.

Practical implementations of QKD over point-to-point fibre optical links are known to suffer from an exponential decay of the secret key rate with increasing distance of communication. Recently, it has been proven mathematically that key distillation over a pure-loss bosonic channel is fundamentally constrained by such a rate-loss trade-off [43, 42], which cannot be circumvented unless augumented by the use of quantum repeaters [41, 33], for which we do not yet have an operational implementation. The primary mathematical tool used in [43, 42] to establish this result is an entanglement measure known as the squashed entanglement [13]. (See also the related works [45, 38].) The squashed entanglement possesses nearly all the desired properties of an entanglement

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

†National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan

‡Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

measure [13, 2, 29, 7]. From this measure, one can construct a function of a channel known as the squashed entanglement of the channel [43], which is defined as the maximum squashed entanglement that can be generated between the input and output of the channel. The idea behind these quantities stems from classical information theory, being inspired by the intrinsic information [35], which can be seen by tracing their roots to earlier work in [10].

Going forward from the results of [43, 42], a natural question of interest is to determine rate-loss trade-offs in a multi-user setting, e.g., in a setting with one sender and multiple receivers. While one possibility is to consider optical switches or wavelength-division multiplexing between the transmitter and each of the receiver nodes, such an architecture would be prohibitively expensive, owing to the need to have a full QKD system for each node. Alternatively, architectures based on point-to-multipoint links, modeled as quantum broadcast channels, have been suggested to accomplish secure multinode networks [44]. Indeed we cannot hope to circumvent the already established rate-loss trade-offs when going to these settings, simply because one could always obtain an upper bound on the achievable rates in such a setting by grouping all receivers together as a single receiver. Nevertheless, we can hope to refine our understanding of the rate-loss trade-off. The main purpose of the present paper is to accomplish just that for a quantum broadcast channel connecting a single sender to an arbitrary number of receivers.

The secret-key agreement capacity of a noisy quantum channel is defined as the highest rate at which arbitrarily secure secret-key bits can be generated by using the channel an arbitrarily large number of times in addition to unlimited forward and backward classical communication. This capacity was first considered in the classical context in [34, 1] and later on in the more general quantum context. Similarly, a related quantity—the entanglement distillation capacity of a channel, is defined as the highest rate at which entanglement can be generated using the channel many times. Note that both of these definitions include "direct" communication: the secret key generated combined with unlimited classical communication allows for secure communication via the one-time pad protocol and the entanglement generated combined with the classical communication allows for quantum communication via the teleportation protocol [5].

In this work, we establish constraints on the secret-key agreement capacity and the entanglement distillation capacity of a quantum broadcast channel. Our bounds are based on multipartite generalizations of the squashed entanglement [53, 3] and constrain the rates at which secret key or entanglement can be established between any subset of the users of a quantum broadcast channel. For an example, see Theorem 12 for our upper bounds on a single-sender two-receiver broadcast channel. It should be noted that the capacity of the quantum broadcast channel has been explored in several contexts, including classical communication [23, 24, 37, 39] and private and quantum communication [16, 56]. However, prior to our work, no nontrivial upper bound had been established for the secret-key agreement and entanglement distillation capacity of a quantum broadcast channel assisted by unlimited classical communication between all parties.

The paper is organized as follows. We begin by recalling some preliminary notions in Section 2. As part of the preliminaries, we include a brief review of the squashed entanglement and its multipartite generalizations in Section 2.6. In Section 3, we prove some new auxiliary lemmas regarding several multipartite squashed entanglements, which play important roles in our main theorem. Following that, we introduce the quantum broadcast channel in Section 4 and describe a protocol for secret-key agreement and entanglement distillation over such a channel. In Section 5, we give upper bounds on the achievable secret-key agreement and entanglement distillation rates over a single-sender, two-receiver quantum broadcast channel. Following that, in Section 6, we give

our general theorem constraining the rates at which secret-key agreement and entanglement distillation are possible when using a quantum broadcast channel with one sender and m receivers. In Section 7, we apply our results to a single-sender, two-receiver bosonic broadcast channel. Finally, we summarize with a conclusion.

2 Preliminaries

2.1 States, systems, channels, and measurements

Let $\mathcal{B}(\mathcal{H})$ denote the algebra of bounded linear operators acting on a Hilbert space $\mathcal{H}$. Let $\mathcal{B}(\mathcal{H})_+$ denote the subset of positive semi-definite operators. An operator ρ is a density operator, representing the state of a quantum system, if $\rho \in \mathcal{B}(\mathcal{H})_+$ and $\operatorname{Tr}\{\rho\} = 1$. Let $\mathcal{S}(\mathcal{H})$ denote the set of density operators acting on $\mathcal{H}$. We also use the term "quantum state" or just "state" interchangeably with the term "density operator." The tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is also denoted by $\mathcal{H}_{AB}$. Given a multipartite density operator $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, the reduced density operator on system A is written in terms of the partial trace as $\rho_A = \operatorname{Tr}_B\{\rho_{AB}\}$. An extension of a state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ is a state $\Omega_{RA} \in \mathcal{S}(\mathcal{H}_{RA})$ such that $\operatorname{Tr}_R\{\Omega_{RA}\} = \rho_A$.

A linear map $\mathcal{N}_{A\to B} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is positive if $\mathcal{N}_{A\to B}(\sigma_A) \in \mathcal{B}(\mathcal{H}_B)_+$ whenever $\sigma_A \in \mathcal{B}(\mathcal{H}_A)_+$. Let id_A denote the identity map acting on a system A. A linear map $\mathcal{N}_{A\to B}$ is completely positive if the map $\mathrm{id}_R \otimes \mathcal{N}_{A\to B}$ is positive for a reference system R of arbitrary size. A linear map $\mathcal{N}_{A\to B}$ is trace-preserving if $\operatorname{Tr}\{\mathcal{N}_{A\to B}(\tau_A)\} = \operatorname{Tr}\{\tau_A\}$ for all input operators $\tau_A \in \mathcal{B}(\mathcal{H}_A)$. A linear map is a quantum channel if it is both completely positive and trace-preserving (CPTP). An isometric extension $U^{\mathcal{N}}_{A\to BE}$ of a channel $\mathcal{N}_{A\to B}$ acting on a state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ is a linear map that satisfies the following:

$$\operatorname{Tr}_E\left\{U^{\mathcal{N}}_{A\to BE}\rho_A(U^{\mathcal{N}}_{A\to BE})^\dagger\right\} = \mathcal{N}_{A\to B}(\rho_A), \qquad U^\dagger_{\mathcal{N}}U_{\mathcal{N}} = I_A, \qquad U_{\mathcal{N}}U^\dagger_{\mathcal{N}} = \Pi_{BE}, \tag{2.1}$$

where Π_{BE} is a projection onto a subspace of the Hilbert space $\mathcal{H}_B \otimes \mathcal{H}_E$.

A measurement channel is a quantum channel with a quantum input and a classical output, specified as follows:

$$\omega \to \sum_m \operatorname{Tr}\{\Lambda^m\omega\}\,|m\rangle\langle m|, \tag{2.2}$$

where $\{\Lambda^m\}$ is a set of positive semi-definite operators such that $\sum_m \Lambda^m = I$ and $\{|m\rangle\}$ is an orthonormal basis. The set $\{\Lambda^m\}$ is also known as a positive operator-valued measure (POVM).

2.2 Maximally entangled states and GHZ states

Along with density operators, we also say that any unit vector $|\psi\rangle \in \mathcal{H}$ is a quantum state. Its corresponding density operator is $|\psi\rangle\langle\psi|$, and we often make the abbreviation $\psi = |\psi\rangle\langle\psi|$. Any bipartite pure state $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ has a Schmidt decomposition as follows:

$$|\psi\rangle_{AB} \equiv \sum_{i=0}^{d-1} \sqrt{\lambda_i}|i\rangle_A|i\rangle_B, \tag{2.3}$$

where $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ form orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, d is the Schmidt rank of the state, $0 < \lambda_i \leq 1$ for all $i \in \{0,\ldots,d-1\}$, and $\sum_{i=0}^{d-1}\lambda_i = 1$. A maximally entangled state

of Schmidt rank d is a pure bipartite state of the following form:

$$|\Phi\rangle_{AB} \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B, \tag{2.4}$$

and is said to contain $H(A)_\Phi \equiv -\operatorname{Tr}\{\Phi_A \log \Phi_A\} = \log d$ entangled bits. In the previous expression, H denotes the von Neumann entropy of the reduced state $\Phi_A = \operatorname{Tr}_B\{\Phi_{AB}\}$.

The Greenberger-Horne-Zeilinger (GHZ) state is a multipartite generalization of the maximally entangled state. An m-party GHZ state shared between systems $A_1, \ldots, A_m$ is written as

$$|\Phi\rangle_{A_1 \cdots A_m} \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{A_1} \otimes \cdots \otimes |i\rangle_{A_m}, \tag{2.5}$$

where $\{|i\rangle_{A_1}\}$, $\ldots$, $\{|i\rangle_{A_m}\}$ are orthonormal bases, and is also said to contain $\log d$ entangled bits. Throughout this paper, we refer to GHZ states $|\Phi\rangle_{A_1 \cdots A_m}$ as maximally entangled states (however, note that this terminology depends on which entanglement measure one employs—for the entanglement measures that we employ in this paper, they are indeed maximally entangled).

2.3 Bipartite and multipartite private states

Let $\gamma_{ABA'B'}$ be a state shared between spatially separated parties Alice and Bob, such that Alice possesses systems A and A' and Bob possesses systems B and B'. $\gamma_{ABA'B'}$ is called a private state [26, 27] 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 $\log d$ private bits if, for any purification $|\varphi^\gamma\rangle_{ABA'B'E}$ of $\gamma_{ABA'B'}$, the following holds:

$$(\mathcal{M}_A \otimes \mathcal{M}_B \otimes \operatorname{Tr}_{A'B'}) \left(\varphi^\gamma_{ABA'B'E}\right) = \frac{1}{d} \sum_{i=0}^{d-1} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E, \tag{2.6}$$

where $\mathcal{M}(\cdot) = \sum_i |i\rangle\langle i|(\cdot)|i\rangle\langle i|$ is a von Neumann 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 $\log d$ private bits can be written in the following form [26, 27]:

$$\gamma_{ABA'B'} = U_{ABA'B'} \left(\Phi_{AB} \otimes \rho_{A'B'}\right) U^\dagger_{ABA'B'}, \tag{2.7}$$

where Φ_{AB} is a maximally entangled state of Schmidt rank d, and

$$U_{ABA'B'} = \sum_{i,j=0}^{d-1} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'} \tag{2.8}$$

is a controlled unitary known as a "twisting unitary." The advantage of the notion of a private state shared between Alice and Bob as opposed to a secret key is that there is no need to consider an eavesdropper in the private state formalism, as where this is necessary when considering a secret key. We return to this point in Section 2.4.

A multipartite private state is a straightforward generalization of the bipartite definition [28]. Indeed, $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ is a state of $\log d$ 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:

$$\left(\mathcal{M}_{A_1}\otimes\cdots\otimes\mathcal{M}_{A_m}\otimes\mathrm{Tr}_{A'_1\cdots A'_m}\right)\left(\varphi^{\gamma}_{A_1\cdots A_m A'_1\cdots A'_m E}\right)=\frac{1}{d}\sum_{i=0}^{d-1}|i\rangle\langle i|_{A_1}\otimes\cdots\otimes|i\rangle\langle i|_{A_m}\otimes\sigma_E, \quad (2.9)$$

where $\mathcal{M}$ and σ are as before. The above implies that an m-partite private state of $\log d$ private bits is a quantum state $\gamma_{A_1\cdots A_m A'_1\cdots A'_m}$ that can be written as

$$\gamma_{A_1\cdots A_m A'_1\cdots A'_m}=U_{A_1\cdots A_m A'_1\cdots A'_m}\left(\Phi_{A_1\cdots A_m}\otimes\rho_{A'_1\cdots A'_m}\right)U^{\dagger}_{A_1\cdots A_m A'_1\cdots A'_m}, \quad (2.10)$$

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

$$U_{A_1\cdots A_m A'_1\cdots A'_m}=\sum_{i_1,\ldots,i_m=0}^{d-1}|i_1,\ldots,i_m\rangle\langle i_1,\ldots,i_m|_{A_1\cdots A_m}\otimes U^{i_1,\ldots,i_m}_{A'_1\cdots A'_m} \quad (2.11)$$

is a twisting unitary, where each unitary $U^{i_1,\ldots,i_m}_{A'_1\cdots A'_m}$ depends on the values $i_1,\ldots,i_m$.

Note that for brevity of notation, we sometimes suppress the shield systems when writing a private state. In such a case, it is implicit that the shield systems are contained within; e.g., the notation γ_{AB} implies that system A contains both Alice's share of the key and a shield and likewise B contains both Bob's share of the key and a shield.

2.4 LOCC and LOPC

Local operations and classical communication (LOCC) is a commonly considered paradigm for distributed quantum information processing between two or more honest parties [6] (for a recent discussion, see, e.g., [9]). In this paradigm, m cooperating parties $A_1,\ldots,A_m$ begin by sharing a quantum state $\rho_{A_1\cdots A_m}$. They are subsequently allowed to perform local quantum operations on their own systems and to communicate with each other using a classical communication channel. A typical goal of an LOCC protocol is to distill a GHZ entangled state or a multipartite private state.

Local operations and public communication (LOPC) is a related paradigm that is particularly relevant for quantum key distribution [26, 27]. In this paradigm, we have the honest parties $A_1,\ldots,A_m$ and an additional untrusted party E. All parties begin by sharing a quantum state $\rho_{A_1\cdots A_m E}$, and the honest parties are allowed to perform local quantum operations and public classical communication, such that all parties have access to the classical data being communicated over a public classical channel. The public classical channel is "authenticated," meaning that the untrusted party can only learn the classical information but is not allowed to tamper with it. The usual aim of the trusted parties in the LOPC paradigm is to distill a state that is nearly indistinguishable from a secret key state of the form in (2.9).

One of the main insights of [26, 27] was to prove that the approximate LOCC distillation of private states is equivalent to the approximate LOPC distillation of a secret key, when we are dealing with the "most paranoid" scenario in which the untrusted party possesses a purifying system of the states of the honest parties. Thus, this result introduces an important simplification in which

it suffices to focus on the LOCC distillation of private states. Also, we can unify this setting with entanglement distillation, in which the goal of a given protocol could be to distill both entangled states and private states at the same time. This is exactly the kind of scenario that we will consider in this paper.

2.5 Conditional mutual information and conditional multipartite information

Let ρ_{ABE} be a tripartite quantum state on systems A, B, and E. The quantum conditional mutual information (QCMI) is defined as

$$I(A;B|E)_\rho \equiv H(AE)_\rho + H(BE)_\rho - H(E)_\rho - H(ABE)_\rho, \tag{2.12}$$

where, e.g., $H(AE)_\rho \equiv -\operatorname{Tr}\{\rho_{AE}\log\rho_{AE}\}$ denotes the von Neumann entropy of the state ρ_{AE}, which is the reduced density operator $\rho_{AE} = \operatorname{Tr}_B\{\rho_{ABE}\}$. The QCMI is non-negative, which is a non-trivial fact known as the strong subadditivity of quantum entropy [32, 31]. The QCMI is non-increasing under the action of local quantum channels performed on the systems A and B [13], i.e.,

$$I(A;B|E)_\rho \geq I(A';B'|E)_\omega, \tag{2.13}$$

where $\omega_{A'B'E} \equiv (\mathcal{N}_{A\to A'}\otimes\mathcal{M}_{B\to B'})(\rho_{ABE})$ with $\mathcal{N}_{A\to A'}$ and $\mathcal{M}_{B\to B'}$ arbitrary local quantum channels performed on the input systems A and B, leading to output systems A' and B', respectively. Another interesting property of the QCMI is that for a four-party pure state ψ_{ABED} it obeys a duality relation given by $I(A;B|E)_\psi = I(A;B|D)_\psi$ [15, 55]. The QCMI finds an operational meaning in the information theoretic task of quantum state redistribution [15].

