Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices

Das, Siddhartha; Bäuml, Stefan; Wilde, Mark M.

DOI
10.1103/PhysRevA.101.012344

Publication date
2020

Document Version
Final published version

Published in
Physical Review A

Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices

Siddhartha Das,[1,2,*] Stefan Bäuml,[3,4,5,†] and Mark M. Wilde[1,6,‡]

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

[2]*Centre for Quantum Information & Communication (QuIC), École polytechnique de Bruxelles, Université libre de Bruxelles, Brussels, B-1050, Belgium*

[3]*ICFO-Institut de Ciencies Fotoniques, Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain*

[4]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*

[5]*NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[6]*Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

(Received 31 December 2018; revised manuscript received 15 July 2019; published 27 January 2020)

A bipartite quantum interaction corresponds to the most general quantum interaction that can occur between two quantum systems in the presence of a bath. In this work, we determine bounds on the capacities of bipartite interactions for entanglement generation and secret-key agreement between two quantum systems. Our upper bound on the entanglement generation capacity of a bipartite quantum interaction is given by a quantity called the bidirectional max-Rains information. Our upper bound on the secret-key-agreement capacity of a bipartite quantum interaction is given by a related quantity called the bidirectional max-relative entropy of entanglement. We also derive tighter upper bounds on the capacities of bipartite interactions obeying certain symmetries. Observing that reading of a memory device is a particular kind of bipartite quantum interaction, we leverage our bounds from the bidirectional setting to deliver bounds on the capacity of a task that we introduce, called private reading of a wiretap memory cell. Given a set of point-to-point quantum wiretap channels, the goal of private reading is for an encoder to form codewords from these channels, in order to establish a secret key with a party who controls one input and one output of the channels, while a passive eavesdropper has access to one output of the channels. We derive both lower and upper bounds on the private reading capacities of a wiretap memory cell. We then extend these results to determine achievable rates for the generation of entanglement between two distant parties who have coherent access to a controlled point-to-point channel, which is a particular kind of bipartite interaction.

DOI: 10.1103/PhysRevA.101.012344

I. INTRODUCTION

In general, any two-body quantum system of interest can be in contact with a bath, and part of the composite system may be inaccessible to observers possessing these systems. The effective interaction between given two constituent systems in the presence of the bath is known as a bipartite quantum interaction. It is well known that a closed quantum system evolves according to a unitary transformation [1,2].

Let $U^{\hat{H}}_{A'B'E'\to ABE}$ denote a unitary transformation associated to a Hamiltonian $\hat{H}$, which governs the underlying interaction between a two-body quantum system and a bath. Here $A'B'$ and E' denote system labels for a two-body quantum system of interest and the inaccessible bath, respectively, at an initial time, and AB and E denote system labels for a two-body quantum system of interest and the inaccessible bath, respectively, at a final time when the evolution is complete. The individual input systems A', B', and E' and the respective output systems A, B, and E can have different dimensions. Initially, in the absence of an interaction Hamiltonian $\hat{H}$, the bath is taken to be in a pure state and the systems of interest have no correlation with the bath; i.e., the state of the composite system $A'B'E'$ is of the form $\omega_{A'B'}\otimes|0\rangle\langle 0|_{E'}$, where $\omega_{A'B'}$ and $|0\rangle\langle 0|_{E'}$ are density operators of the systems $A'B'$ and E', respectively. Under the action of the Hamiltonian $\hat{H}$, the state of the composite system transforms as

$$\rho_{ABE} = U^{\hat{H}}(\omega_{A'B'}\otimes|0\rangle\langle 0|_{E'})(U^{\hat{H}})^{\dagger}. \tag{1}$$

Since the system E in (1) is inaccessible, the evolution of the systems of interest is noisy in general. The noisy evolution of the bipartite system $A'B'$ under the action of Hamiltonian $\hat{H}$ is represented by a completely positive, trace-preserving (CPTP) map [3], called a bipartite quantum channel:

$$\mathcal{N}^{\hat{H}}_{A'B'\to AB}(\omega_{A'B'}) = \mathrm{Tr}_E\{U^{\hat{H}}(\omega_{A'B'}\otimes|0\rangle\langle 0|_{E'})(U^{\hat{H}})^{\dagger}\}, \tag{2}$$

*sidddas@ulb.ac.be

†stefan.baeuml@icfo.eu

‡mwilde@lsu.edu

where system E represents inaccessible degrees of freedom. In particular, when the Hamiltonian $\hat{H}$ is such that there is no interaction between the composite system $A'B'$ and the bath E', and $A'B' \simeq AB$, then $\mathcal{N}^{\hat{H}}$ corresponds to a bipartite unitary, i.e., $\mathcal{N}^{\hat{H}}(\cdot) = U^{\hat{H}}_{A'B'\to AB}(\cdot)(U^{\hat{H}}_{A'B'\to AB})^{\dagger}$.

In an information-theoretic setting, a bipartite quantum channel $\mathcal{N}_{A'B'\to AB}$ is also called *bidirectional quantum channel* when system pairs A', A and B', B belong to two separate parties (cf. Ref. [4]).

Depending on the kind of bipartite quantum interaction, there may be an increase, decrease, or no change in the amount of entanglement [5,6] of a bipartite state after undergoing a bipartite interaction. As entanglement is one of the fundamental and intriguing quantum phenomena [7,8], determining the entangling abilities of bipartite quantum interactions is pertinent.

In this work, we focus on two different information-processing tasks relevant for bipartite quantum interactions, the first being entanglement distillation [9–11] and the second secret-key agreement [12–15]. Entanglement distillation is the task of generating a maximally entangled state, such as the singlet state, when two separated quantum systems undergo a bipartite interaction. Whereas, a secret-key agreement is the task of extracting maximal classical correlation between two separated systems, such that it is independent of the state of the bath system, which an eavesdropper could possess. Both of these tasks are of practical interest: distilling pure maximally entangled states is useful for fundamental tasks such as teleportation [16], super-dense coding [17], and distributed quantum computation, while a distilled secret key is useful for private communication when combined with the one-time pad. Thus, it is of interest to know fundamental limitations for these tasks for the design of actual protocols, and this is what our bounds provide.

In an information-theoretic setting, a bipartite interaction between classical systems was first considered in Ref. [18] in the context of communication; therein, a bipartite interaction was called a two-way communication channel. In the quantum domain, bipartite unitaries have been widely considered in the context of their entangling ability, applications for interactive communication tasks, and the simulation of bipartite Hamiltonians in distributed quantum computation [4,19–28]. These unitaries form the simplest model of nontrivial interactions in many-body quantum systems and have been used as a model of scrambling in the context of quantum chaotic systems [29–31], as well as for the internal dynamics of a black hole [32] in the context of the information-loss paradox [33]. More generally, [34] developed the model of a bipartite interaction or two-way quantum communication channel. Bounds on the rate of entanglement generation in open quantum systems undergoing time evolution have also been discussed for particular classes of quantum dynamics [35,36].

The maximum rate at which a particular task can be accomplished by allowing the use of a bipartite interaction a large number of times, is equal to the capacity of the interaction for the task. The entanglement-generating capacity quantifies the maximum rate of entanglement that can be generated from a bipartite interaction. Various capacities of a general bipartite unitary evolution were formalized in Ref. [4]. Later, various capacities of a general two-way channel were discussed in Ref. [34]. The entanglement-generating capacities of bipartite unitaries for different communication protocols have been widely discussed in the literature [4,20,37–41]. Also, prior to our work here, it was an open question to find a nontrivial, computationally efficient upper bound on the entanglement-generating capacity of a bipartite quantum interaction. Another natural direction left open in prior work is to determine other information-processing tasks for bipartite quantum interactions, beyond those discussed previously [4,34].

In this paper, we determine bounds on the capacities of bipartite interactions for entanglement generation and a secret-key agreement. Observing that the read-out task of memory devices is a particular kind of bipartite quantum interaction (cf. Refs. [22,42]), we leverage our bounds from the bidirectional setting to deliver bounds on the capacity of a task that we introduce here, called private reading of a memory cell. We derive both lower and upper bounds on the capacities of private reading protocols. We then extend these results to determine achievable rates for the generation of entanglement between two distant parties who have coherent access to a controlled point-to-point channel, which is a particular kind of bipartite interaction.

Private reading is a quantum information-processing task in which a classical message from an encoder to a reader is delivered in a *read-only* memory device. The message is encoded in such a way that a reader can reliably decode it, while a passive eavesdropper recovers no information about it. This protocol can be used for a secret-key agreement between two trusted parties. A physical model of a read-only memory device involves encoding the classical message using a *memory cell*, which is a set of point-to-point quantum wiretap channels. Note that a point-to-point quantum wiretap channel is a channel that takes one input and produces two outputs. The reading task is restricted to information-storage devices that are read-only, such as a CD-ROM. One feature of a read-only memory device is that a message is stored for a fairly long duration if it is kept safe from tampering. One can read information from these devices many times without the eavesdropper learning about the encoded message.

The strong converse bounds on the bidirectional quantum and private capacities of bidirectional channels presented in this work have also been stated, in abbreviated form and without proofs, in our companion paper [43]. There we also compute the bounds on the bidirectional quantum capacity for several examples. In the current paper, we present a more comprehensive discussion of the results, including proofs and derivations, as well as a detailed overview of the underlying concepts. The present article also includes additional results on private reading, namely, the computation of the nonadaptive private reading capacity of a wiretap memory cell presented in Theorem 5, an alternative converse bound on the nonadaptive private reading capacity of an isometric memory cell presented in Proposition 4, and the study of entanglement generation from a coherent memory cell or controlled isometry, presented in Sec. VII.

The organization of our paper is as follows. We set notation and review basic definitions in Sec. II. In Sec. III we derive a strong converse upper bound on the rate at which entanglement can be distilled from a bipartite quantum interaction. This bound is given by an information quantity that we call the bidirectional max-Rains information $R_{\max}^{2\to 2}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$. The bidirectional max-Rains information is the solution to a semidefinite program and is thus efficiently computable. In Sec. IV we derive a strong converse upper bound on the rate at which a secret key can be distilled from a bipartite quantum interaction. This bound is given by a related information quantity that we call the bidirectional max-relative entropy of entanglement $E_{\max}^{2\to 2}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$. In Sec. V we derive upper bounds on the entanglement generation and secret-key-agreement capacities of bidirectional PPT- and teleportation-simulable channels, respectively. Our upper bounds on the capacities of such channels depend only on the entanglement of the resource states with which these bidirectional channels can be simulated. In Sec. VI we introduce a protocol called private reading, whose goal is to generate a secret key between an encoder and a reader. We derive both lower and upper bounds on the private reading capacities. In Sec. VII we introduce a protocol whose goal is to generate entanglement between two parties who have coherent access to a memory cell, and we give a lower bound on the entanglement generation capacity in this setting. Finally, we conclude in Sec. VIII with a summary and some open directions.

II. PRELIMINARIES

We begin by establishing some notation and reviewing definitions needed in the rest of the paper.

A. States, channels, isometries, separable states, and positive partial transpose

Let $\mathcal{B}(\mathcal{H})$ denote the algebra of bounded linear operators acting on a Hilbert space $\mathcal{H}$. Throughout this paper, we restrict our development to finite-dimensional Hilbert spaces. The subset of $\mathcal{B}(\mathcal{H})$ containing all positive semidefinite operators is denoted by $\mathcal{B}_+(\mathcal{H})$. We denote the identity operator as I and the identity superoperator as id. The Hilbert space of a quantum system A is denoted by $\mathcal{H}_A$. The state of a quantum system A is represented by a density operator ρ_A, which is a positive semidefinite operator with unit trace. Let $\mathcal{D}(\mathcal{H}_A)$ denote the set of density operators, i.e., all elements $\rho_A \in \mathcal{B}_+(\mathcal{H}_A)$ such that $\mathrm{Tr}\{\rho_A\} = 1$. The Hilbert space for a composite system LA is denoted as $\mathcal{H}_{LA}$ where $\mathcal{H}_{LA} = \mathcal{H}_L \otimes \mathcal{H}_A$. The density operator of a composite system LA is defined as $\rho_{LA} \in \mathcal{D}(\mathcal{H}_{LA})$, and the partial trace over A gives the reduced density operator for system L, i.e., $\mathrm{Tr}_A\{\rho_{LA}\} = \rho_L$ such that $\rho_L \in \mathcal{D}(\mathcal{H}_L)$. The notation $A^n := A_1A_2\dots A_n$ indicates a composite system consisting of n subsystems, each of which is isomorphic to the Hilbert space $\mathcal{H}_A$. A pure state ψ_A of a system A is a rank-one density operator, and we write it as $\psi_A = |\psi\rangle\langle\psi|_A$ for $|\psi\rangle_A$ a unit vector in $\mathcal{H}_A$. A purification of a density operator ρ_A is a pure state ψ^ρ_{EA} such that $\mathrm{Tr}_E\{\psi^\rho_{EA}\} = \rho_A$, where E is called the purifying system. The maximally mixed state is denoted by $\pi_A := I_A/\dim(\mathcal{H}_A) \in \mathcal{D}(\mathcal{H}_A)$. The fidelity of $\tau, \sigma \in \mathcal{B}_+(\mathcal{H})$ is defined as $F(\tau,\sigma) = \|\sqrt{\tau}\sqrt{\sigma}\|_1^2$ [44], with the trace norm $\|X\|_1 = \mathrm{Tr}\sqrt{X^\dagger X}$ for $X \in \mathcal{B}(\mathcal{H})$.

