



# CHORUS

This is the accepted manuscript made available via CHORUS. The article has been published as:

## Energy-constrained two-way assisted private and quantum capacities of quantum channels

Noah Davis, Maksim E. Shirokov, and Mark M. Wilde

Phys. Rev. A **97**, 062310 — Published 7 June 2018

DOI: [10.1103/PhysRevA.97.062310](https://doi.org/10.1103/PhysRevA.97.062310)

# Energy-constrained two-way assisted private and quantum capacities of quantum channels

Noah Davis

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

Maksim E. Shirokov

*Steklov Mathematical Institute, Russian Academy of Sciences, Moscow, Russia*

Mark M. Wilde

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

(Dated: April 30, 2018)

With the rapid growth of quantum technologies, knowing the fundamental characteristics of quantum systems and protocols is essential for their effective implementation. A particular communication setting that has received increased focus is related to quantum key distribution and distributed quantum computation. In this setting, a quantum channel connects a sender to a receiver, and their goal is to distill either a secret key or entanglement, along with the help of arbitrary local operations and classical communication (LOCC). In this work, we establish a general theory of energy-constrained, LOCC-assisted private and quantum capacities of quantum channels, which are the maximum rates at which an LOCC-assisted quantum channel can reliably establish secret key or entanglement, respectively, subject to an energy constraint on the channel input states. We prove that the energy-constrained squashed entanglement of a channel is an upper bound on these capacities. We also explicitly prove that a thermal state maximizes a relaxation of the squashed entanglement of all phase-insensitive, single-mode input bosonic Gaussian channels, generalizing results from prior work. After doing so, we prove that a variation of the method introduced in [Goodenough *et al.*, New J. Phys. 18, 063005 (2016)] leads to improved upper bounds on the energy-constrained secret-key-agreement capacity of a bosonic thermal channel. We then consider a multipartite setting and prove that two known multipartite generalizations of the squashed entanglement are in fact equal. We finally show that the energy-constrained, multipartite squashed entanglement plays a role in bounding the energy-constrained LOCC-assisted private and quantum capacity regions of quantum broadcast channels.

## I. INTRODUCTION

Modern communications from simple web browsing to high-security, governmental discussions rely on encryption protocols that use a private key to secure and interpret messages. The strength of the encryption is directly tied to the security of the key, and the security of most systems currently in use rests on computational assumptions. In contrast, quantum communication allows for generating an information-theoretically secure key, shared among trusted parties, via a method known as quantum key distribution (QKD) [1–3].

The rate (bits of key per channel use) at which QKD can be accomplished using a variety of protocols is known to fall off exponentially with distance [1–4]. This observed rate-loss trade-off previously suggested the question of whether some other protocols could be designed to outperform the exponential fall-off. However, the exponential rate-loss trade-off has been established to be a fundamental limit for bosonic loss channels [5], and a number of works [6–15] have now considered this problem and generalizations of it after [5] appeared. The tightest known non-asymptotic bounds for the pure-loss bosonic channels have been given in [5, 11, 16].

An important notion in addressing this question is the capacity of a quantum channel, which is a fundamental characteristic of the channel and is independent of any specific communication protocol. In the setting of quantum key distribution, it is natural to allow for an authenticated, public classical channel to assist the quantum channel connecting two parties, and so the quantum channel is said to be assisted by local operations and classical communication (LOCC). The secret-key-agreement capacity is the maximum rate at which classical bits can be privately and faithfully transmitted through many uses of a channel, while allowing for free classical communication [5, 17]. Similarly, the LOCC-assisted quantum capacity is the maximum rate at which qubits can be transmitted faithfully through many uses of a channel and with free classical communication [18–20]. Ultimately, the capacity of a quantum channel limits the usefulness of the channel, and so these LOCC-assisted private and quantum capacities of a quantum channel are important factors in determining any practical use of the channel.

Given that current communications (particularly quantum communication experiments) utilize photons, it is important to consider capacities of bosonic, Gaussian channels [21]. Expressions for the unassisted quantum

capacities of channels such as the single-mode quantum-limited amplifier and attenuator have been presented in [21, 22], but the expressions therein suppose that the transmitters in question have no constraint on their energy consumption. While these bounds have been shown to depend only on fundamental characteristics of the channel, any real transmitter will not have unbounded energy available, and so these expressions may have limited applicability to practical scenarios, as argued in [23]. More recently, strides have been made to bound capacities in energy-constrained scenarios [5, 7, 23].

In the effort to bound these capacities, several information measures of quantum channels have been proposed, each of which is based on correlation measures for bipartite quantum states. Among these, an entanglement measure [24] known as the squashed entanglement [25] has played a critical role, as shown in [5–7, 17]. This is due in part to the fact that it possesses several desirable properties, such as additivity, monotonicity under LOCC, uniform (asymptotic) continuity, and faithfulness [25–27]. Most recently, squashed entanglement has been shown to retain several of these attributes for infinite-dimensional states, which allows for its use in rather general scenarios [28].

In this paper, we formally define the task of energy-constrained, LOCC-assisted private and quantum communication, and we show that the energy-constrained squashed entanglement of a channel is an upper bound on its corresponding capacities. We prove this bound in a rather general, infinite-dimensional setting, allowing for applications to physical situations other than those specifically considered in this paper. In this sense, this paper is complementary to the developments from [23] and generalizes those from [5–7, 17]. We then prove that a thermal state is the optimal input to a relaxation of the energy-constrained squashed entanglement of phase-insensitive, single-mode input, bosonic Gaussian channels, which extends various statements from prior work. After doing so, we prove that a variation of the method introduced in [7] leads to improved upper bounds on the energy-constrained secret-key-agreement capacity of a bosonic thermal channel. In particular, these improved upper bounds have the property that they converge to zero in the limit as the thermal channel becomes entanglement breaking. We finally prove that the two most common multipartite generalizations of the squashed entanglement from [29, 30] are in fact equal to one another, and we show how the general framework developed in this paper applies to energy-constrained capacity regions of quantum broadcast channels.

We begin in Section II by giving an introduction to notation, tools, and terminology, as well as defining the important quantities used in the following sections. In Section III we prove two useful lemmas about the conditional quantum mutual information (CQMI) of infinite-dimensional states. Section IV formally defines the task of energy-constrained secret key agreement. We go on to show that the squashed entanglement of a channel is

an upper bound on its energy-constrained LOCC-assisted private and quantum capacities in Section V. Section VI shows that the bosonic thermal state is the optimal input to particular bosonic Gaussian channels in order to maximize relaxations of their squashed entanglement. A subsection of Section VI presents the improved upper bounds on the energy-constrained secret-key-agreement capacity of a bosonic thermal channel. Sections VII A and VII C begin the multipartite segment of this paper by proving the duality of two different multipartite generalizations of conditional quantum mutual information, which implies the equivalence of two multipartite squashed entanglements that have appeared in the literature [6, 29, 30] and were previously thought to be different. In Section VII D more tools for working in a multipartite setting are defined. Broadcast channels are introduced, and the private communication protocol from Section IV is recast with multiple receivers in Section VIII. The energy-constrained multipartite squashed entanglement is shown in Section VIII A to upper bound the energy-constrained LOCC-assisted capacities of broadcast channels with squashed entanglements depending on the partitions of systems. Finally, a calculation of the rate bounds is presented in Section VIII B before closing thoughts are given in Section IX.

## II. BACKGROUND: QUANTUM INFORMATION PRELIMINARIES

### A. Quantum Systems, States, and Channels

In order to study the quantum aspects of information and communication, we first review foundational aspects, consisting of terms and measures which serve to describe and quantify key features of the systems in question, as well as the operations performed on those systems. The reader can find background other than that presented here by consulting [31–34].

We denote some first Hilbert space as  $\mathcal{H}_A$  and another one as  $\mathcal{H}_B$ . Throughout, the Hilbert spaces we consider are generally infinite-dimensional and separable, unless stated otherwise. The tensor product of  $\mathcal{H}_A$  and  $\mathcal{H}_B$  is itself a Hilbert space, represented as  $\mathcal{H}_A \otimes \mathcal{H}_B = \mathcal{H}_{AB}$ . Let  $\mathcal{L}(\mathcal{H}_A)$  denote the set of bounded linear operators acting on  $\mathcal{H}_A$ , and let  $\mathcal{L}_+(\mathcal{H}_A)$  denote the subset of positive, semi-definite operators acting on  $\mathcal{H}_A$ . Let  $\mathcal{L}_1(\mathcal{H})$  denote the set of trace-class operators, those operators  $X$  for which the trace norm is finite:  $\|X\|_1 \equiv \text{Tr}\{|X|\} < \infty$ , where  $|X| \equiv \sqrt{X^\dagger X}$ . The set of states (also called density operators)  $\mathcal{D}(\mathcal{H}_A) \subset \mathcal{L}_+(\mathcal{H}_A)$  contains all operators  $\rho_A \in \mathcal{L}_+(\mathcal{H}_A)$  such that  $\text{Tr}\{\rho_A\} = 1$ . The state  $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$  is called an extension of a state  $\rho_A \in \mathcal{D}(\mathcal{H}_A)$  if  $\rho_A = \text{Tr}_B\{\rho_{AB}\}$ , where  $\text{Tr}_B$  denotes the partial trace over  $\mathcal{H}_B$ .

Every density operator  $\rho \in \mathcal{D}(\mathcal{H})$  can be expressed in terms of a spectral decomposition of a countable number

of eigenvectors and eigenvalues:

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \quad (1)$$

where the probabilities  $\{p_i\}_i$  are the eigenvalues and  $\{|\phi_i\rangle\}_i$  are the eigenvectors. A state  $\rho \in \mathcal{D}(\mathcal{H})$  is called a pure state if there exists a unit vector  $|\psi\rangle \in \mathcal{H}$  such that  $\rho = |\psi\rangle\langle\psi|$ . When this is not the case, we say that the state is a mixed state, because a spectral decomposition indicates that any state can be interpreted as a probabilistic mixture of pure states.

We can purify a state  $\rho_A = \sum_i p_i |\phi_i\rangle\langle\phi_i|_A$  by introducing a set of orthonormal vectors  $\{|i\rangle_R\}_i$  and extending it to a pure state in the tensor-product space  $\mathcal{H}_{RA}$ . Then

$$|\psi\rangle_{RA} = \sum_i \sqrt{p_i} |\phi_i\rangle_A |i\rangle_R \quad (2)$$

is a unit vector in  $\mathcal{H}_{RA}$ , and  $\rho_{RA} = |\psi\rangle\langle\psi|_{RA}$  is a pure state in  $\mathcal{D}(\mathcal{H}_{RA})$ . A state purification is a special kind of extension, given that  $\rho_A = \text{Tr}_R\{\rho_{RA}\}$ .

A key feature of quantum systems is the phenomenon of entanglement [24]. A state made up of multiple systems is said to be entangled if it cannot be written as a probabilistic mixture of product states. For example,  $\rho_{AB} = \sum_z p_Z(z) |\psi^z\rangle\langle\psi^z|_A \otimes |\phi^z\rangle\langle\phi^z|_B$  represents an unentangled, separable state in  $\mathcal{D}(\mathcal{H}_{AB})$  [35], where  $p_Z(z)$  is a probability distribution and  $\{|\psi^z\rangle_A\}_z$  and  $\{|\phi^z\rangle_B\}_z$  are sets of unit vectors.

The Schmidt decomposition theorem gives us a tool for simplifying the form of pure, two-party (bipartite) states and particularly for determining whether a pure, bipartite state is entangled. An arbitrary bipartite unit vector  $|\psi\rangle_{AB}$  can be written as  $|\psi\rangle_{AB} = \sum_i \sqrt{p_i} |i\rangle_A |i\rangle_B$  where  $\{|i\rangle_A\}_i$  and  $\{|i\rangle_B\}_i$  are orthonormal bases in the Hilbert spaces  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , respectively, and  $\{p_i\}_i$  are strictly positive, real probabilities. The set  $\{\sqrt{p_i}\}_i$  is the set of Schmidt coefficients. For finite-dimensional  $|\psi\rangle_{AB}$ , the number  $d$  of Schmidt coefficients is called the Schmidt rank of the vector, and it satisfies the following inequality:  $d \leq \min[\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)]$ . For infinite-dimensional  $|\psi\rangle_{AB}$ , the Schmidt rank  $d$  can clearly be equal to infinity. The state  $|\psi\rangle_{AB}$  is an entangled state if and only if  $d \geq 2$ . For finite-dimensional  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , such that  $\mathcal{H}_A$  is isomorphic to  $\mathcal{H}_B$ , we define a maximally entangled state in terms of the following unit vector:

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A |i\rangle_B. \quad (3)$$

According to the Choi-Kraus theorem, a linear map  $\mathcal{N}_{A \rightarrow B}$  from  $\mathcal{L}_1(\mathcal{H}_A)$  to  $\mathcal{L}_1(\mathcal{H}_B)$  is completely positive and trace preserving (CPTP) if and only if it can be written in the following way:

$$\mathcal{N}_{A \rightarrow B}(X_A) = \sum_l V_l X_A V_l^\dagger, \quad (4)$$

where  $X_A \in \mathcal{L}_1(\mathcal{H}_A)$ ,  $V_l$  is a bounded linear operator mapping  $\mathcal{H}_A \rightarrow \mathcal{H}_B$ , and  $\sum_l V_l^\dagger V_l = I_A$ . This is called the Choi-Kraus representation, and  $\{V_l\}_l$  is called the set of Kraus operators. Such a linear map is referred to as a quantum channel, and it takes quantum states to other quantum states. Quantum channels can be concatenated in a serial or parallel way, and such a combination is also a quantum channel.

An isometric extension  $U_{A \rightarrow BE}^{\mathcal{N}}$  of a quantum channel  $\mathcal{N}_{A \rightarrow B}$  is a linear isometry taking  $\mathcal{H}_A$  to  $\mathcal{H}_B \otimes \mathcal{H}_E$ , satisfying

$$\mathcal{N}_{A \rightarrow B}(X_A) = \text{Tr}_E\{\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}(X_A)\}, \quad (5)$$

for all  $X_A \in \mathcal{L}_1(\mathcal{H}_A)$ , where the isometric channel  $\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}$  is defined in terms of the isometry  $U_{A \rightarrow BE}^{\mathcal{N}}$  as

$$\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}(X_A) = U_{A \rightarrow BE}^{\mathcal{N}} X_A (U_{A \rightarrow BE}^{\mathcal{N}})^\dagger. \quad (6)$$

We can construct a canonical isometric extension of a quantum channel in the following way:

$$U_{A \rightarrow BE}^{\mathcal{N}} = \sum_l V_l \otimes |l\rangle_E, \quad (7)$$

where  $\{|l\rangle_E\}_l$  is an orthonormal basis. One can check that (5) is satisfied for this choice.

An isometric extension of a quantum channel shows that we can think of a channel as involving not only a sender and receiver but also a passive environment represented by system  $E$  above. In order to determine the output of the extended channel  $\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}$  to the environment, we simply trace over the output system  $B$  instead of the environment  $E$ . The resulting channel is known as a complementary channel [36–38] (sometimes “conjugate channel”), with the following action on an input state  $\rho_A$ :

$$\hat{\mathcal{N}}_{A \rightarrow E}(\rho_A) = \text{Tr}_B\{\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}(\rho_A)\}. \quad (8)$$

A channel complementary to  $\mathcal{N}_{A \rightarrow B}$  is a CPTP map from  $\mathcal{L}_1(\mathcal{H}_A)$  to  $\mathcal{L}_1(\mathcal{H}_E)$  and is unique up to an isometry acting on the space  $\mathcal{H}_E$  (see, e.g., [32, 34]).

The quantum instrument formalism provides the most general description of a quantum measurement [39]. A quantum instrument is a set of completely positive, trace non-increasing maps  $\{\mathcal{M}_{A \rightarrow B}^x\}_x$  such that the sum map  $\sum_x \mathcal{M}_{A \rightarrow B}^x$  is a quantum channel [39]. One can equivalently think of it as a quantum channel that takes as input a quantum system and gives as output both a quantum system and a classical system:

$$\mathcal{M}_{A \rightarrow BX}(\rho_A) = \sum_x \mathcal{M}_{A \rightarrow B}^x(\rho_A) \otimes |x\rangle\langle x|_X. \quad (9)$$

Here  $\{|x\rangle\}_x$  is a classical orthonormal basis identified with the outcomes of the instrument. Throughout this paper, we consider only the case when the measurement has a finite or countable number of outcomes.

In discussing quantum systems corresponding to tensor-product Hilbert spaces, it is useful to consider

which parties can influence which subsystems, and we give names to the parties corresponding to the label on their subsystem. For example, it is conventional to say that Alice has access to system  $A$ , Bob to system  $B$ , and Eve to system  $E$ , which we often refer to as the environment as well. Eve is so named because the third party is regarded as a passive adversary or eavesdropper in a cryptographic context. By taking system  $E$  to encompass anything not in another specified system, we can consider the most general cases of Eve's participation.

In what follows, we consider the use of a quantum channel interleaved with rounds of local operations and classical communication (LOCC). These rounds of LOCC can be considered channels themselves as follows:

1. Alice performs a quantum instrument on her system, resulting in both quantum and classical outputs.
2. Alice sends a copy of the classical output to Bob.
3. Bob performs a quantum channel on his system conditioned on the classical data that he receives from Alice.
4. Bob then performs a quantum instrument on his system and forwards the classical output to Alice.
5. Finally, Alice performs a quantum channel on her system conditioned on the classical data from Bob.
6. Iterate the above steps an arbitrarily large, yet finite number of times.

The sequence of actions in the first through third steps is called "local operations and one-way classical communication," and they can be expressed as a quantum channel of the following form:

$$\mathcal{S}_{AB} \equiv \sum_z \mathcal{G}_A^z \otimes \mathcal{J}_B^z, \quad (10)$$

where  $\{\mathcal{G}_A^z\}_z$  is a countable set of completely positive, trace non-increasing maps, such that the sum map  $\sum_z \mathcal{G}_A^z$  is trace preserving, and  $\{\mathcal{J}_B^z\}_z$  is a set of channels. These conditions imply that  $\mathcal{S}_{AB}$  is a channel. The fourth and fifth steps above can also take the form of (10) with the system labels reversed.

As indicated above, a full round of LOCC consists of the concatenation of some number of these channels back and forth between Alice and Bob [19, 40]. This concatenation is a particular kind of separable channel and takes the form

$$\mathcal{L}_{AB} \equiv \sum_y \mathcal{E}_A^y \otimes \mathcal{F}_B^y, \quad (11)$$

where  $\{\mathcal{E}_A^y\}_y$  and  $\{\mathcal{F}_B^y\}_y$  are countable sets of completely positive, trace non-increasing maps such that  $\mathcal{L}_{AB}$  is CPTP. We stress again that we only consider LOCC channels with a finite or countable number of classical values, and we refer to them as countably decomposable LOCC channels.

## B. Trace Distance and Quantum Fidelity

We defined the trace norm  $\|X\|_1$  of an operator  $X$  previously. Being a norm, it is homogeneous, non-negative definite, and obeys the triangle inequality. It is also convex and invariant under multiplication by isometries; i.e., for  $\lambda \in [0, 1]$ , we have that  $\|\lambda X + (1 - \lambda)Y\|_1 \leq \lambda\|X\|_1 + (1 - \lambda)\|Y\|_1$ , and for isometries  $U$  and  $V^\dagger$ , we have that  $\|UXV^\dagger\|_1 = \|X\|_1$ .

The trace norm of an operator leads to the trace distance between two of them. The trace distance between two density operators  $\rho$  and  $\sigma$  quantifies the distinguishability of the two states [41–43] and satisfies the inequality:  $0 \leq \|\rho - \sigma\|_1 \leq 2$ . From the triangle inequality, we see that the trace distance is maximized for orthogonal states; i.e., when  $\rho\sigma = 0$ , then  $\|\rho - \sigma\|_1 = \|\rho\|_1 + \|\sigma\|_1 = 2$ . Note that sometimes we employ the normalized trace distance, which is equal to half the usual trace distance:  $0 \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq 1$ .

Another way to measure the closeness of quantum states is given by the quantum fidelity [44]. The pure-state fidelity for pure-state vectors  $|\psi\rangle_A$  and  $|\phi\rangle_A$  is given by

$$F(\psi_A, \phi_A) \equiv |\langle \psi | \phi \rangle_A|^2, \quad (12)$$

from which we conclude that  $0 \leq F(\psi_A, \phi_A) \leq 1$ . The general definition of the fidelity for arbitrary density operators  $\rho_A$  and  $\sigma_A$  is as follows:

$$F(\rho_A, \sigma_A) \equiv \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2. \quad (13)$$

Uhlmann's theorem is the statement that the following equality holds [44]:

$$F(\rho_A, \sigma_A) = \sup_{U_R} |\langle \phi^\rho |_{RA} U_R \otimes I_A | \phi^\sigma \rangle_{RA}|^2, \quad (14)$$

where  $|\phi^\rho\rangle_{RA}$  and  $|\phi^\sigma\rangle_{RA}$  are purifications of  $\rho_A$  and  $\sigma_A$  with purifying system  $R$  and  $U_R$  is a unitary acting on system  $R$ .

## C. Entropy and Information

In order to study the information contained and transmitted in various systems and operations, we now recall a number of common measures used to quantify information. With these measures defined below, we also focus on generalizations of the quantities as functions of operators acting on infinite-dimensional, separable Hilbert spaces, as considered in, e.g., [28]. The first and most common measure is the quantum entropy and is defined for a state  $\rho \in \mathcal{D}(\mathcal{H})$  as

$$H(\rho) \equiv \text{Tr}\{\eta(\rho)\}, \quad (15)$$

where  $\eta(x) = -x \log_2 x$  if  $x > 0$  and  $\eta(0) = 0$ . The trace in the above equation can be taken with respect to any countable orthonormal basis of  $\mathcal{H}$  [45, Definition 2].

The quantum entropy is a non-negative, concave, lower semicontinuous function on  $\mathcal{D}(\mathcal{H})$  [46]. It is also not necessarily finite (see, e.g., [47]). When  $\rho_A$  is the state of a system  $A$ , we write

$$H(A)_\rho \equiv H(\rho_A). \quad (16)$$

The entropy is a familiar thermodynamic quantity and is roughly a measure of the disorder in a system. One property of quantum entropy that we use here is its duality: for a pure state  $|\psi\rangle\langle\psi|_{RA}$ , quantum entropy is such that  $H(A)_\psi = H(R)_\psi$ .

For a positive semi-definite, trace-class operator  $\omega$  such that  $\text{Tr}\{\omega\} \neq 0$ , we extend the definition of quantum entropy as

$$H(\omega) \equiv \text{Tr}\{\omega\} H\left(\frac{\omega}{\text{Tr}\{\omega\}}\right). \quad (17)$$

Observe that  $H(\omega)$  reduces to the definition in (15) when  $\omega$  is a state with  $\text{Tr}\{\omega\} = 1$ .