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

$$I(A_1;\cdots;A_m|E)_\rho = \sum_{i=1}^m H(A_i|E) - H(A_1\cdots A_m|E)_\rho, \tag{2.14}$$

$$\widetilde{I}(A_1;\cdots;A_m|E)_\rho = \sum_{i=1}^m H(A_{[m]\setminus\{i\}}|E)_\rho - (m-1)\,H(A_1\cdots A_m|E)_\rho \tag{2.15}$$

$$= H(A_1\cdots A_m|E)_\rho - \sum_{i=1}^m H(A_i|A_{[m]\setminus\{i\}}E)_\rho, \tag{2.16}$$

where the shorthand $A_{[m]\setminus\{i\}}$ indicates all systems $A_1\cdots A_m$ except for system A_i.[1] The former is the conditional version of a quantity known as the total correlation [47] and has been used in a variety of contexts [36, 54, 49], while the latter was introduced in [8] and employed later on in [53, 54]. The above two quantities are generally incomparable, but related by the following formula [53]:

$$I(A_1;\cdots;A_m|E)_\rho + \widetilde{I}(A_1;\cdots;A_m|E)_\rho = \sum_{i=1}^m I(A_i;A_{[m]\setminus\{i\}}|E)_\rho. \tag{2.17}$$

[1] In previous work [8], the quantity $\widetilde{I}(A_1;\cdots;A_m|E)_\rho$ was denoted by $S_m(A_1;\cdots;A_m|E)_\rho$, but there are at least two difficulties with using this notation. First and foremost, the letter S is widely used in quantum physics to denote entropy or uncertainty, while the measure here is not a measure of uncertainty but rather of correlations. Second, having the subscript m limits the extension of the notation to the more general scenarios considered in this paper (c.f., Section 2.7).

For a state $\rho_{BA_1A_2\cdots A_mE}$, the above conditional multipartite informations obey the following chain rules, respectively [53, Section III]:

$$I(BA_1;\cdots;A_m|E)_\rho = I(A_1;\cdots;A_m|BE)_\rho + \sum_{i=2}^{m} I(B;A_i|E)_\rho, \tag{2.18}$$

$$\widetilde{I}(BA_1;A_2\cdots;A_m|E)_\rho = \widetilde{I}(A_1;A_2;\cdots;A_m|BE)_\rho + I(B;A_2\cdots A_m|E)_\rho. \tag{2.19}$$

Also, they are additive with respect to tensor-product states, non-negative, and monotone non-increasing under local quantum channels acting on systems $A_1,\ldots,A_m$ [53, Section III], i.e.,

$$I(A_1;\cdots;A_m|E)_\rho \geq I(A_1';\cdots;A_m'|E)_\omega, \tag{2.20}$$

$$\widetilde{I}(A_1;\cdots;A_m|E)_\rho \geq \widetilde{I}(A_1';\cdots;A_m'|E)_\omega, \tag{2.21}$$

where

$$\omega_{A_1'\cdots A_m'E} \equiv \left(\mathcal{N}^{(1)}_{A_1\to A_1'} \otimes \cdots \otimes \mathcal{N}^{(m)}_{A_m\to A_m'}\right)(\rho_{A_1\cdots A_mE}), \tag{2.22}$$

with $\mathcal{N}^{(i)}_{A_i\to A_i'}$ an arbitrary local quantum channel performed on the input system A_i, leading to output system A_i'.

2.6 Bipartite and multipartite squashed entanglement

We begin this section by recalling the definition of the bipartite squashed entanglement [13].

Definition 1 *The squashed entanglement of a bipartite state ρ_{AB} is defined as*

$$E_{\mathrm{sq}}(A;B)_\rho \equiv \frac{1}{2}\inf_{\omega_{ABE}}\left\{I(A;B|E)_\omega : \mathrm{Tr}_E\left\{\omega_{ABE}\right\} = \rho_{AB}\right\}, \tag{2.23}$$

where the infimum is taken over all possible extensions ω_{ABE} of ρ_{AB} and $I(A;B|E)_\omega$ is the quantum conditional mutual information of (2.12).

The squashed entanglement possesses many of the properties that are desired of an entanglement measure. For example, it is monotone non-increasing under LOCC, additive with respect to tensor-product states, and subadditive in general [13]. It is a faithful entanglement measure, in the sense that it is equal to zero if and only if the state is separable [7, 30]. It is also asymptotically continuous [2]. The squashed entanglement is normalized on maximally entangled states and private states: for a maximally entangled state of Schmidt rank d, the squashed entanglement equals $\log d$ [13], and it is at least $\log d$ for a private state of $\log d$ private bits [11, Proposition 4.19]. Furthermore, the squashed entanglement of a state ρ_{AB} is an upper bound on the rate at which Bell states or private states can be distilled per copy of ρ_{AB} when using LOCC [13, 12].

There are at least two different multipartite generalizations of the squashed entanglement [53, 3]:

Definition 2 *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*

$$E_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\omega_{A_1A_2\cdots A_mE}}\left\{I(A_1;\cdots;A_m|E)_\omega : \mathrm{Tr}_E\left\{\omega_{A_1\cdots A_mE}\right\} = \rho_{A_1\cdots A_m}\right\}, \tag{2.24}$$

$$\widetilde{E}_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\omega_{A_1A_2\cdots A_mE}}\left\{\widetilde{I}(A_1;\cdots;A_m|E)_\omega : \mathrm{Tr}_E\left\{\omega_{A_1\cdots A_mE}\right\} = \rho_{A_1\cdots A_m}\right\}, \tag{2.25}$$

where the infima are taken over all possible extensions $\omega_{A_1\cdots A_m E}$ of $\rho_{A_1\cdots A_m}$, and I and $\widetilde{I}$ are the quantum conditional multipartite information quantities given in (2.14) *and* (2.15)*, respectively.*

The squashed entanglements defined above have the following alternative characterization in terms of a "squashing channel," which follows from the same reasoning that justifies [13, Eq. (3)]:

Lemma 3 *Let $|\varphi^\rho\rangle_{A_1\cdots A_m E}$ be a purification of $\rho_{A_1\cdots A_m}$. Then*

$$E_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\mathcal{S}_{E\to E'}} I(A_1;\cdots;A_m|E')_\omega, \tag{2.26}$$

$$\widetilde{E}_{\mathrm{sq}}(A_1;\cdots;A_m)_\rho \equiv \frac{1}{2}\inf_{\mathcal{S}_{E\to E'}} \widetilde{I}(A_1;\cdots;A_m|E')_\omega, \tag{2.27}$$

where the infima are over all squashing channels $\mathcal{S}_{E\to E'}$ and

$$\omega_{A_1\cdots A_m E'} \equiv \mathcal{S}_{E\to E'}\left(\varphi^\rho_{A_1\cdots A_m E}\right). \tag{2.28}$$

The above multipartite squashed entanglements are both monotone non-increasing under LOCC, additive with respect to tensor-product states, subadditive in general, and asymptotically continuous [53, Section IV]. They both reduce to the bipartite squashed entanglement from Definition 1 when $m = 2$. They also satisfy the following lemmas:

Lemma 4 *[53, Section IV-A] For a classical-quantum state*

$$\rho_{XAB_1\cdots B_m} = \sum_x p_X(x)|x\rangle\langle x|_X \otimes \rho^x_{AB_1\cdots B_m}, \tag{2.29}$$

the squashed entanglement measures of Definition 2 satisfy the following property:

$$E_{\mathrm{sq}}(AX;B_1;\cdots;B_m)_\rho = \sum_x p(x) E_{\mathrm{sq}}(A;B_1;\cdots;B_m)_{\rho^x}, \tag{2.30}$$

$$\widetilde{E}_{\mathrm{sq}}(AX;B_1;\cdots;B_m)_\rho = \sum_x p(x) \widetilde{E}_{\mathrm{sq}}(A;B_1;\cdots;B_m)_{\rho^x}. \tag{2.31}$$

Lemma 5 *[53, Observation 1] Let $\Phi_{A_1\cdots A_m}$ be a maximally entangled GHZ state of Schmidt rank d. Then*

$$E_{\mathrm{sq}}(A_1;\cdots;A_m)_\Phi = \widetilde{E}_{\mathrm{sq}}(A_1;\cdots;A_m)_\Phi = \frac{m}{2}\log d. \tag{2.32}$$

Let $\gamma_{A_1\cdots A_m}$ be a private state, such that each key system has dimension d. Then

$$\min\left\{E_{\mathrm{sq}}(A_1;\cdots;A_m)_\gamma, \widetilde{E}_{\mathrm{sq}}(A_1;\cdots;A_m)_\gamma\right\} \geq \frac{m}{2}\log d. \tag{2.33}$$

2.7 Shorthand for multipartite information measures in terms of partitions

A partition $\mathcal{G}$ of a set $\mathcal{K}$ is a set of non-empty subsets of $\mathcal{K}$ such that

$$\bigcup_{\mathcal{X}\in\mathcal{G}} \mathcal{X} = \mathcal{K} \tag{2.34}$$

and for all $\mathcal{X}_1, \mathcal{X}_2 \in \mathcal{G}$,

$$\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset. \tag{2.35}$$

For example, if $\mathcal{K} = \{A, B, C\}$, then $\mathcal{G} = \{\{A\}, \{B, C\}\}$ is a partition of $\mathcal{K}$.

The power set $\mathcal{P}(\mathcal{K})$ of a set $\mathcal{K}$ is the set of all subsets of $\mathcal{K}$. Let $\mathcal{P}_{\geq 1}(\mathcal{K})$ and $\mathcal{P}_{\geq 2}(\mathcal{K})$ denote the set of all non-empty subsets of $\mathcal{K}$ and the set of all non-empty and non-singleton subsets of $\mathcal{K}$, respectively. For example, if $\mathcal{K} = \{A, B, C\}$, then

$$\mathcal{P}(\mathcal{K}) = \{\emptyset, \{A\}, \{B\}, \{C\}, \{A, C\}, \{A, B\}, \{B, C\}, \{A, B, C\}\}, \tag{2.36}$$

$$\mathcal{P}_{\geq 1}(\mathcal{K}) = \{\{A\}, \{B\}, \{C\}, \{A, C\}, \{A, B\}, \{B, C\}, \{A, B, C\}\}, \tag{2.37}$$

$$\mathcal{P}_{\geq 2}(\mathcal{K}) = \{\{A, C\}, \{A, B\}, \{B, C\}, \{A, B, C\}\}. \tag{2.38}$$

Let $\mathcal{S}$ be a set, and let $\omega_{\mathcal{S}}$ be an $|\mathcal{S}|$-partite state shared among parties specified by the elements of $\mathcal{S}$. Let $\mathcal{G}$ be a partition of $\mathcal{S}$. Then we use the shorthand

$$E_{\mathrm{sq}}(\mathcal{G})_\omega \tag{2.39}$$

to denote a multipartite squashed entanglement with grouping of parties according to the partition $\mathcal{G}$. For example, if $\omega \equiv \omega_{ABC}$, $\mathcal{S} = \{A, B, C\}$ and $\mathcal{G}_1 = \{\{A\}, \{B, C\}\}$, then

$$E_{\mathrm{sq}}(\mathcal{G}_1)_\omega = E_{\mathrm{sq}}(A; BC)_\omega. \tag{2.40}$$

Similarly, if $\mathcal{G}_2 = \{\{A\}, \{B\}, \{C\}\}$, then

$$E_{\mathrm{sq}}(\mathcal{G}_2)_\omega = E_{\mathrm{sq}}(A; B; C)_\omega. \tag{2.41}$$

We also employ similar shorthands for I, $\widetilde{I}$, and $\widetilde{E}_{\mathrm{sq}}$.

3 Auxiliary lemmas for the multipartite squashed entanglements

3.1 Subadditivity

The following lemma is a multipartite generalization of [43, Theorem 3], which was one of the main tools used to prove that the squashed entanglement of a quantum channel is an upper bound on its quantum capacity or private capacity when assisted by forward and backward classical communication. Naturally, the following lemma will be one of the important tools used to prove the main result in this paper.

Lemma 6 (Subadditivity) *For a $(2m+3)$-partite pure quantum state $\psi_{SP_1\cdots P_mQ_1\cdots Q_mE_1E_2}$, the following subadditivity inequalities hold*

$$E_{\mathrm{sq}}(S; P_1Q_1; \cdots; P_mQ_m)_\psi \leq E_{\mathrm{sq}}(SQ_{[m]}E_2; P_1; \cdots; P_m)_\psi + E_{\mathrm{sq}}(SP_{[m]}E_1; Q_1; \cdots; Q_m)_\psi, \tag{3.1}$$

$$\widetilde{E}_{\mathrm{sq}}(S; P_1Q_1; \cdots; P_mQ_m)_\psi \leq \widetilde{E}_{\mathrm{sq}}(SQ_{[m]}E_2; P_1; \cdots; P_m)_\psi + \widetilde{E}_{\mathrm{sq}}(SP_{[m]}E_1; Q_1; \cdots; Q_m)_\psi. \tag{3.2}$$

Proof. Let

$$\tau_{SP_1\cdots P_mQ_1\cdots Q_mE_1'E_2} = \mathcal{S}_{E_1\to E_1'}(\psi_{SP_1\cdots P_mQ_1\cdots Q_mE_1E_2}), \tag{3.3}$$

$$\sigma_{SP_1\cdots P_mQ_1\cdots Q_mE_1E_2'} = \mathcal{S}_{E_2\to E_2'}(\psi_{SP_1\cdots P_mQ_1\cdots Q_mE_1E_2}), \tag{3.4}$$

$$\omega_{SP_1\cdots P_mQ_1\cdots Q_mE_1'E_2'} = \left(\mathcal{S}_{E_1\to E_1'} \otimes \mathcal{S}_{E_2\to E_2'}\right)(\psi_{SP_1\cdots P_mQ_1\cdots Q_mE_1E_2}), \tag{3.5}$$

where each $\mathcal{S}_{E_i \to E_i'}$ is an arbitrary local squashing channel. Let

$$|\phi^{\omega}\rangle_{SP_1 \cdots P_m Q_1 \cdots Q_m E_1' E_2' R} \tag{3.6}$$

be a purification of ω with purifying system R.