The adjoint $\mathcal{M}^\dagger : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ of a linear map $\mathcal{M} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is the unique linear map such that

$$\langle Y_B, \mathcal{M}(X_A)\rangle = \langle \mathcal{M}^\dagger(Y_B), X_A\rangle, \tag{3}$$

for all $X_A \in \mathcal{B}(\mathcal{H}_A)$ and $Y_B \in \mathcal{B}(\mathcal{H}_B)$, where $\langle C, D\rangle = \mathrm{Tr}\{C^\dagger D\}$ is the Hilbert-Schmidt inner product. An isometry $U{:}\mathcal{H} \to \mathcal{H}'$ is a linear map such that $U^\dagger U = I_{\mathcal{H}}$.

The evolution of a quantum state is described by a quantum channel. A quantum channel $\mathcal{M}_{A\to B}$ is a CPTP map $\mathcal{M}{:}\mathcal{B}_+(\mathcal{H}_A) \to \mathcal{B}_+(\mathcal{H}_B)$. A memory cell $\{\mathcal{M}^x\}_{x\in\mathcal{X}}$ is defined as a set of quantum channels $\mathcal{M}^x$, for all $x \in \mathcal{X}$, where $\mathcal{X}$ is a finite alphabet, and $\mathcal{M}^x : \mathcal{B}_+(\mathcal{H}_A) \to \mathcal{B}_+(\mathcal{H}_B)$.

Let $U^{\mathcal{M}}_{A\to BE}$ denote an isometric extension of a quantum channel $\mathcal{M}_{A\to B}$, which by definition means that for all $\rho_A \in \mathcal{D}(\mathcal{H}_A)$,

$$\mathrm{Tr}_E\left\{U^{\mathcal{M}}_{A\to BE}\rho_A\left(U^{\mathcal{M}}_{A\to BE}\right)^\dagger\right\} = \mathcal{M}_{A\to B}(\rho_A), \tag{4}$$

along with the following conditions for $U^{\mathcal{M}}$ to be an isometry:

$$(U^{\mathcal{M}})^\dagger U^{\mathcal{M}} = I_A. \tag{5}$$

As a consequence of (5), we conclude that $U^{\mathcal{M}}(U^{\mathcal{M}})^\dagger = \Pi_{BE}$, where Π_{BE} is a projection onto a subspace of the Hilbert space $\mathcal{H}_{BE}$. A complementary channel $\widehat{\mathcal{M}}_{A\to E}$ of $\mathcal{M}_{A\to B}$ is defined as

$$\widehat{\mathcal{M}}_{A\to E}(\rho_A) := \mathrm{Tr}_B\left\{U^{\mathcal{M}}_{A\to BE}\rho_A\left(U^{\mathcal{M}}_{A\to BE}\right)^\dagger\right\}, \tag{6}$$

for all $\rho_A \in \mathcal{D}(\mathcal{H}_A)$.

The Choi isomorphism represents a well-known duality between channels and states. Let $\mathcal{M}_{A\to B}$ be a quantum channel, and let $|\Upsilon\rangle_{L:A}$ denote the following maximally entangled vector:

$$|\Upsilon\rangle_{L:A} := \sum_i |i\rangle_L|i\rangle_A, \tag{7}$$

where $\dim(\mathcal{H}_L) = \dim(\mathcal{H}_A)$, and $\{|i\rangle_L\}_i$ and $\{|i\rangle_A\}_i$ are fixed orthonormal bases. We extend this notation to multiple parties with a given bipartite cut as

$$|\Upsilon\rangle_{L_AL_B:AB} := |\Upsilon\rangle_{L_A:A} \otimes |\Upsilon\rangle_{L_B:B}. \tag{8}$$

The maximally entangled state Φ_{LA} is denoted as

$$\Phi_{LA} := \frac{1}{|A|}|\Upsilon\rangle\langle\Upsilon|_{LA}, \tag{9}$$

where $|A| = \dim(\mathcal{H}_A)$. The Choi operator for a channel $\mathcal{M}_{A\to B}$ is defined as

$$J^{\mathcal{M}}_{LB} := (\mathrm{id}_L \otimes \mathcal{M}_{A\to B})(|\Upsilon\rangle\langle\Upsilon|_{LA}), \tag{10}$$

where id_L denotes the identity map on L. For $A' \simeq A$, the following identity holds:

$$\langle\Upsilon|_{A':L}\left(\rho_{SA'} \otimes J^{\mathcal{M}}_{LB}\right)|\Upsilon\rangle_{A':L} = \mathcal{M}_{A\to B}(\rho_{SA}), \tag{11}$$

where $A' \simeq A$. The above identity can be understood in terms of a postselected variant [45] of the quantum teleportation protocol [16]. Another identity that holds is

$$\langle\Upsilon|_{L:A}[Q_{SL} \otimes I_A]|\Upsilon\rangle_{L:A} = \mathrm{Tr}_L\{Q_{SL}\}, \tag{12}$$

for an operator $Q_{SL} \in \mathcal{B}(\mathcal{H}_S \otimes \mathcal{H}_L)$.

For a fixed basis $\{|i\rangle_B\}_i$, the partial transpose T_B on system B is the following map:

$$(\mathrm{id}_A\otimes \mathrm{T}_B)(Q_{AB}) = \sum_{i,j}(I_A\otimes |i\rangle\langle j|_B)Q_{AB}(I_A\otimes |i\rangle\langle j|_B), \tag{13}$$

where $Q_{AB}\in\mathcal{B}(\mathcal{H}_A\otimes\mathcal{H}_B)$.

Furthermore, it holds that

$$(Q_{SL}\otimes I_A)|\Upsilon\rangle_{L:A} = (\mathrm{T}_A(Q_{SA})\otimes I_L)|\Upsilon\rangle_{L:A}. \tag{14}$$

We note that the partial transpose is self-adjoint, i.e., $\mathrm{T}_B = \mathrm{T}_B^\dagger$, and is also involutory:

$$\mathrm{T}_B\circ\mathrm{T}_B = I_B. \tag{15}$$

The following identity also holds:

$$\mathrm{T}_L(|\Upsilon\rangle\langle\Upsilon|_{LA}) = \mathrm{T}_A(|\Upsilon\rangle\langle\Upsilon|_{LA}). \tag{16}$$

Let $\mathrm{SEP}(A\!:\!B)$ denote the set of all separable states $\sigma_{AB}\in\mathcal{D}(\mathcal{H}_A\otimes\mathcal{H}_B)$, which are states that can be written as

$$\sigma_{AB} = \sum_x p(x)\omega_A^x\otimes\tau_B^x, \tag{17}$$

where $p(x)$ is a probability distribution, $\omega_A^x\in\mathcal{D}(\mathcal{H}_A)$, and $\tau_B^x\in\mathcal{D}(\mathcal{H}_B)$ for all x. This set is closed under the action of the partial transpose maps T_A and T_B [46,47]. Generalizing the set of separable states, we define the set $\mathrm{PPT}(A\!:\!B)$ of all bipartite states ρ_{AB} that remain positive after the action of the partial transpose T_B. A state $\rho_{AB}\in\mathrm{PPT}(A\!:\!B)$ is also called a PPT (positive under partial transpose) state. We can define an even more general set of positive semidefinite operators [48] as follows:

$$\mathrm{PPT}'(A\!:\!B) := \{\sigma_{AB}:\ \sigma_{AB}\geqslant 0\wedge\|\mathrm{T}_B(\sigma_{AB})\|_1\leqslant 1\}. \tag{18}$$

We then have the containments $\mathrm{SEP}\subset\mathrm{PPT}\subset\mathrm{PPT}'$. A bipartite quantum channel $\mathcal{P}_{A'B'\to AB}$ is a completely PPT-preserving channel if the map $\mathrm{T}_B\circ\mathcal{P}_{A'B'\to AB}\circ\mathrm{T}_{B'}$ is a quantum channel [11,49] (see also Ref. [50]). A bipartite quantum channel $\mathcal{P}_{A'B'\to AB}$ is completely PPT-preserving if and only if its Choi state is a PPT state [49],

$$\frac{J^{\mathcal{P}}_{L_AL_B:AB}}{|L_AL_B|}\in\mathrm{PPT}(L_AA\!:\!BL_B), \tag{19}$$

where

$$\frac{J^{\mathcal{P}}_{L_AL_B:AB}}{|L_AL_B|} = \mathcal{P}_{A'B'\to AB}\big(\Phi_{L_AA'}\otimes\Phi_{B'L_B}\big). \tag{20}$$

Any local operations and classical communication (LOCC) channel is a completely PPT-preserving channel [11,49]. For a formal definition of LOCC channels; see Ref. [51].

B. Channels with symmetry

Consider a finite group G. For every $g\in G$, let $g\to U_A(g)$ and $g\to V_B(g)$ be projective unitary representations of g acting on the input space $\mathcal{H}_A$ and the output space $\mathcal{H}_B$ of a quantum channel $\mathcal{M}_{A\to B}$, respectively. A quantum channel $\mathcal{M}_{A\to B}$ is covariant with respect to these representations if the following relation is satisfied [52,53]:

$$\mathcal{M}_{A\to B}[U_A(g)\rho_AU_A^\dagger(g)] = V_B(g)\mathcal{M}_{A\to B}(\rho_A)V_B^\dagger(g), \tag{21}$$

for all $\rho_A\in\mathcal{D}(\mathcal{H}_A)$ and $g\in G$.

Definition 1 (Covariant channel [53]). A quantum channel is covariant if it is covariant with respect to a group G which has a representation $U(g)$, for all $g\in G$, on $\mathcal{H}_A$ that is a unitary one-design; i.e., the map $\frac{1}{|G|}\sum_{g\in G}U(g)(\cdot)U^\dagger(g)$ always outputs the maximally mixed state for all input states.

For an isometric channel $\mathcal{U}^{\mathcal{M}}_{A\to BE}$ extending the above channel $\mathcal{M}_{A\to B}$, there exists a unitary representation $W_E(g)$ acting on the environment Hilbert space $\mathcal{H}_E$ [53], such that for all $g\in G$,

$$\begin{aligned}&\mathcal{U}^{\mathcal{M}}_{A\to BE}[U_A(g)\rho_AU_A^\dagger(g)]\\&\quad= [V_B(g)\otimes W_E(g)]\big[\mathcal{U}^{\mathcal{M}}_{A\to BE}(\rho_A)\big][V_B^\dagger(g)\otimes W_E^\dagger(g)].\end{aligned} \tag{22}$$

We restate this as the following lemma:

Lemma 1 ([53]). Suppose that a channel $\mathcal{M}_{A\to B}$ is covariant with respect to a group G. For an isometric extension $U^{\mathcal{M}}_{A\to BE}$ of $\mathcal{M}_{A\to B}$, there is a set of unitaries $\{W_E^g\}_{g\in G}$ such that the following covariance holds for all $g\in G$:

$$U^{\mathcal{M}}_{A\to BE}U_A^g = \big(V_B^g\otimes W_E^g\big)U^{\mathcal{M}}_{A\to BE}. \tag{23}$$

For convenience, we provide a proof of this interesting lemma in Appendix A.

Definition 2 (Teleportation-simulable [54,55]). A channel $\mathcal{M}_{A\to B}$ is teleportation-simulable with associated resource state ω_{L_AB} if there exists an LOCC channel $\mathcal{L}_{L_AAB\to B}$, such that for all input states $\rho_A\in\mathcal{D}(\mathcal{H}_A)$, the following equality holds:

$$\mathcal{M}_{A\to B}(\rho_A) = \mathcal{L}_{L_AAB\to B}\big(\rho_A\otimes\omega_{L_AB}\big). \tag{24}$$

(A particular example of an LOCC channel is a generalized teleportation protocol [56]).

One can find the defining equation (24) explicitly stated as [55] [Eq. (11)]. All covariant channels, as given in Definition 1, are teleportation-simulable with respect to the resource state $\mathcal{M}_{A\to B}(\Phi_{L_AA})$ [57].

Definition 3 (PPT-simulable [58]). A channel $\mathcal{M}_{A\to B}$ is PPT-simulable with associated resource state ω_{L_AB} if there exists a completely PPT-preserving channel $\mathcal{P}_{L_AAB\to B}$ (acting on systems $L_AA:B$ and where the transposition map is with respect to the system B) such that for all input states $\rho_A\in\mathcal{D}(\mathcal{H}_A)$, the following equality holds:

$$\mathcal{M}_{A\to B}(\rho_A) = \mathcal{P}_{L_AAB\to B}\big(\rho_A\otimes\omega_{L_AB}\big). \tag{25}$$

Definition 4 (Jointly covariant memory cell [59]). A set $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{M}^x_{A\to B}\}_{x\in\mathcal{X}}$ of quantum channels is jointly covariant if there exists a group G such that for all $x\in\mathcal{X}$, the channel $\mathcal{M}^x$ is a covariant channel with respect to the group G (cf. Definition 1).

Remark 1 ([59]). Any jointly covariant memory cell $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{M}^x_{A\to B}\}_x$ is jointly teleportation-simulable with respect to the set $\{\mathcal{M}^x_{A\to B}(\Phi_{L_AA})\}_x$ of resource states.