The quantum relative entropy  $D(\rho\|\sigma)$  of  $\rho, \sigma \in \mathcal{D}(\mathcal{H})$  is defined as [48, 49]

$$\begin{aligned} D(\rho\|\sigma) & \\ & \equiv [\ln 2]^{-1} \sum_{i,j} |\langle\phi_i|\psi_j\rangle|^2 [p(i) \ln\left(\frac{p(i)}{q(j)}\right) + q(j) - p(i)], \end{aligned} \quad (18)$$

where  $\rho = \sum_i p(i) |\phi_i\rangle\langle\phi_i|$  and  $\sigma = \sum_j q(j) |\psi_j\rangle\langle\psi_j|$  are spectral decompositions of  $\rho$  and  $\sigma$  with  $\{|\phi_i\rangle\}_i$  and  $\{|\psi_j\rangle\}_j$  orthonormal bases. The prefactor  $[\ln 2]^{-1}$  is there to ensure that the units of the quantum relative entropy are bits. We take the convention in (18) that  $0 \ln 0 = 0 \ln(\frac{0}{0}) = 0$  but  $\ln(\frac{c}{0}) = +\infty$  for  $c > 0$ . Each term in the sum in (18) is non-negative due to the inequality

$$x \ln(x/y) + y - x \geq 0 \quad (19)$$

holding for all  $x, y \geq 0$  [48]. Thus, by Tonelli's theorem, the sums in (18) may be taken in either order as discussed in [48, 49], and it follows that

$$D(\rho\|\sigma) \geq 0 \quad (20)$$

for all  $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ , with equality holding if and only if  $\rho = \sigma$  [48]. If the support of  $\rho$  is not contained in the support of  $\sigma$ , then  $D(\rho\|\sigma) = +\infty$ . The converse statement need not hold in general: there exist  $\rho, \sigma \in \mathcal{D}(\mathcal{H})$  with the support of  $\rho$  contained in the support of  $\sigma$  such that  $D(\rho\|\sigma) = +\infty$ . Thus, for states  $\rho$  and  $\sigma$ , we have that

$$D(\rho\|\sigma) \in [0, \infty]. \quad (21)$$

It is also worth noting that relative entropy is not generally symmetric; i.e., there exist states  $\rho$  and  $\sigma$  for which

$$D(\rho\|\sigma) \neq D(\sigma\|\rho). \quad (22)$$

One of the most important properties of the quantum relative entropy  $D(\rho\|\sigma)$  is that it is monotone with respect to a quantum channel  $\mathcal{N} : \mathcal{L}_1(\mathcal{H}_A) \rightarrow \mathcal{L}_1(\mathcal{H}_B)$  [50]:

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \quad (23)$$

The above inequality is often called the ‘‘data processing inequality.’’ This inequality implies that the quantum relative entropy is invariant under the action of an isometry  $U$ :

$$D(\rho\|\sigma) = D(U\rho U^\dagger\|U\sigma U^\dagger). \quad (24)$$

The quantum mutual information of a bipartite state  $\rho_{AB}$  is defined in terms of the relative entropy [49] as

$$I(A; B)_\rho \equiv D(\rho_{AB}\|\rho_A \otimes \rho_B). \quad (25)$$

Note that, with the definition in (25), we have that

$$I(A; B)_\rho \in [0, \infty] \quad (26)$$

as a consequence of (21). The following inequality applies to quantum mutual information [49]:

$$I(A; B)_\rho \leq 2 \min\{H(A)_\rho, H(B)_\rho\} \quad (27)$$

and establishes that it is finite if one of the marginal entropies is finite. For a general positive semi-definite trace-class operator  $\omega_{AB}$  such that  $\text{Tr}\{\omega_{AB}\} \neq 0$ , we extend the definition of mutual information as in [51]

$$I(A; B)_\omega \equiv \text{Tr}\{\omega\} I(A; B)_{\frac{\omega}{\text{Tr}\{\omega\}}}. \quad (28)$$

Note that, while the relative entropy is not generally symmetric, mutual information is symmetric under the exchange of systems  $A$  and  $B$

$$I(A; B)_\rho = I(B; A)_\rho, \quad (29)$$

due to (24) and by taking the isometry therein to be a unitary swap of the systems  $A$  and  $B$ . For a state  $\rho_{AB}$  such that the entropies  $H(A)_\rho$  and  $H(B)_\rho$  are finite, the mutual information reduces to

$$I(A; B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho. \quad (30)$$

For a state  $\rho_{AB}$  such that  $H(A)_\rho < \infty$ , the conditional entropy is defined as [52]

$$H(A|B)_\rho \equiv H(A)_\rho - I(A; B)_\rho, \quad (31)$$

and the same definition applies for a positive semi-definite trace-class operator  $\omega_{AB}$ , by employing the extended definitions of entropy in (17) and mutual information in (28). Thus, as a consequence of the definition and (27), we have that

$$H(A|B)_\rho \in [-H(A)_\rho, H(A)_\rho]. \quad (32)$$

If  $H(B)_\rho$  is also finite, then the conditional entropy simplifies to the following more familiar form:

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho. \quad (33)$$

For a tripartite pure state  $\psi_{ABC}$  such that  $H(A)_\psi < \infty$ , the conditional entropy satisfies the following duality relation [52]:

$$H(A|B)_\psi = -H(A|C)_\psi. \quad (34)$$

[52, Proposition 1] states that conditional entropy is sub-additive: for a four-party state  $\rho_{ABCD}$ , we have that

$$H(AB|CD)_\rho \leq H(A|C)_\rho + H(B|D)_\rho. \quad (35)$$

This in turn is a consequence of the strong subadditivity of quantum entropy [53, 54].

The conditional quantum mutual information (CQMI) of tripartite states  $\omega_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$ , with  $\mathcal{H}_{ABE}$  a separable Hilbert space, was defined only recently in [51], as a generalization of the information measure commonly used in the finite-dimensional setting. The definition from [51] involves taking a supremum over all finite-rank projections  $P_A \in \mathcal{L}(\mathcal{H}_A)$  or  $P_B \in \mathcal{L}(\mathcal{H}_B)$ , in order to write CQMI in terms of the quantum mutual information in the following equivalent ways:

$$\begin{aligned} I(A; B|E)_\omega &= \sup_{P_A} I(A; BE)_{Q_A \omega Q_A} - I(A; E)_{Q_A \omega Q_A} \end{aligned} \quad (36)$$

$$= \sup_{P_B} I(AE; B)_{Q_B \omega Q_B} - I(E; B)_{Q_B \omega Q_B}, \quad (37)$$

where  $Q_A = P_A \otimes I_{BE}$  and  $Q_B = P_B \otimes I_{AE}$ . Due to the data-processing inequality in (23), with the channel taken to be a partial trace, we have that

$$I(A; B|E)_\omega \in [0, \infty]. \quad (38)$$

The conditional mutual information, as defined above, is a lower semi-continuous function of tripartite quantum states [51, Theorem 2]; i.e., for any sequence  $\{\omega_{ABE}^n\}_n$  of tripartite states converging to the state  $\omega_{ABE}^0$ , the following inequality holds

$$\liminf_{n \rightarrow \infty} I(A; B|E)_{\omega^n} \geq I(A; B|E)_{\omega^0}. \quad (39)$$

If  $I(A; BE)_\omega, I(A; E)_\omega < \infty$ , as is the case if  $H(A)_\omega < \infty$ , then the definition reduces to the familiar one from the finite-dimensional case:

$$I(A; B|E)_\omega = I(A; BE)_\omega - I(A; E)_\omega. \quad (40)$$

#### D. Squashed Entanglement

The information measure of most concern in our paper is the squashed entanglement. Defined and analyzed in [25], and extended to the infinite-dimensional case in [28], the squashed entanglement of a state  $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$  is defined as

$$E_{\text{sq}}(A; B)_\rho = \frac{1}{2} \inf_{\omega_{ABE}} I(A; B|E)_\omega, \quad (41)$$

where  $\omega_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})$  satisfies  $\text{Tr}_E\{\omega_{ABE}\} = \rho_{AB}$ , with  $\mathcal{H}_E$  taken to be an infinite-dimensional, separable Hilbert space. (See [55, 56] for discussions related to squashed entanglement.) An equivalent definition is given in terms of an optimization over squashing channels, as follows:

$$E_{\text{sq}}(A; B)_\rho = \frac{1}{2} \inf_{\mathcal{S}_{E \rightarrow E'}} I(A; B|E')_\tau, \quad (42)$$

where  $\tau_{ABE'} = \mathcal{S}_{E \rightarrow E'}(\phi_{ABE}^\rho)$ , with  $\phi_{ABE}^\rho$  a purification of  $\rho_{AB}$ . The infimum is with respect to all squashing channels  $\mathcal{S}_{E \rightarrow E'}$  from system  $E$  to a system  $E'$  corresponding to an infinite-dimensional, separable Hilbert space. The reasoning for this equivalence is the same as that given in [25]. Due to the expression in (42), squashed entanglement can be interpreted as the leftover correlation after an adversary attempts to “squash down” the correlations in  $\rho_{AB}$ . Squashed entanglement obeys many of the properties considered important for an entanglement measure, such as LOCC monotonicity, additivity for product states, and convexity [25]. These properties are discussed in the next section.

Suppose that Alice, in possession of the systems  $RA$  of a pure state  $\phi_{RA}$ , wishes to construct a shared state with Bob. If Alice and Bob are connected by a quantum channel  $\mathcal{N}_{A \rightarrow B}$  mapping system  $A$  to  $B$ , then they can establish the shared state

$$\omega_{RB} = \mathcal{N}_{A \rightarrow B}(\phi_{RA}). \quad (43)$$

Going to the purified picture, an isometric channel  $\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}$  extends  $\mathcal{N}_{A \rightarrow B}$ , so that the output state of the extended channel is  $\phi_{RBE} = \mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}(\phi_{RA})$  when the input is  $\phi_{RA}$ . Suppose that a third party Eve has access to the system  $E$ , such that she could then perform a squashing channel  $\mathcal{S}_{E \rightarrow E'}$ , bringing system  $E$  to system  $E'$ . In this way, she could attempt to thwart the correlation between Alice and Bob’s systems, as measured by conditional mutual information. Related to the above physical picture, the squashed entanglement of the channel  $\mathcal{N}_{A \rightarrow B}$  is defined as the largest possible squashed entanglement that can be realized between systems  $R$  and  $B$  [5, 17]:

$$E_{\text{sq}}(\mathcal{N}) \equiv \sup_{\phi_{RA}} E_{\text{sq}}(R; B)_\omega, \quad (44)$$

where the supremum is with respect to all possible pure bipartite input states  $\phi_{RA}$ , with system  $R$  isomorphic to system  $A$ , and  $\omega_{RB}$  is defined in (43).

If specific requirements are placed on the channel input states, such as an energy constraint as discussed in Section IV A below, the optimization should reflect those stipulations, leading to the energy-constrained squashed entanglement of a channel  $\mathcal{N}$ :

$$E_{\text{sq}}(\mathcal{N}, G, P) \equiv \sup_{\phi_{RA}: \text{Tr}\{G\phi_A\} \leq P} E_{\text{sq}}(R; B)_\omega. \quad (45)$$

Here  $G$  is an energy observable acting on the channel input system  $A$ , the positive real  $P \in [0, \infty)$  is a constraint on the expected value of that observable such

that  $\text{Tr}\{G\phi_A\} \leq P$ , and the supremum is with respect to all pure input states  $\phi_{RA}$  to the channel that obey the given constraint. It suffices to optimize the quantity in (45) with respect to pure, bipartite input states, following from purification, the Schmidt decomposition theorem, and LOCC monotonicity of squashed entanglement. These notions are discussed in more detail in Section IV.

As discussed in [17], the squashed entanglement of a channel can be written in a different way by considering an isometric channel  $\mathcal{V}_{E \rightarrow E'F}^S$  extending the squashing channel  $\mathcal{S}_{E \rightarrow E'}$ . Let  $\varphi_{RBE'F}$  denote the following pure output state when the pure state  $\phi_{RA}$  is input:

$$\varphi_{RBE'F} = (\mathcal{V}_{E \rightarrow E'F}^S \circ \mathcal{U}_{A \rightarrow BE}^N)(\phi_{RA}). \quad (46)$$

By taking advantage of the duality of conditional entropy and in the case that the entropy  $H(B)_\varphi$  is finite, the alternate way of writing follows from the equality

$$\begin{aligned} I(R; B|E')_\varphi &= H(B|E')_\varphi - H(B|RE')_\varphi \\ &= H(B|E')_\varphi + H(B|F)_\varphi. \end{aligned} \quad (47)$$

Thus, we can write the energy-constrained squashed entanglement of a channel as

$$E_{\text{sq}}(\mathcal{N}, G, P) = \sup_{\rho_A: \text{Tr}\{G\rho_A\} \leq P} E_{\text{sq}}(\rho_A, \mathcal{N}_{A \rightarrow B}), \quad (49)$$

where

$$E_{\text{sq}}(\rho_A, \mathcal{N}_{A \rightarrow B}) \equiv \inf_{\mathcal{V}_{E \rightarrow E'F}^S} \frac{1}{2} [H(B|E')_\omega + H(B|F)_\omega] \quad (50)$$

$$\omega_{BE'F} = (\mathcal{V}_{E \rightarrow E'F}^S \circ \mathcal{U}_{A \rightarrow BE}^N)(\rho_A), \quad (51)$$

and we take advantage of the representation in (49) in our paper.

### E. Entanglement Monotones and Squashed Entanglement

In this section, we review the notion of an entanglement monotone [24] and how squashed entanglement [25] and its extended definition in [28] satisfies the requirements of being an entanglement monotone. Let  $E(A; B)_\omega$  be a function of an arbitrary bipartite state  $\omega_{AB}$ . Then  $E(A; B)_\omega$  is an entanglement monotone if it satisfies the following conditions:

- 1)  $E(A; B)_\omega = 0$  if and only if  $\omega_{AB}$  is separable.
- 2)  $E$  is monotone under selective unilocal operations.

That is,

$$E(A; B)_\omega \geq \sum_k p_k E(A; B)_{\omega^k}, \quad (52)$$

where

$$p_k = \text{Tr}(\mathcal{N}_A^k(\omega_{AB})), \quad \omega_{AB}^k = p_k^{-1} \mathcal{N}_A^k(\omega_{AB}) \quad (53)$$

for any state  $\omega_{AB}$  and any collection  $\{\mathcal{N}_A^k\}$  of unilocal completely positive maps such that the sum map  $\sum_k \mathcal{N}_A^k$  is a channel.

3)  $E$  is convex, in the sense that for states  $\rho_{AB}^0, \rho_{AB}^1$ , and  $\rho_{AB}^\lambda = (1 - \lambda)\rho_{AB}^0 + \lambda\rho_{AB}^1$ , where  $\lambda \in [0, 1]$ ,

$$E(A; B)_{\rho^\lambda} \leq (1 - \lambda)E(A; B)_{\rho^0} + \lambda E(A; B)_{\rho^1}. \quad (54)$$

When the condition in 3) holds, then the condition in 2) is equivalent to monotonicity under LOCC.

An entanglement monotone is additionally considered an entanglement measure if, for any pure state  $\psi_{AB}$ , it is equal to the quantum entropy of a marginal state:

$$E(A; B)_\psi = H(A)_\psi = H(B)_\psi. \quad (55)$$

Other desirable properties for an entanglement monotone include

- additivity for a product state  $\omega_{AB} \otimes \theta_{A'B'}$ :

$$E(AA'; BB')_{\omega \otimes \theta} = E(A; B)_\omega + E(A'; B')_\theta, \quad (56)$$

- subadditivity for a product state  $\omega_{AB} \otimes \theta_{A'B'}$ :

$$E(AA'; BB')_{\omega \otimes \theta} \leq E(A; B)_\omega + E(A'; B')_\theta, \quad (57)$$

- strong superadditivity for a state  $\omega_{AA'BB'}$ :

$$E(AA'; BB')_\omega \geq E(A; B)_\omega + E(A'; B')_\omega, \quad (58)$$

- monogamy for a state  $\omega_{ABC}$ :

$$E(A; BC)_\omega \geq E(A; B)_\omega + E(A; C)_\omega, \quad (59)$$

- asymptotic continuity:

$$\lim_{n \rightarrow \infty} \frac{E(\rho_{AB}^n) - E(\sigma_{AB}^n)}{1 + \log_2(\dim \mathcal{H}_{AB}^n)} = 0, \quad (60)$$

which should hold for any sequences  $\{\rho_{AB}^n\}_n$  and  $\{\sigma_{AB}^n\}_n$  of states such that  $\|\rho_{AB}^n - \sigma_{AB}^n\|_1$  converges to zero as  $n \rightarrow \infty$ .

As discussed in [28], for states in infinite-dimensional Hilbert spaces, global asymptotic continuity is too restrictive. For example, the discontinuity of the quantum entropy means that any entanglement monotone that possesses property (55) is necessarily discontinuous. It is therefore reasonable to require instead that  $E$  is lower semi-continuous [28]:

$$\liminf_{n \rightarrow \infty} E(\omega_{AB}^n) \geq E(\omega_{AB}^0) \quad (61)$$

for any sequence  $\{\omega_{AB}^n\}$  of states converging to the state  $\omega_{AB}^0$ .

The squashed entanglement, as defined in (41), obeys all of the above properties [25–28, 57–59]. Regarding the last property, the squashed entanglement defined in



(41) has been proved to be lower semicontinuous on the set of states having at least one finite marginal entropy [28]. It additionally satisfies the following uniform continuity inequality: Given states  $\rho_{AB}$  and  $\sigma_{AB}$  satisfying  $\frac{1}{2} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \varepsilon$  for  $\varepsilon \in [0, 1]$  then

$$\begin{aligned} & |E_{\text{sq}}(A; B)_\rho - E_{\text{sq}}(A; B)_\sigma| \\ & \leq \sqrt{2\varepsilon} \log_2 \min[\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)] + g(\sqrt{2\varepsilon}) \end{aligned} \quad (62)$$

where

$$g(x) \equiv (1+x) \log_2(1+x) - x \log_2(x). \quad (63)$$

This follows by combining the well known Fuchs–van de Graaf inequalities [60], Uhlmann’s theorem for fidelity [44], and the continuity bound from [61, Corollary 1] for conditional mutual information.

### F. Private States

The main goal of any key distillation protocol is for two parties Alice and Bob to distill a tripartite state as close as possible to an ideal tripartite secret-key state, which is protected against a third-party Eve. An ideal tripartite secret-key state  $\gamma_{ABE}$  is such that local projective measurements  $\mathcal{M}_A$  and  $\mathcal{M}_B$  on it, in the respective orthonormal bases  $\{|i\rangle_A\}_i$  and  $\{|i\rangle_B\}_i$ , lead to the following form:

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K} \sum_{i=1}^K |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E. \quad (64)$$

The key systems are finite-dimensional, but the eavesdropper’s system  $E$  could be described by an infinite-dimensional, separable Hilbert space. The tripartite key state  $\gamma_{ABE}$  contains  $\log_2 K$  bits of secret key. By inspecting the right-hand side of (64), we see that the key value is uniformly random and perfectly correlated between systems  $A$  and  $B$ , as well as being in tensor product with the state of system  $E$ , implying that the results of any experiment on the  $AB$  systems will be independent of those given by an experiment conducted on the  $E$  system. While a perfect ideal tripartite key state may be difficult to achieve in practice, a state that is nearly indistinguishable from the ideal case is good enough for practical purposes. If a state  $\rho_{ABE}$  satisfies the following inequality:

$$F(\gamma_{ABE}, \rho_{ABE}) \geq 1 - \varepsilon, \quad (65)$$

for some  $\varepsilon \in [0, 1]$  and  $\gamma_{ABE}$  an ideal tripartite key state, then  $\rho_{ABE}$  is called an  $\varepsilon$ -approximate tripartite key state [11, 62, 63].

By purifying a tripartite secret-key state  $\gamma_{ABE}$  with “shield systems”  $A'$  and  $B'$  and then tracing over the system  $E$ , the resulting state is called a bipartite private state, which takes the following form [62, 63]:

$$\gamma_{ABA'B'} = U_{ABA'B'}(|\Phi\rangle\langle\Phi|_{AB} \otimes \sigma_{A'B'})U_{ABA'B'}^\dagger, \quad (66)$$

where

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{K}} \sum_{i=1}^K |i\rangle_A |i\rangle_B \quad (67)$$

is a maximally entangled state with Schmidt rank  $K$  and  $\sigma_{A'B'}$  is an arbitrary state of the shield systems  $A'B'$ . Due to the fact that the system  $E$  of the tripartite key state  $\gamma_{ABE}$  corresponds generally to an infinite-dimensional, separable Hilbert space, the same is true for the shield systems  $A'B'$  of  $\gamma_{ABA'B'}$ . The unitary operator  $U_{ABA'B'}$  is called a “twisting” unitary and has the following form:

$$U_{ABA'B'} = \sum_{i,j=1}^K |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U_{A'B'}^{ij}, \quad (68)$$

where each  $U_{A'B'}^{ij}$  is a unitary operator. Note that, due to the correlation between the  $A$  and  $B$  systems in the state  $\Phi_{AB}$ , only the diagonal terms  $U_{A'B'}^{ii}$  of the twisting unitary are relevant when measuring the systems  $A$  and  $B$  in the orthonormal bases  $\{|i\rangle_A\}_i$  and  $\{|i\rangle_B\}_i$ , respectively [62, 63]. If a state  $\rho_{ABA'B'}$  satisfies

$$F(\gamma_{ABA'B'}, \rho_{ABA'B'}) \geq 1 - \varepsilon, \quad (69)$$

for some  $\varepsilon \in [0, 1]$  and  $\gamma_{ABA'B'}$  an ideal bipartite private state, then  $\rho_{ABA'B'}$  is called an  $\varepsilon$ -approximate bipartite private state [11, 62, 63].

The converse of the above statement holds as well [62, 63], and the fact that it does is one of the main reasons that the above notions are useful in applications. That is, given a bipartite private state of the form in (66), we can then purify it by an  $E$  system, and tracing over the shield systems  $A'B'$  leads to a tripartite key state of the form in (64). These relations extend to the approximate case as well, by an application of Uhlmann’s theorem for fidelity [44]: purifying an  $\varepsilon$ -approximate tripartite key state  $\rho_{ABE}$  with shield systems  $A'B'$  and tracing over system  $E$  leads to an  $\varepsilon$ -approximate bipartite private state, and vice versa.

The squashed entanglement of a bipartite private state of  $\log_2 K$  bits is normalized such that [58]

$$E_{\text{sq}}(AA'; BB')_\gamma \geq \log_2 K. \quad (70)$$

This result has recently been extended to the approximate case: [13, Theorem 2] establishes that, for an  $\varepsilon$ -approximate bipartite private state  $\rho_{ABA'B'}$ , the following inequality holds

$$E_{\text{sq}}(AA'; BB')_\rho + 2\sqrt{\varepsilon} \log_2 K + 2g(\sqrt{\varepsilon}) \geq \log_2 K. \quad (71)$$

### III. PROPERTIES OF CONDITIONAL QUANTUM MUTUAL INFORMATION

In this section, we establish a number of simple properties of conditional quantum mutual information (CQMI) for states of infinite-dimensional, separable Hilbert spaces. These properties will be useful in later sections of our paper.