We first prove (3.1). Consider the following chain of inequalities:

$$\begin{aligned}
&2E_{\text{sq}}(S; P_1 Q_1; \cdots ; P_m Q_m)_{\psi} \\
&\leq I(S; P_1 Q_1; \cdots ; P_m Q_m \left| E_1' E_2' \right.)_{\omega} && (3.7) \\
&= \sum_{i=1}^{m} H(P_i Q_i \left| E_1' E_2' \right.)_{\omega} - H\left(P_1 \cdots P_m Q_1 \cdots Q_m \left| S E_1' E_2' \right.\right)_{\omega} && (3.8) \\
&= \sum_{i=1}^{m} H(P_i Q_i \left| E_1' E_2' \right.)_{\phi} + H\left(P_1 \cdots P_m Q_1 \cdots Q_m \left| R \right.\right)_{\phi} && (3.9) \\
&\leq \sum_{i=1}^{m} \left[H\left(P_i \left| E_1' \right.\right)_{\phi} + H\left(Q_i \left| E_2' \right.\right)_{\phi} \right] + H\left(P_1 \cdots P_m \left| R \right.\right)_{\phi} + H\left(Q_1 \cdots Q_m \left| R \right.\right)_{\phi} && (3.10)
\end{aligned}$$

The first inequality follows from Definition 2. The first equality follows from the definition of the quantum conditional multipartite information. The second equality follows from the duality of conditional entropy, namely, for a tripartite pure state ϕ_{KLM}, $H\left(K \left| L \right.\right)_{\phi} = -H\left(K \left| M \right.\right)_{\phi}$. The second inequality is a consequence of the strong subadditivity of quantum entropy $I\left(K; L \left| M \right.\right) \geq 0$. Continuing from above,

$$\begin{aligned}
&= \sum_{i=1}^{m} H\left(P_i \left| E_1' \right.\right)_{\omega} - H\left(P_1 \cdots P_m \left| S Q_1 \cdots Q_m E_1' E_2' \right.\right)_{\omega} \\
&\qquad + \sum_{i=1}^{m} H\left(Q_i \left| E_2' \right.\right)_{\omega} - H\left(Q_1 \cdots Q_m \left| S P_1 \cdots P_m E_1' E_2' \right.\right)_{\omega} && (3.11) \\
&= I\left(S Q_1 \cdots Q_m E_2'; P_1; \cdots ; P_m \left| E_1' \right.\right)_{\omega} + I\left(S P_1 \cdots P_m E_1'; Q_1; \cdots ; Q_m \left| E_2' \right.\right)_{\omega} && (3.12) \\
&\leq I\left(S Q_1 \cdots Q_m E_2; P_1; \cdots ; P_m \left| E_1' \right.\right)_{\tau} + I\left(S P_1 \cdots P_m E_1; Q_1; \cdots ; Q_m \left| E_2' \right.\right)_{\sigma} && (3.13)
\end{aligned}$$

The first equality follows from the duality of conditional entropy and the second from rewriting the linear sum of conditional entropies in terms of a multipartite conditional mutual information. The final inequality follows from the data processing inequality for the quantum conditional multipartite information. Since the above calculations are independent of the choice of squashing channels $\mathcal{S}_{E_i \to E_i'}$, and since E_1 purifies the state on $S P_1 Q_1 \cdots P_m Q_m E_2$ and E_2 purifies the state on $S P_1 Q_1 \cdots P_m Q_m E_1$, the inequality in (3.1) follows.

We now prove the inequality in (3.2). The proof idea is similar to the above, but we give it below for completeness. Consider the following chain of inequalities:

$$
\begin{aligned}
&2\widetilde{E}_{\text{sq}}(S;P_1Q_1;\cdots;P_mQ_m)_\psi \\
&\leq \widetilde{I}(S;P_1Q_1;\cdots;P_mQ_m\left|E_1'E_2'\right.)_\omega && (3.14)\\
&= H\left(SP_1Q_1\cdots P_mQ_m|E_1'E_2'\right)_\omega - H\left(S|P_1Q_1\cdots P_mQ_mE_1'E_2'\right)_\omega \\
&\qquad - \sum_{i=1}^m H\left(P_iQ_i|SP_{[m]\setminus\{i\}}Q_{[m]\setminus\{i\}}E_1'E_2'\right)_\omega && (3.15)\\
&= H\left(P_1Q_1\cdots P_mQ_m|E_1'E_2'\right)_\omega - \sum_{i=1}^m H\left(P_iQ_i|SP_{[m]\setminus\{i\}}Q_{[m]\setminus\{i\}}E_1'E_2'\right)_\omega && (3.16)\\
&= H\left(P_1Q_1\cdots P_mQ_m|E_1'E_2'\right)_\omega + \sum_{i=1}^m H\left(P_iQ_i|R\right)_\phi && (3.17)
\end{aligned}
$$

The first inequality follows from the definition of $\widetilde{E}_{\text{sq}}$. The first equality follows from expanding $\widetilde{I}$ with (2.16). The second equality follows from $H(AB|C) - H(A|BC) = H(B|C)$ with $A \equiv S$, $B \equiv P_1Q_1\cdots P_mQ_m$, and $C = E_1'E_2'$. The third equality follows from duality of conditional entropy. Continuing from above,

$$
\begin{aligned}
&\leq H\left(P_1\cdots P_m|E_1'\right)_\omega + H\left(Q_1\cdots Q_m|E_2'\right)_\omega + \sum_{i=1}^m H\left(P_i|R\right)_\phi + H\left(Q_i|R\right)_\phi && (3.18)\\
&= H\left(P_1\cdots P_m|E_1'\right)_\omega + H\left(Q_1\cdots Q_m|E_2'\right)_\omega - \sum_{i=1}^m H\left(P_i|E_1'E_2'SP_{[m]\setminus\{i\}}Q_{[m]}\right)_\omega \\
&\qquad - \sum_{i=1}^m H\left(Q_i|E_1'E_2'SP_{[m]}Q_{[m]\setminus\{i\}}\right)_\omega && (3.19)\\
&= \widetilde{I}\left(SQ_1\cdots Q_mE_2';P_1;\cdots;P_m\left|E_1'\right.\right)_\omega + \widetilde{I}\left(SP_1\cdots P_mE_1';Q_1;\cdots;Q_m\left|E_2'\right.\right)_\omega && (3.20)\\
&\leq \widetilde{I}\left(SQ_1\cdots Q_mE_2;P_1;\cdots;P_m\left|E_1'\right.\right)_\tau + \widetilde{I}\left(SP_1\cdots P_mE_1;Q_1;\cdots;Q_m\left|E_2'\right.\right)_\sigma . && (3.21)
\end{aligned}
$$

The first inequality follows from several applications of the strong subadditivity of quantum entropy. The first equality is again duality of conditional entropy. The final equality is from the definition of $\widetilde{I}$ in (2.16) and the last inequality follows from the monotonicity of $\widetilde{I}$ under local quantum operations. Since the above calculations are independent of the choice of squashing channels $\mathcal{S}_{E_i\to E_i'}$, and since E_1 purifies the state on $SP_1Q_1\cdots P_mQ_mE_2$ and E_2 purifies the state on $SP_1Q_1\cdots P_mQ_mE_1$, the inequality in (3.2) follows. ■

3.2 Monotonicity under groupings

Lemma 7 *The squashed entanglement measures of Definition 2 are non-increasing under grouping of subsystems, i.e., for a state $\rho_{A_1\cdots A_m}$,*

$$
\begin{aligned}
E_{\text{sq}}(A_1;\cdots;A_m)_\rho &\geq E_{\text{sq}}\left(A_1A_2;A_{3;}\cdots;A_m\right)_\rho && (3.22)\\
\widetilde{E}_{\text{sq}}(A_1;\cdots;A_m)_\rho &\geq \widetilde{E}_{\text{sq}}\left(A_1A_2;A_{3;}\cdots;A_m\right)_\rho && (3.23)
\end{aligned}
$$

Proof. Consider the chain rule expansion for $I(A_1;\cdots;A_m)_\rho$ given in (2.14):

$$I\left(A_1;\cdots;A_m\left|E\right.\right)_\rho = \sum_{i=1}^{m} H\left(A_i\left|E\right.\right)_\rho - H\left(A_1\cdots A_m\left|E\right.\right)_\rho \tag{3.24}$$

$$= H\left(A_1\left|E\right.\right)_\rho + H\left(A_2\left|E\right.\right)_\rho + \sum_{i=3}^{m} H\left(A_i\left|E\right.\right)_\rho - H\left(A_1\cdots A_m\left|E\right.\right)_\rho . \tag{3.25}$$

Now consider the same chain rule expansion for $I\left(A_1A_2;A_3;\cdots;A_m\right)_\rho$:

$$I\left(A_1A_2;A_3;\cdots;A_m\left|E\right.\right)_\rho = H\left(A_1A_2\left|E\right.\right)_\rho + \sum_{i=3}^{m} H\left(A_i\left|E\right.\right)_\rho - H\left(A_1\cdots A_m\left|E\right.\right)_\rho . \tag{3.26}$$

Taking the difference of (3.25) and (3.26), we find that

$$\begin{aligned} & I\left(A_1;\cdots;A_m\left|E\right.\right)_\rho - I\left(A_1A_2;A_3;\cdots;A_m\left|E\right.\right)_\rho \\ & = H\left(A_1\left|E\right.\right)_\rho + H\left(A_2\left|E\right.\right)_\rho - H\left(A_1A_2\left|E\right.\right)_\rho && (3.27) \\ & = I\left(A_1;A_2\left|E\right.\right)_\rho && (3.28) \\ & \geq 0, && (3.29) \end{aligned}$$

where the last inequality follows from the strong subadditivity of quantum entropy.

Similarly, consider the chain rule expansion for $\widetilde{I}(A_1;\cdots;A_m)$ given in (2.15). We have

$$\widetilde{I}\left(A_1;\cdots;A_m\left|E\right.\right)_\rho = \sum_{i=1}^{m} H\left(A_{[m]\setminus\{i\}}\left|E\right.\right)_\rho - (m-1)\, H\left(A_1\cdots A_m\left|E\right.\right)_\rho \tag{3.30}$$

$$\begin{aligned} & = H\left(A_2\cdots A_m\left|E\right.\right)_\rho + H\left(A_1A_3\cdots A_m\left|E\right.\right)_\rho \\ & \qquad + \sum_{i=3}^{m} H\left(A_{[m]\setminus\{i\}}\left|E\right.\right)_\rho - (m-1)\, H\left(A_1\cdots A_m\left|E\right.\right)_\rho . \end{aligned} \tag{3.31}$$

Now consider the same chain rule expansion for $\widetilde{I}\left(A_1A_2;A_3;\cdots;A_m\right)$ where we have grouped systems A_1 and A_2 into one system. We have

$$\begin{aligned} \widetilde{I}\left(A_1A_2;A_3;\cdots;A_m\left|E\right.\right)_\rho & = H\left(A_3\cdots A_m\left|E\right.\right)_\rho \\ & \qquad + \sum_{i=3}^{m} H\left(A_{[m]\setminus\{i\}}\left|E\right.\right)_\rho - (m-2)\, H\left(A_1\cdots A_m\left|E\right.\right)_\rho . \end{aligned} \tag{3.32}$$

Taking the difference of (3.31) and (3.32), we find that

$$\begin{aligned} & \widetilde{I}\left(A_1;\cdots;A_m\left|E\right.\right)_\rho - \widetilde{I}\left(A_1A_2;A_3;\cdots;A_m\left|E\right.\right)_\rho \\ & = H\left(A_2\cdots A_m\left|E\right.\right)_\rho + H\left(A_1A_3\cdots A_m\left|E\right.\right)_\rho \\ & \qquad - H\left(A_3\cdots A_m\left|E\right.\right)_\rho - H\left(A_1\cdots A_m\left|E\right.\right)_\rho && (3.33) \\ & = I\left(A_1;A_2\left|A_3\cdots A_mE\right.\right)_\rho && (3.34) \\ & \geq 0, && (3.35) \end{aligned}$$

where the last inequality follows from the strong subadditivity of quantum entropy. The statement of the lemma follows from the above inequalities and by taking infima. ∎

3.3 Reduction for product states

Lemma 8 *Let $\omega_{A_1A_2\cdots A_m} = \rho_{A_1} \otimes \sigma_{A_2\cdots A_m}$, where ρ_{A_1} and $\sigma_{A_2\cdots A_m}$ are density operators. Then*

$$E_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega = E_{\text{sq}}\left(A_2; A_{3;} \cdots; A_m\right)_\sigma, \tag{3.36}$$

$$\widetilde{E}_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega = \widetilde{E}_{\text{sq}}\left(A_2; A_3; \cdots; A_m\right)_\sigma. \tag{3.37}$$

Proof. We first prove LHS $\geq$ RHS for the inequalities in the statement of the lemma. Consider that

$$\begin{aligned} E_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega &\geq E_{\text{sq}}\left(A_1A_2; \cdots; A_m\right)_\omega & (3.38)\\ &\geq E_{\text{sq}}\left(A_2; \cdots; A_m\right)_\omega & (3.39)\\ &= E_{\text{sq}}\left(A_2; \cdots; A_m\right)_\sigma, & (3.40) \end{aligned}$$

where the first inequality is from monotonicity under groupings (Lemma 7) and the second inequality is from monotonicity under LOCC. The same reasoning gives

$$\widetilde{E}_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega \geq \widetilde{E}_{\text{sq}}\left(A_2; A_3; \cdots; A_m\right)_\sigma. \tag{3.41}$$

We now prove LHS $\leq$ RHS for the inequalities in the statement of the lemma. Let ρ_{A_1E} extend ρ_{A_1} and $\sigma_{A_2\cdots A_mF}$ extend $\sigma_{A_2\cdots A_m}$. Then

$$\begin{aligned} 2E_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega &\leq I\left(A_1; A_2; \cdots; A_m|EF\right)_{\rho\otimes\sigma} & (3.42)\\ &= H\left(A_1|EF\right)_{\rho\otimes\sigma} + \sum_{i=2}^{m} H\left(A_i|EF\right)_{\rho\otimes\sigma} - H\left(A_1A_2\cdots A_m|EF\right)_{\rho\otimes\sigma} & (3.43)\\ &= H\left(A_1|E\right)_\rho + \sum_{i=2}^{m} H\left(A_i|F\right)_\sigma - \left[H\left(A_1|E\right)_\rho + H\left(A_2\cdots A_m|F\right)_\sigma\right] & (3.44)\\ &= \sum_{i=2}^{m} H\left(A_i|F\right)_\sigma - H\left(A_2\cdots A_m|F\right)_\sigma & (3.45)\\ &= I\left(A_2; \cdots; A_m|F\right)_\sigma. & (3.46) \end{aligned}$$

Since the calculation holds independently of the particular extension of σ, we can conclude that

$$E_{\text{sq}}\left(A_1; A_2; \cdots; A_m\right)_\omega \leq E_{\text{sq}}\left(A_2; \cdots; A_m\right)_\sigma. \tag{3.47}$$

For the other inequality, consider that

$$
\begin{aligned}
2\widetilde{E}_{\text{sq}}\left(A_1;A_2;\cdots;A_m\right)_\omega &\leq \widetilde{I}\left(A_1;A_2;\cdots;A_m|EF\right)_{\rho\otimes\sigma} && (3.48)\\
&= H\left(A_1A_2\cdots A_m|EF\right)_{\rho\otimes\sigma} \\
&\quad - \left[H\left(A_1|A_2\cdots A_mEF\right)_{\rho\otimes\sigma} + \sum_{i=2}^{m} H\left(A_i|A_1A_{[2:m]\setminus\{i\}}EF\right)_{\rho\otimes\sigma}\right] && (3.49)\\
&= H\left(A_1|E\right)_\rho + H\left(A_2\cdots A_m|F\right)_{\rho\otimes\sigma} \\
&\quad - \left[H\left(A_1|E\right)_\rho + \sum_{i=2}^{m} H\left(A_i|A_{[2:m]\setminus\{i\}}F\right)_\sigma\right] && (3.50)\\
&= H\left(A_2\cdots A_m|F\right)_{\rho\otimes\sigma} - \sum_{i=2}^{m} H\left(A_i|A_{[2:m]\setminus\{i\}}F\right)_\sigma && (3.51)\\
&= \widetilde{I}\left(A_2;\cdots;A_m|F\right)_\sigma . && (3.52)
\end{aligned}
$$