C. Bipartite interactions and controlled channels

Let us consider a bipartite quantum interaction between systems X' and B', generated by a Hamiltonian $\hat{H}_{X'B'E'}$, where E' is a bath system. Suppose that the Hamiltonian is time independent, having the following form:

$$\hat{H}_{X'B'E'} := \sum_{x\in\mathcal{X}}|x\rangle\langle x|_{X'}\otimes\hat{H}^x_{B'E'}, \tag{26}$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ is an orthonormal basis for the Hilbert space of system X' and $\hat{H}^x_{B'E'}$ is a Hamiltonian for the composite system $B'E'$. Then the evolution of the composite system $X'B'E'$ is given by the following controlled unitary:

$$U_{\hat{H}}(t) := \sum_{x\in\mathcal{X}} |x\rangle\langle x|_{X'} \otimes \exp\left(-\frac{\iota}{\hbar}\hat{H}^x_{B'E'}t\right), \tag{27}$$

where t denotes time. Suppose that the systems B' and E' are not correlated before the action of Hamiltonian $\hat{H}^x_{B'E'}$ for each $x\in\mathcal{X}$. Then the evolution of the system B' under the interaction $\hat{H}^x_{B'E'}$ is given by a quantum channel $\mathcal{M}^x_{B'\to B}$ for all x.

For some distributed quantum computing and information-processing tasks where the controlling system X and input system B' are jointly accessible, the following bidirectional channel is relevant:

$$\mathcal{N}_{X'B'\to XB}(\cdot) := \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes \mathcal{M}^x_{B'\to B}(\langle x|(\cdot)|x\rangle_{X'}). \tag{28}$$

In the above, X' is a controlling system that determines which evolution from the set $\{\mathcal{M}^x\}_{x\in\mathcal{X}}$ takes place on input system B'. In particular, when X' and B' are spatially separated and the input states for the system $X'B'$ are considered to be in product state, the noisy evolution for such constrained interactions is given by the following bidirectional channel:

$$\begin{aligned}\mathcal{N}_{X'B'\to XB}&(\sigma_{X'}\otimes\rho_{B'})\\ &:= \sum_{x\in\mathcal{X}} \langle x|\sigma_{X'}|x\rangle_{X'} |x\rangle\langle x|_X \otimes \mathcal{M}^x_{B'\to B}(\rho_{B'}).\end{aligned} \tag{29}$$

This kind of bipartite interaction is in one-to-one correspondence with the notion of a memory cell from the context of quantum reading [22,42]. There a memory cell is a collection $\{\mathcal{M}^x_{B'\to B}\}_x$ of quantum channels. One party chooses which channel is applied to another party's input system B' by selecting a classical letter x. Clearly, the description in (28) is a fully quantum description of this process, and thus we see that quantum reading can be understood as the use of a particular kind of bipartite interaction.

D. Entropies and information

The quantum entropy of a density operator ρ_A is defined as [60]

$$S(A)_\rho := S(\rho_A) = -\mathrm{Tr}[\rho_A \log_2 \rho_A]. \tag{30}$$

The conditional quantum entropy $S(A|B)_\rho$ of a density operator ρ_{AB} of a composite system AB is defined as

$$S(A|B)_\rho := S(AB)_\rho - S(B)_\rho. \tag{31}$$

The coherent information $I(A\rangle B)_\rho$ of a density operator ρ_{AB} of a composite system AB is defined as [61]

$$I(A\rangle B)_\rho := -S(A|B)_\rho = S(B)_\rho - S(AB)_\rho. \tag{32}$$

The quantum relative entropy of two quantum states is a measure of their distinguishability. For $\rho\in\mathcal{D}(\mathcal{H})$ and $\sigma\in\mathcal{B}_+(\mathcal{H})$, it is defined as [62]

$$D(\rho\|\sigma) := \begin{cases}\mathrm{Tr}\{\rho[\log_2\rho - \log_2\sigma]\}, & \mathrm{supp}(\rho)\subseteq\mathrm{supp}(\sigma)\\ +\infty, & \text{otherwise.}\end{cases} \tag{33}$$

The quantum relative entropy is nonincreasing under the action of positive trace-preserving maps [63], which is the statement that $D(\rho\|\sigma)\geqslant D(\mathcal{M}(\rho)\|\mathcal{M}(\sigma))$ for any two density operators ρ and σ and a positive trace-preserving map $\mathcal{M}$ (this inequality applies to quantum channels as well [64], since every completely positive map is also a positive map by definition).

The quantum mutual information $I(L;A)_\rho$ is a measure of correlations between quantum systems L and A in a state ρ_{LA}. It is defined as

$$I(L;A)_\rho := \inf_{\sigma_A\in\mathcal{D}(\mathcal{H}_A)} D(\rho_{LA}\|\rho_L\otimes\sigma_A) \tag{34}$$

$$= S(L)_\rho + S(A)_\rho - S(LA)_\rho. \tag{35}$$

The conditional quantum mutual information $I(L;A|C)_\rho$ of a tripartite density operator ρ_{LAC} is defined as

$$I(L;A|C)_\rho := S(L|C)_\rho + S(A|C)_\rho - S(LA|C)_\rho. \tag{36}$$

It is known that quantum entropy, quantum mutual information, and conditional quantum mutual information are all nonnegative quantities (see Refs. [65,66]).

The following Alicki-Fannes-Winter (AFW) inequality gives uniform continuity bounds for conditional entropy:

Lemma 2 ([67,68]). Let $\rho_{LA},\sigma_{LA}\in\mathcal{D}(\mathcal{H}_{LA})$. Suppose that $\frac{1}{2}\|\rho_{LA}-\sigma_{LA}\|_1\leqslant\varepsilon$, where $\varepsilon\in[0,1]$. Then

$$|S(A|L)_\rho - S(A|L)_\sigma| \leqslant 2\varepsilon\log_2\dim(\mathcal{H}_A) + g(\varepsilon), \tag{37}$$

where

$$g(\varepsilon) := (1+\varepsilon)\log_2(1+\varepsilon) - \varepsilon\log_2\varepsilon, \tag{38}$$

and $\dim(\mathcal{H}_A)$ denotes the dimension of the Hilbert space $\mathcal{H}_A$.

Suppose that system L is a classical register X such that ρ_{XA} and σ_{XA} are classical–quantum (cq) states of the following form:

$$\rho_{XA} = \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x|_X\otimes\rho^x_A, \tag{39}$$

$$\sigma_{XA} = \sum_{x\in\mathcal{X}} q_X(x)|x\rangle\langle x|_X\otimes\sigma^x_A, \tag{40}$$

where $\{|x\rangle_X\}_{x\in\mathcal{X}}$ forms an orthonormal basis and for all $x\in\mathcal{X}$, $\rho^x_A,\sigma^x_A\in\mathcal{D}(\mathcal{H}_A)$. Then the following inequalities hold:

$$|S(X|A)_\rho - S(X|A)_\sigma| \leqslant \varepsilon\log_2\dim(\mathcal{H}_X) + g(\varepsilon), \tag{41}$$

$$|S(A|X)_\rho - S(A|X)_\sigma| \leqslant \varepsilon\log_2\dim(\mathcal{H}_A) + g(\varepsilon). \tag{42}$$

E. Generalized divergence and generalized relative entropies

A quantity is called a generalized divergence [69,70] if it satisfies the following monotonicity (data-processing) inequality for all density operators ρ and σ and quantum channels $\mathcal{N}$:

$$\mathbf{D}(\rho\|\sigma) \geqslant \mathbf{D}[\mathcal{N}(\rho)\|\mathcal{N}(\sigma)]. \tag{43}$$

As a direct consequence of the above inequality, any generalized divergence satisfies the following two properties for an isometry U and a state τ [71]:

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(U\rho U^\dagger\|U\sigma U^\dagger), \tag{44}$$

$$\mathbf{D}(\rho\|\sigma) = \mathbf{D}(\rho\otimes\tau\|\sigma\otimes\tau). \tag{45}$$

One can define a generalized mutual information for a quantum state ρ_{RA} as

$$I_{\mathbf{D}}(R;A)_\rho := \inf_{\sigma_A\in\mathcal{D}(\mathcal{H}_A)} \mathbf{D}(\rho_{RA}\|\rho_R\otimes\sigma_A). \tag{46}$$

The sandwiched Rényi relative entropy [71,72] is denoted as $\widetilde{D}_\alpha(\rho\|\sigma)$ and defined for $\rho\in\mathcal{D}(\mathcal{H})$, $\sigma\in\mathcal{B}_+(\mathcal{H})$, and $\forall\alpha\in(0,1)\cup(1,\infty)$ as

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\log_2 \operatorname{Tr}\left\{\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right\}, \tag{47}$$

but it is set to $+\infty$ for $\alpha\in(1,\infty)$ if $\operatorname{supp}(\rho)\nsubseteq\operatorname{supp}(\sigma)$. The sandwiched Rényi relative entropy obeys the following "monotonicity in α" inequality [72]: for $\alpha,\beta\in(0,1)\cup(1,\infty)$:

$$\widetilde{D}_\alpha(\rho\|\sigma)\leqslant\widetilde{D}_\beta(\rho\|\sigma)\quad\text{if}\quad\alpha\leqslant\beta. \tag{48}$$

The following lemma states that the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ is a particular generalized divergence for certain values of α.

Lemma 3 ([73]). Let $\mathcal{N}:\mathcal{B}_+(\mathcal{H}_A)\to\mathcal{B}_+(\mathcal{H}_B)$ be a quantum channel and let $\rho_A\in\mathcal{D}(\mathcal{H}_A)$ and $\sigma_A\in\mathcal{B}_+(\mathcal{H}_A)$. Then, for all $\alpha\in[1/2,1)\cup(1,\infty)$,

$$\widetilde{D}_\alpha(\rho\|\sigma)\geqslant\widetilde{D}_\alpha[\mathcal{N}(\rho)\|\mathcal{N}(\sigma)]. \tag{49}$$

See Ref. [74] for an alternative proof of Lemma 3 and Ref. [75] for an even different proof when $\alpha>1$.

In the limit $\alpha\to1$, the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ converges to the quantum relative entropy [71,72]:

$$\lim_{\alpha\to1}\widetilde{D}_\alpha(\rho\|\sigma) := D_1(\rho\|\sigma) = D(\rho\|\sigma). \tag{50}$$

In the limit $\alpha\to\infty$, the sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ converges to the max-relative entropy [72], which is defined as [76,77]

$$D_{\max}(\rho\|\sigma) = \inf\{\lambda:\ \rho\leqslant 2^\lambda\sigma\}, \tag{51}$$

and if $\operatorname{supp}(\rho)\nsubseteq\operatorname{supp}(\sigma)$ then $D_{\max}(\rho\|\sigma)=\infty$.

Another generalized divergence is the ε-hypothesis-testing divergence [78,79], defined as

$$\begin{aligned} D_h^\varepsilon(\rho\|\sigma) := -\log_2\inf_\Lambda\{&\operatorname{Tr}\{\Lambda\sigma\}\\ &:0\leqslant\Lambda\leqslant I\wedge\operatorname{Tr}\{\Lambda\rho\}\geqslant1-\varepsilon\}, \end{aligned} \tag{52}$$

for $\varepsilon\in[0,1]$, $\rho\in\mathcal{D}(\mathcal{H})$, and $\sigma\in\mathcal{B}_+(\mathcal{H})$.

F. Entanglement measures

Let $E(A;B)_\rho$ denote an entanglement measure [6] that is evaluated for a bipartite state ρ_{AB}. The basic property of an entanglement measure is that it should be an LOCC monotone [6], i.e., nonincreasing under the action of an LOCC channel. Given such an entanglement measure, one can define the entanglement $E(\mathcal{M})$ of a channel $\mathcal{M}_{A\to B}$ in terms of it by optimizing over all pure, bipartite states that can be input to the channel:

$$E(\mathcal{M}) = \sup_{\psi_{LA}} E(L;B)_\omega, \tag{53}$$

where $\omega_{LB}=\mathcal{M}_{A\to B}(\psi_{LA})$. Due to the properties of an entanglement measure and the well-known Schmidt decomposition theorem, it suffices to optimize over pure states ψ_{LA} such that $L\simeq A$ [i.e., one does not achieve a higher value of $E(\mathcal{M})$ by optimizing over mixed states with unbounded reference system L]. In an information-theoretic setting, the entanglement $E(\mathcal{M})$ of a channel $\mathcal{M}$ characterizes the amount of entanglement that a sender A and receiver B can generate by using the channel if they do not share entanglement prior to its use.

Alternatively, one can consider the amortized entanglement $E_A(\mathcal{M})$ of a channel $\mathcal{M}_{A\to B}$ as the following optimization [58] (see also Refs. [4,37,80–82]):

$$E_A(\mathcal{M}) := \sup_{\rho_{L_AAL_B}} [E(L_A;BL_B)_\tau - E(L_AA;L_B)_\rho], \tag{54}$$

where $\tau_{L_ABL_B}=\mathcal{M}_{A\to B}(\rho_{L_AAL_B})$ and $\rho_{L_AAL_B}$ is a state. The supremum is with respect to all states $\rho_{L_AAL_B}$ and the systems L_A, L_B are finite-dimensional but could be arbitrarily large. Thus, in general, $E_A(\mathcal{M})$ need not be computable. The amortized entanglement quantifies the net amount of entanglement that can be generated by using the channel $\mathcal{M}_{A\to B}$, if the sender and the receiver are allowed to begin with some initial entanglement in the form of the state $\rho_{L_AAL_B}$. That is, $E(L_AA;L_B)_\rho$ quantifies the entanglement of the initial state $\rho_{L_AAL_B}$, and $E(L_A;BL_B)_\tau$ quantifies the entanglement of the final state produced after the action of the channel.