### A. CQMI and Duality under a Finite-Entropy Assumption

**Lemma 1 (Duality)** *Let  $\psi_{ABED}$  be a pure state such that  $H(B)_\psi < \infty$ . Then the conditional quantum mutual information  $I(A; B|E)_\psi$  can be written as*

$$I(A; B|E)_\psi = H(B|E)_\psi + H(B|D)_\psi. \quad (72)$$

**Proof.** Begin with the definition of CQMI from (37):

$$I(A; B|E)_\psi = \sup_{P_B} [I(B; AE)_{Q_B \psi_{Q_B}} - I(B; E)_{Q_B \psi_{Q_B}}] : Q_B = P_B \otimes I_{AE}, \quad (73)$$

where we have exploited the symmetry of mutual information as recalled in (29). The assumption  $H(B)_\psi < \infty$  is strong, implying that  $I(B; AE)_\psi, I(B; E)_\psi < \infty$ , so that we can write  $I(A; B|E)_\psi = I(B; AE)_\psi - I(B; E)_\psi$  [51]. Then we find that

$$\begin{aligned} I(A; B|E)_\psi &= H(B)_\psi - H(B)_\psi + I(B; AE)_\psi - I(B; E)_\psi \\ &= [H(B)_\psi - I(B; E)_\psi] - [H(B)_\psi - I(B; AE)_\psi]. \end{aligned} \quad (74)$$

From the definition in (31), it is clear that the last line is equal to a difference of conditional entropies, leading to

$$I(A; B|E)_\psi = H(B|E)_\psi - H(B|AE)_\psi. \quad (75)$$

Finally, we invoke the duality of conditional entropy from (34) in order to arrive at the statement of the lemma. ■

### B. Subadditivity Lemma for Conditional Quantum Mutual Information

In this section, we prove a lemma that generalizes one of the main technical results of [5, 17] to the infinite-dimensional setting of interest here. This lemma was the main tool used in [5, 17] to prove that the squashed entanglement of a quantum channel is an upper bound on its secret-key-agreement capacity. After [5, 17] appeared, this lemma was later interpreted as implying that amortization does not increase the squashed entanglement of a channel [64–66].

**Lemma 2** *Let  $\phi_{A'AB'E''F''}$  be a pure state, and let  $\mathcal{U}_{A \rightarrow BE'F'}$  be an isometric quantum channel. Set*

$$\psi_{A'BB'E'E''F'F''} \equiv \mathcal{U}_{A \rightarrow BE'F'}(\phi_{A'AB'E''F''}), \quad (76)$$

and suppose that  $H(B)_\psi < \infty$ . Then the following inequality holds

$$I(A'; BB'|E'E'')_\psi \leq H(B|E')_\psi + H(B|F')_\psi + I(A'A; B'|E'')_\psi. \quad (77)$$

Note that both sides of the inequality in (77) could be equal to  $+\infty$ .

**Proof.** Let  $\{P_{B'}^k\}_k$  be a sequence of finite-rank projectors acting on the space  $\mathcal{H}_{B'}$ , which strongly converges to the identity  $I_{B'}$ . Define the sequence  $\{\phi_{A'AB'_kE''F''}^k\}_k$  of projected states as

$$\phi_{A'AB'_kE''F''}^k = \lambda_k^{-1} [(P_{B'}^k \otimes \bar{I}) \phi_{A'AB'E''F''} (P_{B'}^k \otimes \bar{I})], \quad (78)$$

where

$$\bar{I} \equiv I_{A'} \otimes I_A \otimes I_{E''} \otimes I_{F''}, \quad (79)$$

$$\lambda_k \equiv \text{Tr}\{(P_{B'}^k \otimes \bar{I}) \phi_{A'AB'E''F''}\}, \quad (80)$$

$$\lim_{k \rightarrow \infty} \lambda_k = 1. \quad (81)$$

This then leads to the following sequence of projected states:

$$\psi_{A'BB'_kE'E''F'F''}^k \equiv \mathcal{U}_{A \rightarrow BE'F'}(\phi_{A'AB'_kE''F''}^k). \quad (82)$$

Note that each state  $\psi_{A'BB'_kE'E''F'F''}^k$  is pure for all  $k \geq 1$ . Then the conditional entropy and the conditional mutual information of the sequence converge to those of the original state [51, 52]:

$$\lim_{k \rightarrow \infty} H(B|E')_{\psi^k} = H(B|E')_\psi, \quad (83)$$

$$\lim_{k \rightarrow \infty} H(B|F')_{\psi^k} = H(B|F')_\psi, \quad (84)$$

$$\lim_{k \rightarrow \infty} I(A'; BB'_k|E'E'')_{\psi^k} = I(A'; BB'|E'E'')_\psi, \quad (85)$$

$$\lim_{k \rightarrow \infty} I(A'A; B'_k|E'')_{\psi^k} = I(A'A; B'|E'')_\psi. \quad (86)$$

The limits in (83)–(84) follow because  $\lim_{k \rightarrow \infty} H(B)_\psi^k = H(B)_\psi < \infty$ , by applying [51, Lemma 2] and [52, Proposition 2]. The limits in (85)–(86) follow, with possible  $+\infty$  on the right-hand side, from the lower semicontinuity of conditional quantum mutual information and its monotonicity under local operations [51, Theorem 2].

Due to the fact that  $H(BB'_k)_\psi^k < \infty$  for all  $k \geq 1$ , we can write the CQMI of the state  $\psi_{A'BB'_kE'E''F'F''}^k$  in terms of conditional entropies as in (75) and then use the duality of conditional entropy as in (34) to find that

$$\begin{aligned} I(A'; BB'_k|E'E'')_{\psi^k} &= H(BB'_k|E'E'')_{\psi^k} - H(BB'_k|A'E'E'')_{\psi^k} \\ &= H(BB'_k|E'E'')_{\psi^k} + H(BB'_k|F'F'')_{\psi^k}. \end{aligned} \quad (87)$$

$$= H(BB'_k|E'E'')_{\psi^k} + H(BB'_k|F'F'')_{\psi^k}. \quad (88)$$

We then employ the subadditivity of conditional entropy from (35) to split up each of these two terms and regroup the resulting terms:

$$\begin{aligned} &H(BB'_k|E'E'')_{\psi^k} + H(BB'_k|F'F'')_{\psi^k} \\ &\leq H(B|E')_{\psi^k} + H(\bar{B}'_k|E'')_{\psi^k} + H(B|F')_{\psi^k} \\ &\quad + H(\bar{B}'_k|F'')_{\psi^k} \\ &= H(B|E')_{\psi^k} + H(B|F')_{\psi^k} \\ &\quad + H(\bar{B}'_k|E'')_{\psi^k} + H(\bar{B}'_k|F'')_{\psi^k}. \end{aligned} \quad (89)$$

$$+ H(\bar{B}'_k|E'')_{\psi^k} + H(\bar{B}'_k|F'')_{\psi^k}. \quad (90)$$

This is then recognizable as two conditional entropies from after the channel use added to the conditional mutual information from before the channel use:

$$I(A'; \overline{BB'_k} | E' E'')_{\psi^k} \leq H(B|E')_{\psi^k} + H(B|F')_{\psi^k} + I(A'A; \overline{B'_k} | E'')_{\phi^k} \quad (91)$$

Taking the limit  $k \rightarrow \infty$  of this expression and applying (83)–(86) gives the inequality stated in (77):

$$\begin{aligned} & I(A'; \overline{BB'} | E' E'')_{\psi} \\ &= \lim_{k \rightarrow \infty} I(A'; \overline{BB'_k} | E' E'')_{\psi^k} \\ &\leq \lim_{k \rightarrow \infty} [H(B|E')_{\psi^k} + H(B|F')_{\psi^k} + I(A'A; \overline{B'_k} | E'')_{\phi^k}] \\ &= H(B|E')_{\psi} + H(B|F')_{\psi} + I(A'A; \overline{B'} | E'')_{\phi}. \end{aligned} \quad (92)$$

This concludes the proof. ■

#### IV. ENERGY-CONSTRAINED SECRET-KEY-AGREEMENT CAPACITY

We now outline a protocol for energy-constrained secret key agreement between two parties Alice and Bob. The resources available to Alice and Bob in such a protocol are  $n$  uses of a quantum channel  $\mathcal{N}$  interleaved by rounds of LOCC. The energy constraint is such that the average energy of the  $n$  states input to each channel use should be bounded from above by a fixed positive real number, where the energy is with respect to a given energy observable. It is sensible to consider an energy constraint  $P$  for any such protocol in light of the fact that any real transmitter is necessarily power limited. A third party Eve has access to all of the classical information exchanged between Alice and Bob, as well as the environment of each of the  $n$  uses of the channel  $\mathcal{N}$ . For a photon-loss channel, the physical meaning of the latter assumption is that Eve retains all of the light that is lost along the way from Alice to Bob.

##### A. Secret-Key-Agreement Protocol with an Average Energy Constraint

We first recall the notion of an energy observable:

**Definition 1 (Energy Observable)** For a Hilbert space  $\mathcal{H}$ , let  $G \in \mathcal{L}_+(\mathcal{H})$  denote a positive semi-definite operator, defined in terms of its action on a vector  $|\psi\rangle$  as

$$G|\psi\rangle = \sum_{j=1}^{\infty} g_j |e_j\rangle \langle e_j | \psi\rangle, \quad (93)$$

for  $|\psi\rangle$  such that  $\sum_{j=1}^{\infty} g_j |\langle e_j | \psi\rangle|^2 < \infty$ . In the above,  $\{|e_j\rangle\}_j$  is an orthonormal basis and  $\{g_j\}_j$  is a sequence

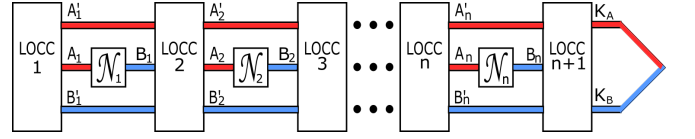


FIG. 1. A secret-key-agreement protocol begins with Alice and Bob preparing a separable state of systems  $A'_1 A_1 B'_1$  using LOCC. Alice then feeds the  $A_1$  system into the first channel use to generate the  $B_1$  system. After repeating this procedure  $n$  times, with rounds of LOCC interleaved between every channel use, Alice and Bob perform a final round of LOCC, which yields the key systems  $K_A$  and  $K_B$ .

of non-negative, real numbers. Then  $\{|e_j\rangle\}_j$  is an eigenbasis for  $G$  with corresponding eigenvalues  $\{g_j\}_j$ . We also follow the convention that

$$\text{Tr}\{G\rho\} = \sup_n \text{Tr}\{\Pi_n G \Pi_n \rho\}, \quad (94)$$

where  $\Pi_n$  is a spectral projector for  $G$  corresponding to the interval  $[0, n]$  [32, 67].

We now formally define an energy-constrained secret-key-agreement protocol. Fix  $n, K \in \mathbb{N}$ , an energy observable  $G$ , a positive real  $P \in [0, \infty)$ , and  $\varepsilon \in [0, 1]$ . An  $(n, K, G, P, \varepsilon)$  secret-key-agreement protocol invokes  $n$  uses of a quantum channel  $\mathcal{N}$ , with each channel use interleaved by a countably decomposable LOCC channel. Such a protocol generates an  $\varepsilon$ -approximate tripartite key state of dimension  $K$ . Furthermore, the average energy of the channel input states, with respect to the energy observable  $G$ , is no larger than  $P$ . Such a protocol is depicted in Figure 1.

In more detail, such a protocol begins with Alice and Bob performing an LOCC channel  $\mathcal{L}_{\emptyset \rightarrow A'_1 A_1 B'_1}^{(1)}$  to generate a state  $\rho_{A'_1 A_1 B'_1}^{(1)}$  that is separable with respect to the cut  $A'_1 A_1 | B'_1$ . Since the channel is a countably decomposable LOCC channel, the state  $\rho_{A'_1 A_1 B'_1}^{(1)}$  is a countably decomposable separable state, as considered in [28, Definition 1]. Alice then inputs the system  $A_1$  to the first channel use, resulting in the state

$$\sigma_{A'_1 B_1 B'_1}^{(1)} \equiv \mathcal{N}_{A_1 \rightarrow B_1}(\rho_{A'_1 A_1 B'_1}^{(1)}). \quad (95)$$

For now, we do not describe the systems that the eavesdropper obtains, and we only do so in the next subsection. Alice and Bob then perform a second LOCC channel, producing the state

$$\rho_{A'_2 A_2 B'_2}^{(2)} \equiv \mathcal{L}_{A'_1 B_1 B'_1 \rightarrow A'_2 A_2 B'_2}^{(2)}(\sigma_{A'_1 B_1 B'_1}^{(1)}). \quad (96)$$

Next, Alice feeds system  $A_2$  into the second channel use, which leads to the state

$$\sigma_{A'_2 B_2 B'_2}^{(2)} \equiv \mathcal{N}_{A_2 \rightarrow B_2}(\rho_{A'_2 A_2 B'_2}^{(2)}). \quad (97)$$

The procedure continues in this manner with a total of  $n$  rounds of LOCC interleaved with  $n$  uses of the channel as follows. For  $i \in \{2, \dots, n\}$ , the relevant states of the protocol are as follows:

$$\rho_{A'_i A_i B'_i}^{(i)} \equiv \mathcal{L}_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i B'_i}(\sigma_{A'_{i-1} B_{i-1} B'_{i-1}}^{(i-1)}), \quad (98)$$

$$\sigma_{A'_i B_i B'_i}^{(i)} \equiv \mathcal{N}_{A_i \rightarrow B_i}(\rho_{A'_i A_i B'_i}^{(i)}). \quad (99)$$

The primed systems correspond to separable Hilbert spaces. After the  $n$ th channel use, a final LOCC channel is performed to produce key systems  $K_A$  and  $K_B$  for Alice and Bob, respectively, such that the final state is as follows:

$$\omega_{K_A K_B} \equiv \mathcal{L}_{A'_n B_n B'_n \rightarrow K_A K_B}(\sigma_{A'_n B_n B'_n}^{(n)}). \quad (100)$$

The average energy of the  $n$  channel input states with respect to the energy observable  $G$  is constrained by  $P$  as follows:

$$\frac{1}{n} \sum_{i=1}^n \text{Tr}\{G \rho_{A_i}^{(i)}\} \leq P. \quad (101)$$

In the above,  $\rho_{A_i}^{(i)}$  is the marginal of the channel input states defined in (98).

One could alternatively demand a uniform bound on each channel input state, rather than a bound on the average energy. That is, one could demand that

$$\forall i \in \{1, \dots, n\} : \text{Tr}\{G \rho_{A_i}^{(i)}\} \leq P. \quad (102)$$

Such an energy constraint would lead to a slightly different notion of capacity, and we return to this point later in Section IV C.

## B. The Purified Protocol

We now consider the role of a third party Eve in a secret-key-agreement protocol. The initial state  $\rho_{A'_1 A_1 B'_1}^{(1)}$  is a separable state of the following form:

$$\rho_{A'_1 A_1 B'_1}^{(1)} \equiv \sum_{y_1} p_{Y_1}(y_1) \tau_{A'_1 A_1}^{y_1} \otimes \zeta_{B'_1}^{y_1}, \quad (103)$$

where  $Y_1$  is a classical random variable corresponding to the message exchanged between Alice and Bob, which is needed to establish this state. The state  $\rho_{A'_1 A_1 B'_1}^{(1)}$  can be purified as

$$|\rho^{(1)}\rangle_{A'_1 A_1 S_{A_1} B'_1 S_{B_1} Y_1} \equiv \sum_{y_1} \sqrt{p_{Y_1}(y_1)} |\tau^{y_1}\rangle_{A'_1 A_1 S_{A_1}} \otimes |\zeta^{y_1}\rangle_{B'_1 S_{B_1}} \otimes |y_1\rangle_{Y_1}, \quad (104)$$

where the local shield systems  $S_{A_1}$  and  $S_{B_1}$  are described by separable Hilbert spaces and in principle could be held by Alice and Bob, respectively,  $|\tau^{y_1}\rangle_{A'_1 A_1 S_{A_1}}$  and

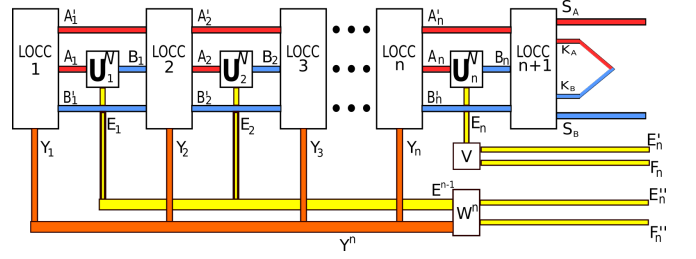


FIG. 2. Alice and Bob alternate rounds of LOCC and channel uses, just as in Figure 1. Each channel use is now purified, which yields outputs to Eve, the environment. Classical data is also collected by Eve from the LOCC. Eve's squashing channels are also purified and depicted above for the  $n$ th channel use.

$|\zeta^{y_1}\rangle_{B'_1 S_{B_1}}$  purify  $\tau_{A'_1 A_1}^{y_1}$  and  $\zeta_{B'_1}^{y_1}$ , respectively, and Eve possesses system  $Y_1$ , which contains a coherent classical copy of the classical data exchanged.

Each LOCC channel  $\mathcal{L}_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i B'_i}^{(i)}$  for  $i \in \{2, \dots, n\}$  is of the form in (11) as

$$\mathcal{L}_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i B'_i}^{(i)} = \sum_{y_i} \mathcal{E}_{A'_{i-1} \rightarrow A'_i A_i}^{y_i} \otimes \mathcal{F}_{B_{i-1} B'_{i-1} \rightarrow B'_i}^{y_i}, \quad (105)$$

and can be purified to an isometry in the following way:

$$U_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i S_{A_i} B'_i S_{B_i} Y_i}^{\mathcal{L}^{(i)}} \equiv \sum_{y_i} U_{A'_{i-1} \rightarrow A'_i A_i S_{A_i}}^{\mathcal{E}^{y_i}} \otimes U_{B_{i-1} B'_{i-1} \rightarrow B'_i S_{B_i}}^{\mathcal{F}^{y_i}} \otimes |y_i\rangle_{Y_i}, \quad (106)$$

where  $\{U_{A'_{i-1} \rightarrow A'_i A_i S_{A_i}}^{\mathcal{E}^{y_i}}\}_{y_i}$  and  $\{U_{B_{i-1} B'_{i-1} \rightarrow B'_i S_{B_i}}^{\mathcal{F}^{y_i}}\}_{y_i}$  are collections of linear operators (each of which is a contraction, that is,  $\|U_{A'_{i-1} \rightarrow A'_i A_i S_{A_i}}^{\mathcal{E}^{y_i}}\|_{\infty}, \|U_{B_{i-1} B'_{i-1} \rightarrow B'_i S_{B_i}}^{\mathcal{F}^{y_i}}\|_{\infty} \leq 1$ ) such that the linear operator in (106) is an isometry. The systems  $S_{A_i}$  and  $S_{B_i}$  are shield systems belonging to Alice and Bob, respectively, and  $Y_i$  is a system held by Eve, containing a coherent classical copy of the classical data exchanged in this round. So a purification of the state  $\rho_{A'_i A_i B'_i}^{(i)}$  after each LOCC channel is as follows:

$$|\rho^{(i)}\rangle_{A'_i A_i S_{A_i} B'_i S_{B_i} E_1^{i-1} Y_1^i} \equiv U_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i S_{A_i} B'_i S_{B_i} Y_i}^{\mathcal{L}^{(i)}} |\sigma^{(i-1)}\rangle_{A'_{i-1} B_{i-1} B'_{i-1} S_{A_1^{i-1}} S_{B_1^{i-1}} E_1^{i-1} Y_1^{i-1}}, \quad (107)$$

where we have employed the shorthands  $S_{A_i} \equiv S_{A_1} \cdots S_{A_i}$  and  $S_{B_i} \equiv S_{B_1} \cdots S_{B_i}$ , with a similar shorthand for  $E_1^{i-1}$  and  $Y_1^i$ . A purification of the state  $\sigma_{A'_i B'_i}^{(i)}$

after each use of the channel  $\mathcal{N}_{A \rightarrow B}$  is

$$|\sigma^{(i)}\rangle_{A'_i B_i S_{A'_i} B'_i S_{B'_i} E'_i Y_1^i} \equiv U_{A'_i \rightarrow B_i E_i}^{\mathcal{N}} |\rho^{(i)}\rangle_{A'_i A_i S_{A'_i} B'_i S_{B'_i} E_1^{i-1} Y_1^i}, \quad (108)$$

where  $U_{A'_i \rightarrow B_i E_i}^{\mathcal{N}}$  is an isometric extension of  $i$ th channel use  $\mathcal{N}_{A_i \rightarrow B_i}$ . The final LOCC channel also takes the form in (11)

$$\mathcal{L}_{A'_n B_n B'_n \rightarrow K_A K_B}^{(n+1)} = \sum_{y_{n+1}} \mathcal{E}_{A'_n \rightarrow K_A}^{y_{n+1}} \otimes \mathcal{F}_{B_n B'_n \rightarrow K_B}^{y_{n+1}}, \quad (109)$$

and it can be purified to an isometry similarly as

$$\begin{aligned} & U_{A'_n B_n B'_n \rightarrow K_A S_{A_{n+1}} K_B S_{B_{n+1}} Y_{n+1}}^{\mathcal{L}^{(n+1)}} \\ \equiv & \sum_{y_{n+1}} U_{A'_n \rightarrow K_A S_{A_{n+1}}}^{\mathcal{E}^{y_{n+1}}} \otimes U_{B_n B'_n \rightarrow K_B S_{B_{n+1}}}^{\mathcal{F}^{y_{n+1}}} \otimes |y_{n+1}\rangle_{Y_{n+1}}. \end{aligned} \quad (110)$$

The systems  $S_{A_{n+1}}$  and  $S_{B_{n+1}}$  are again shield systems belonging to Alice and Bob, respectively, and  $Y_{n+1}$  is a system held by Eve, containing a coherent classical copy of the classical data exchanged in this round. As written above, each channel use  $\mathcal{N}_{A_i \rightarrow B_i}$  can be purified, as in (6) and (7), to an isometric channel  $\mathcal{U}_{A_i \rightarrow B_i E_i}^{\mathcal{N}}$  such that Eve possesses system  $E_i$  for all  $i \in \{1, \dots, n\}$ .

The final state at the end of the purified protocol is a pure state  $|\omega\rangle_{K_A S_A K_B S_B E^n Y^{n+1}}$ , given by

$$|\omega\rangle_{K_A S_A K_B S_B E^n Y^{n+1}} = U_{A'_n B_n B'_n \rightarrow K_A S_{A_{n+1}} K_B S_{B_{n+1}} Y_{n+1}}^{\mathcal{L}^{(n+1)}} |\sigma^{(n)}\rangle_{A'_n B_n S_{A'_n} B'_n S_{B'_n} E_1^n Y_1^n}. \quad (111)$$

Alice is in possession of the key system  $K_A$  and the shield systems  $S_A \equiv S_{A_1} \dots S_{A_{n+1}}$ , Bob possesses the key system  $K_B$  and the shield systems  $S_B \equiv S_{B_1} \dots S_{B_{n+1}}$ , and Eve holds the environment systems  $E^n \equiv E_1 \dots E_n$ . The  $S_A$ ,  $S_B$ , and  $E^n$  systems all correspond to separable Hilbert spaces of generally infinite dimensions. Additionally, Eve has coherent copies  $Y^{n+1} \equiv Y_1 \dots Y_{n+1}$  of all the classical data exchanged. By tracing over the systems  $E^n$  and  $Y^{n+1}$ , it is clear that the protocol is an LOCC-assisted protocol whose aim is to generate an approximate bipartite private state on the systems  $K_A S_A K_B S_B$ .