By the same reasoning as above, we can conclude

$$\widetilde{E}_{\text{sq}}\left(A_1;A_2;\cdots;A_m\right)_\omega \leq \widetilde{E}_{\text{sq}}\left(A_2;\cdots;A_m\right)_\sigma . \tag{3.53}$$

This completes the proof. ■

3.4 Multipartite squashed entanglements of maximally entangled states and private states

Consider a set $\mathcal{S} = \{A, B, C\}$. Let Ψ_{ABC} be a joint state over A, B, and C of the form

$$
\begin{aligned}
\Psi_{ABC} \equiv \Phi_{A^{(1)}B^{(1)}} \otimes \Phi_{A^{(2)}C^{(2)}} \otimes \Phi_{B^{(3)}C^{(3)}} \otimes \Phi_{A^{(4)}B^{(4)}C^{(4)}} \\
\otimes \gamma_{A^{(5)}B^{(5)}} \otimes \gamma_{A^{(6)}C^{(6)}} \otimes \gamma_{B^{(7)}C^{(7)}} \otimes \gamma_{A^{(8)}B^{(8)}C^{(8)}}, \quad (3.54)
\end{aligned}
$$

where each Φ represents a maximally entangled state of the form in (2.5) and each γ represents a private state of the form in (2.10), and where the quantum system A, e.g., has been split into subsystems $A^{(1)}A^{(2)}A^{(4)}A^{(5)}A^{(6)}A^{(8)}$ to segregate the different kinds of correlations that it holds with B and C. Thus, if $\mathcal{S}$ corresponds to a set of three parties Alice A, Bob B, and Charlie C, then the state Ψ_{ABC} represents a collection of maximally entangled states and private states shared between all the non-trivial subsets of the parties, which are enlisted in the following set:

$$\mathcal{P}_{\geq 2}(\mathcal{S}) = \left\{\{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\right\}. \tag{3.55}$$

Let us denote the number of entangled bits and private bits shared between the three parties over the various elements of $\mathcal{P}_{\geq 2}(\mathcal{S})$ by the tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ (where E stands for "Entanglement" and K for "Key"). Then, for the state Ψ_{ABC} in (3.54), we have

$$E_{AB} \equiv H\left(A^{(1)}\right)_\Phi, \quad E_{AC} \equiv H\left(A^{(2)}\right)_\Phi, \quad E_{BC} \equiv H\left(B^{(3)}\right)_\Phi, \quad E_{ABC} \equiv H\left(A^{(4)}\right)_\Phi, \tag{3.56}$$

$$K_{AB} \equiv H\left(A^{(5)}\right)_\gamma, \quad K_{AC} \equiv H\left(A^{(6)}\right)_\gamma, \quad K_{BC} \equiv H\left(B^{(7)}\right)_\gamma, \quad K_{ABC} \equiv H\left(A^{(8)}\right)_\gamma, \tag{3.57}$$

where H denotes the von Neumann entropy. Note that the quantity E_{AB}, which, e.g., is the amount of entanglement shared between Alice and Bob, is to be understood as the amount of entanglement between the systems $A^{(1)}$ and $B^{(1)}$. Also, for the private γ-states it is implicit that we are evaluating the entropies with respect to the key systems, so that the entropy is equal to the number of private bits in the state.

Our goal in this section is as follows. For a given state Ψ_{ABC} of the form in (3.54), we want to establish constraints relating the elements of the tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ using the multipartite squashed entanglement quantities discussed in Section 2.6. For this, we are interested in determining the multipartite squashed entanglements of Ψ_{ABC} with respect to various nontrivial partitions of $\mathcal{S} = \{A, B, C\}$, which are given by

$$\mathcal{G}_1 = \{\{A\}, \{B, C\}\}, \tag{3.58}$$
$$\mathcal{G}_2 = \{\{A, B\}, \{C\}\}, \tag{3.59}$$
$$\mathcal{G}_3 = \{\{A, C\}, \{B\}\}, \tag{3.60}$$
$$\mathcal{G}_4 = \{\{A\}, \{B\}, \{C\}\}. \tag{3.61}$$

(Note that we have excluded the trivial partition $\mathcal{G}_5 = \{\mathcal{S}\}$.)

For partition $\mathcal{G}_1$, we obtain

$$E_{\mathrm{sq}}(\mathcal{G}_1)_\Psi = \widetilde{E}_{\mathrm{sq}}(\mathcal{G}_1)_\Psi \tag{3.62}$$
$$= E_{\mathrm{sq}}\left(A^{(1)}A^{(2)}A^{(4)}A^{(5)}A^{(6)}A^{(8)}; B^{(1)}B^{(3)}B^{(4)}B^{(5)}B^{(7)}B^{(8)}C^{(2)}C^{(3)}C^{(4)}C^{(6)}C^{(7)}C^{(8)}\right)_\Psi \tag{3.63}$$
$$= E_{\mathrm{sq}}(A^{(1)}; B^{(1)})_\Phi + E_{\mathrm{sq}}(A^{(2)}; C^{(2)})_\Phi + E_{\mathrm{sq}}(A^{(4)}; B^{(4)}C^{(4)})_\Phi + E_{\mathrm{sq}}(A^{(5)}; B^{(5)})_\gamma + E_{\mathrm{sq}}(A^{(6)}; C^{(6)})_\gamma + E_{\mathrm{sq}}(A^{(8)}; B^{(8)}C^{(8)})_\gamma \tag{3.64}$$
$$\geq E_{AB} + E_{AC} + E_{ABC} + K_{AB} + K_{AC} + K_{ABC}. \tag{3.65}$$

The first equality follows because the two squashed entanglements are identical in the bipartite case. The second equality follows from the additivity of squashed entanglement with respect to tensor-product states and from Lemma 8. The inequality follows from Lemma 5. A similar line of reasoning for partitions $\mathcal{G}_2$ and $\mathcal{G}_3$ yields the following constraints:

$$E_{\mathrm{sq}}(\mathcal{G}_2)_\Psi = \widetilde{E}_{\mathrm{sq}}(\mathcal{G}_2)_\Psi \geq E_{AC} + E_{BC} + E_{ABC} + K_{AC} + K_{BC} + K_{ABC}, \tag{3.66}$$
$$E_{\mathrm{sq}}(\mathcal{G}_3)_\Psi = \widetilde{E}_{\mathrm{sq}}(\mathcal{G}_3)_\Psi \geq E_{AB} + E_{BC} + E_{ABC} + K_{AB} + K_{BC} + K_{ABC}. \tag{3.67}$$

Finally, for partition $\mathcal{G}_4$, we obtain

$$E_{\mathrm{sq}}(\mathcal{G}_4)_\Psi = E_{\mathrm{sq}}\left(A^{(1)}A^{(2)}A^{(4)}A^{(5)}A^{(6)}A^{(8)}; B^{(1)}B^{(3)}B^{(4)}B^{(5)}B^{(7)}B^{(8)}; C^{(2)}C^{(3)}C^{(4)}C^{(6)}C^{(7)}C^{(8)}\right)_\Psi \tag{3.68}$$
$$= E_{\mathrm{sq}}(A^{(1)}; B^{(1)})_\Phi + E_{\mathrm{sq}}(A^{(2)}; C^{(2)})_\Phi + E_{\mathrm{sq}}(B^{(3)}; C^{(3)})_\Phi + E_{\mathrm{sq}}(A^{(4)}; B^{(4)}; C^{(4)})_\Phi + E_{\mathrm{sq}}(A^{(5)}; B^{(5)})_\gamma + E_{\mathrm{sq}}(A^{(6)}; C^{(6)})_\gamma + E_{\mathrm{sq}}(B^{(7)}; C^{(7)})_\gamma + E_{\mathrm{sq}}(A^{(8)}; B^{(8)}; C^{(8)})_\gamma \tag{3.69}$$
$$\geq E_{AB} + E_{AC} + E_{BC} + \frac{3}{2}E_{ABC} + K_{AB} + K_{AC} + K_{BC} + \frac{3}{2}K_{ABC}. \tag{3.70}$$

The second equality follows from the additivity of squashed entanglement with respect to tensor-product states and from Lemma 8. The inequality follows from Lemma 5. Similarly, we also obtain

$$\widetilde{E}_{\text{sq}}(\mathcal{G}_4)_\Psi \geq E_{AB} + E_{AC} + E_{BC} + \frac{3}{2}E_{ABC} + K_{AB} + K_{AC} + K_{BC} + \frac{3}{2}K_{ABC}. \tag{3.71}$$

Since $\mathcal{G}_4$ is a tripartition and the two multipartite squashed entanglements are not identical in general, we can pick the minimum of $\widetilde{E}_{\text{sq}}(\mathcal{G}_4)_\Psi$ and $E_{\text{sq}}(\mathcal{G}_4)_\Psi$ to give a tighter upper bound.

The above analysis can be further extended to sets containing more than three elements. Consider a set of $m+1$ elements, $\mathcal{S} = \{A, B_1, \ldots, B_m\}$, for arbitrary but finite m. Let $\Psi_{\mathcal{S}}$ be the following state:

$$\Psi_{\mathcal{S}} \equiv \bigotimes_{\mathcal{K} \in \mathcal{P}_{\geq 2}(\mathcal{S})} \Phi_{\mathcal{K}} \otimes \gamma_{\mathcal{K}}, \tag{3.72}$$

which is a tensor product of all possible entangled states and private states that could be shared between all subsets of the parties in $\mathcal{S}$, with it understood that each $\mathcal{K}$ has a set of distinct subsystems in the tensor product (as is the case for the example in (3.54)). For a given subset $\mathcal{K} \in \mathcal{P}_{\geq 2}(\mathcal{S})$, let $E_{\mathcal{K}}$ denote the number of entangled bits (logarithm of the Schmidt rank) in the multiparty GHZ entangled state $\Phi_{\mathcal{K}}$, and let $K_{\mathcal{K}}$ denote the number of private bits in the private state $\gamma_{\mathcal{K}}$.

Definition 9 *For a given nontrivial partition $\mathcal{G}$ of a set $\mathcal{S}$, we define the set $\mathcal{C}(\mathcal{G})$ of sets by the following procedure. Let $\mathcal{X}_1, \ldots, \mathcal{X}_{|\mathcal{G}|}$ denote all of the sets in the partition $\mathcal{G}$. For each $\mathcal{L}_{\mathcal{X}_1} \in \mathcal{P}(\mathcal{X}_1)$, $\ldots$, $\mathcal{L}_{\mathcal{X}_{|\mathcal{G}|}} \in \mathcal{P}\left(\mathcal{X}_{|\mathcal{G}|}\right)$, form the set $\mathcal{L}_{\mathcal{X}_1} \cup \cdots \cup \mathcal{L}_{\mathcal{X}_{|\mathcal{G}|}}$ and add it to $\mathcal{C}(\mathcal{G})$. At the end, remove the null set and any singleton sets.*

For example, for the partition $\mathcal{G}_1 = \{\{A\}, \{B, C\}\}$ of $\mathcal{S} = \{A, B, C\}$, this procedure leads to

$$\mathcal{C}(\mathcal{G}_1) = \{\{A, B\}, \{A, C\}, \{A, B, C\}\}. \tag{3.73}$$

Definition 10 *For a given nontrivial partition $\mathcal{G}$ of a set $\mathcal{S}$ and an element $\mathcal{M}$ of $\mathcal{C}(\mathcal{G})$, we define the set $\mathcal{A}(\mathcal{M}, \mathcal{G})$ as*

$$\mathcal{A}(\mathcal{M}, \mathcal{G}) \equiv \{\mathcal{X} \cap \mathcal{M} \mid \mathcal{X} \in \mathcal{G}\} \setminus \{\emptyset\}. \tag{3.74}$$

For example, for the partition $\mathcal{G}_4 = \{\{A\}, \{B\}, \{C\}\}$ of $\mathcal{S} = \{A, B, C\}$, we have

$$\mathcal{C}(\mathcal{G}_4) = \{\{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}. \tag{3.75}$$

Let us denote the elements of $\mathcal{C}(\mathcal{G}_4)$ as $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \mathcal{M}_4\}$. Then, we have

$$\mathcal{A}(\mathcal{M}_1, \mathcal{G}_4) = \{\{A\}, \{B\}\}, \tag{3.76}$$
$$\mathcal{A}(\mathcal{M}_2, \mathcal{G}_4) = \{\{A\}, \{C\}\}, \tag{3.77}$$
$$\mathcal{A}(\mathcal{M}_3, \mathcal{G}_4) = \{\{B\}, \{C\}\}, \tag{3.78}$$
$$\mathcal{A}(\mathcal{M}_4, \mathcal{G}_4) = \{\{A\}, \{B\}, \{C\}\}. \tag{3.79}$$

Lemma 11 *Let $\mathcal{S}$ be a set of parties and let $\Psi_{\mathcal{S}}$ be the tensor product of states defined in* (3.72)*. Then for a given nontrivial partition $\mathcal{G}$ of $\mathcal{S}$, the squashed entanglements $E_{\mathrm{sq}}(\mathcal{G})_{\Psi}$ and $\widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Psi}$ from Definition 2 constrain the number of entangled bits $E_{\mathcal{M}}$ and private bits $K_{\mathcal{M}}$ between the elements of $\mathcal{G}$ as follows:*

$$\frac{1}{2}\sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})}\left|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)\right|\left(K_{\mathcal{M}}+E_{\mathcal{M}}\right)\leq\min\left\{E_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}},\ \widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}}\right\}. \tag{3.80}$$

Proof. Let $\mathcal{G}$ be a nontrivial partition of $\mathcal{S}$. We begin by considering $E_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}}$:

$$\begin{aligned}E_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}} &= \sum_{\mathcal{K}\in\mathcal{P}_{\geq 2}(\mathcal{S})}\left(E_{\mathrm{sq}}(\mathcal{G})_{\Phi_{\mathcal{K}}}+E_{\mathrm{sq}}(\mathcal{G})_{\gamma_{\mathcal{K}}}\right) &(3.81)\\ &= \sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})}\left(E_{\mathrm{sq}}(\mathcal{G})_{\Phi_{\mathcal{M}}}+E_{\mathrm{sq}}(\mathcal{G})_{\gamma_{\mathcal{M}}}\right). &(3.82)\end{aligned}$$

The first equality is a consequence of the additivity of squashed entanglement with respect to tensor product states. The second equality follows because $E_{\mathrm{sq}}(\mathcal{G})_{\Phi_{\mathcal{K}}}=E_{\mathrm{sq}}(\mathcal{G})_{\gamma_{\mathcal{K}}}=0$ if $\mathcal{K}\subseteq\mathcal{X}$ for some $\mathcal{X}\in\mathcal{G}$ and the algorithm that constructs $\mathcal{C}(\mathcal{G})$ removes all such $\mathcal{K}$. Now consider that

$$\begin{aligned}2E_{\mathrm{sq}}(\mathcal{G})_{\Phi_{\mathcal{M}}} &= I(\mathcal{G})_{\Phi_{\mathcal{M}}} &(3.83)\\ &= \sum_{\mathcal{X}\in\mathcal{G}} H\left(\mathcal{X}\cap\mathcal{M}\right)_{\Phi_{\mathcal{M}}}-H\left(\mathcal{M}\right)_{\Phi_{\mathcal{M}}} &(3.84)\\ &= \sum_{\mathcal{X}\in\mathcal{G}} H\left(\mathcal{X}\cap\mathcal{M}\right)_{\Phi_{\mathcal{M}}} &(3.85)\\ &= \left|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)\right|E_{\mathcal{M}}. &(3.86)\end{aligned}$$

The first equality holds because any pure entangled state is not extendible, so that any extension system is product with it. The next equality is from the definition of $I(\mathcal{G})$ (similar to (2.14) without the conditioning system). The third equality follows because the state $\Phi_{\mathcal{M}}$ is pure. The final equality is a consequence of the definition of the set $\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)$ and the fact that for all $\mathcal{X}\in\mathcal{G}$, where $\mathcal{G}$ is a nontrivial partition of $\mathcal{S}$, $\mathcal{X}\cap\mathcal{M}\subset\mathcal{M}$ and therefore $H\left(\mathcal{X}\cap\mathcal{M}\right)_{\Phi_{\mathcal{M}}}$ equals the number of entangled bits in $\Phi_{\mathcal{M}}$.