The Rains relative entropy of a state ρ_{AB} is defined as [48,49]

$$R(A;B)_\rho := \min_{\sigma_{AB}\in\mathrm{PPT}'(A:B)} D(\rho_{AB}\|\sigma_{AB}), \tag{55}$$

and it is monotone nonincreasing under the action of a completely PPT-preserving quantum channel $\mathcal{P}_{A'B'\to AB}$,

$$R(A';B')_\rho\geqslant R(A;B)_\omega, \tag{56}$$

where $\omega_{AB}=\mathcal{P}_{A'B'\to AB}(\rho_{A'B'})$. The sandwiched Rains relative entropy of a state ρ_{AB} is defined as follows [83]:

$$\widetilde{R}_\alpha(A;B)_\rho := \min_{\sigma_{AB}\in\mathrm{PPT}'(A:B)} \widetilde{D}_\alpha(\rho_{AB}\|\sigma_{AB}). \tag{57}$$

The max-Rains relative entropy of a state ρ_{AB} is defined as [84]

$$R_{\max}(A;B)_\rho := \min_{\sigma_{AB}\in\mathrm{PPT}'(A:B)} D_{\max}(\rho_{AB}\|\sigma_{AB}). \tag{58}$$

The max-Rains information of a quantum channel $\mathcal{M}_{A\to B}$ is defined as [85]

$$R_{\max}(\mathcal{M}) := \max_{\phi_{SA}} R_{\max}(S;B)_\omega, \tag{59}$$

where $\omega_{SB}=\mathcal{M}_{A\to B}(\phi_{SA})$ and ϕ_{SA} is a pure state, with $\dim(\mathcal{H}_S)=\dim(\mathcal{H}_A)$. The amortized max-Rains information of a channel $\mathcal{M}_{A\to B}$, denoted as $R_{\max,A}(\mathcal{M})$, is defined by replacing E in (54) with the max-Rains relative entropy $R_{\max}$ [86]. It was shown in Ref. [86] that amortization does not enhance the max-Rains information of an arbitrary point-to-point channel,

$$R_{\max,A}(\mathcal{M}) = R_{\max}(\mathcal{M}). \tag{60}$$

Recently, in Ref. [87] (Eq. (8); see also Ref. [85]), the max-Rains relative entropy of a state ρ_{AB} was expressed as

$$R_{\max}(A;B)_\rho = \log_2 W(A;B)_\rho, \tag{61}$$

TABLE I. Overview of where one can find the definitions of various entanglement measures for states ρ_{AB}, point-to-point channels $M_{A\to B}$, bidirectional channels $N_{A'B'\to AB}$, and their amortized versions.

E	$E(\rho_{AB})$	$E(M_{A\to B})$	$E_A(M_{A\to B})$	$E^{2\to2}(N_{A'B'\to AB})$	$E_A^{2\to2}(N_{A'B'\to AB})$
$\tilde{R}_\alpha$	Eq. (57)	via Eq. (53)	via Eq. (54)		
R	Eq. (55)	via Eq. (53)	via Eq. (54)		
$R_{\max}$	Eq. (61)	Eq. (59)	via Eq. (54)	Definition 5	Eq. (111)
$\tilde{E}_\alpha$	Eq. (65)	via Eq. (53)	via Eq. (54)		
E_R	Eq. (66)	via Eq. (53)	via Eq. (54)		
$E_{\max}$	Eq. (68)	via Eq. (53)	via Eq. (54)	Definition 6	Eq. (139)
$E_{\rm sq}$	Eq. (70)	via Eq. (53)	via Eq. (54)		

where $W(A;B)_\rho$ is the solution to the following semidefinite program:

$$\begin{aligned}&\text{minimize} \quad \operatorname{Tr}\{C_{AB}+D_{AB}\}\\ &\text{subject to} \quad C_{AB}, D_{AB}\geqslant 0,\\ &\qquad\qquad T_B(C_{AB}-D_{AB})\geqslant \rho_{AB}.\end{aligned} \tag{62}$$

Similarly, in Ref. [85] [Eq. (21)], the max-Rains information of a quantum channel $\mathcal{M}_{A\to B}$ was expressed as

$$R_{\max}(\mathcal{M}) = \log_2 \Gamma(\mathcal{M}), \tag{63}$$

where $\Gamma(\mathcal{M})$ is the solution to the following semidefinite program:

$$\begin{aligned}&\text{minimize} \quad \|\operatorname{Tr}_B\{V_{SB}+Y_{SB}\}\|_\infty\\ &\text{subject to} \quad Y_{SB}, V_{SB}\geqslant 0,\\ &\qquad\qquad T_B(V_{SB}-Y_{SB})\geqslant J^{\mathcal{M}}_{SB}.\end{aligned} \tag{64}$$

The sandwiched relative entropy of entanglement of a bipartite state ρ_{AB} is defined as [88]

$$\widetilde{E}_\alpha(A;B)_\rho := \min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} \widetilde{D}_\alpha(\rho_{AB}\|\sigma_{AB}). \tag{65}$$

In the limit $\alpha\to 1$, $\widetilde{E}_\alpha(A;B)_\rho$ converges to the relative entropy of entanglement [89],

$$\lim_{\alpha\to1}\widetilde{E}_\alpha(A;B)_\rho = E_R(A;B)_\rho \tag{66}$$

$$:= \min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} D(\rho_{AB}\|\sigma_{AB}). \tag{67}$$

The max-relative entropy of entanglement [76,77] is defined for a bipartite state ρ_{AB} as

$$E_{\max}(A;B)_\rho := \min_{\sigma_{AB}\in \mathrm{SEP}(A:B)} D_{\max}(\rho_{AB}\|\sigma_{AB}). \tag{68}$$

The max-relative entropy of entanglement $E_{\max}(\mathcal{M})$ of a channel $\mathcal{M}_{A\to B}$ is defined as in (53), by replacing E with $E_{\max}$ [80]. It was shown in Ref. [80] that amortization does not increase max-relative entropy of entanglement of a channel $\mathcal{M}_{A\to B}$,

$$E_{\max,A}(\mathcal{M}) = E_{\max}(\mathcal{M}). \tag{69}$$

The squashed entanglement of a state $\rho_{AB}\in\mathcal{D}(\mathcal{H}_{AB})$ is defined as [90] (see also Refs. [91,92])

$$E_{\rm sq}(A;B)_\rho := \frac{1}{2}\inf_{\omega_{ABE}\in\mathcal{D}(\mathcal{H}_{ABE})}\{I(A;B|E)_\omega : \operatorname{Tr}_E\{\omega_{ABE}\}=\rho_{AB}\}. \tag{70}$$

In general, the extension system E is finite-dimensional but can be arbitrarily large. We can directly infer from the above definition that $E_{\rm sq}(B;A)_\rho = E_{\rm sq}(A;B)_\rho$ for any $\rho_{AB}\in\mathcal{D}(\mathcal{H}_{AB})$. We can similarly define the squashed entanglement $E_{\rm sq}(\mathcal{M})$ of a channel $\mathcal{M}_{A\to B}$ [93], and it is known that amortization does not increase the squashed entanglement of a channel [93]:

$$E_{{\rm sq},A}(\mathcal{M}) = E_{\rm sq}(\mathcal{M}). \tag{71}$$

For an overview of the various entanglement measures used in this work see Table I.

G. Private states and privacy test

Private states [14,15] are an essential notion in any discussion of secret-key distillation in quantum information, and we review their basics here.

A tripartite key state $\gamma_{K_AK_BE}$ contains $\log_2 K$ bits of a secret key, shared between systems K_A and K_B, such that $|K_A| = |K_B| = K$, and protected from an eavesdropper possessing system E, if there exists a state σ_E and a projective measurement channel $\mathcal{M}(\cdot)=\sum_i |i\rangle\langle i|(\cdot)|i\rangle\langle i|$, where $\{|i\rangle\}_i$ is an orthonormal basis, such that

$$(\mathcal{M}_{K_A}\otimes\mathcal{M}_{K_B})(\gamma_{K_AK_BE}) = \frac{1}{K}\sum_{i=0}^{K-1}|i\rangle\langle i|_{K_A}\otimes|i\rangle\langle i|_{K_B}\otimes\sigma_E. \tag{72}$$

The systems K_A and K_B are maximally classically correlated, and the key value is uniformly random and independent of the system E.

A bipartite private state $\gamma_{S_AK_AK_BS_B}$ containing $\log_2 K$ bits of a secret key has the following form:

$$\gamma_{S_AK_AK_BS_B} = U^t_{S_AK_AK_BS_B}(\Phi_{K_AK_B}\otimes\theta_{S_AS_B})(U^t_{S_AK_AK_BS_B})^\dagger, \tag{73}$$

where $\Phi_{K_AK_B}$ is a maximally entangled state of Schmidt rank K, $U^t_{S_AK_AK_BS_B}$ is a "twisting" unitary of the form

$$U^t_{S_AK_AK_BS_B} := \sum_{i,j=0}^{K-1}|i\rangle\langle i|_{K_A}\otimes|j\rangle\langle j|_{K_B}\otimes U^{ij}_{S_AS_B}, \tag{74}$$

with each $U^{ij}_{S_AS_B}$ a unitary, and $\theta_{S_AS_B}$ is a state. The systems S_A, S_B are called "shield" systems because they, along with the twisting unitary, can help to protect the key in systems K_A and K_B from any party possessing a purification of $\gamma_{S_AK_AK_BS_B}$.

Bipartite private states and tripartite key states are equivalent [14,15]. That is, for $\gamma_{S_AK_AK_BS_B}$ a bipartite private state and $\gamma_{S_AK_AK_BS_BE}$ some purification of it, $\gamma_{K_AK_BE}$ is a tripartite key state. Conversely, for any tripartite key state $\gamma_{K_AK_BE}$ and any purification $\gamma_{S_AK_AK_BS_BE}$ of it, $\gamma_{S_AK_AK_BS_B}$ is a bipartite private state.

A state $\rho_{K_AK_BE}$ is an ε-approximate tripartite key state if there exists a tripartite key state $\gamma_{K_AK_BE}$ such that

$$F\left(\rho_{K_AK_BE}, \gamma_{K_AK_BE}\right) \geqslant 1-\varepsilon, \tag{75}$$

where $\varepsilon \in [0,1]$. Similarly, a state $\rho_{S_AK_AK_BS_B}$ is an ε-approximate bipartite private state if there exists a bipartite private state $\gamma_{S_AK_AK_BS_B}$ such that

$$F\left(\rho_{S_AK_AK_BS_BE}, \gamma_{S_AK_AK_BS_BE}\right) \geqslant 1-\varepsilon. \tag{76}$$

If $\rho_{S_AK_AK_BS_B}$ is an ε-approximate bipartite key state with K key values, then Alice and Bob hold an ε-approximate tripartite key state with K key values, and the converse is true as well [14,15].

A privacy test corresponding to $\gamma_{S_AK_AK_BS_B}$ (a γ-privacy test) is defined as the following dichotomic measurement [88]:

$$\left\{\Pi^{\gamma}_{S_AK_AK_BS_B}, I_{S_AK_AK_BS_B} - \Pi^{\gamma}_{S_AK_AK_BS_B}\right\}, \tag{77}$$

where

$$\Pi^{\gamma}_{S_AK_AK_BS_B} := U^t_{S_AK_AK_BS_B}\left(\Phi_{K_AK_B}\otimes I_{S_AS_B}\right)\left(U^t_{S_AK_AK_BS_B}\right)^{\dagger} \tag{78}$$

and $U^t_{S_AK_AK_BS_B}$ is the twisting unitary discussed earlier. Let $\varepsilon \in [0,1]$ and $\rho_{S_AK_AK_BS_B}$ be an ε-approximate bipartite private state. The probability for $\rho_{S_AK_AK_BS_B}$ to pass the γ-privacy test is never smaller than $1-\varepsilon$ [88]:

$$\mathrm{Tr}\left\{\Pi^{\gamma}_{S_AK_AK_BS_B}\rho_{S_AK_AK_BS_B}\right\} \geqslant 1-\varepsilon. \tag{79}$$

For a state $\sigma_{S_AK_AK_BS_B} \in \mathrm{SEP}(S_AK_A : K_BS_B)$, the probability of passing any γ-privacy test is never greater than $\frac{1}{K}$ [15]:

$$\mathrm{Tr}\left\{\Pi^{\gamma}_{S_AK_AK_BS_B}\sigma_{S_AK_AK_BS_B}\right\} \leqslant \frac{1}{K}, \tag{80}$$

where K is the number of values that the secret key can take [i.e., $K = \dim(\mathcal{H}_{K_A}) = \dim(\mathcal{H}_{K_B})$]. These two inequalities are foundational for some of the converse bounds established in this paper, as was the case in Refs. [15,88].

III. ENTANGLEMENT DISTILLATION FROM BIPARTITE QUANTUM INTERACTIONS

In this section, we define the bidirectional max-Rains information $R^{2\to 2}_{\max}(\mathcal{N})$ of a bidirectional channel $\mathcal{N}$ and show that it is not enhanced by amortization. We also prove that $R^{2\to 2}_{\max}(\mathcal{N})$ is an upper bound on the amount of entanglement that can be distilled from a bidirectional channel $\mathcal{N}$. We do so by adapting to the bidirectional setting, the result from Ref. [58] discussed below and recent techniques developed in Refs. [80,82,86] for point-to-point quantum communication protocols.