For a fixed  $n, K \in \mathbb{N}$  and  $\varepsilon \in [0, 1]$ , the protocol is an  $(n, K, G, P, \varepsilon)$  secret-key-agreement protocol if the final state  $\omega_{K_A S_A K_B S_B}$  satisfies

$$F(\omega_{K_A S_A K_B S_B}, \gamma_{K_A S_A K_B S_B}) \geq 1 - \varepsilon, \quad (112)$$

where  $\gamma_{K_A S_A K_B S_B}$  is a bipartite private state as in (66). Alternatively (and equivalently), the criterion is that the final state  $\omega_{K_A K_B E^n Y^{n+1}}$  satisfies

$$F(\omega_{K_A K_B E^n Y^{n+1}}, \gamma_{K_A K_B E^n Y^{n+1}}) \geq 1 - \varepsilon, \quad (113)$$

where  $\gamma_{K_A K_B E^n Y^{n+1}}$  is a tripartite key state as in (64).

### C. Achievable Rates and Energy-Constrained Secret-Key-Agreement Capacity

The rate  $R = \frac{\log_2 K}{n}$  is a measure of the efficiency of the protocol, measured in secret key bits communicated per channel use. We say that the rate  $R$  is achievable if, for all  $\varepsilon \in (0, 1)$ ,  $\delta > 0$ , and for sufficiently large  $n$ , there exists an  $(n, 2^{n(R-\delta)}, G, P, \varepsilon)$  secret-key-agreement protocol.

We call  $P_2(\mathcal{N}, G, P)$  the energy-constrained secret-key-agreement capacity of the channel  $\mathcal{N}$ , and it is equal to the supremum of all achievable rates subject to the energy constraint  $P$  with respect to the energy observable  $G$ .

As discussed previously in Section IV A, one could have a modified notion of energy-constrained communication based on a uniform energy constraint, and this would lead to a different definition of capacity. However, it is clear from the definitions that for the same parameters  $n, G, P$ , and  $\varepsilon$ , the number of secret key values  $K$  can only be the same or larger for a protocol having an average energy constraint, when compared to one that has a uniform energy constraint (simply because meeting the average energy constraint implies that the uniform energy constraint is met). Accordingly, the capacity with a uniform energy constraint can never exceed that with an average energy constraint. Since one of the main results of our paper is to obtain upper bounds on the (average) energy-constrained capacities, our results are much stronger than they would be had we only reported upper bounds on the uniform energy-constrained capacities.

### D. Energy-Constrained LOCC-assisted Quantum Communication

We define the energy-constrained LOCC-assisted quantum capacity  $Q_2(\mathcal{N}, G, P)$  of a channel  $\mathcal{N}$  similarly. In this case, an  $(n, K, G, P, \varepsilon)$  energy-constrained LOCC-assisted quantum communication protocol is defined similarly as in Section IV A, but the main difference is that the final state  $\omega_{K_A K_B}$  should satisfy the following inequality:

$$F(\omega_{K_A K_B}, \Phi_{AB}) \geq 1 - \varepsilon, \quad (114)$$

where  $\Phi_{AB}$  is a maximally entangled state. Achievable rates are defined similarly as in the previous subsection, and the energy-constrained LOCC-assisted quantum capacity  $Q_2(\mathcal{N}, G, P)$  of the channel  $\mathcal{N}$  is defined to be equal to the supremum of all achievable rates.

It is worthwhile to note that the end goal of an LOCC-assisted quantum communication protocol is more difficult to achieve than a secret-key-agreement protocol for the same channel  $\mathcal{N}$ , energy observable  $G$ , energy constraint  $P$ , number  $n$  of channel uses, and error parameter  $\varepsilon$ . This is because a maximally entangled state  $\Phi_{K_A K_B}$  is a very particular kind of bipartite private state

$\gamma_{K_A S_A K_B S_B}$ , as observed in [62, 63]. Given this observation, it immediately follows that the energy-constrained LOCC-assisted quantum capacity is bounded from above by the energy-constrained secret-key-agreement capacity:

$$Q_2(\mathcal{N}, G, P) \leq P_2(\mathcal{N}, G, P). \quad (115)$$

## V. ENERGY-CONSTRAINED SQUASHED ENTANGLEMENT IS AN UPPER BOUND ON ENERGY-CONSTRAINED SECRET-KEY-AGREEMENT CAPACITY

The main goal of this section is to prove that the energy-constrained squashed entanglement of a quantum channel is an upper bound on its energy-constrained secret-key-agreement capacity. Before doing so, we recall the notion of a Gibbs observable [32, 67–71] and the finite output-entropy condition [32, 68, 69] for quantum channels.

**Definition 2 (Gibbs Observable)** *An energy observable  $G$  is a Gibbs observable if*

$$\text{Tr}\{\exp(-\beta G)\} < \infty \quad (116)$$

for all  $\beta > 0$ .

This condition implies that there exists a well defined thermal state for  $G$ , having the following form for all  $\beta > 0$  [72] (see also [68, 70]):

$$e^{-\beta G} / \text{Tr}\{e^{-\beta G}\}. \quad (117)$$

**Condition 1 (Finite Output Entropy)** *Let  $G$  be a Gibbs observable as in Definition 2, and let  $P \in [0, \infty)$  be an energy constraint. A quantum channel  $\mathcal{N}$  satisfies the finite output-entropy condition with respect to  $G$  and  $P$  if [32, 68, 69]*

$$\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\mathcal{N}(\rho)) < \infty. \quad (118)$$

If a channel  $\mathcal{N}$  satisfies the finite output-entropy condition with respect to  $G$  and  $P$ , then any complementary channel  $\hat{\mathcal{N}}$  of  $\mathcal{N}$  also satisfies the condition [23]:

$$\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\hat{\mathcal{N}}(\rho)) < \infty. \quad (119)$$

**Lemma 3** *Finiteness of the output entropy of a channel  $\mathcal{N}$  implies finiteness of the squashed entanglement of that channel. That is, if*

$$\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\mathcal{N}(\rho)) < \infty \quad (120)$$

holds, then

$$E_{\text{sq}}(\mathcal{N}) < \infty. \quad (121)$$

**Proof.** The statement is a consequence of (27). Indeed, Applying the definition of squashed entanglement and picking the extension system  $E$  to be trivial, we then get that

$$E_{\text{sq}}(A; B)_\omega \leq \frac{1}{2} I(A; B)_\omega. \quad (122)$$

Applying Condition 1 to (27) and combining (122) with the definition in (44) yields the statement of the lemma. ■

We now establish the following weak-converse bound that applies to an arbitrary  $(n, K, G, P, \varepsilon)$  energy-constrained secret-key-agreement protocol.

**Proposition 1** *Let  $\mathcal{N}$  be a quantum channel satisfying the finite output-entropy condition (Condition 1), let  $G$  be a Gibbs observable as in Definition 2, and let  $P \in [0, \infty)$  be an energy constraint. Fix  $n, K \in \mathbb{N}$  and  $\varepsilon \in (0, 1)$ . Then an  $(n, K, G, P, \varepsilon)$  energy-constrained secret-key-agreement protocol for  $\mathcal{N}$  is subject to the following upper bound in terms of the energy-constrained squashed entanglement of the channel  $\mathcal{N}$ :*

$$\frac{1 - 2\sqrt{\varepsilon}}{n} \log_2 K \leq E_{\text{sq}}(\mathcal{N}, G, P) + \frac{2}{n} g(\sqrt{\varepsilon}), \quad (123)$$

where  $g(\cdot)$  is defined in (63).

**Proof.** By assumption, the final state  $\omega_{K_A S_A K_B S_B}$  of any  $(n, K, G, P, \varepsilon)$  secret-key-agreement protocol is an  $\varepsilon$ -approximate bipartite private state, as given in (112). Thus, the bound in (71) applies, leading to the following bound:

$$\log_2 K \leq E_{\text{sq}}(K_A S_A; K_B S_B)_\omega + 2\sqrt{\varepsilon} \log_2 K + 2g(\sqrt{\varepsilon}). \quad (124)$$

Let  $\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}$  be an isometric channel extending the original channel  $\mathcal{N}_{A \rightarrow B}$ . Let  $V_{E \rightarrow E'F}^S$  denote an isometric extension of a squashing channel that can act on the environment system  $E$  of the isometric channel  $\mathcal{U}_{A \rightarrow BE}^{\mathcal{N}}$ , and let  $W_{E_1^{n-1} Y^n \rightarrow E''_n F''_n}$  denote an isometric extension of a squashing channel that can act on the systems  $E^{n-1} Y^n$ . Then we define the states

$$\begin{aligned} |\tau^{(n)}\rangle_{A'_n B_n S_{A_1^n} B'_n S_{B_1^n} E'_n F_n E''_n F''_n} &\equiv \\ &(V_{E_n \rightarrow E'_n F_n}^S \otimes W_{E_1^{n-1} Y^n \rightarrow E''_n F''_n}) \times \\ &|\sigma^{(n)}\rangle_{A'_n B_n S_{A_1^n} B'_n S_{B_1^n} E_1^n Y_1^n}, \end{aligned} \quad (125)$$

and

$$\begin{aligned} |\zeta^{(n)}\rangle_{A'_n A_n S_{A_1^n} B'_n S_{B_1^n} E''_n F''_n} &\equiv W_{E_1^{n-1} Y^n \rightarrow E''_n F''_n} \times \\ &|\rho^{(n)}\rangle_{A'_n A_n S_{A_1^n} B'_n S_{B_1^n} E_1^{n-1} Y_1^n}. \end{aligned} \quad (126)$$

We invoke the LOCC monotonicity of squashed entanglement and the definition of squashed entanglement from (41), as well as Lemma 2, to find that

$$2E_{\text{sq}}(K_A S_A; K_B S_B)_\omega \leq 2E_{\text{sq}}(A'_n S_{A_1^n}; B_n S_{B_1^n} B'_n)_{\sigma^{(n)}} \quad (127)$$

$$\leq I(A'_n S_{A_1^n}; B_n B'_n S_{B_1^n} | E'_n E''_n)_{\tau^{(n)}} \quad (128)$$

$$\leq H(B_n | E'_n)_{\tau^{(n)}} + H(B_n | F_n)_{\tau^{(n)}} \\ I(A'_n S_{A_1^n} A_n; B'_n S_{B_1^n} | E''_n)_{\zeta^{(n)}}. \quad (129)$$

The conditions needed to apply Lemma 2 indeed hold, following by hypothesis from (101) and the finite output-entropy condition. Since the isometric extension  $W_{E^{n-1} Y^n \rightarrow E''_n F''_n}$  of a squashing channel is an arbitrary choice, the inequality above holds for the infimum over all such squashing channel extensions, and we find that

$$E_{\text{sq}}(A'_n S_{A_1^n}; B_n S_{B_1^n} B'_n)_{\sigma^{(n)}} \leq \frac{1}{2} [H(B_n | E'_n)_{\tau^{(n)}} + H(B_n | F_n)_{\tau^{(n)}}] \\ + E_{\text{sq}}(A'_n S_{A_1^n} A_n; B'_n S_{B_1^n})_{\rho^{(n)}}. \quad (130)$$

We can then again invoke the LOCC monotonicity of squashed entanglement to find that

$$E_{\text{sq}}(A'_n S_{A_1^n} A_n; B'_n S_{B_1^n})_{\rho^{(n)}} \leq E_{\text{sq}}(A'_{n-1} S_{A_1^{n-1}}; B_{n-1} B'_{n-1} S_{B_1^{n-1}})_{\sigma^{(n-1)}}. \quad (131)$$

Now repeating the above reasoning  $n-1$  more times (applying Lemma 2 and LOCC monotonicity of squashed entanglement iteratively), we find that

$$2E_{\text{sq}}(K_A S_A; K_B S_B)_\omega \leq \sum_{i=1}^n [H(B_i | E'_i)_{\tau^{(i)}} + H(B_i | F_i)_{\tau^{(i)}}] \\ + 2E_{\text{sq}}(A'_1 A_1; B'_1)_{\rho^{(1)}} \quad (132)$$

$$= \sum_{i=1}^n [H(B_i | E'_i)_{\tau^{(i)}} + H(B_i | F_i)_{\tau^{(i)}}] \quad (133)$$

$$= n \frac{1}{n} \sum_{i=1}^n [H(B_i | E'_i)_{\tau^{(i)}} + H(B_i | F_i)_{\tau^{(i)}}] \quad (134)$$

$$\leq n [H(B | E')_{\bar{\tau}} + H(B | F)_{\bar{\tau}}]. \quad (135)$$

The first equality follows because the state  $\rho_{A'_1 A_1 B'_1}^{(1)}$  is separable, being the result of the initial LOCC, and so  $E_{\text{sq}}(A'_1 A_1; B'_1)_{\rho^{(1)}} = 0$ . Note here that we are invoking the assumption that the protocol begins with a countably decomposable separable state [28, Definition 1] and the fact that  $E_{\text{sq}} = 0$  for such states [28, Proposition 2]. The last inequality follows from the concavity of conditional entropy [52], defining  $\bar{\tau}_{BE'F}$  as the average output state of the channel:

$$\bar{\tau}_{BE'F} \equiv \frac{1}{n} \sum_{i=1}^n \mathcal{V}_{E_i \rightarrow E'_i F_i}^{\mathcal{S}}(\sigma_{B_i E_i}^{(i)}). \quad (136)$$

Since the inequality above holds for an arbitrary choice of the isometric channel  $\mathcal{V}_{E \rightarrow E' F}^{\mathcal{S}}$  extending a squashing channel, and the average channel input state for the protocol satisfies the energy constraint in (101) by assumption, we find that

$$E_{\text{sq}}(K_A S_A; K_B S_B)_\omega \leq n \inf_{\mathcal{V}_{E \rightarrow E' F}^{\mathcal{S}}} \frac{1}{2} [H(B | E')_{\bar{\tau}} + H(B | F)_{\bar{\tau}}] \quad (137)$$

$$\leq n E_{\text{sq}}(\mathcal{N}, G, P), \quad (138)$$

where we have employed the alternative representation of squashed entanglement from (49). Now combining (124) and (138), we conclude the proof. ■

By applying Proposition 1 and taking the limit as  $n \rightarrow \infty$  and then as  $\varepsilon \rightarrow 0$ , we arrive at the following theorem:

**Theorem 4** *Let  $\mathcal{N}$  be a quantum channel satisfying the finite output-entropy condition (Condition 1), let  $G$  be a Gibbs observable as in Definition 2, and let  $P \in [0, \infty)$  be an energy constraint. Then the energy-constrained squashed entanglement of the channel  $\mathcal{N}$  is an upper bound on its energy-constrained secret-key-agreement capacity:*

$$P_2(\mathcal{N}, G, P) \leq E_{\text{sq}}(\mathcal{N}, G, P). \quad (139)$$

Immediate consequences of Proposition 1 and Theorem 4 are bounds for rates of LOCC-assisted quantum communication. Indeed, let  $\mathcal{N}$  be a quantum channel satisfying the finite output-entropy condition (Condition 1), let  $G$  be a Gibbs observable as in Definition 2, and let  $P \in [0, \infty)$  be an energy constraint. Fix  $n, K \in \mathbb{N}$  and  $\varepsilon \in (0, 1)$ . Then an  $(n, K, G, P, \varepsilon)$  energy-constrained LOCC-assisted quantum communication protocol for  $\mathcal{N}$  is subject to the following upper bound in terms of its energy-constrained squashed entanglement:

$$\frac{1 - 2\sqrt{\varepsilon}}{n} \log_2 K \leq E_{\text{sq}}(\mathcal{N}, G, P) + \frac{2}{n} g(\sqrt{\varepsilon}). \quad (140)$$

Then this implies that

$$Q_2(\mathcal{N}, G, P) \leq E_{\text{sq}}(\mathcal{N}, G, P). \quad (141)$$

## VI. BOUNDS ON ENERGY-CONSTRAINED SECRET-KEY-AGREEMENT CAPACITIES OF PHASE-INSENSITIVE QUANTUM GAUSSIAN CHANNELS

The main result of Section V is that the energy-constrained squashed entanglement is an upper bound on the energy-constrained secret-key-agreement capacity of quantum channels that satisfy the finite output-entropy condition with respect to a given Gibbs observable. In this section, we specialize this result to particular phase-insensitive bosonic Gaussian channels that accept as input a single mode and output multiple modes. We prove

here that a relaxation of the energy-constrained squashed entanglement of these channels is optimized by a thermal state input (when the squashed entanglement is written with respect to the representation in (49)). Our results in this section thus generalize statements from prior works in [5, 7, 17].

We also note the following point here before proceeding with the technical development. The prior works [5, 7, 17] argued that a thermal-state input should be the optimal choice for a particular relaxation of the energy-constrained squashed entanglement. However, it appears that these works have not given a full justification of these claims. In particular, [5, 17] appealed only to the extremality of Gaussian states [73] to argue that a thermal state should be optimal. However, it is necessary to argue that, among all Gaussian states, the thermal state is optimal. In [7], arguments about covariance of single-mode phase-insensitive Gaussian channels with respect to displacements and squeezing unitaries were given, but there was not an explicit proof of the latter covariance with respect to the squeezers, and furthermore, the squeezing unitaries can change the energy of the input state. Thus, in light of these questionable aspects, it seems worthwhile to provide a clear proof of the optimality of the thermal-state input, and our development in this section accomplishes this goal. The approach taken here is strongly related to that given in Section 5.2 and Remark 21 of [74].

### A. Single-Mode, Phase-Insensitive Bosonic Gaussian Channels and Their Properties

We begin in what follows by considering the argument for the particular case of phase-insensitive single-mode bosonic Gaussian channels. Three classes of channels of primary interest are thermal, amplifier, and additive-noise channels.

A thermal channel can be described succinctly in terms of the following Heisenberg-picture evolution:

$$\hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}, \quad (142)$$

where  $\hat{a}$ ,  $\hat{b}$ , and  $\hat{e}$  represent respective bosonic annihilation operators for the sender, receiver, and environment. The parameter  $\eta \in (0, 1)$  represents the transmissivity of the channel, and the state of the environment is a bosonic thermal state  $\theta(N_B)$  of the following form:

$$\theta(N_B) \equiv \frac{1}{N_B + 1} \sum_{n=0}^{\infty} \left( \frac{N_B}{N_B + 1} \right)^n |n\rangle\langle n|, \quad (143)$$

where  $N_B \geq 0$  is the mean photon number of the above thermal state. So a thermal channel is characterized by two parameters:  $\eta \in (0, 1)$  and  $N_B \geq 0$ . If  $N_B = 0$ , then the channel is called a pure-loss channel because the environment state is prepared in a vacuum state and the only corruption of the input signal is due to loss. An

alternate description of a thermal channel in terms of its Kraus operators is available in [75], and in what follows, we denote it by  $\mathcal{L}_{\eta, N_B}$ .

It is helpful to consider a unitary extension of a thermal channel. That is, we can consider a thermal channel arising as the result of a beamsplitter interaction between the input mode and the thermal-state environment mode, followed by a partial trace over the output environment mode. We can represent this interaction in the Heisenberg picture as follows:

$$\begin{aligned} \hat{b} &= \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e}, \\ \hat{e}' &= -\sqrt{1-\eta}\hat{a} + \sqrt{\eta}\hat{e}, \end{aligned} \quad (144)$$

where  $\hat{e}'$  denotes the output environment mode. Let  $U^{\mathcal{L}_{\eta, N_B}}$  denote the Schrödinger-picture, two-mode unitary describing this interaction. It is well known that this unitary obeys the following phase covariance symmetry for all  $\phi \in \mathbb{R}$ :

$$U^{\mathcal{L}_{\eta, N_B}} e^{i\hat{n}_{AE}\phi} = e^{i\hat{n}_{BE'}\phi} U^{\mathcal{L}_{\eta, N_B}}, \quad (145)$$

where  $\hat{n}_{AE} = \hat{n}_A + \hat{n}_E$  is the total photon number operator for the input mode  $A$  and environment mode  $E$ , while  $\hat{n}_{BE'} = \hat{n}_B + \hat{n}_{E'}$  is that for the output mode  $B$  and the output environment mode  $E'$ . Thus, we can equivalently write the above phase covariance symmetry as

$$U^{\mathcal{L}_{\eta, N_B}} (e^{i\hat{n}_A\phi} \otimes e^{i\hat{n}_E\phi}) = (e^{i\hat{n}_B\phi} \otimes e^{i\hat{n}_{E'}\phi}) U^{\mathcal{L}_{\eta, N_B}}. \quad (146)$$

Due to this relation, the fact that a thermal state is phase invariant (i.e.,  $e^{i\hat{n}_E\phi}\theta(N_B)e^{-i\hat{n}_E\phi} = \theta(N_B)$ ), and the fact that the thermal channel results from a partial trace after the unitary transformation  $U^{\mathcal{L}_{\eta, N_B}}$ , it follows that the thermal channel is phase covariant in the following sense:

$$\mathcal{L}_{\eta, N_B} (e^{i\hat{n}_A\phi} \rho_A e^{-i\hat{n}_A\phi}) = e^{i\hat{n}_B\phi} \mathcal{L}_{\eta, N_B} (\rho_A) e^{-i\hat{n}_B\phi}, \quad (147)$$

where  $\rho_A$  is an arbitrary input state. This is the reason that thermal channels are called phase-insensitive.

Another class of channels to consider are amplifier channels. An amplifier channel can also be described succinctly in terms of the following Heisenberg-picture evolution:

$$\hat{b} = \sqrt{\mathcal{G}}\hat{a} + \sqrt{\mathcal{G}-1}\hat{e}^\dagger, \quad (148)$$

where  $\hat{a}$ ,  $\hat{b}$ , and  $\hat{e}$  again represent respective bosonic annihilation operators for the sender, receiver, and environment. The parameter  $\mathcal{G} \in (1, \infty)$  represents the gain of the channel, and the state of the environment is a bosonic thermal state  $\theta(N_B)$  with  $N_B \geq 0$ . So an amplifier channel is characterized by two parameters:  $\mathcal{G} \in (1, \infty)$  and  $N_B \geq 0$ . If  $N_B = 0$ , then the channel is called a pure-amplifier channel because the environment state is prepared in a vacuum state and the only corruption of the input signal is due to amplification, which inevitably introduces noise due to the no-cloning theorem [76]. An alternate description of an amplifier channel in terms of



its Kraus operators is available in [75], and in what follows, we denote it by  $\mathcal{A}_{\mathcal{G}, N_B}$ .