We now prove the following lower bound:

$$E_{\mathrm{sq}}(\mathcal{G})_{\gamma_{\mathcal{M}}}\geq\frac{1}{2}\left|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)\right|K_{\mathcal{M}}, \tag{3.87}$$

which extends Lemma 5 and just applies the idea behind [11, Proposition 4.19] to this more general case. To do so, let us consider both the key and shield systems of $\gamma_{\mathcal{M}}$ and label them by $\mathcal{M}$ and $\mathcal{M}'$, respectively, so that we relabel $\gamma_{\mathcal{M}}$ as $\gamma_{\mathcal{M}\mathcal{M}'}$. Then $\gamma_{\mathcal{M}\mathcal{M}'}$ has the following form:

$$\gamma_{\mathcal{M}\mathcal{M}'}=U_{\mathcal{M}\mathcal{M}'}\left(\Phi_{\mathcal{M}}\otimes\rho_{\mathcal{M}'}\right)U_{\mathcal{M}\mathcal{M}'}^{\dagger}, \tag{3.88}$$

where the twisting unitary is

$$U_{\mathcal{M}\mathcal{M}'}=\sum_{i=0}^{2^{K_{\mathcal{M}}}-1}|i\rangle\langle i|_{\mathcal{M}}\otimes U_{\mathcal{M}'}^{i}, \tag{3.89}$$

and where $K_{\mathcal{M}}$ is the number of private bits contained in $\gamma_{\mathcal{M}\mathcal{M}'}$. An extension $\gamma_{\mathcal{M}\mathcal{M}'E}$ of $\gamma_{\mathcal{M}\mathcal{M}'}$ has the following form:

$$\gamma_{\mathcal{M}\mathcal{M}'E} = U_{\mathcal{M}\mathcal{M}'} \left(\Phi_{\mathcal{M}} \otimes \rho_{\mathcal{M}'E}\right) U^{\dagger}_{\mathcal{M}\mathcal{M}'}, \tag{3.90}$$

where $\rho_{\mathcal{M}'E}$ is some extension of $\rho_{\mathcal{M}'}$. Let $\gamma^i_{\mathcal{M}'E}$ denote the following state:

$$\gamma^i_{\mathcal{M}'E} \equiv U^i_{\mathcal{M}'} \rho_{\mathcal{M}'E} \left(U^i_{\mathcal{M}'}\right)^{\dagger}. \tag{3.91}$$

Then consider that

$$H\left(\mathcal{M}\mathcal{M}'E\right)_{\gamma} = H\left(\mathcal{M}'E\right)_{\rho} = H\left(\mathcal{M}'E\right)_{\gamma^i}, \tag{3.92}$$

$$H(E)_{\gamma} = H(E)_{\gamma^i}, \tag{3.93}$$

where we have used some well-known properties of the von Neumann entropy, namely that it is invariant under unitary transformations, it is additive on tensor product states and that it is zero for pure states. Then, for all i, we have

$$H\left(\mathcal{M}\mathcal{M}'|E\right)_{\gamma} = H\left(\mathcal{M}'|E\right)_{\gamma^i}. \tag{3.94}$$

This allows us to conclude that

$$H\left(\mathcal{M}\mathcal{M}'|E\right)_{\gamma} = \sum_{i=0}^{2^{K_{\mathcal{M}}}-1} \frac{1}{2^{K_{\mathcal{M}}}} H\left(\mathcal{M}'|E\right)_{\gamma^i}, \tag{3.95}$$

where we have simply rewritten the right hand side, since $H\left(\mathcal{M}'|E\right)_{\gamma^i}$ is the same for all i. For all $\mathcal{X} \in \mathcal{G}$, we have that

$$H\left(\left[\mathcal{X} \cap \mathcal{M}\right]\left[\mathcal{X}' \cap \mathcal{M}'\right] E\right)_{\gamma} = H\left(\mathcal{X} \cap \mathcal{M}\right)_{\gamma} + H\left(\left[\mathcal{X}' \cap \mathcal{M}'\right] E | \left[\mathcal{X} \cap \mathcal{M}\right]\right)_{\gamma} \tag{3.96}$$

$$= K_{\mathcal{M}} + \sum_{i=0}^{2^{K_{\mathcal{M}}}-1} \frac{1}{2^{K_{\mathcal{M}}}} H\left(\left[\mathcal{X}' \cap \mathcal{M}'\right] E\right)_{\gamma^i}, \tag{3.97}$$

where we have used $\mathcal{X}'$ to label the shield systems corresponding to the key systems in $\mathcal{X}$. The first term in (3.97) follows because $H\left(\mathcal{X} \cap \mathcal{M}\right)_{\gamma} = H\left(\mathcal{X} \cap \mathcal{M}\right)_{\Phi_{\mathcal{M}}}$, the number of entangled bits in $\Phi_{\mathcal{M}}$, which indeed equals the number of private bits in γ. Thus, from (3.97) and (3.93), we have

$$H\left(\left[\mathcal{X} \cap \mathcal{M}\right]\left[\mathcal{X}' \cap \mathcal{M}'\right] |E\right)_{\gamma} = K_{\mathcal{M}} + \sum_i \frac{1}{2^{K_{\mathcal{M}}}} H\left(\left[\mathcal{X}' \cap \mathcal{M}'\right] |E\right)_{\gamma^i} \tag{3.98}$$

The multipartite conditional mutual information of γ across the partition $\mathcal{G}$ of the key systems and the analogous partition $\mathcal{G}'$ of the shield systems can thus be written as

$$I(\mathcal{G}\mathcal{G}'|E)_{\gamma} = \sum_{\mathcal{X} \in \mathcal{G}} H\left(\left[\mathcal{X} \cap \mathcal{M}\right]\left[\mathcal{X}' \cap \mathcal{M}'\right] |E\right)_{\gamma} - H\left(\mathcal{M}\mathcal{M}'|E\right)_{\gamma} \tag{3.99}$$

$$= \left|\mathcal{A}\left(\mathcal{M}, \mathcal{G}\right)\right| K_{\mathcal{M}} + \sum_{\mathcal{X} \in \mathcal{G}} \sum_i \frac{1}{2^{K_{\mathcal{M}}}} H\left(\left[\mathcal{X}' \cap \mathcal{M}'\right] |E\right)_{\gamma^i} \tag{3.100}$$

$$- \sum_i \frac{1}{2^{K_{\mathcal{M}}}} H\left(\mathcal{M}'|E\right)_{\gamma^i} \tag{3.101}$$

$$= \left|\mathcal{A}\left(\mathcal{M}, \mathcal{G}\right)\right| K_{\mathcal{M}} + \sum_i \frac{1}{2^{K_{\mathcal{M}}}} I\left(\mathcal{G}'|E\right)_{\gamma^i} \tag{3.102}$$

$$\geq \left|\mathcal{A}\left(\mathcal{M}, \mathcal{G}\right)\right| K_{\mathcal{M}}. \tag{3.103}$$

The first equality follows from the definition of conditional multipartite information in (2.14). The second equality follows from (3.97) and (3.98) and the definition of the set $\mathcal{A}(\mathcal{M},\mathcal{G})$. The third equality follows once again from the definition of conditional multipartite information in (2.14). Finally, the fourth inequality in (3.103) from the strong subadditivity of quantum entropy, namely that $I(\mathcal{G}'|E)_{\gamma^i} \geq 0$ for any quantum state γ^i. Since the inequality is independent of the particular extension of $\gamma_{\mathcal{M}\mathcal{M}'}$, from the definition of the multipartite squashed entanglement in (2), we can conclude (3.87). Putting together (3.81)-(3.86) and (3.87), we find that

$$E_{\text{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}} \geq \frac{1}{2} \sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})} |\mathcal{A}(\mathcal{M},\mathcal{G})| \left(K_{\mathcal{M}} + E_{\mathcal{M}}\right) \tag{3.104}$$

Similarly, we have

$$\widetilde{E}_{\text{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}} = \sum_{\mathcal{K}\in\mathcal{P}_{\geq 2}(\mathcal{S})} \left(\widetilde{E}_{\text{sq}}(\mathcal{G})_{\Phi_{\mathcal{K}}} + \widetilde{E}_{\text{sq}}(\mathcal{G})_{\gamma_{\mathcal{K}}}\right) \tag{3.105}$$

$$= \sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})} \left(\widetilde{E}_{\text{sq}}(\mathcal{G})_{\Phi_{\mathcal{M}}} + \widetilde{E}_{\text{sq}}(\mathcal{G})_{\gamma_{\mathcal{M}}}\right) \tag{3.106}$$

The proof is similar to the proof of (3.104). Using the definition of $\tilde{I}(\mathcal{G})$ similar to (2.16) (except for the conditioning system) and that of the the multipartite squashed entanglement $\widetilde{E}_{\text{sq}}$ in Definition 2, and a similar line of reasoning as given before for (3.81)-(3.86), we obtain

$$2\widetilde{E}_{\text{sq}}(\mathcal{G})_{\Phi_{\mathcal{M}}} = \widetilde{I}(\mathcal{G})_{\Phi_{\mathcal{M}}} \tag{3.107}$$

$$= H(\mathcal{S})_{\Phi_{\mathcal{M}}} - \sum_{\mathcal{X}\in\mathcal{G}} H\left(\mathcal{X}\cap\mathcal{M}|\left(\mathcal{S}\backslash\mathcal{X}\right)\cap\mathcal{M}\right)_{\Phi_{\mathcal{M}}} \tag{3.108}$$

$$= \sum_{\mathcal{X}\in\mathcal{G}} H\left(\mathcal{X}\cap\mathcal{M}\right)_{\Phi_{\mathcal{M}}} \tag{3.109}$$

$$= |\mathcal{A}(\mathcal{M},\mathcal{G})|\, E_{\mathcal{M}}. \tag{3.110}$$

By the same reasoning used to conclude (3.98), we can conclude that

$$H\left(\left[\mathcal{M}\backslash\left[\mathcal{X}\cap\mathcal{M}\right]\right]\left[\mathcal{M}'\backslash\left[\mathcal{X}'\cap\mathcal{M}'\right]\right]|E\right)_{\gamma} = K_{\mathcal{M}} + \sum_i \frac{1}{2^{K_{\mathcal{M}}}} H\left(\mathcal{M}'\backslash\left[\mathcal{X}'\cap\mathcal{M}'\right]|E\right)_{\gamma^i} \tag{3.111}$$

Consider that

$$\widetilde{E}_{\text{sq}}(\mathcal{G})_{\gamma_{\mathcal{M}}} \geq \frac{1}{2}|\mathcal{A}(\mathcal{M},\mathcal{G})|\, K_{\mathcal{M}}. \tag{3.112}$$

This is because

$$\begin{aligned}
\widetilde{I}(\mathcal{G}\mathcal{G}'|E)_{\gamma_{\mathcal{M}\mathcal{M}'E}} &= \sum_{\mathcal{X}\in\mathcal{G}} H\left(\left[\mathcal{M}\backslash\left[\mathcal{X}\cap\mathcal{M}\right]\right]\left[\mathcal{M}'\backslash\left[\mathcal{X}'\cap\mathcal{M}'\right]\right]|E\right)_{\gamma} \\
&\quad - \left(|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)|-1\right) H\left(\mathcal{M}\mathcal{M}'|E\right)_{\gamma} \qquad (3.113)\\
&= |\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)| K_{\mathcal{M}} + \sum_{\mathcal{X}\in\mathcal{G}}\sum_{i}\frac{1}{2^{K_{\mathcal{M}}}} H\left(\mathcal{M}'\backslash\left[\mathcal{X}'\cap\mathcal{M}'\right]|E\right)_{\gamma^i} \\
&\quad - \left(|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)|-1\right)\sum_{i}\frac{1}{2^{K_{\mathcal{M}}}} H\left(\mathcal{M}'|E\right)_{\gamma^i} \qquad (3.114)\\
&= |\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)| K_{\mathcal{M}} + \sum_{i}\frac{1}{2^{K_{\mathcal{M}}}}\widetilde{I}(\mathcal{G}'|E)_{\gamma^i} \qquad (3.115)\\
&\geq |\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)| K_{\mathcal{M}} \qquad (3.116)
\end{aligned}$$

The reasons for these steps are similar to those used to justify (3.99)-(3.103), and we can then conclude (3.112). So this implies that

$$\widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}} \geq \frac{1}{2}\sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})} |\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)|\left(K_{\mathcal{M}}+E_{\mathcal{M}}\right) \qquad (3.117)$$

Equations (3.104) and (3.117) together conclude the proof. ■

4 Entanglement distillation and secret key agreement using a quantum broadcast channel

A quantum broadcast channel is a CPTP map $\mathcal{N}_{A\to B_1\cdots B_m}$ from one sender A to multiple receivers $B_1, \ldots, B_m$. Several communication tasks have already been considered for a quantum broadcast channel [56, 16, 39, 37], and in classical information theory, the secret-key agreement capacity of certain classes of point-to-multipoint noisy discrete memoryless channels has been characterized [14] and further generalizations have been obtained as well [20, 21].

In this work, we are interested in bounding the achievable entanglement distillation and secret key agreement rates between any subset of the parties when using a quantum broadcast channel an arbitrarily large number of times, such that the sender and receivers are allowed to engage in an arbitrary number of rounds of LOCC between each channel use. It is customary to consider the paradigm of local operations and classical communication (LOCC) for entanglement distillation and local operations and public communication (LOPC) for secret key agreement. However, as mentioned in Section 2.4, the approximate LOPC distillation of secret key is equivalent to the approximate LOCC distillation of private states [27, 26]. Therefore, the two tasks can be studied together under the common umbrella of LOCC.

Let us now define a general protocol for secret key agreement and entanglement distillation by using a quantum broadcast channel and LOCC. For simplicity, we begin by considering the case in which we have a sender Alice and two receivers Bob and Charlie. The most general $(n, E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC}, \varepsilon)$ protocol to distill entanglement and secret key between all subsets of the parties, where $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ denotes a rate tuple, involves the following steps:

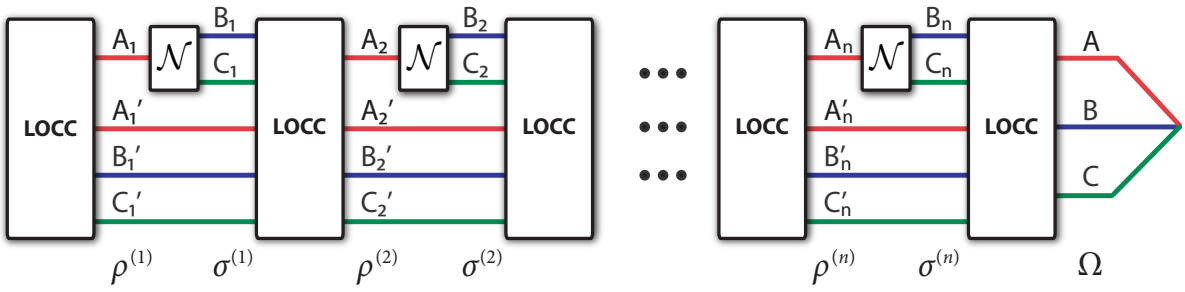

Figure 1: A general protocol for entanglement distillation and secret key agreement using LOCC and a quantum broadcast channel $\mathcal{N}_{A\to BC}$ with one sender and two receivers. The protocol uses the channel n times, and the primed registers represent "scratch" registers that each party uses for local processing. The state Ω_{ABC} at the end is ε-close in trace distance to the ideal state given in (3.54).