Recently, it was shown in Ref. [58], connected to related developments in Refs. [4,37,59,80,81], that the amortized entanglement of a point-to-point channel $\mathcal{M}_{A\to B}$ serves as an upper bound on the entanglement of the final state, say ω_{AB}, generated at the end of an LOCC- or PPT-assisted quantum communication protocol that uses $\mathcal{M}_{A\to B}$ n times:

$$E(A;B)_{\omega} \leqslant nE_A(\mathcal{M}). \tag{81}$$

Thus, the physical question of determining meaningful upper bounds on the LOCC- or PPT-assisted capacities of point-to-point channel $\mathcal{M}$ is equivalent to the mathematical question of whether amortization can enhance the entanglement of a given channel, i.e., whether the following equality holds for a given entanglement measure E:

$$E_A(\mathcal{M}) \stackrel{?}{=} E(\mathcal{M}). \tag{82}$$

A. Bidirectional max-Rains information

The following definition generalizes the max-Rains information from (59), (63), and (64) to the bidirectional setting:

Definition 5 (Bidirectional max-Rains information). The bidirectional max-Rains information of a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ is defined as

$$R^{2\to 2}_{\max}(\mathcal{N}) := \log_2 \Gamma^{2\to 2}(\mathcal{N}), \tag{83}$$

where $\Gamma^{2\to 2}(\mathcal{N})$ is the solution to the following semidefinite program:

$$\begin{aligned} &\text{minimize} \quad \left\|\mathrm{Tr}_{AB}\left\{V_{S_AABS_B} + Y_{S_AABS_B}\right\}\right\|_{\infty} \\ &\text{subject to} \quad V_{S_AABS_B}, Y_{S_AABS_B} \geqslant 0, \\ &\qquad \mathrm{T}_{BS_B}\left(V_{S_AABS_B} - Y_{S_AABS_B}\right) \geqslant J^{\mathcal{N}}_{S_AABS_B}, \end{aligned} \tag{84}$$

such that $S_A \simeq A'$, and $S_B \simeq B'$.

Remark 2. By employing the Lagrange multiplier method, the bidirectional max-Rains information of a bidirectional channel $\mathcal{N}_{A'B'\to AB}$ can also be expressed as

$$R^{2\to 2}_{\max}(\mathcal{N}) = \log_2 \Gamma^{2\to 2}(\mathcal{N}), \tag{85}$$

where $\Gamma^{2\to 2}(\mathcal{N})$ is solution to the following semidefinite program (SDP):

$$\begin{aligned} &\text{maximize} \qquad \mathrm{Tr}\left\{J^{\mathcal{N}}_{S_AABS_B}X_{S_AABS_B}\right\} \\ &\text{subject to:} \\ &X_{S_AABS_B}, \rho_{S_AS_B} \geqslant 0, \quad \mathrm{Tr}\{\rho_{S_AS_B}\} = 1, \\ &-\rho_{S_AS_B}\otimes I_{AB} \leqslant \mathrm{T}_{BS_B}\left(X_{S_AABS_B}\right) \leqslant \rho_{S_AS_B}\otimes I_{AB}, \end{aligned} \tag{86}$$

such that $S_A \simeq A'$ and $S_B \simeq B'$. Strong duality holds by employing Slater's condition [94] (see also Ref. [87]). Thus, as indicated above, the optimal values of the primal and dual semidefinite programs, i.e., (86) and (84), respectively, are equal.

The following proposition constitutes one of our main technical results, and an immediate corollary of it is that the bidirectional max-Rains information of a bidirectional quantum channel is an upper bound on the amortized max-Rains information of the same channel.

Proposition 1. Let $\rho_{L_AA'B'L_B}$ be a state and let $\mathcal{N}_{A'B'\to AB}$ be a bidirectional channel. Then

$$R_{\max}(L_AA;BL_B)_{\omega} \leqslant R_{\max}(L_AA';B'L_B)_{\rho} + R^{2\to 2}_{\max}(\mathcal{N}), \tag{87}$$

where $\omega_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$ and $R^{2\to 2}_{\max}(\mathcal{N})$ is the bidirectional max-Rains information of $\mathcal{N}_{A'B'\to AB}$.

Proof. We adapt the proof steps of Ref. [86] (Proposition 1) to the bidirectional setting. By removing logarithms and applying (61) and (83), the desired inequality is equivalent to the following one:

$$W(L_AA;BL_B)_\omega \leqslant W(L_AA';B'L_B)_\rho \cdot \Gamma^{2\to 2}(\mathcal{N}), \tag{88}$$

and so we aim to prove this one. Exploiting the identity in (62), we find that

$$W(L_AA';B'L_B)_\rho = \min \mathrm{Tr}\left\{C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right\}, \tag{89}$$

subject to the constraints

$$C_{L_AA'B'L_B}, D_{L_AA'B'L_B} \geqslant 0, \tag{90}$$

$$\mathrm{T}_{B'L_B}\left(C_{L_AA'B'L_B} - D_{L_AA'B'L_B}\right) \geqslant \rho_{L_AA'B'L_B}, \tag{91}$$

while the definition in (84) gives that

$$\Gamma^{2\to 2}(\mathcal{N}) = \min \left\|\mathrm{Tr}_{AB}\left\{V_{S_AABS_B} + Y_{S_AABS_B}\right\}\right\|_\infty, \tag{92}$$

subject to the constraints

$$V_{S_AABS_B}, Y_{S_AABS_B} \geqslant 0, \tag{93}$$

$$\mathrm{T}_{BS_B}\left(V_{S_AABS_B} - Y_{S_AABS_B}\right) \geqslant J^{\mathcal{N}}_{S_AABS_B}. \tag{94}$$

The identity in (62) implies that the left-hand side of (88) is equal to

$$W(L_AA;BL_B)_\omega = \min \mathrm{Tr}\left\{E_{L_AABL_B} + F_{L_AABL_B}\right\}, \tag{95}$$

subject to the constraints

$$E_{L_AABL_B}, \quad F_{L_AABL_B} \geqslant 0, \tag{96}$$

$$\mathcal{N}_{A'B'\to AB}\big(\rho_{L_AA'B'L_B}\big) \leqslant \mathrm{T}_{BL_B}\left(E_{L_AABL_B} - F_{L_AABL_B}\right). \tag{97}$$

Once we have these SDP formulations, we can now show that the inequality in (88) holds by making appropriate choices for $E_{L_AABL_B}$ and $F_{L_AABL_B}$. Let $C_{L_AA'B'L_B}$ and $D_{L_AA'B'L_B}$ be optimal for $W(L_AA';B'L_B)_\rho$, and let $V_{S_AABS_B}$ and $Y_{S_AABS_B}$ be optimal for $\Gamma^{2\to 2}(\mathcal{N})$. Let $|\Upsilon\rangle_{S_AS_B:A'B'}$ be the maximally entangled vector. Choose

$$E_{L_AABL_B} = \langle\Upsilon|_{S_AS_B:A'B'} C_{L_AA'B'L_B} \otimes V_{S_AABS_B} + D_{L_AA'B'L_B} \otimes Y_{S_AABS_B}|\Upsilon\rangle_{S_AS_B:A'B'}, \tag{98}$$

$$F_{L_AABL_B} = \langle\Upsilon|_{S_AS_B:A'B'} C_{L_AA'B'L_B} \otimes Y_{S_AABS_B} + D_{L_AA'B'L_B} \otimes V_{S_AABS_B}|\Upsilon\rangle_{S_AS_B:A'B'}. \tag{99}$$

Then we have $E_{L_AABL_B}, F_{L_AABL_B} \geqslant 0$, because

$$C_{L_AA'B'L_B}, D_{L_AA'B'L_B}, Y_{S_AABS_B}, V_{S_AABS_B} \geqslant 0. \tag{100}$$

Also, consider that

$$\begin{aligned} E_{L_AABL_B} - F_{L_AABL_B} &= \langle\Upsilon|_{S_AS_B:A'B'}\left(C_{L_AA'B'L_B} - D_{L_AA'B'L_B}\right) \otimes \left(V_{S_AABS_B} - Y_{S_AABS_B}\right)|\Upsilon\rangle_{S_AS_B:A'B'} \\ &= \mathrm{Tr}_{S_AA'B'S_B}\left\{|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'}\left(C_{L_AA'B'L_B} - D_{L_AA'B'L_B}\right) \otimes \left(V_{S_AABS_B} - Y_{S_AABS_B}\right)\right\}. \end{aligned} \tag{101}$$

Then, using the abbreviations $E' := E_{L_AABL_B}$, $F' := F_{L_AABL_B}$, $C' := C_{L_AA'B'L_B}$, $D' := D_{L_AA'B'L_B}$, $V' := V_{S_AABS_B}$, and $Y' := Y_{S_AABS_B}$, we have

$$\begin{aligned} \mathrm{T}_{BL_B}(E' - F') &= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{S_AA'B'S_B}\left\{|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'}(C' - D') \otimes (V' - Y')\right\}\right] && (102)\\ &= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{S_AA'B'S_B}\left\{|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'}(C' - D') \otimes (\mathrm{T}_{S_B} \circ \mathrm{T}_{S_B})(V' - Y')\right\}\right] && (103)\\ &= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{S_AA'B'S_B}\left\{\mathrm{T}_{S_B}(|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'})(C' - D') \otimes \mathrm{T}_{S_B}(V' - Y')\right\}\right] && (104)\\ &= \mathrm{T}_{BL_B}\left[\mathrm{Tr}_{S_AA'B'S_B}\left\{|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'}\,\mathrm{T}_{B'}(C' - D') \otimes \mathrm{T}_{S_B}(V' - Y')\right\}\right] && (105)\\ &= \mathrm{Tr}_{S_AA'B'S_B}\left\{|\Upsilon\rangle\langle\Upsilon|_{S_AS_B:A'B'}\,\mathrm{T}_{B'L_B}(C' - D') \otimes \mathrm{T}_{BS_B}(V' - Y')\right\} && (106)\\ &\geqslant \langle\Upsilon|_{S_AS_B:AB}\rho_{L_AA'B'L_B} \otimes J^{\mathcal{N}}_{S_AABS_B}|\Upsilon\rangle_{S_AS_B:AB} && (107)\\ &= \mathcal{N}_{A'B'\to AB}\big(\rho_{L_AA'B'L_B}\big). && (108) \end{aligned}$$

In the above, we employed properties of the partial transpose reviewed in (13)–(16). In particular, the third equality follows from the fact that $\mathrm{T}^\dagger_{S_B} = \mathrm{T}_{S_B}$. For the fourth equality we have used (16) to change T_{S_B} to $\mathrm{T}_{B'}$ and then $\mathrm{T}^\dagger_{B'} = \mathrm{T}_{B'}$. Now, consider that

$$\begin{aligned} \mathrm{Tr}\{E_{L_AABL_B} + F_{L_AABL_B}\} &= \mathrm{Tr}\left\{\langle\Upsilon|_{S_AS_B:A'B'}\left(C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right) \otimes \left(V_{S_AABS_B} + Y_{S_AABS_B}\right)|\Upsilon\rangle_{S_AS_B:A'B'}\right\} \\ &= \mathrm{Tr}\left\{\left(C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right)T_{A'B'}(V_{A'ABB'} + Y_{A'ABB'})\right\} \\ &= \mathrm{Tr}\left\{\left(C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right)T_{A'B'}(\mathrm{Tr}_{AB}[V_{A'ABB'} + Y_{A'ABB'}])\right\} \\ &\leqslant \mathrm{Tr}\left\{\left(C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right)\right\}\left\|T_{A'B'}\left\{\mathrm{Tr}_{AB}\left(V_{A'ABB'} + Y_{A'ABB'}\right)\right\}\right\|_\infty \\ &= \mathrm{Tr}\left\{\left(C_{L_AA'B'L_B} + D_{L_AA'B'L_B}\right)\right\}\|\mathrm{Tr}_{AB}\{V_{A'ABB'} + Y_{A'ABB'}\}\|_\infty \\ &= W(L_AA';B'L_B)_\rho \cdot \Gamma^{2\to 2}(\mathcal{N}). \end{aligned} \tag{109}$$

The second equality follows from (12) and (14). The inequality is a consequence of Hölder's inequality [95]. The second-to-last equality follows because the spectrum of a positive semidefinite operator is invariant under the action of a full transpose (note, in this case, $T_{A'B'}$ is the full transpose as it acts on reduced positive semidefinite operators $V_{A'B'}$ and $Y_{A'B'}$).

Therefore, we can infer that our choices of $E_{L_AABL_B}$ and $F_{L_AABL_B}$ are feasible for $W(L_AA;BL_B)_\omega$. Since $W(L_AA;BL_B)_\omega$ involves a minimization over all operators $E_{L_AABL_B}$ and $F_{L_AABL_B}$ satisfying (96) and (97), this concludes our proof of (88). ■

Remark 3. The choices made for $E_{L_AABL_B}$ and $F_{L_AABL_B}$ in (98) and (99), respectively, can be thought of as bidirectional generalizations of those made in the proof of Ref. [86] (Proposition 1) (see also Ref. [85], Proposition 6), and they can be understood roughly via (11) as a postselected teleportation of the optimal operators of $W(L_AA';B'L_B)_\rho$ through the optimal operators of $\Gamma^{2\to 2}(\mathcal{N})$, with the optimal operators of $W(L_AA';B'L_B)_\rho$ being in correspondence with the Choi operator $J^{\mathcal{N}}_{S_AABS_B}$ through (94).

An immediate corollary of Proposition 1 is the following:

Corollary 1. The amortized max-Rains information of a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ is bounded from above by its bidirectional max-Rains information; i.e., the following inequality holds:

$$R^{2\to 2}_{\max,A}(\mathcal{N}) \leqslant R^{2\to 2}_{\max}(\mathcal{N}), \tag{110}$$

where $R^{2\to 2}_{\max,A}(\mathcal{N})$ is the amortized max-Rains information of a bidirectional channel $\mathcal{N}$,

$$R^{2\to 2}_{\max,A}(\mathcal{N}) := \sup_{\rho_{L_AA'B'L_B}} [R_{\max}(L_AA;BL_B)_\sigma - R_{\max}(L_AA';B'L_B)_\rho], \tag{111}$$

where $\rho_{L_AA'B'L_B} \in \mathcal{D}(\mathcal{H}_{L_AA'B'L_B})$ and $\sigma_{L_AABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$.