It is again helpful to consider a unitary extension of an amplifier channel. That is, we can consider an amplifier channel arising as the result of a two-mode squeezer interaction between the input mode and the thermal-state environment mode, followed by a partial trace over the output environment mode. We can represent this interaction in the Heisenberg picture as follows:

$$\begin{aligned}\hat{b} &= \sqrt{\mathcal{G}}\hat{a} + \sqrt{\mathcal{G}-1}e^\dagger, \\ \hat{e}' &= \sqrt{\mathcal{G}-1}\hat{a}^\dagger + \sqrt{\mathcal{G}}\hat{e},\end{aligned}\quad (149)$$

where  $\hat{e}'$  denotes the output environment mode. Let  $U^{\mathcal{A}_{\mathcal{G}, N_B}}$  denote the Schrödinger-picture, two-mode unitary describing this interaction. It is well known that this unitary obeys the following phase covariance symmetry for all  $\phi \in \mathbb{R}$

$$U^{\mathcal{A}_{\mathcal{G}, N_B}}(e^{i\hat{n}_A\phi} \otimes e^{-i\hat{n}_E\phi}) = (e^{i\hat{n}_B\phi} \otimes e^{-i\hat{n}_{E'}\phi})U^{\mathcal{A}_{\mathcal{G}, N_B}}. \quad (150)$$

Due to this relation, the fact that a thermal state is phase invariant, and the fact that the amplifier channel results from a partial trace of the unitary transformation  $U^{\mathcal{A}_{\mathcal{G}, N_B}}$ , it follows that the amplifier channel is phase covariant in the following sense:

$$\mathcal{A}_{\mathcal{G}, N_B}(e^{i\hat{n}_A\phi}\rho_A e^{-i\hat{n}_A\phi}) = e^{i\hat{n}_B\phi}\mathcal{A}_{\mathcal{G}, N_B}(\rho_A)e^{-i\hat{n}_B\phi}, \quad (151)$$

where  $\rho_A$  is an arbitrary input state. So amplifier channels are also called phase-insensitive.

Another class of single-mode, phase-insensitive bosonic Gaussian channels are called additive-noise channels. These channels are easily described in the Schrödinger picture and are characterized by a single parameter  $\xi \geq 0$ , which is the variance of the channel. Additive-noise channels can be written as the following transformation:

$$\rho_A \rightarrow \int d^2\alpha \frac{\exp(-|\alpha|^2/\xi)}{\pi\xi} D(\alpha)\rho_A D(-\alpha), \quad (152)$$

and can be interpreted as applying a unitary displacement operator  $D(\alpha)$  randomly chosen according to a complex, isotropic Gaussian distribution  $\frac{\exp(-|\alpha|^2/\xi)}{\pi\xi}$  of variance  $\xi$ . These channels are phase-covariant as well and are thus phase-insensitive.

A well known theorem from [77, 78] establishes that any single-mode, phase-insensitive bosonic Gaussian channel  $\mathcal{N}$  can be written as the serial concatenation of a pure-loss channel  $\mathcal{L}_{T,0}$  of transmissivity  $T \in [0, 1]$  followed by a pure-amplifier channel  $\mathcal{A}_{\mathcal{G},0}$  of gain  $\mathcal{G} > 1$ :

$$\mathcal{N} = \mathcal{A}_{\mathcal{G},0} \circ \mathcal{L}_{T,0}. \quad (153)$$

This theorem has been extremely helpful in obtaining good upper bounds on various capacities of single-mode, phase-insensitive bosonic Gaussian channels [5, 7, 17, 74, 79–82].

## B. Bounds for Single-Mode, Phase-Insensitive Bosonic Gaussian Channels

In the following theorem, we prove that a thermal input state is the optimal state for a relaxation of the energy-constrained squashed entanglement of a single-mode, phase-insensitive bosonic Gaussian channel. This in turn gives an upper bound on the energy-constrained secret-key-agreement capacities of these channels, which has already been claimed in [5, 7, 17].

**Theorem 5** *Let  $\mathcal{N}$  be a single-mode, phase-insensitive bosonic Gaussian channel as in (153). Then its energy-constrained squashed entanglement is bounded as*

$$E_{\text{sq}}(\mathcal{N}, \hat{n}, N_S) \leq \frac{1}{2}[H(B|E'_1E'_2)_\omega + H(B|F'_1F'_2)_\omega], \quad (154)$$

where  $\hat{n}$  is the photon number operator acting on the channel input mode,  $N_S \geq 0$  is an energy constraint,  $\omega_{BE'_1E'_2F'_1F'_2}$  is the following state:

$$\omega_{BE'_1E'_2F'_1F'_2} = \mathcal{W}_{A \rightarrow BE'_1E'_2F'_1F'_2}(\theta(N_S)), \quad (155)$$

and  $\mathcal{W}$  is an isometric channel of the form

$$\begin{aligned}\mathcal{W}_{A \rightarrow BE'_1E'_2F'_1F'_2} &= (\mathcal{V}_{E_2 \rightarrow E'_2F'_2}^A \circ \mathcal{U}_{B_1 \rightarrow BE_2}^{\mathcal{A}_{\mathcal{G},0}}) \\ &\quad \circ (\mathcal{V}_{E_1 \rightarrow E'_1F'_1}^{\mathcal{L}} \circ \mathcal{U}_{A \rightarrow B_1E_1}^{\mathcal{L}_{T,0}}).\end{aligned}\quad (156)$$

In the above,  $\mathcal{U}^{\mathcal{L}_{T,0}}$  is an isometric channel extending the pure-loss channel  $\mathcal{L}_{T,0}$  and realized from (144). Also,  $\mathcal{U}^{\mathcal{A}_{\mathcal{G},0}}$  is an isometric channel extending the pure-amplifier channel  $\mathcal{A}_{\mathcal{G},0}$  and realized from (149). Both  $\mathcal{V}_{E_1 \rightarrow E'_1F'_1}^{\mathcal{L}}$  and  $\mathcal{V}_{E_2 \rightarrow E'_2F'_2}^A$  are bosonic Gaussian isometric channels that are phase covariant. Figure 3 depicts an example of the isometric channel  $\mathcal{W}_{A \rightarrow BE'_1E'_2F'_1F'_2}$ .

An immediate consequence of Theorems 4 and 5 is the following corollary:

**Corollary 1** *With the same notation as in Theorem 5, the energy-constrained secret-key-agreement capacity of the channel  $\mathcal{N}$  is bounded as*

$$P_2(\mathcal{N}, \hat{n}, N_S) \leq \frac{1}{2}[H(B|E'_1E'_2)_\omega + H(B|F'_1F'_2)_\omega]. \quad (157)$$

**Proof of Theorem 5.** For convenience, we summarize the main steps of the proof here. We note that certain aspects of the proof bear some similarities to related approaches given in the literature [23, 32, 82], and the strongest overlap is with Remark 21 and Section 5.2 in [74].

1. First, we employ the representation of a channel's squashed entanglement in (49), and set  $\mathcal{U}_{B_1 \rightarrow BE_2}^{\mathcal{A}_{\mathcal{G},0}} \circ \mathcal{U}_{A \rightarrow B_1E_1}^{\mathcal{L}_{T,0}}$  to be the isometric extension of  $\mathcal{N} = \mathcal{A}_{\mathcal{G},0} \circ \mathcal{L}_{T,0}$ .

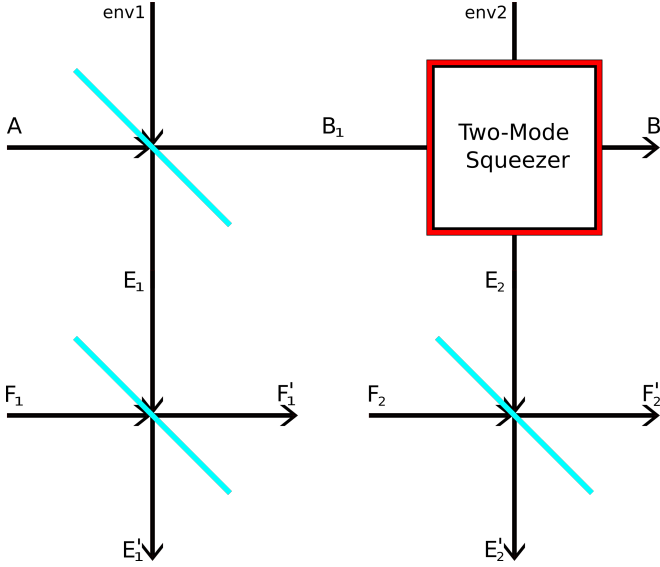


FIG. 3. A depiction of the isometric channel  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  from Theorem 5. Note that this is the precise construction used in [7]. As stated in Theorem 5, the isometric channel  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  is equal to  $(\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^A \circ \mathcal{U}_{B_1 \rightarrow BE_2}^{A_{g,0}}) \circ (\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^{\mathcal{L}} \circ \mathcal{U}_{A \rightarrow B_1 E_1}^{\mathcal{L}_{T,0}})$ . The modes labeled “env1” and “env2” are respective environmental modes for the isometric channels  $\mathcal{U}^{\mathcal{L}_{T,0}}$  (top left) and  $\mathcal{U}^{A_{g,0}}$  (top right) and are prepared in the pure vacuum state. The other isometric channels  $\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^{\mathcal{L}}$  (bottom left) and  $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^A$  (bottom right) are chosen here to be 50-50 beamsplitters, following [7]. The modes  $F_1$  and  $F_2$  are also prepared in the pure vacuum state. Given this setup, Theorem 5 states that, among all possible input states with mean photon number  $\leq N_S$ , the thermal state  $\theta(N_S)$  maximizes the entropy function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$ .

2. Then, we relax the infimum over all squashing isometries by setting it to be equal to  $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^{\mathcal{L}} \otimes \mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^A$ . This leads to the isometric channel  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  described in the theorem statement.
3. Next, we employ the extremality of Gaussian states [73] to conclude that the entropy objective function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$  is maximized when the input state to mode  $A$  is Gaussian.
4. We then employ the phase covariance of  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  and concavity of conditional entropy to conclude that, for input states having a fixed mean photon number  $N_S$ , the entropy objective function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$  is maximized when the input state to mode  $A$  is phase invariant.
5. Steps 3 and 4 imply that, for input states having a fixed mean photon number  $N_S$ , the optimal input state to mode  $A$  should be a thermal state  $\theta(N_S)$ .

This follows because  $\theta(N_S)$  is the unique single-mode state of fixed mean photon number  $N_S$  that is both Gaussian and phase invariant.

6. Finally, we use the displacement covariance of  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  and concavity of conditional entropy to conclude that the entropy objective function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$  is monotone with respect to  $N_S$ . This finally implies that  $\theta(N_S)$  is the optimal input state among all those having mean photon number  $\leq N_S$ .

Steps one through three do not require any further justification, and so we proceed to step four. In what follows, we take the isometric channels  $\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^{\mathcal{L}}$  and  $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^A$  to be 50-50 beamsplitters, following the heuristic from [7] (based on numerical evidence that these are the best choices among all local phase-insensitive Gaussian channels). Thus, the isometries are manifestly phase covariant. However, note that our argument applies to arbitrary phase-covariant, bosonic Gaussian isometries  $\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^{\mathcal{L}}$  and  $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^A$ .

Let  $\rho_A$  denote an arbitrary input state of mean photon number  $N_S$ . The state  $\rho_A$  can be input to the isometric channel  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$ . The entropy objective function  $H(B|E'_1 E'_2)_{\mathcal{W}(\rho)} + H(B|F'_1 F'_2)_{\mathcal{W}(\rho)}$  is equal to a sum of conditional entropies and so we make use of two properties of conditional entropy: its invariance under local unitaries and concavity. Set

$$\hat{N} \equiv \hat{n}_B + \hat{n}_{E'_1} - \hat{n}_{E'_2} + \hat{n}_{F'_1} - \hat{n}_{F'_2}, \quad (158)$$

and consider the following phase shift unitary, depending on a phase  $\phi \in \mathbb{R}$ :

$$e^{i\hat{N}\phi} \equiv e^{i\hat{n}_B\phi} \otimes e^{i\hat{n}_{E'_1}\phi} \otimes e^{-i\hat{n}_{E'_2}\phi} \otimes e^{i\hat{n}_{F'_1}\phi} \otimes e^{-i\hat{n}_{F'_2}\phi}. \quad (159)$$

Then it follows from the invariance of conditional entropy under local unitaries that

$$\begin{aligned} H(B|E'_1 E'_2)_{\mathcal{W}(\rho)} + H(B|F'_1 F'_2)_{\mathcal{W}(\rho)} \\ = H(B|E'_1 E'_2)_{e^{i\hat{N}\phi}\mathcal{W}(\rho)e^{-i\hat{N}\phi}} \\ + H(B|F'_1 F'_2)_{e^{i\hat{N}\phi}\mathcal{W}(\rho)e^{-i\hat{N}\phi}}. \end{aligned} \quad (160)$$

Now exploiting the phase covariance of all of the isometric channels involved in  $\mathcal{W}_{A \rightarrow BE'_1 E'_2 F'_1 F'_2}$  (see (146) and (150)), we find that the last line above is equal to

$$H(B|E'_1 E'_2)_{\mathcal{W}(e^{i\hat{n}\phi}\rho e^{-i\hat{n}\phi})} + H(B|F'_1 F'_2)_{\mathcal{W}(e^{i\hat{n}\phi}\rho e^{-i\hat{n}\phi})}. \quad (161)$$

These equalities hold for any phase  $\phi$  on the input, and so we can average over the input phase  $\phi$  without changing the entropy objective function:

$$\begin{aligned} H(B|E'_1 E'_2)_{\mathcal{W}(\rho)} + H(B|F'_1 F'_2)_{\mathcal{W}(\rho)} \\ = \frac{1}{2\pi} \int_0^{2\pi} d\phi \left[ H(B|E'_1 E'_2)_{\mathcal{W}(e^{i\hat{n}\phi}\rho e^{-i\hat{n}\phi})} \right. \\ \left. + H(B|F'_1 F'_2)_{\mathcal{W}(e^{i\hat{n}\phi}\rho e^{-i\hat{n}\phi})} \right]. \end{aligned} \quad (162)$$

Let us define the phase-invariant state  $\bar{\rho}_A$  as

$$\bar{\rho}_A \equiv \frac{1}{2\pi} \int_0^{2\pi} d\phi e^{i\hat{n}\phi} \rho_A e^{-i\hat{n}\phi}, \quad (163)$$

and note that the mean photon number of  $\bar{\rho}_A$  is equal to  $N_S$ , which follows from the assumption that  $\rho_A$  has mean photon number  $N_S$  and the fact that phase averaging does not change the mean photon number. Now exploiting the concavity of conditional entropy and the equality in (162), we find that

$$\begin{aligned} & H(B|E'_1 E'_2)_{\mathcal{W}(\rho)} + H(B|F'_1 F'_2)_{\mathcal{W}(\rho)} \\ & \leq H(B|E'_1 E'_2)_{\mathcal{W}(\bar{\rho})} + H(B|F'_1 F'_2)_{\mathcal{W}(\bar{\rho})}. \end{aligned} \quad (164)$$

By combining with step three (extremality of Gaussian states), we conclude that, for an arbitrary state  $\rho_A$  of mean photon number  $N_S$ , there exists a Gaussian, phase-invariant state that achieves the same or higher value of the entropy objective function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$ . So this completes step four, and step five is the next conclusion, which is that the thermal state  $\theta(N_S)$  maximizes the entropy objective function with respect to all input states with mean photon number equal to  $N_S$ .

We now move on to the final step six. In order to prove that the entropy objective function monotonically increases as a function of the mean photon number  $N_S$  of an input thermal state, we repeat steps similar to those above that we used for step four. Recall again that conditional entropy is invariant under local unitaries, and so we can apply arbitrary displacements without changing the entropy objective function. In particular, since the local displacements can be arbitrary, we take advantage of the specific covariances of beam splitters and two-mode squeezers from (144) and (149) when choosing the local displacements. We employ the following shorthand for the local displacements acting on the output modes of  $\mathcal{W}$ :

$$\begin{aligned} D_{\text{out}}^\alpha & \equiv D_B(\sqrt{T}\mathcal{G}\alpha) \otimes D_{E'_1}(\sqrt{\eta_2(1-T)}\alpha) \\ & \otimes D_{F'_1}(\sqrt{(1-\eta_2)(1-T)}\alpha) \\ & \otimes D_{E'_2}(\sqrt{\eta_3 T}(\mathcal{G}-1)\alpha^*) \\ & \otimes D_{F'_2}(\sqrt{(1-\eta_3)T}(\mathcal{G}-1)\alpha^*), \end{aligned} \quad (165)$$

where  $\eta_2$  and  $\eta_3$  are the transmissivities of the beamsplitters  $\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}^{\mathcal{L}}$  and  $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}^{\mathcal{A}}$ , respectively (here, however just set to 1/2 for both). Let  $\theta(N_1)$  be a thermal state of mean photon number  $N_1 \geq 0$ . Then we find that

$$\begin{aligned} & H(B|E'_1 E'_2)_{\mathcal{W}(\theta(N_1))} + H(B|F'_1 F'_2)_{\mathcal{W}(\theta(N_1))} \\ & = H(B|E'_1 E'_2)_{D_{\text{out}}^\alpha \mathcal{W}(\theta(N_1)) D_{\text{out}}^{\alpha\dagger}} \\ & \quad + H(B|F'_1 F'_2)_{D_{\text{out}}^\alpha \mathcal{W}(\theta(N_1)) D_{\text{out}}^{\alpha\dagger}}. \end{aligned} \quad (166)$$

Employing the displacement covariance of the isometric Gaussian channel  $\mathcal{W}$ , we recast the local displacements on the outputs as a displacement of the input state:

$$D_{\text{out}}^\alpha \mathcal{W}(\theta(N_1)) D_{\text{out}}^{\alpha\dagger} = \mathcal{W}(D_A(\alpha)\theta(N_1)D_A^\dagger(\alpha)). \quad (167)$$

Since this is true for any displacement  $\alpha$ , an expectation with respect to a probability distribution over  $\alpha$  does not change the quantity, and by combining with (166), we find that

$$\begin{aligned} & H(B|E'_1 E'_2)_{\mathcal{W}(\theta(N_1))} + H(B|F'_1 F'_2)_{\mathcal{W}(\theta(N_1))} \\ & = \int d^2\alpha p^{N_2}(\alpha) \left[ H(B|E'_1 E'_2)_{\mathcal{W}(D(\alpha)\theta(N_1)D^\dagger(\alpha))} \right. \\ & \quad \left. + H(B|F'_1 F'_2)_{\mathcal{W}(D(\alpha)\theta(N_1)D^\dagger(\alpha))} \right]. \end{aligned} \quad (168)$$

In the above, we choose the distribution  $p^{N_2}(\alpha)$  to be a complex, isotropic Gaussian with variance  $N_2 \geq 0$ . Now recall the well known fact that Gaussian random displacements of a thermal state produce a thermal state of higher mean photon number:

$$\int d^2\alpha p^{N_2}(\alpha) D(\alpha)\theta(N_1)D^\dagger(\alpha) = \theta(N_1 + N_2). \quad (169)$$

The concavity of conditional entropy and the equality in (169) then imply that

$$\begin{aligned} & H(B|E'_1 E'_2)_{\mathcal{W}(\theta(N_1))} + H(B|F'_1 F'_2)_{\mathcal{W}(\theta(N_1))} \\ & \leq H(B|E'_1 E'_2)_{\mathcal{W}(\theta(N_1+N_2))} \\ & \quad + H(B|F'_1 F'_2)_{\mathcal{W}(\theta(N_1+N_2))}. \end{aligned} \quad (170)$$

Since  $N_1, N_2 \geq 0$  are arbitrary, we conclude that the entropy objective function  $H(B|E'_1 E'_2) + H(B|F'_1 F'_2)$  is monotone increasing with respect to the mean photon number of the input thermal state. This now completes step six, and as such, we conclude the proof. ■

**Remark 1** We note here that [7, Section C.2] provided an alternative way to handle step six in the above proof.

**Remark 2** Following Remark 21 of [74], the method used in the proof of Theorem 5 to establish the upper bound in (154) on  $E_{\text{sq}}(\mathcal{N}, \hat{n}, N_S)$  can be applied in far more general situations. Suppose that  $\mathcal{N}$  is a single-mode input and multi-mode output channel. Suppose that  $\mathcal{N}$  is phase covariant, such that a phase rotation on the input state is equivalent to a product of local phase rotations on the output. Suppose that  $\mathcal{N}$  is covariant with respect to displacement operators, such that a displacement operator acting on the input state is equivalent to a product of local displacement operators on the output. Then by relaxing the energy-constrained squashed entanglement in such a way that the squashing isometry has the same general phase and displacement covariances, it follows that, among all input states with mean photon number  $\leq N_S$ , the resulting objective function is maximized by a thermal state input with mean photon number equal to  $N_S$ .

**Remark 3** We can apply Theorem 5 and Corollary 1 to the pure-loss channel in order to recover one of the main

claims of [5, 17]. That is, the energy-constrained secret-key-agreement capacity of the pure-loss channel  $\mathcal{L}_{\eta,0}$  is bounded from above as

$$P_2(\mathcal{L}_{\eta,0}, \hat{n}, N_S) \leq g(N_S(1+\eta)/2) - g(N_S(1-\eta)/2). \quad (171)$$

Also, the following bound holds for the pure-amplifier channel  $\mathcal{A}_{\mathcal{G},0}$ , as a special case of a more general result stated in [7]:

$$P_2(\mathcal{A}_{\mathcal{G},0}, \hat{n}, N_S) \leq g(N_S[\mathcal{G}+1]/2 + [\mathcal{G}-1]/2) - g([N_S+1][\mathcal{G}-1]/2). \quad (172)$$

Since the bound in (172) was not explicitly stated in [7], for convenience, the arXiv posting of this paper includes a Mathematica file that can be used to derive (172). Furthermore, other bounds on energy-constrained secret-key-agreement capacities of more general phase-insensitive channels are stated in [7].

### C. Improved Bounds for Energy-Constrained Secret-Key-Agreement Capacities of Bosonic Thermal Channels

In this section, we discuss a variation of the method from [7] that leads to improvements of the bounds reported there. To begin with, we note that any single-mode phase-insensitive channel  $\mathcal{M}$ , which is not entanglement breaking [83], can be decomposed as a pure-amplifier channel of gain  $\mathcal{G} > 1$  followed by a pure-loss channel of transmissivity  $T \in (0, 1]$ :

$$\mathcal{M} = \mathcal{L}_{T,0} \circ \mathcal{A}_{\mathcal{G},0}. \quad (173)$$

This result was found independently in [74, Theorem 30] and [82, 84] (see also [85]). It has been used in [84] to bound the unconstrained (and unassisted) quantum capacity of a thermal channel, and it has been used in [74] to bound the energy-constrained (and unassisted) quantum and private capacities of an amplifier channel. After [84] appeared, it was subsequently used in [74] to bound the energy-constrained (and unassisted) quantum and private capacities of a thermal channel. It has also been used most recently in [82] in similar contexts.