1. Alice, Bob, and Charlie engage in a round of LOCC to prepare a state $\rho^{(1)}_{A_1A_1'B_1'C_1'}$. Necessarily, this state is separable with respect to the cut $A_1A_1' : B_1' : C_1'$. Set $i = 1$.

2. Alice transmits system A_i through the broadcast channel $\mathcal{N}_{A_i\to B_iC_i} \equiv \mathcal{N}_{A\to BC}$, leading to the state
$$\sigma^{(i)}_{A_i'B_iB_i'C_iC_i'} \equiv \mathcal{N}_{A_i\to B_iC_i}\left(\rho^{(i)}_{A_iA_i'B_i'C_i'}\right).$$
Thus, the primed registers $A_i'B_i'C_i'$ represent "scratch" registers of arbitrary size that the three parties can use for their local processing.

3. Alice, Bob, and Charlie engage in a round of LOCC, leading to the state $\rho^{(i+1)}_{A_{i+1}A_{i+1}'B_{i+1}'C_{i+1}'}$. Set $i := i + 1$.

4. If $i < n$, then go to step 2. Otherwise, Alice, Bob, and Charlie engage in a final round of LOCC to produce a state Ω_{ABC}. The protocol is depicted in Figure 1.

At the end of the protocol, the state Ω_{ABC} is ε-close in trace distance to the ideal state Ψ_{ABC} given in (3.54):
$$\|\Omega_{ABC} - \Psi_{ABC}\|_1 \leq \varepsilon. \tag{4.1}$$
Furthermore, the entanglement distillation and secret key agreement rates (similar to (3.56) and (3.57), but with a factor of $1/n$ to take into account n uses of the channel) are given as
$$E_{AB} \equiv \frac{1}{n}H\left(A_1\right)_\Phi, \quad E_{AC} \equiv \frac{1}{n}H\left(A_2\right)_\Phi, \quad E_{BC} \equiv \frac{1}{n}H\left(B_3\right)_\Phi, \quad E_{ABC} \equiv \frac{1}{n}H\left(A_4\right)_\Phi, \tag{4.2}$$
$$K_{AB} \equiv \frac{1}{n}H\left(A_5\right)_\gamma, \quad K_{AC} \equiv \frac{1}{n}H\left(A_6\right)_\gamma, \quad K_{BC} \equiv \frac{1}{n}H\left(B_7\right)_\gamma, \quad K_{ABC} \equiv \frac{1}{n}H\left(A_8\right)_\gamma, \tag{4.3}$$
where the entropies are once again evaluated with respect to the ideal state in (3.54) and for the private γ-states, it is implicit that we are evaluating the entropies of the key systems (so that the entropy is equal to the number of private bits in the state).

A rate tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ is achievable if for all $\varepsilon > 0$ and sufficiently large n, there exists an $(n, E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC}, \varepsilon)$ protocol of the above form. The capacity region is defined to be the closure of the set of all achievable rates.

The main goal of this paper is to give an outer bound on the capacity region as defined above. As such, it is helpful to describe the action of the channel in each round by an isometric extension $U^{\mathcal{N}}_{A_i \to B_i C_i E_i}$, where E_i is an environment system. Including the environment systems, we then write the state at the conclusion of i steps of the protocol as $\sigma^{(i)}_{A'_i B_i B'_i C_i C'_i E^i}$, where $E^i \equiv E_1 \cdots E_i$. It is also helpful to consider a system $R^{(i)}$ that purifies the state before the ith channel use, so that

$$\varphi^{\rho^{(i)}}_{A_i A'_i B'_i C'_i E^{i-1} R^{(i)}} \tag{4.4}$$

is a purification of $\rho^{(i)}_{A_i A'_i B'_i C'_i E^{i-1}}$. Let $\sigma^{(i)}_{A'_i B_i B'_i C_i C'_i E^i R^{(i)}}$ denote the state which results from applying an isometric extension $U^{\mathcal{N}}_{A_i \to B_i C_i E_i}$ of the channel $\mathcal{N}_{A_i \to B_i C_i}$ to the purification $\varphi^{\rho^{(i)}}_{A_i A'_i B'_i C'_i E^{i-1} R^{(i)}}$.

The generalization of the above protocol to multiple parties is straightforward, so we only discuss the main points. The channel is $\mathcal{N}_{A \to B_1 \cdots B_m}$ and let $\mathcal{S} = \{A, B_1, \ldots, B_m\}$. For a given subset $\mathcal{K} \in \mathcal{P}_{\geq 2}(\mathcal{S})$, let $K_{\mathcal{K}}$ denote the rate at which a $|\mathcal{K}|$ multiparty secret key can be distilled between the members of $\mathcal{K}$, and let $E_{\mathcal{K}}$ denote the rate at which a $|\mathcal{K}|$ multiparty GHZ entangled state can be distilled between the members of $\mathcal{K}$. The rate tuple is specified by $(E_{\mathcal{K}}, K_{\mathcal{K}})_{\mathcal{K} \in \mathcal{P}_{\geq 2}(\mathcal{S})}$. After each round of LOCC, the state is $\rho^{(i)}_{A_i \mathcal{S}'_i}$ and after each channel use, the state is $\sigma^{(i)}_{[\mathcal{S}_i \setminus A_i] \mathcal{S}'_i}$. The state generated after the last round of LOCC is $\Omega_{\mathcal{S}}$, which is ε-close to the ideal state $\Psi_{\mathcal{S}}$ given in (3.72). Achievable rates and the capacity region are defined in a similar way, and it is again helpful to consider environments resulting from an isometric extension $U^{\mathcal{N}}_{A \to B_1 \cdots B_m E}$ of the channel $\mathcal{N}_{A \to B_1 \cdots B_m}$.

5 Bounds on entanglement distillation and secret key agreement for a two-receiver quantum broadcast channel

In this section, we establish constraints on achievable rates for entanglement distillation and secret-key agreement for a quantum broadcast channel with two receivers. The bounds are given in terms of the squashed entanglement measures of Section 2.6.

Theorem 12 *Let $\mathcal{N}_{A \to BC}$ be a quantum broadcast channel from a sender Alice to receivers Bob and Charlie. If the rate tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ is achievable, then there exists a pure state ϕ_{RA} with*

$$\omega_{RBC} \equiv \mathcal{N}_{A \to BC}(\phi_{RA}), \tag{5.1}$$

such that the following bounds hold

$$E_{AB} + K_{AB} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}(RC; B)_\omega \tag{5.2}$$

$$E_{AC} + K_{AC} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}(RB; C)_\omega \tag{5.3}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}(R; BC)_\omega \tag{5.4}$$

$$\begin{aligned} E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} \\ + \frac{3}{2}(E_{ABC} + K_{ABC}) \leq \min\left\{ E_{\text{sq}}(R; B; C)_\omega, \widetilde{E}_{\text{sq}}(R; B; C)_\omega \right\}. \end{aligned} \tag{5.5}$$

The dimension of system R need not be any larger than the dimension of the channel input.

Proof. It is important to realize that since we allow all three parties to participate in each round of LOCC, the bounds we give on these rates should involve all three of them. Consider an arbitrary protocol as described in Section 4. We work our way backwards through the protocol, starting at the end and unraveling it until we reach the beginning. The ideal state at the end of the protocol is Ψ_{ABC}, as specified in (3.54), and the actual state is Ω_{ABC}, as described in Step 4 of Section 4. They are related by (4.1). Recall the partitions of $\{A, B, C\}$ discussed in (3.58)-(3.61).

We begin by considering the constraint in (5.2), which corresponds to the partition $\mathcal{G}_3$ in (3.60). Consider that

$$\begin{aligned} n\left(E_{AB}+K_{AB}+E_{BC}+K_{BC}+E_{ABC}+K_{ABC}\right) &\leq E_{\mathrm{sq}}\left(AC;B\right)_{\Psi} && (5.6)\\ &\leq E_{\mathrm{sq}}\left(AC;B\right)_{\Omega}+f_1\left(n,\varepsilon\right). && (5.7)\end{aligned}$$

The first inequality follows from (3.67) and the second follows from an application of the continuity of squashed entanglement to (4.1), with $f_i\left(n,\varepsilon\right)$ a function such that $\lim_{\varepsilon\searrow 0}\lim_{n\to\infty}\frac{1}{n}f_i\left(n,\varepsilon\right)=0$ (we will have more such functions later on). Continuing, we have that

$$\begin{aligned} &E_{\mathrm{sq}}\left(AC;B\right)_{\Omega}\\ &\leq E_{\mathrm{sq}}\left(A_n'C_n'C_n;B_n'B_n\right)_{\sigma^{(n)}} && (5.8)\\ &\leq E_{\mathrm{sq}}\left(A_n'C_n'C_nB_nE_n;B_n'\right)_{\sigma^{(n)}}+E_{\mathrm{sq}}\left(A_n'C_n'C_nB_n'E_1\cdots E_{n-1}R^{(n)};B_n\right)_{\sigma^{(n)}} && (5.9)\\ &= E_{\mathrm{sq}}\left(A_n'C_n'A_n;B_n'\right)_{\rho^{(n)}}+E_{\mathrm{sq}}\left(A_n'C_n'C_nB_n'E_1\cdots E_{n-1}R^{(n)};B_n\right)_{\sigma^{(n)}} && (5.10)\\ &\leq E_{\mathrm{sq}}\left(A_{n-1}'C_{n-1}'C_{n-1};B_{n-1}'B_{n-1}\right)_{\sigma^{(n-1)}}+E_{\mathrm{sq}}\left(A_n'C_n'C_nB_n'E_1\cdots E_{n-1}R^{(n)};B_n\right)_{\sigma^{(n)}} && (5.11)\\ &\leq \sum_{i=1}^{n}E_{\mathrm{sq}}\left(A_i'C_i'C_iB_i'E_1\cdots E_{i-1}R^{(i)};B_i\right)_{\sigma^{(i)}}. && (5.12)\end{aligned}$$

The first inequality follows from monotonicity of the squashed entanglement under LOCC. The second inequality follows from applying Lemma 6. The equality follows from the fact that systems A_n and $B_nC_nE_n$ are related by an isometry (i.e., an isometric extension of the channel). The third inequality is again monotonicity under LOCC. To conclude the final inequality, we repeat (5.9)-(5.11) iteratively. Putting the two inequality chains together, we find that

$$\begin{aligned} &E_{AB}+K_{AB}+E_{BC}+K_{BC}+E_{ABC}+K_{ABC}\\ &\qquad\leq \frac{1}{n}\sum_{i=1}^{n}E_{\mathrm{sq}}\left(A_i'C_i'C_iB_i'E_1\cdots E_{i-1}R^{(i)};B_i\right)_{\sigma^{(i)}}+\frac{1}{n}f_1\left(n,\varepsilon\right) && (5.13)\\ &\qquad= E_{\mathrm{sq}}\left(QSC;B\right)_{\tau}+\frac{1}{n}f_1\left(n,\varepsilon\right), && (5.14)\end{aligned}$$

where

$$\tau_{QSBC}\equiv\sum_{i=1}^{n}\frac{1}{n}|i\rangle\langle i|_Q\otimes\mathcal{N}_{A\to BC}\left(\varphi^{(i)}_{A_i'B_i'C_i'E_1\cdots E_{i-1}R^{(i)}A}\right), \tag{5.15}$$

and $\varphi^{(i)}_{A_i'B_i'C_i'E_1\cdots E_{i-1}R^{(i)}A}$ is the purification defined in (4.4), with it understood that systems B_iC_i are isomorphic to systems BC. In the above, Q is a time-sharing or auxiliary classical system, and S is a register with size

$$|S|\geq\max_i\left|A_i'C_i'B_i'E_1\cdots E_{i-1}R^{(i)}\right|, \tag{5.16}$$

such that it is large enough to contain the largest of the systems $A_i' C_i' B_i' E_1 \cdots E_{i-1} R^{(i)}$ (and simply padded with zeros for smaller systems). Observe that the state τ_{QSBC} is constructed from the given protocol. The equality in (5.14) follows from the application of Lemma 4. Thus, we arrive at a single-letter bound.

A similar line of reasoning leads to the following inequalities:

$$E_{AC} + K_{AC} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}\left(QSB; C\right)_{\tau} + \frac{1}{n} f_2\left(n, \varepsilon\right), \tag{5.17}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{ABC} + K_{ABC} \leq E_{\text{sq}}\left(QS; BC\right)_{\tau} + \frac{1}{n} f_3\left(n, \varepsilon\right), \tag{5.18}$$

where we observe that the constraints involve the same state τ_{QSBC} from (5.15).

We now consider the constraint in (5.5). The reasoning that follows holds for both multipartite squashed entanglements E_{sq} and $\widetilde{E}_{\text{sq}}$. The entanglement distillation and secret key agreement rates of any protocol can be upper bounded as follows:

$$\begin{aligned} n \left(E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left[E_{ABC} + K_{ABC}\right] \right) & \\ \leq E_{\text{sq}}(A;B;C)_{\Psi} \leq E_{\text{sq}}(A;B;C)_{\Omega} + f_4\left(n, \varepsilon\right), & \end{aligned} \tag{5.19}$$

where the first inequality is a consequence of (3.70) and the second from applying continuity of squashed entanglement to (4.1). Continuing, we find that

$$\begin{aligned} & E_{\text{sq}}(A;B;C)_{\Omega} \\ & \leq E_{\text{sq}}\left(A_n'; B_n' B_n; C_n' C_n\right)_{\sigma^{(n)}} && (5.20) \\ & \leq E_{\text{sq}}\left(A_n' C_n B_n E_n; B_n'; C_n'\right)_{\sigma^{(n)}} + E_{\text{sq}}\left(A_n' B_n' C_n' E_1 \cdots E_{n-1} R^{(n)}; B_n; C_n\right)_{\sigma^{(n)}} && (5.21) \\ & = E_{\text{sq}}\left(A_n' A_n; B_n'; C_n'\right)_{\rho^{(n)}} + E_{\text{sq}}\left(A_n' B_n' C_n' E_1 \cdots E_{n-1} R^{(n)}; B_n; C_n\right)_{\sigma^{(n)}} && (5.22) \\ & \leq E_{\text{sq}}\left(A_{n-1}'; B_{n-1}' B_{n-1}; C_{n-1}' C_{n-1}\right)_{\sigma^{(n-1)}} + E_{\text{sq}}\left(A_n' B_n' C_n' E_1 \cdots E_{n-1} R^{(n)}; B_n; C_n\right)_{\sigma^{(n)}} && (5.23) \\ & \leq \sum_{i=1}^{n} E_{\text{sq}}\left(A_i' B_i' C_i' E_1 \cdots E_{i-1} R^{(i)}; B_i; C_i\right)_{\sigma^{(i)}}. && (5.24) \end{aligned}$$

Putting the above two inequality chains together, we find that

$$\begin{aligned} E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left(E_{ABC} + K_{ABC}\right) & \\ \leq \frac{1}{n} \sum_{i=1}^{n} E_{\text{sq}}\left(A_i' B_i' C_i' E_1 \cdots E_{i-1} R^{(i)}; B_i; C_i\right)_{\sigma^{(i)}} + \frac{1}{n} f_4\left(n, \varepsilon\right) & \\ = E_{\text{sq}}\left(QS; B; C\right)_{\tau} + \frac{1}{n} f_4\left(n, \varepsilon\right), & \end{aligned} \tag{5.25}$$

where τ is defined in (5.15). By the same reasoning, we have that

$$\begin{aligned} E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left(E_{ABC} + K_{ABC}\right) & \\ \leq \widetilde{E}_{\text{sq}}\left(QS; B; C\right)_{\tau} + \frac{1}{n} f_5\left(n, \varepsilon\right), & \end{aligned} \tag{5.26}$$

Note that unlike in the bipartite case, in the multipartite case with three or more parties, we have the two possible squashed entanglement measures $\widetilde{E}_{\text{sq}}$ and E_{sq}. Since in general they are incomparable, either could give a tighter bound.