Proof. The inequality in (110) is an immediate consequence of Proposition 1. To see this, let $\rho_{L_AA'B'L_B}$ denote an arbitrary input state. Then from Proposition 1

$$R_{\max}(L_AA;BL_B)_\omega - R_{\max}(L_AA';B'L_B)_\rho \leqslant R^{2\to 2}_{\max}(\mathcal{N}), \tag{112}$$

where $\omega_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$. As the inequality holds for any state $\rho_{L_AA'B'L_B}$, we conclude the inequality in (110).

B. Application to entanglement generation

In this section, we discuss the implication of Proposition 1 for PPT-assisted entanglement generation from a bidirectional channel. Suppose that two parties Alice and Bob are connected by a bipartite quantum interaction. Suppose that the systems that Alice and Bob hold are A' and B', respectively. The bipartite quantum interaction between them is represented by a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$, where output systems A and B are in possession of Alice and Bob, respectively. This kind of protocol was considered in Ref. [4] when there is LOCC assistance.

1. Protocol for PPT-assisted bidirectional entanglement generation

We now discuss PPT-assisted entanglement generation protocols that make use of a bidirectional quantum channel. We do so by generalizing the point-to-point communication protocol discussed in Ref. [58] to the bidirectional setting.

In a PPT-assisted bidirectional protocol, as depicted in Fig. 1, Alice and Bob are spatially separated and they are allowed to undergo a bipartite quantum interaction $\mathcal{N}_{A'B'\to AB}$, where for a fixed basis $\{|i\rangle_B|j\rangle_{L_B}\}_{i,j}$, the partial transposition T_{BL_B} is considered on systems associated to Bob. Alice holds systems labeled by A', A whereas Bob holds B', B. They begin by performing a completely PPT-preserving channel $\mathcal{P}^{(1)}_{\emptyset\to L_{A_1}A'_1B'_1L_{B_1}}$, which leads to a PPT state $\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}}$, where L_{A_1}, L_{B_1} are finite-dimensional systems of arbitrary size and A'_1, B'_1 are input systems to the first channel use. Alice and Bob send systems A'_1 and B'_1, respectively, through the first channel use, which yields the output state

$$\sigma^{(1)}_{L_{A_1}A_1B_1L_{B_1}} := \mathcal{N}_{A'_1B'_1\to A_1B_1}\left(\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}}\right). \tag{113}$$

Alice and Bob then perform the completely PPT-preserving channel $\mathcal{P}^{(2)}_{L_{A_1}A_1B_1L_{B_1}\to L_{A_2}A'_2B'_2L_{B_2}}$, which leads to the state

$$\rho^{(2)}_{L_{A_2}A'_2B'_2L_{B_2}} := \mathcal{P}^{(2)}_{L_{A_1}A_1B_1L_{B_1}\to L_{A_2}A'_2B'_2L_{B_2}}\left(\sigma^{(1)}_{L_{A_1}A_1B_1L_{B_1}}\right). \tag{114}$$

Both parties then send systems A'_2, B'_2 through the second channel use $\mathcal{N}_{A'_2B'_2\to A_2B_2}$, which yields the state

$$\sigma^{(2)}_{L_{A_2}A_2B_2L_{B_2}} := \mathcal{N}_{A'_2B'_2\to A_2B_2}\left(\rho^{(2)}_{L_{A_2}A'_2B'_2L_{B_2}}\right). \tag{115}$$

They iterate this process such that the protocol makes use of the channel n times. In general, we have the following states for the ith use, for $i \in \{2, 3, \dots, n\}$:

$$\rho^{(i)}_{L_{A_i}A'_iB'_iL_{B_i}} := \mathcal{P}^{(i)}\left(\sigma^{(i-1)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}}\right), \tag{116}$$

$$\sigma^{(i)}_{L_{A_i}A_iB_iL_{B_i}} := \mathcal{N}_{A'_iB'_i\to A_iB_i}\left(\rho^{(i)}_{L_{A_i}A'_iB'_iL_{B_i}}\right), \tag{117}$$

where $\mathcal{P}^{(i)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}\to L_{A_i}A'_iB'_iL_{B_i}}$ is a completely PPT-preserving channel, with the partial transposition acting on systems $B_{i-1}, L_{B_{i-1}}$ associated to Bob. In the final step of the protocol, a completely PPT-preserving channel $\mathcal{P}^{(n+1)}_{L_{A_n}A_nB_nL_{B_n}\to M_AM_B}$ is applied, which generates the final state:

$$\omega_{M_AM_B} := \mathcal{P}^{(n+1)}_{L_{A_n}A_nB_nL_{B_n}\to M_AM_B}\left(\sigma^{(n)}_{L_{A_n}A'_nB'_nL_{B_n}}\right), \tag{118}$$

where M_A and M_B are held by Alice and Bob, respectively.

The goal of the protocol is for Alice and Bob to distill entanglement in the end; i.e., the final state $\omega_{M_AM_B}$ should be close to a maximally entangled state. For a fixed n, $M \in \mathbb{N}$, $\varepsilon \in [0, 1]$, the original protocol is an (n, M, ε) protocol if the channel is used n times as discussed above, $|M_A| = |M_B| = M$, and if

$$F\left(\omega_{M_AM_B}, \Phi_{M_AM_B}\right) = \langle\Phi|_{M_AM_B}\omega_{M_AM_B}|\Phi\rangle_{AB} \geqslant 1-\varepsilon, \tag{119}$$

where $\Phi_{M_AM_B}$ is the maximally entangled state.

A rate R is achievable for PPT-assisted bidirectional entanglement generation if for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n, there exists an $(n, 2^{n(R-\delta)}, \varepsilon)$ protocol. The PPT-assisted bidirectional quantum capacity of a bidirectional channel $\mathcal{N}$, denoted as $Q^{2\to 2}_{\mathrm{PPT}}(\mathcal{N})$, is equal to the supremum of all achievable rates. Whereas a rate R is a strong converse

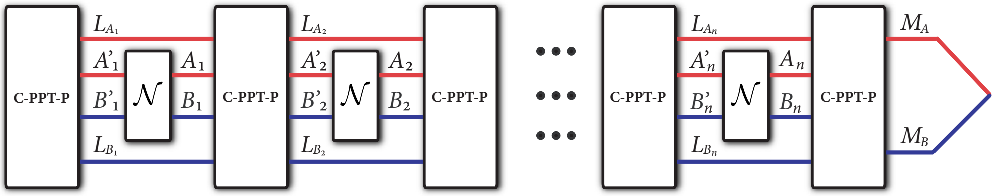

FIG. 1. A protocol for PPT-assisted bidirectional quantum communication that employs n uses of a bidirectional quantum channel $\mathcal{N}$. Every channel use is interleaved by a completely PPT-preserving channel. The goal of such a protocol is to produce an approximate maximally entangled state in the systems M_A and M_B, where Alice possesses system M_A and Bob system M_B.

rate for PPT-assisted bidirectional entanglement generation if for all $\varepsilon \in [0,1)$, $\delta > 0$, and sufficiently large n, there does not exist an $(n, 2^{n(R+\delta)}, \varepsilon)$ protocol. The strong converse PPT-assisted bidirectional quantum capacity $\widetilde{Q}^{2\to 2}_{\mathrm{PPT}}(\mathcal{N})$ is equal to the infimum of all strong converse rates. A bidirectional channel $\mathcal{N}$ is said to obey the strong converse property for PPT-assisted bidirectional entanglement generation if $Q^{2\to 2}_{\mathrm{PPT}}(\mathcal{N}) = \widetilde{Q}^{2\to 2}_{\mathrm{PPT}}(\mathcal{N})$.

We note that every LOCC channel is a completely PPT-preserving channel. Given this, the well-known fact that teleportation [16] is an LOCC channel, and completely PPT-preserving channels are allowed for free in the above protocol, there is no difference between an (n, M, ε) entanglement generation protocol and an (n, M, ε) quantum communication protocol. Thus, all of the capacities for quantum communication are equal to those for entanglement generation.

Also, one can consider the whole development discussed above for LOCC-assisted bidirectional quantum communication instead of more general PPT-assisted bidirectional quantum communication. All the notions discussed above follow when we restrict the class of assisting completely PPT-preserving channels allowed to be LOCC channels. It follows that the LOCC-assisted bidirectional quantum capacity $Q^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N})$ and the strong converse LOCC-assisted quantum capacity $\widetilde{Q}^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N})$ are bounded from above as

$$Q^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N}) \leqslant Q^{2\to 2}_{\mathrm{PPT}}(\mathcal{N}), \tag{120}$$

$$\widetilde{Q}^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N}) \leqslant \widetilde{Q}^{2\to 2}_{\mathrm{PPT}}(\mathcal{N}). \tag{121}$$

Also, the capacities of bidirectional quantum communication protocols without any assistance are always less than or equal to the LOCC-assisted bidirectional quantum capacities.

The following lemma is useful in deriving upper bounds on the bidirectional quantum capacities in the forthcoming sections, and it represents a generalization of the amortization idea to the bidirectional setting (see Ref. [4] in this context).

Lemma 4. Let $E_{\mathrm{PPT}}(A;B)_\rho$ be a bipartite entanglement measure for an arbitrary bipartite state ρ_{AB}. Suppose that $E_{\mathrm{PPT}}(A;B)_\rho$ vanishes for all $\rho_{AB} \in \mathrm{PPT}(A\!:\!B)$ and is monotone nonincreasing under completely PPT-preserving channels. Consider an (n, M, ε) protocol for PPT-assisted entanglement generation over a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$, as described in Sec. III B 1. Then the following bound holds:

$$E_{\mathrm{PPT}}(M_A;M_B)_\omega \leqslant nE_{\mathrm{PPT},A}(\mathcal{N}), \tag{122}$$

where $E_{\mathrm{PPT},A}(\mathcal{N})$ is the amortized entanglement of a bidirectional channel $\mathcal{N}$,

$$E_{\mathrm{PPT},A}(\mathcal{N}) := \sup_{\rho_{L_AA'B'L_B}} [E_{\mathrm{PPT}}(L_AA;BL_B)_\sigma - E_{\mathrm{PPT}}(L_AA';B'L_B)_\rho], \tag{123}$$

$\rho_{L_AA'B'L_B} \in \mathcal{D}(\mathcal{H}_{L_AA'B'L_B})$, and $\sigma_{L_AABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$.

Proof. From Sec. III B 1, as E is monotonically nonincreasing under the action of completely PPT-preserving channels, we get that

$$\begin{aligned}
E_{\mathrm{PPT}}(M_A;M_B)_\omega &\leqslant E_{\mathrm{PPT}}\big(L_{A_n}A_n;B_nL_{B_n}\big)_{\sigma^{(n)}}\\
&= E_{\mathrm{PPT}}\big(L_{A_n}A_n;B_nL_{B_n}\big)_{\sigma^{(n)}} - E_{\mathrm{PPT}}\big(L_{A_1}A'_1;B'_1L_{B_1}\big)_{\rho^{(1)}}\\
&= E_{\mathrm{PPT}}\big(L_{A_n}A_n;B_nL_{B_n}\big)_{\sigma^{(n)}} + \sum_{i=2}^{n}\big[E_{\mathrm{PPT}}\big(L_{A_i}A'_i;B'_iL_{B_i}\big)_{\rho^{(i)}} - E_{\mathrm{PPT}}\big(L_{A_i}A'_i;B'_iL_{B_i}\big)_{\rho^{(i)}}\big] - E_{\mathrm{PPT}}\big(L_{A_1}A'_1;B'_1L_{B_1}\big)_{\rho^{(1)}}\\
&\leqslant \sum_{i=1}^{n}\big[E_{\mathrm{PPT}}\big(L_{A_i}A_i;B_iL_{B_i}\big)_{\sigma^{(i)}} - E_{\mathrm{PPT}}\big(L_{A_i}A'_i;B'_iL_{B_i}\big)_{\rho^{(i)}}\big] \leqslant nE_{\mathrm{PPT},A}(\mathcal{N}).
\end{aligned} \tag{124}$$

The first equality follows because $\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}}$ is a PPT state with vanishing E_{PPT}. The second equality follows trivially because we add and subtract the same terms. The second inequality follows because $E_{\mathrm{PPT}}(L_{A_i}A'_i;B'_iL_{B_i})_{\rho^{(i)}} \leqslant E_{\mathrm{PPT}}(L_{A_{i-1}}A_{i-1};B_{i-1}L_{B_{i-1}})_{\sigma^{(i-1)}}$ for all $i \in \{2,3,\dots,n\}$, due to monotonicity of the entanglement measure E_{PPT} with respect to completely PPT-preserving channels. The final inequality follows by applying the definition in (123) to each summand. ■

2. Strong converse rate for PPT-assisted bidirectional entanglement generation

We now establish the following upper bound on the bidirectional entanglement generation rate $\frac{1}{n}\log_2 M$ (qubits per channel use) of any (n, M, ε) PPT-assisted protocol:

Theorem 1. For a fixed $n,\ M \in \mathbb{N},\ \varepsilon \in (0,1)$, the following bound holds for an (n, M, ε) protocol for PPT-assisted bidirectional entanglement generation over a bidirectional quantum channel $\mathcal{N}$:

$$\frac{1}{n}\log_2 M \leqslant R_{\max}^{2\to 2}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{125}$$

Proof. From Sec. III B 1, we have that

$$\mathrm{Tr}\{\Phi_{M_AM_B}\omega_{M_AM_B}\} \geqslant 1-\varepsilon, \tag{126}$$

while Ref. [11] (Lemma 2) implies that, for all $\sigma_{M_AM_B} \in \mathrm{PPT}'(M_A{:}M_B)$,

$$\mathrm{Tr}\left\{\Phi_{M_AM_B}\sigma_{M_AM_B}\right\} \leqslant \frac{1}{M}. \tag{127}$$

Under an "entanglement test," which is a measurement with POVM $\{\Phi_{M_AM_B}, I_{M_AM_B} - \Phi_{M_AM_B}\}$, and applying the data processing inequality for the max-relative entropy, we find that [for details, see (56)–(59) in Ref. [86]]

$$R_{\max}(M_A; M_B)_\omega \geqslant \log_2[(1-\varepsilon)M]. \tag{128}$$

Applying Lemma 4 and Proposition 1, we get that

$$R_{\max}(M_A; M_B)_\omega \leqslant nR_{\max}^{2\to 2}(\mathcal{N}). \tag{129}$$

Combining (128) and (129), we arrive at the desired inequality in (125).