For a thermal channel  $\mathcal{L}_{\eta,N_B}$  of transmissivity  $\eta \in [0, 1]$  and thermal photon number  $N_B \geq 0$ , the decomposition is as above with

$$T = \eta - (1-\eta)N_B, \quad (174)$$

$$\mathcal{G} = \eta/T. \quad (175)$$

Thus, given that a thermal channel is entanglement breaking when  $\eta \leq (1-\eta)N_B$  [86], it is clear that the decomposition is only valid (i.e.,  $T \in (0, 1]$ ) whenever the thermal channel is not entanglement breaking. However, this is no matter when bounding secret-key-agreement or LOCC-assisted quantum capacities, due to the fact that they vanish for any entanglement-breaking channel.

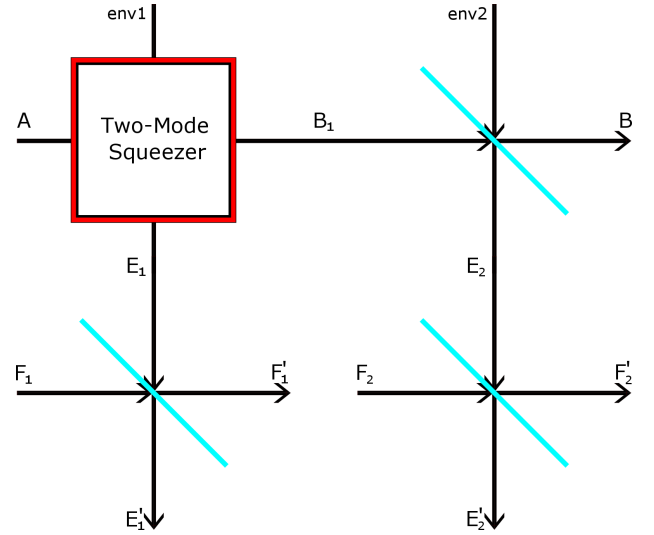


FIG. 4. A depiction of the isometric channel  $\mathcal{W}_{A \rightarrow B E_1' E_2' F_1' F_2'}$  needed for the bound in Proposition 2. This construction swaps the top-left beamsplitter and top-right two-mode squeezer from Figure 3 and corresponds to the channel decomposition in (173). This construction leads to an improvement of the bound from [7].

Now, the main idea that leads to an improved energy-constrained bound is simply to employ the decomposition in (173) and the same squashing isometries used in [7]. In other words, we are just swapping the top-left beamsplitter with the top-right two-mode squeezer in Figure 3. For concreteness, we have depicted this change in Figure 4. Let  $\mathcal{W}$  denote the overall isometry taking the input mode  $A$  to the output modes  $B E_1' E_2' F_1' F_2'$ , as depicted in Figure 4. Then by the same reasoning as in the proof of Theorem 5 and subsequently given in Remark 2, it follows that the thermal state  $\theta(N_S)$  of mean photon number  $N_S \geq 0$  optimizes a relaxation of the energy-constrained squashed entanglement corresponding to  $\mathcal{W}$ . This relaxation evaluates to

$$\begin{aligned} & \frac{1}{2} [H(B|E_1' E_2')_{\mathcal{W}(\theta(N_S))} + H(B|F_1' F_2')_{\mathcal{W}(\theta(N_S))}] \\ & = H(B|E_1' E_2')_{\mathcal{W}(\theta(N_S))}, \end{aligned} \quad (176)$$

with the latter equality following due the symmetry resulting from choosing each squashing isometry to be a 50-50 beamsplitter. This in turn implies the following:

**Proposition 2** For a thermal channel  $\mathcal{L}_{\eta,N_B}$  of transmissivity  $\eta \in [0, 1]$  and thermal photon number  $N_B \geq 0$  such that  $\eta > (1-\eta)N_B$ , its energy-constrained secret-key-agreement capacity is bounded as

$$P_2(\mathcal{L}_{\eta,N_B}, \hat{n}, N_S) \leq H(B|E_1' E_2')_{\mathcal{W}(\theta(N_S))}, \quad (177)$$

where  $\mathcal{W}$  is the isometry depicted in Figure 4.

Now consider a general phase-insensitive single-mode bosonic Gaussian channel  $\mathcal{M}$  that is not entanglement-breaking. By applying Proposition 2 and step six in

the proof of Theorem 5, we find that the quantity  $H(B|E'_1E'_2)_{\mathcal{W}(\theta(N_S))}$  is monotone increasing with  $N_S$ , with  $\mathcal{W}$  the corresponding isometry in Figure 4. Furthermore, the limit exists for all  $T \in (0, 1)$  and  $\mathcal{G} > 1$  and converges to the same expression as given in [7, Eq. (29)]:

$$\begin{aligned} & \lim_{N_S \rightarrow \infty} H(B|E'_1E'_2)_{\mathcal{W}(\theta(N_S))} \\ &= \frac{(1 - T^2)\mathcal{G} \log_2\left(\frac{1+T}{1-T}\right) - (\mathcal{G}^2 - 1)T \log_2\left(\frac{\mathcal{G}+1}{\mathcal{G}-1}\right)}{1 - \mathcal{G}^2 T^2}. \end{aligned} \quad (178)$$

We evaluated the latter limit with the aid of Mathematica and note here that the source files are available for download with the arXiv posting of this paper.

The fact that the expression in (178) is no different from that found in [7, Eq. (29)] can be intuitively explained in the following way: Given that the input state to  $\mathcal{W}$  is a thermal state, the limit  $N_S \rightarrow \infty$  in some sense is like a classical limit, and in this limit, the commutation of the pure-loss channel and the pure-amplifier channel in (173) makes no difference for the resulting expression. However, the values for  $T$  and  $\mathcal{G}$  for a thermal channel  $\mathcal{L}_{\eta, N_B}$  for the decomposition in (173) are quite different from the values that  $T$  and  $\mathcal{G}$  would take in the decomposition in (153), and this is part of the reason that the decomposition in (173) leads to an improved bound for a thermal channel  $\mathcal{L}_{\eta, N_B}$ .

In particular, for a thermal channel  $\mathcal{L}_{\eta, N_B}$ , the expression in (178) converges to zero in the entanglement-breaking limit  $\eta \rightarrow N_B/(N_B + 1)$  (or, equivalently,  $N_B \rightarrow \eta/(1 - \eta)$  (this limit calculation is included in our Mathematica files also). Due to this fact and the monotonicity of  $H(B|E'_1E'_2)_{\mathcal{W}(\theta(N_S))}$  with  $N_S$ , **we conclude that the bound from Proposition 2 converges to zero in the entanglement-breaking limit for any finite photon number  $N_S$** . This explains the improved behavior of the bound in (177), as compared to that from [7], as we discuss in what follows.

### 1. Comparison of bounds on energy-constrained secret-key-agreement capacity of a thermal channel

We have evaluated the bound in (177) numerically, and we found strong numerical evidence that it outperforms the bound from [7] for any values of  $N_S \geq 0$ ,  $\eta \in [0, 1]$ , and  $N_B \geq 0$  such that  $\eta > (1 - \eta)N_B$ .

It is also interesting to compare the bound in (177) with the bounds from [7] and [8, 11], for particular parameter regimes. In [8, 11], the following photon-number-independent bound was established:

$$P_2(\mathcal{L}_{\eta, N_B}, \hat{n}, N_S) \leq -\log_2([1 - \eta]\eta^{N_B}) - g(N_B). \quad (179)$$

Figure 5 plots the three different bounds for a fixed photon number  $N_S = 0.1$  and thermal photon number  $N_B = 1$ . Therein, we see that the bound in (177)

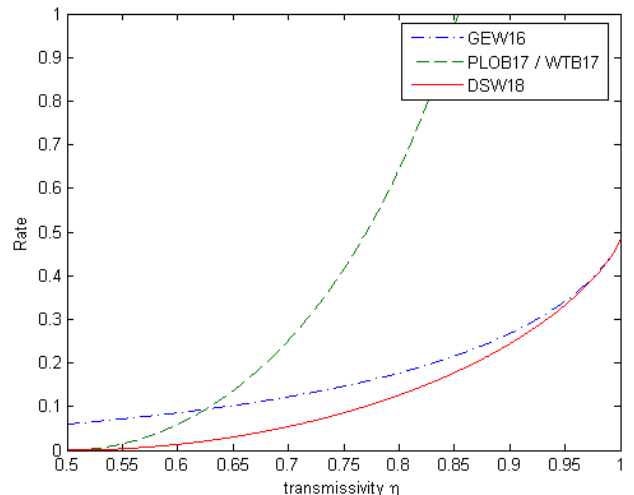


FIG. 5. Comparison of the “DSW18 bound” from (177) with prior bounds from [7] and [8, 11], with  $\eta \in [0.5, 1]$ ,  $N_S = 0.1$  and  $N_B = 1$ . The plot shows that the bound in (177) converges to zero as the channel becomes entanglement breaking.

improves upon the bounds from [7] and [8, 11] for all transmissivities  $\eta \in [1/2, 1]$ . At  $\eta = 1/2$ , the channel becomes entanglement breaking for the aforementioned choice  $N_B = 1$ , and we see that the bound in (177) is converging to zero in the entanglement-breaking limit  $\eta \rightarrow 1/2$ , for fixed  $N_B = 1$ . The bound in (177) is also tighter than the one in (179) for all values depicted in the plot.

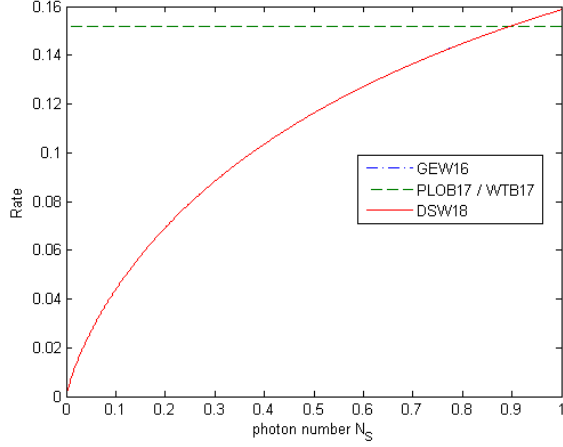
Figure 6 plots the three different bounds for other parameter regimes, now with  $N_S \in [0, 1]$ ,  $\eta = 0.1$ , and  $N_B$  set to  $3 \times 10^{-7}$ ,  $1 \times 10^{-3}$ , and 0.1. These choices correspond to values expected in a variety of experimental scenarios, as first discussed in [15] and subsequently considered in [16]. The bound in (177) is essentially indistinguishable from that in [7] for  $N_B = 3 \times 10^{-7}$ , but then the bound in (177) performs better as  $N_B$  increases.

The Matlab files used to generate Figures 5 and 6 are available for download with the arXiv posting of this paper.

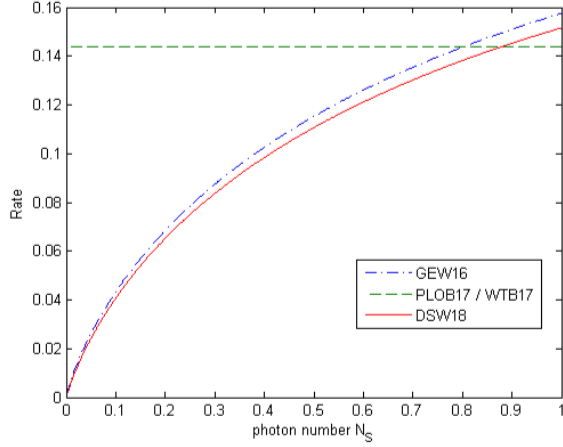
## VII. MULTIPARTITE CONDITIONAL MUTUAL INFORMATIONS AND SQUASHED ENTANGLEMENT

In this section, we review two different definitions of multipartite conditional mutual information from [29, 30, 87–90], and we prove that they satisfy a duality relation that generalizes the following well known duality relation for conditional mutual information:

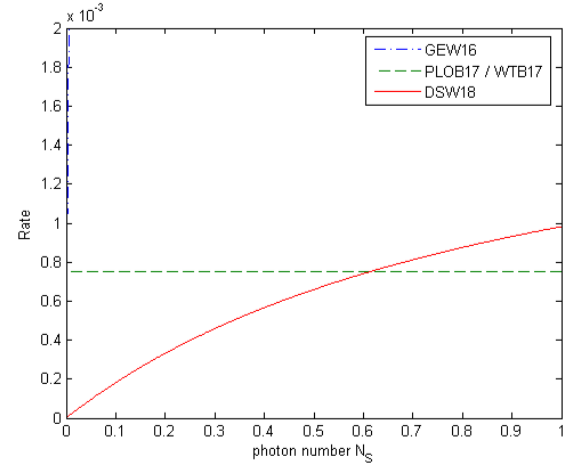
$$I(A; B|C)_\psi = I(A; B|D)_\psi, \quad (180)$$



(a)



(b)



(c)

FIG. 6. Comparison of the “DSW18 bound” from (177) with prior bounds from [7] and [8, 11], with  $N_S \in [0, 1]$ ,  $\eta = 0.1$ , and  $N_B \in \{3 \times 10^{-7}, 1 \times 10^{-3}, 0.1\}$  (respectively, (a), (b), (c), above). The DSW18 bound from (177) is indistinguishable from the bound from [7] for small  $N_B$ , but then the bounds are very different for higher  $N_B$ . In (a), GEW16 is not visible because it overlaps with DSW18.

which holds for an arbitrary four-party pure state  $\psi_{ABCD}$ . This duality relation was established in [91] and interpreted operationally therein in terms of the quantum state redistribution protocol [91, 92], and it was recently generalized to the infinite-dimensional case in [51], by employing the definition of conditional mutual information from (36)–(37).

After establishing the multipartite generalization of the duality relation in (180), we prove that it implies that two definitions of multipartite squashed entanglement [29, 30] that were previously thought to be different are in fact equal to each other.

We finally then recall various properties of multipartite squashed entanglement, including how to evaluate it for multipartite GHZ and private states.

### A. Multipartite Conditional Quantum Mutual Informations

We now recall two different multipartite generalizations of conditional mutual information [29, 30, 87–90]. Consider an  $m$ -party state  $\rho_{A_1 \dots A_m}$  acting on a tensor product of infinite-dimensional, separable Hilbert spaces. Let  $\rho_{A_1 \dots A_m E}$  denote an extension of this state, which in turn can be purified to  $\phi_{A_1 \dots A_m E F}$ . The two generalizations of conditional quantum mutual information are known as the conditional total correlation and the conditional dual total correlation:

**Definition 3** ([29, 30, 51, 87]) *The conditional total correlation of a state  $\rho_{A_1 \dots A_m E}$  is defined as*

$$I(A_1; \dots; A_m | E)_\rho \equiv \sum_{i=2}^m I(A_i; A_1^{i-1} | E)_\rho. \quad (181)$$

The notation  $A_1^{i-1}$  refers to all the systems  $A_1 \dots A_{i-1}$ .

**Definition 4** ([51, 88–90]) *The conditional dual total correlation of a state  $\rho_{A_1 \dots A_m E}$  is defined as*

$$\tilde{I}(A_1; \dots; A_m | E)_\rho \equiv \sum_{i=2}^m I(A_i; A_1^{i-1} | A_{i+1}^m E)_\rho, \quad (182)$$

where  $A_{i+1}^m \equiv A_{i+1} \dots A_m$ .

Many years after the dual total correlation was defined and analyzed in [88, 89], the conditional version of it was called “secrecy monotone” in [90] and analyzed there.

Note that the above quantities are invariant with respect to permutations of the systems  $A_1, \dots, A_m$ . This is more easily seen in the finite-dimensional case. That is, if the state  $\rho_{A_1 \dots A_m E}$  is finite-dimensional, then we have the following identities:

$$\begin{aligned} I(A_1; \dots; A_m | E)_\rho &= \sum_{i=1}^m H(A_i | E)_\rho - H(A_1 \dots A_m | E)_\rho \quad (183) \end{aligned}$$

and

$$\begin{aligned} & \tilde{I}(A_1; \dots; A_m | E)_\rho \\ &= \sum_{i=1}^m H(A_{[m] \setminus \{i\}} | E)_\rho - (m-1)H(A_1 \dots A_m | E)_\rho \\ &= H(A_1 \dots A_m | E)_\rho - \sum_{i=1}^m H(A_i | A_{[m] \setminus \{i\}} | E)_\rho. \end{aligned} \quad (184)$$

Although the two generalizations of CQMI in (181) and (182) are generally incomparable, they are related by the following identity [29]:

$$\begin{aligned} I(A_1; \dots; A_m | E)_\rho + \tilde{I}(A_1; \dots; A_m | E)_\rho \\ = \sum_{i=1}^m I(A_i; A_{[m] \setminus \{i\}} | E)_\rho. \end{aligned} \quad (185)$$

The invariance of the above quantities with respect to permutations of the subsystems, as well as the validity of the identity in (185) in the general infinite-dimensional case, are consequences of Propositions 5 and 7 in [51].

## B. Duality for the Conditional Total Correlation and the Conditional Dual Total Correlation

We now generalize the duality of CQMI in (180) to the multipartite setting:

**Theorem 6** *For a multipartite pure state  $\phi_{A_1 \dots A_m E F}^\rho$ , the following equality holds*

$$I(A_1; \dots; A_m | E)_{\phi^\rho} = \tilde{I}(A_1; \dots; A_m | F)_{\phi^\rho}. \quad (186)$$

**Proof.** There are at least two ways to see this. For the general infinite-dimensional case, we can simply apply definitions and the duality relation in (180). We find that

$$I(A_1; \dots; A_m | E)_{\phi^\rho} = \sum_{i=2}^m I(A_i; A_1^{i-1} | E)_{\phi^\rho} \quad (187)$$

$$= \sum_{i=2}^m I(A_i; A_1^{i-1} | A_{i+1}^m F)_{\phi^\rho} \quad (188)$$

$$= \tilde{I}(A_1; \dots; A_m | F)_{\phi^\rho}. \quad (189)$$

In the less general case in which conditional entropies are finite, we can apply a slightly different, but related method. Recall that conditional entropy obeys a duality property: for a pure state  $\psi_{ABC}$ , we have that  $H(A|B)_\psi = -H(A|C)_\psi$ . Using the identities given above

and this duality, we find that

$$\begin{aligned} & I(A_1; \dots; A_m | E)_{\phi^\rho} \\ &= \sum_{i=1}^m H(A_i | E)_{\phi^\rho} - H(A_1 \dots A_m | E)_{\phi^\rho} \end{aligned} \quad (190)$$

$$= - \sum_{i=1}^m H(A_i | A_{[m] \setminus \{i\}} | F)_{\phi^\rho} + H(A_1 \dots A_m | F)_{\phi^\rho} \quad (191)$$

$$= \tilde{I}(A_1; \dots; A_m | F)_{\phi^\rho}. \quad (192)$$

This concludes the proof. ■

**Remark 4** *It is interesting to compare the somewhat long route by which Han arrived at the conditional dual total correlation in [89], versus the comparatively short route by which we arrive at it in Theorem 6. This latter method of using purifications and related entropy identities is unique to quantum information theory. It is also pleasing to find that the conditional total correlation and the conditional dual total correlation are dual to each other in the entropic sense of Theorem 6.*

## C. Equivalence of Multipartite Squashed Entanglements

Two multipartite generalizations of the squashed entanglement of a state  $\rho_{A_1 \dots A_m}$  are based on the conditional total correlation and the conditional dual total correlation [29, 30]:

$$\begin{aligned} E_{\text{sq}}(A_1; \dots; A_m)_\rho &\equiv \frac{1}{2} \inf_{\rho_{A_1 \dots A_m E}} \left\{ I(A_1; \dots; A_m | E)_\rho \right. \\ &\quad \left. : \text{Tr}_E \{ \rho_{A_1 \dots A_m E} \} = \rho_{A_1 \dots A_m} \right\}, \end{aligned} \quad (193)$$

$$\begin{aligned} \tilde{E}_{\text{sq}}(A_1; \dots; A_m)_\rho &\equiv \frac{1}{2} \inf_{\rho_{A_1 \dots A_m E}} \left\{ \tilde{I}(A_1; \dots; A_m | E)_\rho \right. \\ &\quad \left. : \text{Tr}_E \{ \rho_{A_1 \dots A_m E} \} = \rho_{A_1 \dots A_m} \right\}. \end{aligned} \quad (194)$$

By employing Theorem 6, we find that these quantities are in fact always equal to each other, so that there is no need to consider two separate definitions, as was previously done in [6, 29]:

**Theorem 7** *For a multipartite state  $\rho_{A_1 \dots A_m}$ , the following equality holds*

$$E_{\text{sq}}(A_1; \dots; A_m)_\rho = \tilde{E}_{\text{sq}}(A_1; \dots; A_m)_\rho. \quad (195)$$

**Proof.** Let  $\rho_{A_1 \dots A_m E}$  be an extension of  $\rho_{A_1 \dots A_m}$ , and let  $\phi_{A_1 \dots A_m E F}^\rho$  be a purification of  $\rho_{A_1 \dots A_m E}$ . Then by Theorem 6,

$$I(A_1; \dots; A_m | E)_\rho = \tilde{I}(A_1; \dots; A_m | F)_{\phi^\rho} \quad (196)$$

$$\geq 2\tilde{E}_{\text{sq}}(A_1; \dots; A_m)_\rho. \quad (197)$$

The inequality holds because  $\phi_{A_1 \dots A_m F}^\rho$  is a particular extension of  $\rho_{A_1 \dots A_m}$ , and the squashed entanglement involves an infimum over all extensions of  $\rho_{A_1 \dots A_m}$ . Since the inequality holds for all extensions of  $\rho_{A_1 \dots A_m}$ , we can conclude that

$$E_{\text{sq}}(A_1; \dots; A_m)_\rho \geq \tilde{E}_{\text{sq}}(A_1; \dots; A_m)_\rho. \quad (198)$$

A proof for the other inequality  $\tilde{E}_{\text{sq}}(A_1; \dots; A_m)_\rho \geq E_{\text{sq}}(A_1; \dots; A_m)_\rho$  goes similarly. ■

**Remark 5** *One of the main results of [6] was to establish bounds on the secret-key-agreement capacity region of a quantum broadcast channel in terms of multipartite squashed entanglements. Theorem 7 demonstrates that essentially half of the upper bounds written down in [6] were in fact redundant. The same is true for the key distillation bounds from [29].*

#### D. Partitions and multipartite squashed entanglement

In this brief section, we recall some notation from [6, Section 2.7], which we use in what follows as a shorthand for describing various partitions of a set of quantum systems and their corresponding multipartite squashed entanglements. Given a set  $\mathcal{W}$  of quantum systems, a partition  $\mathbb{G} = \{\chi_1, \dots, \chi_{|\mathbb{G}|}\}$  is a set of non-empty subsets of  $\mathcal{W}$  such that

$$\bigcup_{\chi_i \in \mathbb{G}} \chi_i = \mathcal{W}, \quad (199)$$

and for all  $\chi_i, \chi_j \in \mathbb{G}$ ,  $i \neq j$ ,

$$\chi_i \cap \chi_j = \emptyset. \quad (200)$$

For example, one possible partition of  $\mathcal{W} = \{A, B, C\}$  is given by  $\mathbb{G} = \{\{AB\}, \{C\}\}$ . The power set  $\mathcal{P}(\mathcal{W})$  is the set of all subsets of  $\mathcal{W}$ . The sets  $\mathcal{P}_{\geq 1}(\mathcal{W})$  and  $\mathcal{P}_{\geq 2}(\mathcal{W})$  are the sets of all subsets of  $\mathcal{W}$  with greater than or equal to one and two members, respectively. That is, for  $\mathcal{W} = \{A, B, C\}$ ,

$$\mathcal{P}(\mathcal{W}) = \{\emptyset, \{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}, \quad (201)$$

$$\mathcal{P}_{\geq 1}(\mathcal{W}) = \{\{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}, \quad (202)$$

$$\mathcal{P}_{\geq 2}(\mathcal{W}) = \{\{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}. \quad (203)$$