The assumption that the rate tuple $(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$ is achievable implies that we can take $\varepsilon \searrow 0$ as $n \to \infty$. So we have shown that the rate tuple satisfies (5.2)-(5.5) for some input state ρ_{RA} and $\omega_{RBC} \equiv \mathcal{N}_{A\to BC}(\rho_{RA})$. Let $\phi^{\rho}_{R'RA}$ be a purification of ρ_{RA} and let $\omega_{R'RBC} \equiv \mathcal{N}_{A\to BC}(\phi^{\rho}_{R'RA})$. By monotonicity of squashed entanglement under quantum operations, we have that

$$E_{\text{sq}}\left(RC;B\right)_{\omega} \leq E_{\text{sq}}\left(R'RC;B\right)_{\omega}, \tag{5.27}$$

$$E_{\text{sq}}\left(RB;C\right)_{\omega} \leq E_{\text{sq}}\left(R'RB;C\right)_{\omega}, \tag{5.28}$$

$$E_{\text{sq}}\left(R;BC\right)_{\omega} \leq E_{\text{sq}}\left(R'R;BC\right)_{\omega}, \tag{5.29}$$

$$E_{\text{sq}}\left(R;B;C\right)_{\omega} \leq E_{\text{sq}}\left(R'R;B;C\right)_{\omega}, \tag{5.30}$$

$$\widetilde{E}_{\text{sq}}\left(R;B;C\right)_{\omega} \leq \widetilde{E}_{\text{sq}}\left(R'R;B;C\right)_{\omega}. \tag{5.31}$$

By the Schmidt decomposition, note that we can take $|RR'| = |A|$. The dimension bound appearing in the statement of theorem comes about by redefining $R := RR'$. ■

6 Bounds on entanglement distillation and secret key agreement for an m-receiver quantum broadcast channel

Let $\mathcal{N}_{A\to B_1\cdots B_m}$ be a quantum broadcast channel with one sender A and m receivers B_1, ..., B_m. Let $\mathcal{S} = \{R, B_1, \ldots, B_m\}$, where R is a system that the sender possesses. For a given subset $\mathcal{K} \in \mathcal{P}_{\geq 2}(\mathcal{S})$, let $K_{\mathcal{K}}$ denote the rate at which a $|\mathcal{K}|$ multiparty secret key can be distilled between the members of $\mathcal{K}$, and let $E_{\mathcal{K}}$ denote the rate at which a $|\mathcal{K}|$ multiparty GHZ entangled state can be distilled between the members of $\mathcal{K}$. We now state our main theorem:

Theorem 13 *If the rates $(K_{\mathcal{K}}, E_{\mathcal{K}})_{\mathcal{K}\in\mathcal{P}_{\geq 2}(\mathcal{S})}$ are achievable, then there exists a pure state ϕ_{RA} with*

$$\omega_{RB_1\cdots B_m} \equiv \mathcal{N}_{A\to B_1\cdots B_m}(\phi_{RA}), \tag{6.1}$$

such that the following bounds hold. For all partitions $\mathcal{G}$ of $\mathcal{S}$,

$$\frac{1}{2}\sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})} \left|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)\right| \left(K_{\mathcal{M}} + E_{\mathcal{M}}\right) \leq \min\left\{E_{\text{sq}}(\mathcal{G})_{\omega},\ \widetilde{E}_{\text{sq}}(\mathcal{G})_{\omega}\right\}, \tag{6.2}$$

and

$$\mathcal{A}\left(\mathcal{M},\mathcal{G}\right) \equiv \{X \cap \mathcal{M} \mid X \in \mathcal{G}\} \setminus \{\emptyset\}. \tag{6.3}$$

The dimension of system R need not be any larger than the dimension of the channel input.

Proof. We sketch a proof of this theorem, which proceeds along the lines of reasoning employed in proving Theorem 12. The proof involves the following steps, again working backwards through the protocol:

1. Let $\mathcal{G}$ be a partition of $\mathcal{S}$. The ideal state at the end of the protocol is $\Psi_{\mathcal{S}}$, as given in (3.72). Lemma 11 establishes the following bound:

$$\frac{1}{2}\sum_{\mathcal{M}\in\mathcal{C}(\mathcal{G})}\left|\mathcal{A}\left(\mathcal{M},\mathcal{G}\right)\right|\left(K_{\mathcal{M}}+E_{\mathcal{M}}\right)\leq\min\left\{E_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}},\ \widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}}\right\}. \tag{6.4}$$

2. The actual state generated by the protocol is $\Omega_{\mathcal{S}}$, as specified in Section 4. Use the fact that $\Omega_{\mathcal{S}}$ is ε-close to $\Psi_{\mathcal{S}}$ and the continuity of squashed entanglement to establish that

$$E_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}}\leq E_{\mathrm{sq}}(\mathcal{G})_{\Omega_{\mathcal{S}}}+f_{\mathcal{G}}^{1}\left(n,\varepsilon\right), \tag{6.5}$$

$$\widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Psi_{\mathcal{S}}}\leq\widetilde{E}_{\mathrm{sq}}(\mathcal{G})_{\Omega_{\mathcal{S}}}+f_{\mathcal{G}}^{2}\left(n,\varepsilon\right), \tag{6.6}$$

   for $f_{\mathcal{G}}^{i}\left(n,\varepsilon\right)$ some function with the property that $\lim_{\varepsilon\searrow 0}\lim_{n\to\infty}\frac{1}{n}f_{\mathcal{G}}^{i}\left(n,\varepsilon\right)=0$.

3. Use the fact that the squashed entanglement is non-increasing under LOCC.

4. Invoke the subadditivity lemma (Lemma 6).

5. Invert the action of the channel on the ith input to replace $B_iC_iE_i\to A_i$ since the systems $B_iC_iE_i$ and A_i are related by an isometric extension of the channel.

6. Iterate Steps 3-5 for every step of the protocol.

7. As in (5.25), use Lemma 4 to rewrite the linear sum of squashed entanglements as the squashed entanglement of a single state to obain a single letter bound. We can use the same reasoning as at the end of the proof of Theorem 12 to restrict the input state to be pure.

That concludes the proof sketch. ■

7 Application to a pure-loss bosonic broadcast channel

We now apply our results to a pure-loss bosonic broadcast channel, generalizing prior results for the single-sender single-receiver case [43, 42]. For simplicity, we consider a one-sender two-receiver channel from a sender Alice to receivers Bob and Charlie. However, note that the methods given here can be combined with Theorem 13 to determine bounds for an arbitrary number of receivers. A pure-loss bosonic channel of the above type can be modeled as

$$\hat{b}=\sqrt{\eta_B}\,\hat{a}'+\sqrt{\frac{\eta_B(1-\eta_B-\eta_C)}{\eta_B+\eta_C}}\,\hat{f}+\sqrt{\frac{\eta_C}{\eta_B+\eta_C}}\,\hat{g}, \tag{7.1}$$

$$\hat{c}=-\sqrt{\eta_C}\,\hat{a}'-\sqrt{\frac{\eta_C(1-\eta_B-\eta_C)}{\eta_B+\eta_C}}\,\hat{f}+\sqrt{\frac{\eta_C}{\eta_B+\eta_C}}\,\hat{g}, \tag{7.2}$$

$$\hat{e}=-\sqrt{1-\eta_B-\eta_C}\,\hat{a}'+\sqrt{\eta_B+\eta_C}\,\hat{f}, \tag{7.3}$$

where $\hat{a}'$, $\hat{b}$, $\hat{c}$, $\hat{e}$ are annihilation operators for Alice's input, Bob's output, and Charlie's output modes, respectively, $\hat{f}$ and $\hat{g}$ are annihilation operators for vacuum inputs from the environment, and the $\eta_B,\ \eta_C>0$ are transmission coefficients such that $\eta_B+\eta_C\leq 1$. The model generalizes

the bosonic broadcast channel from prior work [23, 24], in that all of the light does not necessarily make it to the two receivers and that which does not is given to the eavesdropper.

In any protocol for entanglement distillation and secret key agreement, we assume that the final step of the protocol outputs a finite-dimensional state, i.e., the goal is to generate maximally entangled states of finite Schmidt rank and finite-dimensional private states. This is a common approach in continuous-variable quantum information theory [25, 19, 50, 51], simply because both quantum capacity and private capacity are measured in qubits and private bits per channel use, respectively. This approach furthermore provides a mathematical convenience: the only aspect of our analysis here which requires finite-dimensional states is when we apply continuity of squashed entanglement at the end of the protocol. All other steps rely on properties of entropy or the quantum data processing inequality, which is known to hold in very general settings [46]. Furthermore, we begin by assuming that each channel input has a mean photon number constraint $\langle \hat{a}^\dagger \hat{a} \rangle \leq N_S$ for some N_S such that $0 \leq N_S < \infty$, but we eventually take a limit as $N_S \to \infty$, indicating that our bounds are photon-number independent as is the case in [43, 42].

We then need to determine the (multipartite) squashed entanglement. In this regard, it is not necessarily an easy task to optimize over all possible squashing channels of Eve. However, since any squashing channel can be used to give an upper bound for the rates, we choose to optimize over squashing channels that are also pure-loss bosonic channels, modeled by a beamsplitter given by the following mode transformation:

$$\hat{e} \to \sqrt{\eta_{E'}}\hat{e}' + \sqrt{1-\eta_{E'}}\hat{f}', \quad \eta_{E'} \in [0,1]. \tag{7.4}$$

We begin by stating and proving the following proposition, which is more general than what we need, but the proof indicates a general approach that we employ to establish the main theorem of this section.

Proposition 14 *Let $\mathcal{N}_{A\to B_1 B_2 \ldots B_m}$ be a pure-loss bosonic broadcast channel from a sender A to m receivers $B_1, \ldots, B_m$ with transmission coefficients $\eta_i \geq 0$ for all $i \in \{1, \ldots, m\}$, such that*

$$\eta \equiv \sum_{i=1}^{m} \eta_i \leq 1. \tag{7.5}$$

Then the following upper bound holds for the squashed entanglements of the bosonic broadcast channel

$$\begin{aligned} &\max\left\{ \sup_{\phi_{RA}} E_{\mathrm{sq}}\left(R; B_1; \cdots; B_m\right)_\omega, \ \sup_{\phi_{RA}} \widetilde{E}_{\mathrm{sq}}\left(R; B_1; \cdots; B_m\right)_\omega \right\} \\ &\qquad \leq \frac{1}{2}\left[\sum_{i=1}^{m} \log\left(\frac{\eta_i}{(1-\eta)\,\eta^*_{E'}} + 1 \right) + \log\left(\frac{\eta}{(1-\eta)\left(1-\eta^*_{E'}\right)} + 1 \right) \right], \end{aligned} \tag{7.6}$$

where

$$\omega_{RB_1\cdots B_m} \equiv \mathcal{N}_{A\to B_1\cdots B_m}\left(\phi_{RA}\right), \tag{7.7}$$

and $\eta^*_{E'}$ is the solution of

$$\sum_{i=1}^{m} \frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_i + \eta_{E'}} = \frac{1}{\left(1-\eta_{E'}\right)^2\left(1-\eta\right)/\eta + 1 - \eta_{E'}}. \tag{7.8}$$

Proof. Our proof of this proposition generalizes the proof of [43, Eq. (27)]. Let $\varphi_{RB_1\cdots B_m E}$ be the pure state that results from applying the channel to a pure state input ϕ_{RA} satisfying $\left\langle \hat{a}^\dagger \hat{a} \right\rangle_{\phi_A} \leq N_S$. Let $\varphi_{RB_1\cdots B_m E'F'}$ be the state resulting from applying the squashing transformation in (7.4) to the system E of $\varphi_{RB_1\cdots B_m E}$. Then

$$2E_{\text{sq}}\left(R;B_1;\cdots;B_m\right)_\omega \leq H\left(R|E'\right)_\varphi + \sum_{i=1}^m H\left(B_i|E'\right)_\varphi - H\left(RB_1\cdots B_m|E'\right)_\varphi \tag{7.9}$$

$$= \sum_{i=1}^m H\left(B_i|E'\right)_\varphi - H\left(B_1\cdots B_m|RE'\right)_\varphi \tag{7.10}$$

$$= \sum_{i=1}^m H\left(B_i|E'\right)_\varphi + H\left(B_1\cdots B_m|F'\right)_\varphi \tag{7.11}$$

As written, the conditional entropies in the last line are now functions of the input density operator ϕ_A. Applying the extremality of Gaussian states for the conditional entropy [17, 52], we can conclude that these quantities are all optimized by a thermal state of mean photon number N_S. For such a state, one can work out using the symplectic formalism for bosonic states [48] that

$$H\left(B_i E'\right) = g\left(\left[\eta_i + \left(1-\eta\right)\eta_{E'}\right] N_S\right), \tag{7.12}$$

$$H\left(E'\right) = g\left(\left(1-\eta\right)\eta_{E'} N_S\right), \tag{7.13}$$

$$H\left(B_1\cdots B_m F'\right) = g\left(\left[\eta + \left(1-\eta\right)\left(1-\eta_{E'}\right)\right] N_S\right), \tag{7.14}$$

$$H\left(F'\right) = g\left(\left(1-\eta\right)\left(1-\eta_{E'}\right) N_S\right), \tag{7.15}$$

where

$$g(x) \equiv \left(x+1\right)\log_2\left(x+1\right) - x\log_2 x \tag{7.16}$$

is the entropy of a thermal state of mean photon number x. Each entropy above can be understood in a simple way: for a simple pure loss bosonic broadcast channel $\mathcal{N}_{A\to B_1 B_2\ldots B_m}$, each state held by any group of parties at the receiving end is unitarily equivalent to a thermal state with mean photon number proportional to the fraction of light that makes it to them. So this leads to the photon-number dependent upper bound

$$2E_{\text{sq}}\left(R;B_1;\cdots;B_m\right)_\omega \leq \sum_{i=1}^m \left(g\left(\left[\eta_i + \left(1-\eta\right)\eta_{E'}\right] N_S\right) - g\left(\left(1-\eta\right)\eta_{E'} N_S\right)\right)$$
$$+ g\left(\left[\eta + \left(1-\eta\right)\left(1-\eta_{E'}\right)\right] N_S\right) - g\left(\left(1-\eta\right)\left(1-\eta_{E'}\right) N_S\right). \tag{7.17}$$

One can easily compute the derivative of $g(x) - g\left(\lambda x\right)$ to show that this function is monotonically increasing in x for $x \geq 0$ and $\lambda \in [0,1]$, and furthermore, one can easily show that

$$\lim_{x\to\infty} g(x) - g\left(\lambda x\right) = \log\left(1/\lambda\right). \tag{7.18}$$

So we can conclude that the right hand side (RHS) above is a monotonically increasing function of $N_S \geq 0$ and taking the limit $N_S \to \infty$ only increases the upper bound. This leads to the following photon-number independent upper bound:

$$2E_{\text{sq}}\left(R;B_1;\cdots;B_m\right)_\omega \leq \sum_{i=1}^m \log\left(\frac{\eta_i}{\left(1-\eta\right)\eta_{E'}} + 1\right) + \log\left(\frac{\eta}{\left(1-\eta\right)\left(1-\eta_{E'}\right)} + 1\right). \tag{7.19}$$

which holds for arbitrary $\eta_{E'} \in [0,1]$. To get the tightest upper bound, we should minimize the RHS of (7.19) with respect to $\eta_{E'}$. Any local minimum of this function is a global minimum because the function $\log(1+a/x)$ is convex in x for $a \geq 0$ and $x \geq 0$ (as can be checked by computing the second derivative) and the RHS of (7.19) is convex in $\eta_{E'}$ as it is a sum of convex functions. Since we need to solve for $\eta_{E'}$ in

$$\frac{\partial}{\partial \eta_{E'}} \left[\sum_{i=1}^{m} \log\left(\frac{\eta_i}{(1-\eta)\,\eta_{E'}} + 1 \right) + \log\left(\frac{\eta}{(1-\eta)\,(1-\eta_{E'})} + 1 \right) \right] = 0, \tag{7.20}$$

we can use that the first derivative of $\log(1+a/x)$ is equal to $-1/\left(x^2/a + x\right)$, which leads to solving the following equation for $\eta_{E'}$:

$$\sum_{i=1}^{m} \frac{1}{\eta_{E'}^2\,(1-\eta)/\eta_i + \eta_{E'}} = \frac{1}{(1-\eta_{E'})^2\,(1-\eta)/\eta + 1 - \eta_{E'}}. \tag{7.21}$$

This establishes one of the inequalities in (7.6).