Remark 4. The bound in (125) can also be rewritten as

$$1-\varepsilon \leqslant 2^{-n[Q-R_{\max}^{2\to 2}(\mathcal{N})]}, \tag{130}$$

where we set the rate $Q = \frac{1}{n}\log_2 M$. Thus, if the bidirectional communication rate Q is strictly larger than the bidirectional max-Rains information $\mathcal{R}_{\max}^{2\to 2}(\mathcal{N})$, then the fidelity of the transmission $(1-\varepsilon)$ decays exponentially fast to zero in the number n of channel uses.

An immediate corollary of the above remark is the following strong converse statement:

Corollary 2. The strong converse PPT-assisted bidirectional quantum capacity of a bidirectional channel $\mathcal{N}$ is bounded from above by its bidirectional max-Rains information:

$$\widetilde{Q}_{\mathrm{PPT}}^{2\to 2}(\mathcal{N}) \leqslant R_{\max}^{2\to 2}(\mathcal{N}). \tag{131}$$

IV. SECRET-KEY DISTILLATION FROM BIPARTITE QUANTUM INTERACTIONS

In this section, we define the bidirectional max-relative entropy of entanglement $E_{\max}^{2\to 2}(\mathcal{N})$. The main goal of this section is to derive an upper bound on the rate at which a secret key can be distilled from a bipartite quantum interaction. In deriving this bound, we consider private communication protocols that use a bidirectional quantum channel, and we make use of recent techniques developed in quantum information theory for point-to-point private communication protocols [15,58,80,88].

A. Bidirectional max-relative entropy of entanglement

The following definition generalizes a channel's max-relative entropy of entanglement from [80] to the bidirectional setting:

Definition 6. The bidirectional max-relative entropy of entanglement of a bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is defined as

$$E_{\max}^{2\to 2}(\mathcal{N}) = \sup_{\psi_{S_AA'}\otimes\varphi_{B'S_B}} E_{\max}(S_AA; BS_B)_\omega, \tag{132}$$

where $\omega_{S_AABS_B} := \mathcal{N}_{A'B'\to AB}(\psi_{S_AA'}\otimes\varphi_{B'S_B})$ and $\psi_{S_AA'}$ and $\varphi_{B'S_B}$ are pure bipartite states such that $S_A \simeq A'$, and $S_B \simeq B'$.

Remark 5. Note that we could define $E_{\max}^{2\to 2}(\mathcal{N})$ to have an optimization over separable input states $\rho_{S_AA'B'S_B} \in \mathrm{SEP}(S_AA'{:}B'S_B)$ with finite-dimensional but arbitrarily large auxiliary systems S_A and S_B. However, the quasiconvexity of the max-relative entropy of entanglement [76,77] and the Schmidt decomposition theorem guarantee that it suffices to restrict the optimization to be as stated in Definition 6.

Proposition 2. Let $\rho_{L_AA'B'L_B}$ be a state and let $\mathcal{N}_{A'B'\to AB}$ be a bidirectional channel. Then

$$E_{\max}(L_AA; BL_B)_\omega \leqslant E_{\max}(L_AA'; B'L_B)_\rho + E_{\max}^{2\to 2}(\mathcal{N}), \tag{133}$$

where $\omega_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$ and $E_{\max}^{2\to 2}(\mathcal{N})$ is the bidirectional max-relative entropy of entanglement of $\mathcal{N}_{A'B'\to AB}$.

Proof. Let us consider states $\sigma'_{L_AA'B'L_B} \in \mathrm{SEP}(L_AA'{:}B'L_B)$ and $\sigma_{L_AABL_B} \in \mathrm{SEP}(L_AA{:}BL_B)$, where L_A and L_B are finite-dimensional but arbitrarily large. With respect to the bipartite cut $L_AA : BL_B$, the following inequality holds:

$$E_{\max}(L_AA; BL_B)_\omega \leqslant D_{\max}(\mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})\|\sigma_{L_AABL_B}). \tag{134}$$

Applying the data-processed triangle inequality [80] (Theorem III.1), we find that

$$\begin{aligned} &D_{\max}\left(\mathcal{N}_{A'B'\to AB}\left(\rho_{L_AA'B'L_B}\right)\|\sigma_{L_AABL_B}\right)\\ &\quad\leqslant D_{\max}\left(\rho_{L_AA'B'L_B}\|\sigma'_{L_AA'B'L_B}\right)\\ &\qquad+D_{\max}\left(\mathcal{N}_{A'B'\to AB}\left(\sigma'_{L_AA'B'L_B}\right)\|\sigma_{L_AABL_B}\right). \end{aligned} \tag{135}$$

Since $\sigma'_{L_AA'B'L_B}$ and $\sigma_{L_AABL_B}$ are arbitrary separable states, we arrive at

$$E_{\max}(L_AA; BL_B)_\omega \leqslant E_{\max}(L_AA'; B'L_B)_\rho + E_{\max}(L_AA; BL_B)_\tau, \tag{136}$$

where

$$\omega_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}\left(\rho_{L_AA'B'L_B}\right), \tag{137}$$

$$\tau_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}\left(\sigma'_{L_AA'B'L_B}\right). \tag{138}$$

This implies the desired inequality after applying the observation in Remark 5, given that $\sigma'_{L_AA'B'L_B} \in \mathrm{SEP}(L_AA'{:}B'L_B)$. ■

An immediate consequence of Proposition 2 is the following corollary:

Corollary 3. Amortization does not enhance the bidirectional max-relative entropy of entanglement of a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$; and the following equality holds:

$$E^{2\to 2}_{\max,A}(\mathcal{N}) = E^{2\to 2}_{\max}(\mathcal{N}), \tag{139}$$

where $E^{2\to 2}_{\max,A}(\mathcal{N})$ is the amortized entanglement of a bidirectional channel $\mathcal{N}$,

$$E^{2\to 2}_{\max,A}(\mathcal{N}) := \sup_{\rho_{L_A A'B'L_B}} [E_{\max}(L_A A; BL_B)_\sigma - E_{\max}(L_A A'; B'L_B)_\rho], \tag{140}$$

where $\rho_{L_A A'B'L_B} \in \mathcal{D}(\mathcal{H}_{L_A A'B'L_B})$ and $\sigma_{L_A ABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_A A'B'L_B})$.

Proof. The inequality $E^{2\to 2}_{\max,A}(\mathcal{N}) \geqslant E^{2\to 2}_{\max}(\mathcal{N})$ always holds. The other inequality $E^{2\to 2}_{\max,A}(\mathcal{N}) \leqslant E^{2\to 2}_{\max}(\mathcal{N})$ is an immediate consequence of Proposition 2 (the argument is similar to that given in the proof of Corollary 1). ■

B. Application to secret-key agreement

1. Protocol for LOCC-assisted bidirectional secret-key agreement

We first introduce an LOCC-assisted secret-key-agreement protocol that employs a bidirectional quantum channel.

In an LOCC-assisted bidirectional secret-key-agreement protocol, Alice and Bob are spatially separated, and they are allowed to make use of a bipartite quantum interaction $\mathcal{N}_{A'B'\to AB}$, where the bipartite cut is considered between systems associated to Alice and Bob, $L_A A : L_B B$. Let $\mathcal{U}^{\mathcal{N}}_{A'B'\to ABE}$ be an isometric channel extending $\mathcal{N}_{A'B'\to AB}$:

$$\mathcal{U}^{\mathcal{N}}_{A'B'\to ABE}(\cdot) = U^{\mathcal{N}}_{A'B'\to ABE}(\cdot)\big(U^{\mathcal{N}}_{A'B'\to ABE}\big)^\dagger, \tag{141}$$

where $U^{\mathcal{N}}_{A'B'\to ABE}$ is an isometric extension of $\mathcal{N}_{A'B'\to AB}$. We assume that the eavesdropper Eve has access to the system E, also referred to as the environment, as well as a coherent copy of the classical communication exchanged between Alice and Bob. One could also consider a weaker assumption, in which the eavesdropper has access to only part of $E = E'E''$.

Alice and Bob begin by performing an LOCC channel $\mathcal{L}^{(1)}_{\emptyset\to L_{A_1}A'_1B'_1L_{B_1}}$, which leads to a state $\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}} \in \mathrm{SEP}(L_{A_1}A'_1 : B'_1L_{B_1})$, where L_{A_1}, L_{B_1} are finite-dimensional systems of arbitrary size and A'_1, B'_1 are input systems to the first channel use. Alice and Bob send systems A'_1 and B'_1, respectively, through the first channel use, that outputs the state

$$\sigma^{(1)}_{L_{A_1}A_1B_1L_{B_1}} := \mathcal{N}_{A'_1B'_1\to A_1B_1}\big(\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}}\big). \tag{142}$$

They then perform the LOCC channel $\mathcal{L}^{(2)}_{L_{A_1}A_1B_1L_{B_1}\to L_{A_2}A'_2B'_2L_{B_2}}$, which leads to the state

$$\rho^{(2)}_{L_{A_2}A'_2B'_2L_{B_2}} := \mathcal{L}^{(2)}_{L_{A_1}A_1B_1L_{B_1}\to L_{A_2}A'_2B'_2L_{B_2}}\big(\sigma^{(1)}_{L_{A_1}A_1B_1L_{B_1}}\big). \tag{143}$$

Both parties then send systems A'_2, B'_2 through the second channel use $\mathcal{N}_{A'_2B'_2\to A_2B_2}$, which yields the state $\sigma^{(2)}_{L_{A_2}A_2B_2L_{B_2}} := \mathcal{N}_{A'_2B'_2\to A_2B_2}(\rho^{(2)}_{L_{A_2}A'_2B'_2L_{B_2}})$. They iterate the process such that the protocol uses the channel n times. In general, we have the following states for the ith channel use, for $i \in \{2, 3, \dots, n\}$:

$$\rho^{(i)}_{L_{A_i}A'_iB'_iL_{B_i}} := \mathcal{L}^{(i)}\big(\sigma^{(i-1)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}}\big), \tag{144}$$

$$\sigma^{(i)}_{L_{A_i}A_iB_iL_{B_i}} := \mathcal{N}_{A'_iB'_i\to A_iB_i}\big(\rho^{(i)}_{L_{A_i}A'_iB'_iL_{B_i}}\big), \tag{145}$$

where $\mathcal{L}^{(i)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}\to L_{A_i}A'_iB'_iL_{B_i}}$ is an LOCC channel corresponding to the bipartite cut $L_{A_{i-1}}A_{i-1}:B_{i-1}L_{B_{i-1}}$. In the final step of the protocol, an LOCC channel $\mathcal{L}^{(n+1)}_{L_{A_n}A_nB_nL_{B_n}\to K_AK_B}$ is applied, which generates the final state:

$$\omega_{K_AK_B} := \mathcal{L}^{(n+1)}_{L_{A_n}A'_nB'_nL_{B_n}\to K_AK_B}\big(\sigma^{(n)}_{L_{A_n}A'_nB'_nL_{B_n}}\big), \tag{146}$$

where the key systems K_A and K_B are held by Alice and Bob, respectively.

The goal of the protocol is for Alice and Bob to distill a secret-key state, such that the systems K_A and K_B are maximally classical correlated and tensor product with all of the systems that Eve possesses (see Sec. II G for a review of tripartite secret-key states). See Fig. 2 for a depiction of the protocol.

2. Purifying an LOCC-assisted bidirectional secret-key-agreement protocol

As observed in Refs. [14,15] and reviewed in Sec. II G, any protocol of the above form, discussed in Sec. IV B 1, can be purified in the following sense.