Given a set  $\mathcal{Y}$ , let  $\omega_{\mathcal{Y}}$  denote a  $|\mathcal{Y}|$ -partite state shared by the parties specified by the elements of  $\mathcal{Y}$ . If  $\mathbb{G}$  is a partition of  $\mathcal{Y}$ , then the notation

$$E_{\text{sq}}(\mathbb{G})_\omega \quad (204)$$

refers to the multipartite squashed entanglement with parties grouped according to partition  $\mathbb{G}$ . For example,

if  $\mathcal{Y} = \{A, B, C\}$ ,  $\omega_{\mathcal{Y}} = \omega_{ABC}$ ,  $\mathbb{G}_1 = \{\{A\}, \{B\}, \{C\}\}$ , and  $\mathbb{G}_2 = \{\{AB\}, \{C\}\}$ , then

$$E_{\text{sq}}(\mathbb{G}_1)_\omega = E_{\text{sq}}(A; B; C)_\omega, \quad \text{and} \quad (205)$$

$$E_{\text{sq}}(\mathbb{G}_2)_\omega = E_{\text{sq}}(AB; C)_\omega. \quad (206)$$

#### E. Multipartite Private States

One multipartite generalization of the maximally entangled state in (3) is the Greenberger-Horne-Zeilinger (GHZ) state. A GHZ state of  $\log_2 K$  entangled bits of an  $m$ -party system  $A_1, \dots, A_m$  takes the form

$$|\Phi\rangle_{A_1 \dots A_m} = \frac{1}{\sqrt{K}} \sum_{i=1}^K |i\rangle_{A_1} \otimes \dots \otimes |i\rangle_{A_m} \quad (207)$$

where  $\{|i\rangle_{A_1}\}, \dots, \{|i\rangle_{A_m}\}$  are orthonormal basis sets for their respective systems. The bipartite private states from (66) are similarly generalized to the multipartite case [93], so that a state of  $\log_2 K$  private bits is as follows:

$$\begin{aligned} & \gamma_{A_1 \dots A_m A'_1 \dots A'_m} \\ &= U_{A_1 \dots A_m A'_1 \dots A'_m} (|\Phi\rangle\langle\Phi|_{A_1 \dots A_m} \otimes \rho_{A'_1 \dots A'_m}) \times \\ & \quad U_{A_1 \dots A_m A'_1 \dots A'_m}^\dagger, \end{aligned} \quad (208)$$

with the GHZ state generalizing the role of the maximally entangled state, and the twisting unitary from (68) is generalized as

$$\begin{aligned} U_{A_1 \dots A_m A'_1 \dots A'_m} &= \sum_{i_1, \dots, i_m=1}^K |i_1, \dots, i_m\rangle\langle i_1, \dots, i_m|_{A_1 \dots A_m} \\ & \quad \otimes U_{A'_1 \dots A'_m}^{i_1, \dots, i_m}, \end{aligned} \quad (209)$$

where  $U_{A'_1 \dots A'_m}^{i_1, \dots, i_m}$  are unitary operators depending on the values  $i_1, \dots, i_m$ .

#### F. Properties of Multipartite Squashed Entanglement

Multipartite squashed entanglement possesses a number of useful properties that have been proven separately in [6] for the quantities in (193) and (194). In light of Theorem 7, we now know that these measures are equal. Since we require these properties in what follows, we recall some of them here:

**Lemma 8 (Subadditivity [6])** *Given a pure state  $\phi_{RA_1 \dots A_m B_1 \dots B_m EF}$ , the following inequality holds*

$$\begin{aligned} E_{\text{sq}}(R; A_1 B_1; \dots; A_m B_m)_\phi &\leq \\ & E_{\text{sq}}(R A^m E; B_1; \dots; B_m)_\phi + \\ & E_{\text{sq}}(R B^m F; A_1; \dots; A_m)_\phi \end{aligned} \quad (210)$$

where the notation  $A^m$  refers to all systems  $A_1 \dots A_m$  and a similar convention for  $B^m$ .



Technically speaking, [6] did not establish the above statement in the general infinite-dimensional case, but we note here that the approach from [51] can be used to establish the lemma above.

**Lemma 9 (Monotonicity for Groupings [6])**

*Squashed entanglement is non-increasing when subsystems are grouped. That is, given a state  $\rho_{A_1 \dots A_m}$ , the following inequality holds*

$$E_{\text{sq}}(A_1; A_2; \dots; A_m)_\rho \geq E_{\text{sq}}(A_1 A_2; A_3; \dots; A_m)_\rho. \quad (211)$$

**Lemma 10 (Product States [6])** *Let*

$$\omega_{AB_1 \dots B_m} = \rho_A \otimes \sigma_{B_1 \dots B_m} \quad (212)$$

where  $\rho_A$  and  $\sigma_{B_1 \dots B_m}$  are density operators. Then

$$E_{\text{sq}}(A; B_1; \dots; B_m)_\omega = E_{\text{sq}}(B_1; \dots; B_m)_\sigma. \quad (213)$$

We also have the following alternative representation of multipartite squashed entanglement, which was employed implicitly in [6]:

**Lemma 11** *Let  $\rho_{A_1 \dots A_m}$  be a multipartite density operator such that the entropy  $H(A_i)_\rho < \infty$  for all  $i \in \{2, \dots, m\}$ . Then its multipartite squashed entanglement can be written as*

$$E_{\text{sq}}(A_1; A_2; \dots; A_m)_\rho = \frac{1}{2} \inf_{\mathcal{V}_{E \rightarrow E'F}} \left[ \sum_{i=2}^m H(A_i|E')_\omega + H(A_2 \dots A_m|F)_\omega \right], \quad (214)$$

where the infimum is with respect to an isometric channel  $\mathcal{V}_{E \rightarrow E'F}$ ,

$$\omega_{A_1 \dots A_m E'F} \equiv \mathcal{V}_{E \rightarrow E'F}(\phi_{A_1 \dots A_m E}^\rho), \quad (215)$$

and  $\phi_{A_1 \dots A_m E}^\rho$  is a purification of  $\rho_{A_1 \dots A_m}$ .

**Proof.** A proof follows easily from the definition of  $E_{\text{sq}}(A_1; A_2; \dots; A_m)_\rho$  in (193), rewriting it in terms of a squashing isometry as has been done in the bipartite case, and employing duality of conditional entropy. ■

**G. Multipartite Squashed Entanglement for GHZ and Private States**

The multipartite squashed entanglement of a maximally entangled state or a private state scales linearly with the number of parties [6, 29]. That is, for  $\Phi_{A_1 \dots A_m}$  a GHZ state as in (207) and  $\gamma_{A_1 \dots A_m}$  a private state as in (208), then the following relations hold

$$E_{\text{sq}}(A_1; \dots; A_m)_\Phi = \frac{m}{2} \log_2 K, \quad (216)$$

$$E_{\text{sq}}(A_1; \dots; A_m)_\gamma \geq \frac{m}{2} \log_2 K. \quad (217)$$

Now consider a set  $\mathcal{W} = \{A, B, C\}$  of systems and let  $\Psi_{ABC}$  be composed of maximally entangled states  $\Phi$  and private states  $\gamma$  over the systems  $A, B$ , and  $C$ , according to the power set in (203) for two or more members:

$$\begin{aligned} \Psi_{ABC} = & \Phi_{A_1 B_1} \otimes \Phi_{A_2 C_2} \otimes \Phi_{B_3 C_3} \otimes \Phi_{A_4 B_4 C_4} \\ & \otimes \gamma_{A_5 B_5} \otimes \gamma_{A_6 C_6} \otimes \gamma_{B_7 C_7} \otimes \gamma_{A_8 B_8 C_8}. \end{aligned} \quad (218)$$

In the above, we have subdivided the systems  $A, B$ , and  $C$  for the various correlations so that, in the given example,

$$A = A_1 A_2 A_4 A_5 A_6 A_8, \quad (219)$$

$$B = B_1 B_3 B_4 B_5 B_7 B_8, \quad (220)$$

$$C = C_2 C_3 C_4 C_6 C_7 C_8. \quad (221)$$

For each of the constituent states given in (218), we note the number of entangled bits or private bits as  $E$  or  $K$ , respectively, as done in [6]. For example,

$$E_{AB} = H(A_1)_\Phi = H(B_1)_\Phi = \log_2 K_{A_1}, \quad (222)$$

$$K_{ABC} = H(A_8)_\gamma = H(B_8)_\gamma = H(C_8)_\gamma = \log_2 K_{A_8}, \quad (223)$$

and so the tuple

$$(E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})$$

characterizes the entangled and private bit content of the state. By using (216) and (217), along with the additivity of squashed entanglement for tensor-product states and adopting the notation in (222) and (223), we find that

$$\begin{aligned} E_{\text{sq}}(A; B; C)_\Psi &= E_{\text{sq}}(A_1; B_1)_\Phi + E_{\text{sq}}(A_2; C_2)_\Phi + E_{\text{sq}}(B_3; C_3)_\Phi \\ &\quad + E_{\text{sq}}(A_4; B_4; C_4)_\Phi + E_{\text{sq}}(A_5; B_5)_\gamma + E_{\text{sq}}(A_6; C_6)_\gamma \\ &\quad + E_{\text{sq}}(B_7; C_7)_\gamma + E_{\text{sq}}(A_8; B_8; C_8)_\gamma \\ &\geq E_{AB} + E_{AC} + E_{BC} + \frac{3}{2} E_{ABC} \\ &\quad + K_{AB} + K_{AC} + K_{BC} + \frac{3}{2} K_{ABC} \end{aligned} \quad (224)$$

As in (205) and (206), if  $\Psi_{ABC} = \Psi_{\mathcal{Y}}$  for  $\mathcal{Y} = \{A, B, C\}$ , and for partitions  $\mathbb{G}_1 = \{\{A\}, \{B\}, \{C\}\}$  and  $\mathbb{G}_2 = \{\{AB\}, \{C\}\}$  then  $E_{\text{sq}}(\mathbb{G}_1) = E_{\text{sq}}(A; B; C)_\Psi$  as shown in (205). For  $E_{\text{sq}}(\mathbb{G}_2)$ , we have that

$$\begin{aligned} E_{\text{sq}}(\mathbb{G}_2) &= E_{\text{sq}}(AB; C)_\Psi \\ &= E_{\text{sq}}(A_2; C_2)_\Phi + E_{\text{sq}}(B_3; C_3)_\Phi + E_{\text{sq}}(A_4 B_4; C_4)_\Phi \\ &\quad + E_{\text{sq}}(A_6; C_6)_\gamma + E_{\text{sq}}(B_7; C_7)_\gamma + E_{\text{sq}}(A_8 B_8; C_8)_\gamma \end{aligned} \quad (225)$$

$$\geq E_{AC} + E_{BC} + E_{ABC} + K_{AC} + K_{BC} + K_{ABC} \quad (228)$$

**VIII. QUANTUM BROADCAST CHANNELS AND SECRET-KEY-AGREEMENT CAPACITY REGIONS**

A quantum broadcast channel is a channel as defined in (4), except that it is a map from one sender to *multiple*

receivers [94]. A protocol for energy-constrained, multipartite secret key agreement is much the same as in the bipartite case outlined in Section IV, with a constraint on the average energy of the channel input states and with rounds of LOCC between channel uses. For demonstrative purposes, in this section we focus exclusively on the case of a single sender and two receivers. We make use of an energy observable  $G$  and energy constraint  $P \in [0, \infty)$ . A quantum broadcast channel  $\mathcal{N}_{A \rightarrow BC}$  satisfies the finite output-entropy condition with respect to  $G$  and  $P$  if

$$\sup_{\rho_A: \text{Tr}\{G\rho_A\} \leq P} H(\mathcal{N}_{A \rightarrow BC}(\rho_A)) < \infty. \quad (229)$$

In what follows, for example, we denote the rate of entanglement generation between the sender  $A$  and the receiver  $B$  by  $R_{AB}^E$  and the rate of key generation by  $R_{AB}^K$ . Generalizing this, we have a vector  $\vec{R}$  of rates, for which we employ the following shorthand:

$$\vec{R} \equiv (R_{AB}^E, R_{AC}^E, R_{BC}^E, R_{ABC}^E, R_{AB}^K, R_{AC}^K, R_{BC}^K, R_{ABC}^K). \quad (230)$$

In a general  $(n, \vec{R}, G, P, \varepsilon)$  protocol, the sender Alice and the receivers Bob and Charlie are tasked to use a quantum broadcast channel  $\mathcal{N}_{A \rightarrow BC}$   $n$  times to establish a shared state  $\Omega_{ABC}$  such that

$$F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon, \quad (231)$$

with  $\Psi$  defined in (218) and the elements of  $\vec{R}$  are given by, e.g., [6]

$$R_{AB}^E = \frac{E_{AB}}{n} = \frac{1}{n} H(A_1)_\Psi, \quad (232)$$

$$R_{AB}^K = \frac{K_{AB}}{n} = \frac{1}{n} H(A_5)_\Psi. \quad (233)$$

In such a protocol, Alice, Bob, and Charlie begin by performing an LOCC channel  $\mathcal{L}_{\emptyset \rightarrow A'_1 A_1 B'_1 C'_1}^{(1)}$  to create a state  $\rho_{A'_1 A_1 B'_1 C'_1}^{(1)}$  that is separable with respect to the cut  $A'_1 A_1 | B'_1 | C'_1$ , and where  $A'_1$ ,  $B'_1$ , and  $C'_1$  are scratch systems. Alice then uses  $A_1$  as the input to the first channel use, resulting in the state

$$\sigma_{A'_1 B_1 B'_1 C_1 C'_1}^{(1)} \equiv \mathcal{N}_{A_1 \rightarrow B_1 C_1}(\rho_{A'_1 A_1 B'_1 C'_1}^{(1)}). \quad (234)$$

Alice, Bob, and Charlie then perform a second LOCC channel, producing

$$\begin{aligned} \rho_{A'_2 A_2 B'_2 C'_2}^{(2)} &\equiv \\ \mathcal{L}_{A'_1 B_1 B'_1 C_1 C'_1 \rightarrow A'_2 A_2 B'_2 C'_2}^{(2)}(\sigma_{A'_1 B_1 B'_1 C_1 C'_1}^{(1)}). \end{aligned} \quad (235)$$

The procedure continues in this manner, as in Section IV, with a total of  $n$  rounds of LOCC interleaved with  $n$  uses of the channel as follows: for  $i \in \{2, \dots, n\}$

$$\begin{aligned} \rho_{A'_i A_i B'_i C'_i}^{(i)} &\equiv \\ \mathcal{L}_{A'_{i-1} B_{i-1} B'_{i-1} C_{i-1} C'_{i-1} \rightarrow A'_i A_i B'_i C'_i}^{(i)}(\sigma_{A'_{i-1} B_{i-1} B'_{i-1} C_{i-1} C'_{i-1}}^{(i-1)}), \end{aligned}$$

$$\sigma_{A'_i B_i B'_i C_i C'_i}^{(i)} \equiv \mathcal{N}_{A_i \rightarrow B_i C_i}(\rho_{A'_i A_i B'_i C'_i}^{(i)}). \quad (236)$$

After the  $n$ th channel use, a final,  $(n+1)$ th LOCC channel is performed. Going to the purified picture as before, tracing over the eavesdropper's systems while retaining the shield systems, the goal is to establish the state  $\Omega_{ABC}$  satisfying  $F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon$ , where  $\Psi_{ABC}$  is the ideal state from (218). Finally, the same average energy constraint for the channel input states, as in (101), should be satisfied.

The rate tuple  $\vec{R}$  is achievable if for all  $\varepsilon \in (0, 1)$ ,  $\vec{\delta} \succeq 0$ , and sufficiently large  $n$ , there exists an  $(n, \vec{R} - \vec{\delta}, G, P, \varepsilon)$  protocol as outlined above. The energy-constrained secret-key-agreement capacity region of the channel  $\mathcal{N}$  is the closure of the region mapped out by all achievable rate tuples subject to the energy constraint  $P$ .

### A. Energy-Constrained Squashed Entanglement Upper Bound for the LOCC-Assisted Capacity Region of a Quantum Broadcast Channel

The main result of this section is a generalization of the result in Section V, as well as a generalization of the main result in [6]. In particular, we prove that the energy-constrained, multipartite squashed entanglement is a key tool in bounding the LOCC-assisted capacity region of a quantum broadcast channel.

**Theorem 12** *Let  $G$  be a Gibbs observable, and let  $P \in [0, \infty)$  be an energy constraint. Let  $\mathcal{N}_{A \rightarrow BC}$  be a quantum broadcast channel satisfying the finite-output entropy condition in (229) with respect to  $G$  and  $P$ . Suppose that  $\vec{R}$  is an achievable rate tuple for LOCC-assisted private and quantum communication. Then the elements of the rate tuple  $\vec{R}$  are bounded in terms of multipartite squashed entanglement as*

$$\begin{aligned} R_{AC}^E + R_{AC}^K + R_{BC}^E + R_{BC}^K + R_{ABC}^E + R_{ABC}^K \\ \leq E_{\text{sq}}(SB; C)_\omega \end{aligned} \quad (237)$$

$$\begin{aligned} R_{AB}^E + R_{AB}^K + R_{BC}^E + R_{BC}^K + R_{ABC}^E + R_{ABC}^K \\ \leq E_{\text{sq}}(SC; B)_\omega \end{aligned} \quad (238)$$

$$\begin{aligned} R_{AB}^E + R_{AB}^K + R_{AC}^E + R_{AC}^K + R_{ABC}^E + R_{ABC}^K \\ \leq E_{\text{sq}}(S; BC)_\omega \end{aligned} \quad (239)$$

$$\begin{aligned} R_{AB}^E + R_{AB}^K + R_{AC}^E + R_{AC}^K + R_{BC}^E + R_{BC}^K \\ + \frac{3}{2}(R_{ABC}^E + R_{ABC}^K) \\ \leq E_{\text{sq}}(S; B; C)_\omega, \end{aligned} \quad (240)$$

for some pure state  $\psi_{SA}$  satisfying  $\text{Tr}\{G\psi_A\} \leq P$ , with the state  $\omega_{SBC}$  defined in terms of it as

$$\omega_{SBC} = \mathcal{N}_{A \rightarrow BC}(\psi_{SA}). \quad (241)$$

**Proof.** The proof of this bound follows that of Proposition 1 and [6, Theorem 12], working backward through

the communication protocol one channel use at a time in order to demonstrate the inequalities. For this reason, we keep the proof brief. Let us begin by considering the partition  $\mathbb{G}_1 = \{\{A\}, \{B\}, \{C\}\}$ . From reasoning as in (225) but instead applying an estimate in [13, Theorem 6] to the condition  $F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon$ , we find that

$$n \left( R_{AC}^E + R_{AC}^K + R_{BC}^E + R_{BC}^K + R_{AB}^E + R_{AB}^K + \frac{3}{2}(R_{ABC}^E + R_{ABC}^K) \right) \leq E_{\text{sq}}(A; B; C)_\Omega + f_2(n, \varepsilon), \quad (242)$$

where  $f_2(n, \varepsilon)$  is a function such that  $f_2(n, \varepsilon)/n$  tends to zero as  $n \rightarrow \infty$  and as  $\varepsilon \rightarrow 0$ .

If we look at just the squashed entanglement term of (242), we can split it and group terms, working backward through the  $n$  channel uses of the protocol:

$$E_{\text{sq}}(A; B; C)_\Omega \leq E_{\text{sq}}(A'_n; B_n B'_n; C_n C'_n)_{\sigma^{(n)}} \quad (243)$$

$$\leq E_{\text{sq}}(A'_n B_n C_n E_n; B'_n; C'_n)_{\sigma^{(n)}} + E_{\text{sq}}(A'_n B'_n C'_n R_n; B_n; C_n)_{\sigma^{(n)}} \quad (244)$$

$$= E_{\text{sq}}(A'_n A_n; B'_n; C'_n)_{\rho^{(n)}} + E_{\text{sq}}(A'_n B'_n C'_n R_n; B_n; C_n)_{\sigma^{(n)}} \quad (245)$$

$$\leq E_{\text{sq}}(A'_{n-1}; B_{n-1} B'_{n-1}; C_{n-1} C'_{n-1})_{\sigma^{(n-1)}} + E_{\text{sq}}(A'_n B'_n C'_n R_n; B_n; C_n)_{\sigma^{(n)}} \quad (246)$$

$$\leq \sum_{i=1}^n E_{\text{sq}}(A'_i B'_i C'_i R_i; B_i; C_i)_{\sigma^{(i)}}. \quad (247)$$

The first inequality follows from the monotonicity of squashed entanglement under LOCC. For the second inequality the quantity has been split using the subadditivity property from Lemma 8 (there are also some implicit purifying systems  $R$  and  $E$ , which we have not explicitly defined, but note that  $E$  denotes an environment of the broadcast channel). The equality is a result of the invariance of squashed entanglement under isometries, because an isometric extension of  $\mathcal{N}$  relates  $A_n$  to  $B_n C_n E_n$ . The third inequality is the beginning of the first repetition of this procedure, in which we again apply the monotonicity of squashed entanglement under LOCC. Iterating this reasoning  $n$  times leads to the final inequality in (247). Working backward another step yields no additional terms, because the initial state is separable, having been created through LOCC. However, with purifying systems  $R_i$ , we combine (247) with (242) to conclude that there exists a state  $\omega$ , as defined in (241), such that

$$\sum_{i=1}^n E_{\text{sq}}(A'_i B'_i C'_i R_i; B_i; C_i)_{\sigma^{(i)}} \leq n E_{\text{sq}}(S; B; C)_\omega \quad (248)$$

and

$$R_{AC}^E + R_{AC}^K + R_{BC}^E + R_{BC}^K + R_{AB}^E + R_{AB}^K + \frac{3}{2}(R_{ABC}^E + R_{ABC}^K) \leq E_{\text{sq}}(S; B; C)_\omega + \frac{1}{n} f_2(n, \varepsilon). \quad (249)$$

Taking the limit  $n \rightarrow \infty$  and then  $\varepsilon \rightarrow 0$  yields (240). A similar rationale can be applied to obtain the other bounds, and key to the claim, as in the proof of [6, Theorem 12], is that the same state  $\omega$  can be used in all of the bounds. ■

**Remark 6** *Just as [6, Theorem 12] was generalized from the single-sender, two-receiver case to the single sender,  $m$ -receiver case in [6, Theorem 13], our above bounds for the energy-constrained capacity region of the quantum broadcast channel can be generalized to an  $m$ -receiver case through the consideration of the many possible partitions, as described in Section VII D.*

## B. Upper Bounds on the Energy-Constrained LOCC-Assisted Capacity Regions of a Pure-Loss Bosonic Broadcast Channel

In this section, we focus on a concrete quantum broadcast channel, known as the pure-loss broadcast channel. The model for this channel was introduced in [95] and subsequently studied in [6, 9]. It is equivalent to a linear sequence of beamsplitters, in which the sender inputs into the first one, the vacuum state is injected into all of the environment ports, the receivers each get one output from the sequence of beamsplitters and one output of the beamsplitters is lost to the environment (see Figure 3-13 of [95] or Figure 1c of [9]). In what follows, we adopt the same strategy as before for the single-mode pure-loss channel (and what was subsequently used in [6]), and we relax the squashing isometry for the environment mode to be a 50-50 beamsplitter.