By a similar line of reasoning as above, consider that

$$\begin{aligned} &2\widetilde{E}_{\mathrm{sq}}\left(R; B_1; \cdots; B_m\right)_{\omega} \\ &\leq H\left(RB_1 \cdots B_m | E'\right)_{\varphi} - H\left(R | B_1 \cdots B_m E'\right)_{\varphi} - \sum_{i=1}^{m} H\left(B_i | RB_{[m]\setminus\{i\}} E'\right)_{\varphi} \qquad (7.22) \\ &= H\left(B_1 \cdots B_m | E'\right)_{\varphi} + \sum_{i=1}^{m} H\left(B_i | F'\right)_{\varphi} \qquad (7.23) \end{aligned}$$

Here again we have written the entropies as a function of the input density operator, which we know from the extremality of Gaussian states is optimized by a thermal state for a fixed photon number. For such an input, we have that

$$\begin{aligned} H\left(B_1 \cdots B_m E'\right) &= g\left(\left[\eta + (1-\eta)\,\eta_{E'}\right] N_S\right), &(7.24)\\ H\left(E'\right) &= g\left((1-\eta)\,\eta_{E'} N_S\right), &(7.25)\\ H\left(B_i F\prime\right) &= g\left(\left[\eta_i + (1-\eta)\,(1-\eta_{E'})\right] N_S\right), &(7.26)\\ H\left(F\prime\right) &= g\left((1-\eta)\,(1-\eta_{E'})\,N_S\right), &(7.27) \end{aligned}$$

so that (7.23) is bounded from above by

$$\begin{aligned} &g\left(\left[\eta + (1-\eta)\,\eta_{E'}\right] N_S\right) - g\left((1-\eta)\,\eta_{E'} N_S\right) \\ &\qquad + \sum_{i=1}^{m} \left(g\left(\left[\eta_i + (1-\eta)\,(1-\eta_{E'})\right] N_S\right) - g\left((1-\eta)\,(1-\eta_{E'})\,N_S\right) \right) \\ &\qquad\qquad \leq \sum_{i=1}^{m} \log\left(\frac{\eta_i}{(1-\eta)\,(1-\eta_{E'})} + 1 \right) + \log\left(\frac{\eta}{(1-\eta)\,\eta_{E'}} + 1 \right). \end{aligned} \tag{7.28}$$

This bound applies for every $\eta_{E'} \in [0,1]$, so we can take a minimum over all such $\eta_{E'}$. However, we can now observe that this minimum is exactly the same as the one above because the RHS of (7.28) is related to the RHS of (7.19) by $\eta_{E'} \leftrightarrow 1 - \eta_{E'}$. ∎

We now state the main theorem of this section, which bounds the entanglement distillation and secret key agreement rates achievable with a pure-loss bosonic broadcast channel that has one sender and two receivers.

Theorem 15 *Let a pure-loss bosonic broadcast channel from a sender Alice to receivers Bob and Charlie be described by the mode transformations in* (7.1)-(7.3)*. Then the achievable entanglement distillation and secret key agreement rates (see Section 4) are bounded as follows:*

$$E_{AB} + K_{AB} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_B-\eta_C}{1-\eta_B-\eta_C}\right), \tag{7.29}$$

$$E_{AC} + K_{AC} + E_{BC} + K_{BC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_C-\eta_B}{1-\eta_B-\eta_C}\right), \tag{7.30}$$

$$E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{ABC} + K_{ABC} \leq \log\left(\frac{1+\eta_B+\eta_C}{1-\eta_B-\eta_C}\right), \tag{7.31}$$

and

$$\begin{aligned} &E_{AB} + K_{AB} + E_{AC} + K_{AC} + E_{BC} + K_{BC} + \frac{3}{2}\left(E_{ABC} + K_{ABC}\right) \\ &\leq \frac{1}{2}\left[\log\left(\frac{\eta_B}{(1-\eta)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta_C}{(1-\eta)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta}{(1-\eta)\,\eta^*_{E'}}+1\right)\right], \end{aligned} \tag{7.32}$$

where $\eta^*_{E'}$ is the solution of

$$\frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_B + \eta_{E'}} + \frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_C + \eta_{E'}} = \frac{1}{\left(1-\eta_{E'}\right)^2\left(1-\eta\right)/\eta + 1 - \eta_{E'}}. \tag{7.33}$$

Proof. Here we only highlight the main steps without giving reasons, as much of it is the same as in the proof of Proposition 14. Our approach is simply to bound the quantities $E_{\mathrm{sq}}\left(RC;B\right)_\omega$, $E_{\mathrm{sq}}\left(RB;C\right)_\omega$, $E_{\mathrm{sq}}\left(R;BC\right)_\omega$, $E_{\mathrm{sq}}\left(R;B;C\right)_\omega$ from Theorem 12. Consider that

$$\begin{aligned} 2E_{\mathrm{sq}}\left(RC;B\right)_\omega &\leq I\left(RC;B|E'\right) && (7.34)\\ &= H\left(B|E'\right) - H\left(B|RCE'\right) && (7.35)\\ &= H\left(B|E'\right) + H\left(B|F'\right) && (7.36)\\ &\leq \log\left(\frac{\eta_B}{(1-\eta)\,\eta_{E'}}+1\right) + \log\left(\frac{\eta_B}{(1-\eta)\left(1-\eta_{E'}\right)}+1\right) && (7.37) \end{aligned}$$

Picking $\eta_{E'} = 1/2$ then gives the bound:

$$E_{\mathrm{sq}}\left(RC;B\right)_\omega \leq \log\left(\frac{2\eta_B}{1-\eta}+1\right) = \log\left(\frac{2\eta_B+1-\eta}{1-\eta}\right) = \log\left(\frac{1+\eta_B-\eta_C}{1-\eta_B-\eta_C}\right) \tag{7.38}$$

This is optimal because the function in (7.37) is convex in $\eta_{E'}$ and symmetric about $\eta_{E'} = 1/2$.

Similarly, we have

$$E_{\mathrm{sq}}\left(RB;C\right)_\omega \leq \log\left(\frac{1+\eta_C-\eta_B}{1-\eta_B-\eta_C}\right), \qquad E_{\mathrm{sq}}\left(R;BC\right)_\omega \leq \log\left(\frac{1+\eta_B+\eta_C}{1-\eta_B-\eta_C}\right). \tag{7.39}$$

Furthermore, we can apply Proposition 14 to find that

$$2E_{\mathrm{sq}}\left(R;B;C\right)_{\omega} \leq \log\left(\frac{\eta_B}{\left(1-\eta\right)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta_C}{\left(1-\eta\right)\left(1-\eta^*_{E'}\right)}+1\right) + \log\left(\frac{\eta}{\left(1-\eta\right)\eta^*_{E'}}+1\right), \quad (7.40)$$

where $\eta^*_{E'}$ is the solution of

$$\frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_B+\eta_{E'}} + \frac{1}{\eta^2_{E'}\left(1-\eta\right)/\eta_C+\eta_{E'}} = \frac{1}{\left(1-\eta_{E'}\right)^2\left(1-\eta\right)/\eta+1-\eta_{E'}}. \quad (7.41)$$

This completes the proof. ■

8 Conclusion

We have shown how multipartite generalizations of the squashed entanglement [53, 3] lead to several constraints on the rates at which secret key and entanglement can be generated between any subset of the users of a quantum broadcast channel. Along the way, we developed several new properties of these measures, which include the subadditivity lemma (Lemma 6), monotonicity under groupings, reductions for product states, and the evaluation of the measures for a tensor product of entangled and private states shared between all subsets of a given set of parties. Finally, we applied our results to a single-sender two-receiver bosonic broadcast channel.

Some future directions include to determine upper bounds on the secret key agreement and entanglement distillation capacity of a multiple access or more general quantum network channel. One could also attempt the challenging task of proving that the bounds given here are strong converse rates. However, it is not yet known whether the single-sender single-receiver squashed entanglement is a strong converse rate.

Acknowledgements. We are grateful to Saikat Guha for discussions related to the topic of this paper. KS acknowledges support from NSF Grant No. CCF-1350397, the DARPA Quiness Program through US Army Research Office award W31P4Q-12-1-0019, and the Graduate School of Louisiana State University for the 2014-2015 Dissertation Year Fellowship. MMW acknowledges support from startup funds from the Department of Physics and Astronomy at LSU, the NSF under Award No. CCF-1350397, and the DARPA Quiness Program through US Army Research Office award W31P4Q-12-1-0019. MT acknowledges support from Open Partnership Joint Projects of JSPS Bilateral Joint Research Projects and ImPACT Program of Council for Science, Technology and Innovation, Japan. He is also grateful to members of the Hearne Institute for Theoretical Physics at LSU for their hospitality during his research visit in February 2015.

References

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

[2] 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.

[3] 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.

[4] Charles H. Bennett and Gilles 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, December 1984.

[5] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[6] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[7] 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.

[8] 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.

[9] Eric Chitambar, Debbie Leung, Laura Mancinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, May 2014. arXiv:1210.4583.

[10] Matthias Christandl. The quantum analog to intrinsic information. Diploma Thesis, ETH Zurich, unpublished, 2002.

[11] 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.

[12] 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.

[13] 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.

[14] Imre Csiszar and Prakash Narayan. Secrecy capacities for multiterminal channel models. *IEEE Transactions on Information Theory*, 54(6):2437–2452, June 2008.

[15] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Physical Review Letters*, 100(23):230501, June 2008.

[16] Frederic Dupuis, Patrick Hayden, and Ke Li. A father protocol for quantum broadcast channels. *IEEE Transactions on Information Theory*, 56(6):2946–2956, June 2010. arXiv:quant-ph/0612155.

[17] Jens Eisert and Michael M. Wolf. *Quantum Information with Continous Variables of Atoms and Light*, chapter Gaussian quantum channels, pages 23–42. Imperial College Press, 2007. arXiv:quant-ph/0505151.

[18] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[19] Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Jeffrey H. Shapiro, and Horace P. Yuen. Classical capacity of the lossy bosonic channel: The exact solution. *Physical Review Letters*, 92(2):027902, January 2004. arXiv:quant-ph/0308012.

[20] Amin A. Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals - Part I: Source model. *IEEE Transactions on Information Theory*, 56(8):3973–3996, August 2010.

[21] Amin A. Gohari and Venkat Anantharam. Information-theoretic key agreement of multiple terminals - Part II: Channel model. *IEEE Transactions on Information Theory*, 56(8):3997–4010, August 2010.

[22] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88(5):057902, January 2002. arXiv:quant-ph/0109084.

[23] Saikat Guha and Jeffrey H. Shapiro. Classical information capacity of the bosonic broadcast channel. In *Proceedings of the IEEE International Symposium on Information Theory*, pages 1896–1900, Nice, France, June 2007. arXiv:0704.1901.

[24] Saikat Guha, Jeffrey H. Shapiro, and Baris I. Erkmen. Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture. *Physical Review A*, 76(3):032303, September 2007. arXiv:0706.3416.

[25] Alexander S. Holevo and Reinhard F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63(3):032312, February 2001. arXiv:quant-ph/9912067.

[26] 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.

[27] 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.

[28] 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.

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

[30] Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps. 2014. arXiv:1410.4184.

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

[32] 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.

[33] Alexander I. Lvovsky, Barry C. Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature Photonics*, 3(12):706–714, December 2009. arXiv:1002.4659.

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

[35] Ueli M. Maurer and Stephan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, March 1999.

[36] 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.

[37] Jaikumar Radhakrishnan, Pranab Sen, and Naqueeb Warsi. One-shot Marton inner bound for classical-quantum broadcast channel. October 2014. arXiv:1410.3248.

[38] Robert R.Tucci. Entanglement of Distillation and Conditional Mutual Information, 2002. arXiv:quant-ph/0202144v2.

[39] Ivan Savov and Mark M. Wilde. Classical codes for quantum broadcast channels. *IEEE Transactions on Information Theory*, 61(12):1–12, December 2015. arXiv:1111.3645.

[40] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, September 2009. arXiv:0802.4155.

[41] Artur Scherer, Barry C. Sanders, and Wolfgang Tittel. Long-distance practical quantum key distribution by entanglement swapping. *Optics Express*, 19(4):3004, February 2011. arXiv:1012.5675.

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

[43] 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.

[44] Paul D. Townsend. Quantum cryptography on multiuser optical fibre networks. *Nature*, 385:47–49, January 1997.

[45] Robert R. Tucci. Quantum Entanglement and Conditional Information Transmission, 1999. arXiv:quant-ph/9909041v2.

[46] Armin Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Communications in Mathematical Physics*, 54:21–32, 1977.

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

[48] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621–669, May 2012. arXiv:1110.3234.

[49] Mark M. Wilde. Multipartite quantum correlations and local recoverability. *Accepted for publication in the Proceedings of the Royal Society A*, December 2014. arXiv:1412.0333.

[50] Mark M. Wilde, Patrick Hayden, and Saikat Guha. Information trade-offs for optical quantum communication. *Physical Review Letters*, 108(14):140501, April 2012. arXiv:1105.0119.

[51] Mark M. Wilde, Patrick Hayden, and Saikat Guha. Quantum trade-off coding for bosonic communication. *Physical Review A*, 86(6):062306, December 2012. arXiv:1105.0119.

[52] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of Gaussian quantum states. *Physical Review Letters*, 96(8):080502, March 2006. arXiv:quant-ph/0509154.

[53] 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.

[54] 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.

[55] Jon Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55(11):5339–5351, November 2009. arXiv:0706.2907.

[56] Jon Yard, Patrick Hayden, and Igor Devetak. Quantum broadcast channels. *IEEE Transactions on Information Theory*, 57(10):7147–7162, October 2011. arXiv:quant-ph/0603098.