Using this strategy, we now calculate bounds on rates of energy-constrained entanglement generation and key distillation achievable between the sender and one of the receivers. The same reasoning as in Remark 2, along with the representation of multipartite squashed entanglement in Lemma 11 and the relaxation of it described above, allow us to conclude that, for a given input mean photon number constraint  $N_S \geq 0$ , a thermal state of that photon number is optimal.

Before stating the theorem, we establish the following notation:

- The set of all receivers is denoted by  $\mathcal{B} = \{B_1, \dots, B_m\}$ . The total transmissivity for all receivers is  $\eta_{\mathcal{B}} \in [0, 1]$ .
- In the theorem below, the set  $\mathcal{T}$  denotes a subset of the receivers ( $\mathcal{T} \subseteq \mathcal{B}$ ), and its complement

set is denoted by  $\bar{\mathcal{T}} = \mathcal{B} \setminus \mathcal{T}$ . The total transmissivity to the members of the set  $\mathcal{T}$  is denoted by  $\eta_{\mathcal{T}} = \sum_{B_i \in \mathcal{T}} \eta_{B_i}$ , and the total transmissivity to the members of the complement set is denoted by  $\eta_{\bar{\mathcal{T}}} = \sum_{B_i \in \bar{\mathcal{T}}} \eta_{B_i}$ , such that  $\eta_{\mathcal{T}} + \eta_{\bar{\mathcal{T}}} = \eta_{\mathcal{B}}$ .

- The transmissivity to the adversary Eve is denoted by  $\eta_E = 1 - \eta_{\mathcal{B}} = 1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}}$ .

With this notation, we can now establish the following theorem:

**Theorem 13** *The energy-constrained LOCC-assisted capacity region of a pure-loss quantum broadcast channel, for entanglement and key distillation between the sender and each receiver, is bounded as*

$$\sum_{B_i \in \mathcal{T}} R_{AB_i}^E + R_{AB_i}^K \leq g(N_S(1 + \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2) - g(N_S(1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2). \quad (250)$$

for all non-empty  $\mathcal{T} \subseteq \mathcal{B}$ .

**Proof.** For the choices discussed above, it simply suffices to calculate various relaxations of the multipartite squashed entanglements when the thermal state of mean photon number  $N_S$  is input. As mentioned above, the same reasoning as in Remark 2, along with the representation of multipartite squashed entanglement in Lemma 11 and the relaxation of it described above, allow us to conclude that, for a given input mean photon number constraint  $N_S \geq 0$ , a thermal state of that photon number is optimal. By applying Theorem 12 and Remark 6, the following bounds apply

$$\sum_{B_i \in \mathcal{T}} R_{AB_i}^E + R_{AB_i}^K \leq E_{\text{sq}}(R\bar{\mathcal{T}}; \mathcal{T}), \quad (251)$$

$$\leq \frac{1}{2} [H(\mathcal{T}|E_1) + H(\mathcal{T}|E_2)] \quad (252)$$

where the second inequality follows from relaxing the squashing isometry to be a 50-50 beamsplitter as discussed above, with output systems  $E_1$  and  $E_2$ , and then it follows that the thermal state of mean photon number  $N_S$  into the pure-loss bosonic broadcast channel is optimal. Now employing entropy identities, we find that

$$\begin{aligned} & \frac{1}{2} [H(\mathcal{T}|E_1) + H(\mathcal{T}|E_2)] \\ &= \frac{1}{2} [H(\mathcal{T}E_1) - H(E_1) + H(\mathcal{T}E_2) - H(E_2)] \quad (253) \end{aligned}$$

$$= H(\mathcal{T}E_1) - H(E_1). \quad (254)$$

The last line in (254) combines terms that are equal, due to the fact that the transmissivity of the squashing channel is balanced (coming from a 50-50 beamsplitter). We then use the  $g$  function to represent the entropies of

the thermal states resulting from the use of the quantum broadcast channel, giving that

$$\begin{aligned} & H(\mathcal{T}E_1) - H(E_1) \\ &= g(N_S(\eta_{\mathcal{T}} + \eta_E/2)) - g(N_S\eta_E/2) \quad (255) \end{aligned}$$

$$\begin{aligned} &= g(N_S(\eta_{\mathcal{T}} + (1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2)) \\ &\quad - g(N_S(1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2) \quad (256) \end{aligned}$$

$$\begin{aligned} &= g(N_S(1 + \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2) \\ &\quad - g(N_S(1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}})/2). \quad (257) \end{aligned}$$

This concludes the proof. ■

We conclude this section with a few brief remarks. In the limit of large photon number  $N_S \rightarrow \infty$ , the bound in Theorem 13 reduces to

$$\sum_{B_i \in \mathcal{T}} R_{AB_i}^E + R_{AB_i}^K \leq \log_2 \left( \frac{1 + \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}}}{1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}}} \right), \quad (258)$$

which is not as tight as the result of [9], in which the upper bound was found to be  $\log_2 \left( \frac{1 - \eta_{\bar{\mathcal{T}}}}{1 - \eta_{\mathcal{T}} - \eta_{\bar{\mathcal{T}}}} \right)$ . However, for low photon number, the energy-constrained bounds of Theorem 13 can be tighter.

Let us look at some particular examples of the bound. For the case of two receivers, Bob and Charlie, the set  $\mathcal{T}$  can take a few different values. If  $\mathcal{T} = \{B, C\}$  then  $\bar{\mathcal{T}} = 0$  and

$$\begin{aligned} & R_{AB}^E + R_{AB}^K + R_{AC}^E + R_{AC}^K + R_{ABC}^E + R_{ABC}^K \\ & \leq \log_2 \left( \frac{1 + \eta_B + \eta_C}{1 - \eta_B - \eta_C} \right) \quad (259) \end{aligned}$$

which has been discussed already in [6]. For the case  $\mathcal{T} = C$ , then  $\bar{\mathcal{T}} = B$ , and so

$$R_{AC}^E + R_{AC}^K \leq \log_2 \left( \frac{1 + \eta_C - \eta_B}{1 - \eta_B - \eta_C} \right). \quad (260)$$

Other permutations of the sets  $\mathcal{T}$  and  $\bar{\mathcal{T}}$  can naturally be worked out for scenarios involving any number of receivers.

## IX. CONCLUSION

Knowing not only the achievable rates of current protocols but also fundamental limitations of a channel for secret key agreement or LOCC-assisted quantum communication is important for the implementation of rapidly progressing quantum technologies. In this paper, we formally defined the task of energy-constrained secret key agreement and LOCC-assisted quantum communication. We proved that the energy-constrained squashed entanglement is an upper bound on these capacities. We also proved that a thermal-state input is optimal for a relaxation of the energy-constrained squashed entanglement of a single-mode input, phase-insensitive bosonic Gaussian channel, generalizing results from prior work on this

topic. After doing so, we proved that a variation of the method introduced in [7] leads to improved upper bounds on the energy-constrained secret-key-agreement capacity of a bosonic thermal channel. In particular, these improved upper bounds have the property that they converge to zero in the limit as the thermal channel becomes entanglement breaking.

We then generalized the results to the multipartite setting, along the lines of [6]. Here, we began by proving that two multipartite squashed entanglements are in fact equal even though they were previously thought to be different. We also proved that the energy-constrained multipartite squashed entanglement serves as an upper bound on the energy-constrained, secret key agreement and LOCC-assisted quantum capacity region of a quantum broadcast channel. We then applied the presented squashed entanglement bounds to the pure-loss bosonic broadcast channel with an arbitrary number of receivers, and the special case of communication between a sender and each of the individual receivers.

Since the squashed entanglement bounds presented here are independent of the physical examples given, we expect it to apply to other systems not discussed here.

In the future, our bound should be examined in the context of a limited number of channel uses in addition to the energy constraint. It still remains an open question

from [5, 6, 17] to determine whether the squashed entanglement bounds could serve as strong converse rates. We also think it is clear that our formalism can be generalized to even more settings, such as those considered in [10, 14, 65]. An important technical question is whether the energy-constrained squashed entanglement bounds could apply when the LOCC channels involved are not countably decomposable, and answering this question is directly related to the question discussed in [28, Remark 1]. Finally, we think it would be interesting to find physical examples outside of the bosonic setting to which our general theory could apply.

## ACKNOWLEDGMENTS

We are grateful to Kenneth Goodenough, Saikat Guha, Masahiro Takeoka, and Kaushik Seshadreesan for discussions regarding this research. We are especially grateful to Kenneth Goodenough for many insightful discussions about his prior results in [7] and for his suggestions regarding the bound in (177). ND acknowledges support from the Department of Physics and Astronomy at LSU and the National Science Foundation under Grant No. 1714215. MMW acknowledges support from the Office of Naval Research.

- 
- [1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Bangalore India, Dec. 1984)* (1984), p. 175.
- [2] A. K. Ekert, *Physical Review Letters* **67**, 661 (1991).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Reviews of Modern Physics* **81**, 1301 (2009), arXiv:0802.4155.
- [4] F. Grosshans and P. Grangier, *Physical Review Letters* **88**, 057902 (2002), arXiv:quant-ph/0109084.
- [5] M. Takeoka, S. Guha, and M. M. Wilde, *Nature Communications* **5**, 5235 (2014), arXiv:1504.06390.
- [6] K. Seshadreesan, M. Takeoka, and M. M. Wilde, *IEEE Transactions on Information Theory* **62**, 289 (2016), arXiv:1503.08139.
- [7] K. Goodenough, D. Elkouss, and S. Wehner, *New Journal of Physics* **18**, 063005 (2016), arXiv:1511.08710v2.
- [8] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi (2017), arXiv:1510.08863v5.
- [9] M. Takeoka, K. Seshadreesan, and M. M. Wilde, *Physical Review Letters* **119**, 150501 (2017), arXiv:1706.06746.
- [10] K. Azuma, A. Mizutani, and H.-K. Lo, *Nature Communications* **7**, 13523 (2016), arXiv:1601.02933.
- [11] M. M. Wilde, M. Tomamichel, and M. Berta, *IEEE Transactions on Information Theory* **63**, 1792 (2017), arXiv:1602.08898.
- [12] M. Christandl and A. Müller-Hermes, *Communications in Mathematical Physics* **353**, 821 (2017), ISSN 1432-0916, arXiv:1604.03448, URL <http://dx.doi.org/10.1007/s00220-017-2885-y>.
- [13] M. M. Wilde, *Quantum Information Processing* **15**, 4563 (2016), arXiv:1606.08028.
- [14] S. Bäuml and K. Azuma, *Quantum Science and Technology* **2**, 024004 (2017), arXiv:1609.03994, URL <http://stacks.iop.org/2058-9565/2/i=2/a=024004>.
- [15] F. Rozpedek, K. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss (2017), arXiv:1705.00043.
- [16] E. Kaur and M. M. Wilde, *Physical Review A* **96**, 062318 (2017), arXiv:1706.04590.
- [17] M. Takeoka, S. Guha, and M. M. Wilde, *IEEE Transactions on Information Theory* **60**, 4987 (2014), arXiv:1310.0129.
- [18] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Physical Review Letters* **76**, 722 (1996), arXiv:quant-ph/9511027.
- [19] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Physical Review A* **54**, 3824 (1996), arXiv:quant-ph/9604024.
- [20] A. Müller-Hermes, Master's thesis, Technical University of Munich (2012).
- [21] A. S. Holevo and R. F. Werner, *Physical Review A* **63**, 032312 (2001), arXiv:quant-ph/9912067.
- [22] M. M. Wolf, D. Pérez-García, and G. Giedke, *Physical Review Letters* **98**, 130501 (2007), arXiv:quant-ph/0606132.
- [23] M. M. Wilde and H. Qi (2016), arXiv:1609.01997.
- [24] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Reviews of Modern Physics* **81**, 865 (2009), arXiv:quant-ph/0702225.
- [25] M. Christandl and A. Winter, *Journal of Mathematical Physics* **45**, 829 (2004), arXiv:quant-ph/0308088.

- [26] R. Alicki and M. Fannes, *Journal of Physics A: Mathematical and General* **37**, L55 (2004), arXiv:quant-ph/0312081.
- [27] F. G. S. L. Brandao, M. Christandl, and J. Yard, *Communications in Mathematical Physics* **306**, 805 (2011), ISSN 0010-3616, arXiv:1010.1750.
- [28] M. E. Shirokov, *Journal of Mathematical Physics* **57**, 032203 (2016), arXiv:1507.08964.
- [29] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song, *IEEE Transactions on Information Theory* **55**, 3375 (2009), arXiv:07042236.
- [30] D. Avis, P. Hayden, and I. Savov, *Journal of Physics A: Mathematical and General* **41**, 115301 (2008), arXiv:0707.2792.
- [31] M. Hayashi, *Quantum Information: An Introduction* (Springer, 2006).
- [32] A. S. Holevo, *Quantum Systems, Channels, Information, de Gruyter Studies in Mathematical Physics* (Book 16) (de Gruyter, 2012).
- [33] T. Heinosaari and M. Ziman, *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement* (Cambridge University Press, 2012).
- [34] M. M. Wilde, *From classical to quantum Shannon theory* (2016), arXiv:1106.1445v7.
- [35] R. F. Werner, *Physical Review A* **40**, 4277 (1989).
- [36] I. Devetak and P. W. Shor, *Communications in Mathematical Physics* **256**, 287 (2005), arXiv:quant-ph/0311131.
- [37] A. S. Holevo, *Theory of Probability & Its Applications* **51**, 92 (2007), arXiv:quant-ph/0509101, <https://doi.org/10.1137/S0040585X97982244>, URL <https://doi.org/10.1137/S0040585X97982244>.
- [38] C. King, K. Matsumoto, M. Nathanson, and M. B. Ruskai, *Markov Processes and Related Fields* **13**, 391 (2007), j. T. Lewis memorial issue. arXiv:quant-ph/0509126.
- [39] E. B. Davies and J. T. Lewis, *Communications in Mathematical Physics* **17**, 239 (1970).
- [40] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, *Communications in Mathematical Physics* **328**, 303 (2014), ISSN 1432-0916, arXiv:1210.4583, URL <http://dx.doi.org/10.1007/s00220-014-1953-9>.
- [41] C. W. Helstrom, *Journal of Statistical Physics* **1**, 231 (1969), ISSN 0022-4715.
- [42] A. S. Holevo, *Journal of Multivariate Analysis* **3**, 337 (1973).
- [43] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
- [44] A. Uhlmann, *Reports on Mathematical Physics* **9**, 273 (1976).
- [45] H. Araki and E. H. Lieb, *Communications in Mathematical Physics* **18**, 160 (1970).
- [46] A. Wehrl, *Reports on Mathematical Physics* **10**, 159 (1976), ISSN 0034-4877, URL <http://www.sciencedirect.com/science/article/pii/0034487776900379>.
- [47] V. Baccetti and M. Visser, *Journal of Statistical Mechanics: Theory and Experiment* **2013**, P04010 (2013), URL <http://stacks.iop.org/1742-5468/2013/i=04/a=P04010>.
- [48] H. Falk, *American Journal of Physics* **38**, 858 (1970).
- [49] G. Lindblad, *Communications in Mathematical Physics* **33**, 305 (1973), ISSN 1432-0916, URL <http://dx.doi.org/10.1007/BF01646743>.
- [50] G. Lindblad, *Communications in Mathematical Physics* **40**, 147 (1975), ISSN 1432-0916.
- [51] M. E. Shirokov, *Sbornik: Mathematics* **207**, 724 (2015), arXiv:1506.06377.
- [52] A. A. Kuznetsova, *Theory of Probability & Its Applications* **55**, 709 (2011), arXiv:1004.4519, <http://dx.doi.org/10.1137/S0040585X97985121>, URL <http://dx.doi.org/10.1137/S0040585X97985121>.
- [53] E. H. Lieb and M. B. Ruskai, *Journal of Mathematical Physics* **14**, 1938 (1973).
- [54] E. H. Lieb and M. B. Ruskai, *Physical Review Letters* **30**, 434 (1973).
- [55] R. R. Tucci (2000), quant-ph/0005119v1, quant-ph/0005119v1.
- [56] R. R. Tucci (2002), arXiv:quant-ph/0202144, quant-ph/0202144v2.
- [57] M. Koashi and A. Winter, *Physical Review A* **69**, 022309 (2004), arXiv:quant-ph/0310037, URL <http://link.aps.org/doi/10.1103/PhysRevA.69.022309>.
- [58] M. Christandl, Ph.D. thesis, University of Cambridge (2006), arXiv:quant-ph/0604183.
- [59] K. Li and A. Winter (2014), arXiv:1410.4184.
- [60] C. A. Fuchs and J. van de Graaf, *IEEE Transactions on Information Theory* **45**, 1216 (1998), arXiv:quant-ph/9712042.
- [61] M. Shirokov, *Journal of Mathematical Physics* **58**, 102202 (2017), arXiv:1512.09047, 1604.00568v1.
- [62] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Physical Review Letters* **94**, 160502 (2005), arXiv:quant-ph/0309110, URL <http://link.aps.org/doi/10.1103/PhysRevLett.94.160502>.
- [63] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *IEEE Transactions on Information Theory* **55**, 1898 (2009), arXiv:quant-ph/0506189.
- [64] E. Kaur and M. M. Wilde, *Journal of Physics A* **51**, 035303 (2018), arXiv:1707.07721.
- [65] L. Rigovacca, G. Kato, S. Baeuml, M. S. Kim, W. J. Munro, and K. Azuma (2017), arXiv:1707.05543.
- [66] M. Berta and M. M. Wilde (2017), arXiv:1709.04907.
- [67] A. S. Holevo and M. E. Shirokov, *Problems of Information Transmission* **49**, 15 (2013), arXiv:1210.6926.
- [68] A. S. Holevo, *Proceedings of SPIE, First International Symposium on Quantum Informatics* **5128**, 62 (2003), arXiv:quant-ph/0211170, URL <http://dx.doi.org/10.1117/12.517873>.
- [69] A. S. Holevo, *Theory of Probability & Its Applications* **48**, 243 (2004), arXiv:quant-ph/0211170, <http://dx.doi.org/10.1137/S0040585X97980415>, URL <http://dx.doi.org/10.1137/S0040585X97980415>.
- [70] A. S. Holevo and M. E. Shirokov, *Theory of Probability & Its Applications* **50**, 86 (2006), arXiv:quant-ph/0408176, <http://dx.doi.org/10.1137/S0040585X97981470>, URL <http://dx.doi.org/10.1137/S0040585X97981470>.
- [71] A. S. Holevo, *Doklady Mathematics* **82**, 730 (2010), ISSN 1531-8362, arXiv:1003.5765, URL <http://dx.doi.org/10.1134/S1064562410050133>.
- [72] A. Wehrl, *Reviews of Modern Physics* **50**, 221 (1978), URL <https://link.aps.org/doi/10.1103/RevModPhys.50.221>.
- [73] M. M. Wolf, G. Giedke, and J. I. Cirac, *Physical Review Letters* **96**, 080502 (2006), arXiv:quant-ph/0509154, URL <http://link.aps.org/doi/10.1103/PhysRevLett.96.080502>.
- [74] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka

- (2018), arXiv:1708.07257v2.
- [75] J. S. Ivan, K. K. Sabapathy, and R. Simon, *Physical Review A* **84**, 042311 (2011), arXiv:1012.4266.
- [76] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982).
- [77] F. Caruso, V. Giovannetti, and A. S. Holevo, *New Journal of Physics* **8**, 310 (2006), arXiv:quant-ph/0609013, URL <http://stacks.iop.org/1367-2630/8/i=12/a=310>.
- [78] R. Garcia-Patron, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, *Physical Review Letters* **108**, 110505 (2012), arXiv:1111.1986, URL <http://link.aps.org/doi/10.1103/PhysRevLett.108.110505>.
- [79] R. Koenig and G. Smith, *Physical Review Letters* **110**, 040501 (2013), arXiv:1207.0256, URL <http://link.aps.org/doi/10.1103/PhysRevLett.110.040501>.
- [80] B. R. Bardhan and M. M. Wilde, *Physical Review A* **89**, 022302 (2014), arXiv:1312.3287, URL <https://link.aps.org/doi/10.1103/PhysRevA.89.022302>.
- [81] B. R. Bardhan, R. Garcia-Patron, M. M. Wilde, and A. Winter, *IEEE Transactions on Information Theory* **61**, 1842 (2015), arXiv:1401.4161.
- [82] K. Noh, V. V. Albert, and L. Jiang (2018), arXiv:1801.07271.
- [83] M. Horodecki, P. W. Shor, and M. B. Ruskai, *Reviews in Mathematical Physics* **15**, 629 (2003), arXiv:quant-ph/0302031.
- [84] M. Rosati, A. Mari, and V. Giovannetti (2018), arXiv:1801.04731.
- [85] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, Unpublished notes available upon request (2017).
- [86] A. S. Holevo, *Problems of Information Transmission* **44**, 171 (2008), ISSN 1608-3253, arXiv:0802.0235, URL <http://dx.doi.org/10.1134/S0032946008030010>.
- [87] S. Watanabe, *IBM Journal of Research and Development* **4**, 66 (1960).
- [88] T. S. Han, *Information and Control* **29**, 337 (1975), ISSN 0019-9958, URL <http://www.sciencedirect.com/science/article/pii/S0019995875800040>.
- [89] T. S. Han, *Information and Control* **36**, 133 (1978), ISSN 0019-9958, URL <http://www.sciencedirect.com/science/article/pii/S0019995878902759>.
- [90] N. J. Cerf, S. Massar, and S. Schneider, *Physical Review A* **66**, 042309 (2002), arXiv:quant-ph/0202103, URL <http://link.aps.org/doi/10.1103/PhysRevA.66.042309>.
- [91] I. Devetak and J. Yard, *Physical Review Letters* **100**, 230501 (2008).
- [92] J. Yard and I. Devetak, *IEEE Transactions on Information Theory* **55**, 5339 (2009), arXiv:0706.2907.
- [93] P. Horodecki and R. Augusiak, *Physical Review A* **74**, 010302 (2006), arXiv:quant-ph/0602176, URL <http://link.aps.org/doi/10.1103/PhysRevA.74.010302>.
- [94] J. Yard, P. Hayden, and I. Devetak, *IEEE Transactions on Information Theory* **57**, 7147 (2011), arXiv:quant-ph/0603098.
- [95] S. Guha, Ph.D. thesis, Massachusetts Institute of Technology (2008).