The initial state $\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}} \in \mathrm{SEP}(L_{A_1}A'_1 : B'_1L_{B_1})$ is of the following form:

$$\rho^{(1)}_{L_{A_1}A'_1B'_1L_{B_1}} := \sum_{y_1} p_{Y_1}(y_1)\tau^{y_1}_{L_{A_1}A'_1} \otimes \varsigma^{y_1}_{L_{B_1}B'_1}. \tag{147}$$

The classical random variable Y_1 corresponds to a message exchanged between Alice and Bob to establish this state. It can be purified in the following way:

$$|\psi^{(1)}\rangle_{Y_1S_{A_1}L_{A_1}A'_1B'_1L_{B_1}S_{B_1}} := \sum_{y_1} \sqrt{p_{Y_1}(y_1)}|y_1\rangle_{Y_1} \otimes |\tau^{y_1}\rangle_{S_{A_1}L_{A_1}A'_1} \otimes |\varsigma^{y_1}\rangle_{S_{B_1}L_{B_1}B'_1}, \tag{148}$$

where S_{A_1} and S_{B_1} are local "shield" systems that in principle could be held by Alice and Bob, respectively, $|\tau^{y_1}\rangle_{S_{A_1}L_{A_1}A'_1}$ and $|\varsigma^{y_1}\rangle_{S_{B_1}L_{B_1}B'_1}$ purify $\tau^{y_1}_{L_{A_1}A'_1}$ and $\varsigma^{y_1}_{L_{B_1}B'_1}$, respectively, and Eve possesses system Y_1, which contains a coherent classical copy of the classical data exchanged between Alice and Bob. Each LOCC channel $\mathcal{L}^{(i)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}\to L_{A_i}A'_iB'_iL_{B_i}}$ can be written in the following form [94], for all $i \in 2, 3, \dots, n$:

$$\mathcal{L}^{(i)}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}\to L_{A_i}A'_iB'_iL_{B_i}} := \sum_{y_i} \mathcal{E}^{y_i}_{L_{A_{i-1}}A_{i-1}\to L_{A_i}A'_i} \otimes \mathcal{F}^{y_i}_{B_{i-1}L_{B_{i-1}}\to B'_iL_{B_i}}, \tag{149}$$

where $\{\mathcal{E}^{y_i}_{L_{A_{i-1}}A_{i-1}\to L_{A_i}A'_i}\}_{y_i}$ and $\{\mathcal{F}^{y_i}_{B_{i-1}L_{B_{i-1}}\to B'_iL_{B_i}}\}_{y_i}$ are collections of completely positive, trace nonincreasing maps such that the map in (149) is trace preserving. Such an LOCC channel can be purified to an isometry in the

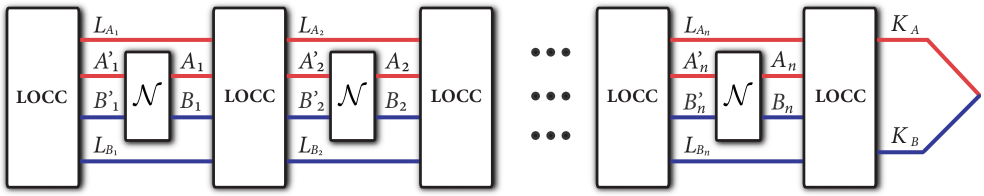

FIG. 2. A protocol for LOCC-assisted bidirectional private communication that employs n uses of a bidirectional quantum channel $\mathcal{N}$. Every channel use is interleaved by an LOCC channel. The goal of such a protocol is to produce an approximate private state in the systems K_A and K_B, where Alice possesses system K_A and Bob system K_B.

following way:

$$\begin{aligned} &U^{\mathcal{L}^{(i)}}_{L_{A_{i-1}}A_{i-1}B_{i-1}L_{B_{i-1}}\to Y_iS_{A_i}L_{A_i}A'_iB'_iL_{B_i}S_{B_i}} \\ &\quad := \sum_{y_i} |y_i\rangle_{Y_i} \otimes U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}}A_{i-1}\to S_{A_i}L_{A_i}A'_i} \\ &\quad\quad \otimes U^{\mathcal{F}^{y_i}}_{B_{i-1}L_{B_{i-1}}\to B'_iL_{B_i}S_{B_i}}, \end{aligned} \tag{150}$$

where $\{U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}}A_{i-1}\to S_{A_i}L_{A_i}A'_i}\}_{y_i}$ and $\{U^{\mathcal{F}^{y_i}}_{B_{i-1}L_{B_{i-1}}\to B'_iL_{B_i}S_{B_i}}\}_{y_i}$ are collections of linear operators (each of which is a contraction,

$$\left\|U^{\mathcal{E}^{y_i}}_{L_{A_{i-1}}A_{i-1}\to S_{A_i}L_{A_i}A'_i}\right\|_\infty, \left\|U^{\mathcal{F}^{y_i}}_{B_{i-1}L_{B_{i-1}}\to B'_iL_{B_i}S_{B_i}}\right\|_\infty \leqslant 1 \tag{151}$$

for all y_i) such that the linear operator $U^{\mathcal{L}^{(i)}}$ in (150) is an isometry, the system Y_i being held by Eve. The final LOCC channel can be written similarly as

$$\mathcal{L}^{(n+1)}_{L_{A_n}A'_nB'_nL_{B_n}\to K_AK_B} := \sum_{y_{n+1}} \mathcal{E}^{y_{n+1}}_{L_{A_n}A_n\to K_A} \otimes \mathcal{F}^{y_{n+1}}_{B_nL_{B_n}\to K_B}, \tag{152}$$

and it can be purified to an isometry similarly as

$$\begin{aligned} &U^{\mathcal{L}^{(n+1)}}_{L_{A_n}A_nB_nL_{B_n}\to Y_{n+1}S_{A_{n+1}}K_AK_BS_{B_{n+1}}} \\ &\quad := \sum_{y_{n+1}} |y_{n+1}\rangle_{Y_{n+1}} \otimes U^{\mathcal{E}^{y_{n+1}}}_{L_{A_n}A_n\to S_{A_{n+1}}K_A} \otimes U^{\mathcal{F}^{y_{n+1}}}_{K_BS_{B_{n+1}}}. \end{aligned} \tag{153}$$

Furthermore, each channel use $\mathcal{N}_{A'_iB'_i\to A_iB_i}$, for all $i \in \{1, 2, \ldots, n\}$, is purified by an isometry $U^{\mathcal{N}}_{A'_iB'_i\to A_iB_iE_i}$, such that Eve possesses the environment system E_i.

At the end of the purified protocol, Alice possesses the key system K_A and the shield systems $S_A := S_{A_1}S_{A_2}\cdots S_{A_{n+1}}$, Bob possesses the key system K_B and the shield systems $S_B := S_{B_1}S_{B_2}\cdots S_{B_{n+1}}$, and Eve possesses the environment systems $E^n := E_1E_2\cdots E_n$ as well as the coherent copies $Y^{n+1} := Y_1Y_2\cdots Y_{n+1}$ of the classical data exchanged between Alice and Bob. The state at the end of the protocol is a pure state $\omega_{Y^{n+1}S_AK_AK_BS_BE^n}$.

For a fixed $n, K \in \mathbb{N}$, $\varepsilon \in [0, 1]$, the original protocol is an (n, K, ε) protocol if the channel is used n times as discussed above, $|K_A| = |K_B| = K$, and if

$$F\left(\omega_{S_AK_AK_BS_B}, \gamma_{S_AK_AK_BS_B}\right) \geqslant 1 - \varepsilon, \tag{154}$$

where $\gamma_{S_AK_AK_BS_B}$ is a bipartite private state.

A rate R is achievable for LOCC-assisted bidirectional secret-key agreement if for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n, there exists an $(n, 2^{n(R-\delta)}, \varepsilon)$ protocol. The LOCC-assisted bidirectional secret-key-agreement capacity of a bidirectional channel $\mathcal{N}$, denoted as $P^{2\to2}_{\text{LOCC}}(\mathcal{N})$, is equal to the supremum of all achievable rates. Whereas a rate R is a strong converse rate for LOCC-assisted bidirectional secret-key agreement if for all $\varepsilon \in [0, 1)$, $\delta > 0$, and sufficiently large n, there does not exist an $(n, 2^{n(R+\delta)}, \varepsilon)$ protocol. The strong converse LOCC-assisted bidirectional secret-key-agreement capacity $\widetilde{P}^{2\to2}_{\text{LOCC}}(\mathcal{N})$ is equal to the infimum of all strong converse rates. A bidirectional channel $\mathcal{N}$ is said to obey the strong converse property for LOCC-assisted bidirectional secret-key agreement if $P^{2\to2}_{\text{LOCC}}(\mathcal{N}) = \widetilde{P}^{2\to2}_{\text{LOCC}}(\mathcal{N})$.

We note that the identity channel corresponding to no assistance is an LOCC channel. Therefore, one can consider the whole development discussed above for bidirectional private communication without any assistance or feedback instead of LOCC-assisted communication. All the notions discussed above follow when we exempt the employment of any nontrivial LOCC assistance. It follows that the nonadaptive bidirectional private capacity $P^{2\to2}_{\text{n-a}}(\mathcal{N})$ and the strong converse nonadaptive bidirectional private capacity $\widetilde{P}^{2\to2}_{\text{n-a}}(\mathcal{N})$ are bounded from above as

$$P^{2\to2}_{\text{n-a}}(\mathcal{N}) \leqslant P^{2\to2}_{\text{LOCC}}(\mathcal{N}), \tag{155}$$

$$\widetilde{P}^{2\to2}_{\text{n-a}}(\mathcal{N}) \leqslant \widetilde{P}^{2\to2}_{\text{LOCC}}(\mathcal{N}). \tag{156}$$

The following lemma is useful in deriving upper bounds on the bidirectional secret-key-agreement capacity of a bidirectional channel. Its proof is very similar to the proof of Lemma 4, and so we omit it.

Lemma 5. Let $E_{\text{LOCC}}(A;B)_\rho$ be a bipartite entanglement measure for an arbitrary bipartite state ρ_{AB}. Suppose that $E_{\text{LOCC}}(A;B)_\rho$ vanishes for all $\rho_{AB} \in \text{SEP}(A\!:\!B)$ and is monotone nonincreasing under LOCC channels. Consider an (n, K, ε) protocol for LOCC-assisted secret-key agreement over a bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ as described in Sec. IV B 2. Then the following bound holds:

$$E_{\text{LOCC}}(S_AK_A;K_BS_B)_\omega \leqslant nE_{\text{LOCC},A}(\mathcal{N}), \tag{157}$$

where $E_{\text{LOCC},A}(\mathcal{N})$ is the amortized entanglement of a bidirectional channel $\mathcal{N}$,

$$\begin{aligned} &E_{\text{LOCC},A}(\mathcal{N}) \\ &\quad := \sup_{\rho_{L_AA'B'L_B}} [E_{\text{LOCC}}(L_AA;BL_B)_\sigma - E_{\text{LOCC}}(L_AA';B'L_B)_\rho], \end{aligned} \tag{158}$$

and $\sigma_{L_AABL_B} := \mathcal{N}_{A'B'\to AB}(\rho_{L_AA'B'L_B})$.

3. Strong converse rate for LOCC-assisted bidirectional secret-key agreement

We now prove the following upper bound on the bidirectional secret-key-agreement rate $\frac{1}{n}\log_2 K$ (secret bits per channel use) of any (n, K, ε) LOCC-assisted secret-key-agreement protocol:

Theorem 2. For a fixed $n,\ K \in \mathbb{N},\ \varepsilon \in (0,1)$, the following bound holds for an (n, K, ε) protocol for LOCC-assisted bidirectional secret-key agreement over a bidirectional quantum channel $\mathcal{N}$:

$$\frac{1}{n}\log_2 K \leqslant E_{\max}^{2\to 2}(\mathcal{N}) + \frac{1}{n}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{159}$$

Proof. From Sec. IV B 2, the following inequality holds for an (n, K, ε) protocol:

$$F\left(\omega_{S_A K_A K_B S_B}, \gamma_{S_A K_A K_B S_B}\right) \geqslant 1-\varepsilon, \tag{160}$$

for some bipartite private state $\gamma_{S_A K_A K_B S_B}$ with key dimension K. From Sec. II G, $\omega_{S_A K_A K_B S_B}$ passes a γ-privacy test with probability at least $1-\varepsilon$, whereas any $\tau_{S_A K_A K_B S_B} \in \mathrm{SEP}(S_A K_A : K_B S_B)$ does not pass with probability greater than $\frac{1}{K}$ [15] (see also Ref. [88]). Making use of the discussion in Ref. [80] (Secs. III and IV; i.e., from the monotonicity of the max-relative entropy of entanglement under the γ-privacy test), we conclude that

$$\log_2 K \leqslant E_{\max}(S_A K_A; K_B S_B)_\omega + \log_2\left(\frac{1}{1-\varepsilon}\right). \tag{161}$$

Applying Lemma 5 and Corollary 3, we get that

$$E_{\max}(S_A K_A; K_B S_B)_\omega \leqslant n E_{\max}^{2\to 2}(\mathcal{N}). \tag{162}$$

Combining (161) and (162), we get the desired inequality in (159). ■

Remark 6. The bound in (159) can also be rewritten as

$$1-\varepsilon \leqslant 2^{-n[P - E_{\max}^{2\to 2}(\mathcal{N})]}, \tag{163}$$

where we set the rate $P = \frac{1}{n}\log_2 K$. Thus, if the bidirectional secret-key-agreement rate P is strictly larger than the bidirectional max-relative entropy of entanglement $\mathcal{E}_{\max}^{2\to 2}(\mathcal{N})$, then the reliability and security of the transmission $(1-\varepsilon)$ decays exponentially fast to zero in the number n of channel uses.

An immediate corollary of the above remark is the following strong converse statement:

Corollary 4. The strong converse LOCC-assisted bidirectional secret-key-agreement capacity of a bidirectional channel $\mathcal{N}$ is bounded from above by its bidirectional max-relative entropy of entanglement:

$$\widetilde{P}_{\mathrm{LOCC}}^{2\to 2}(\mathcal{N}) \leqslant E_{\max}^{2\to 2}(\mathcal{N}). \tag{164}$$

V. BIDIRECTIONAL CHANNELS WITH SYMMETRY

Channels obeying particular symmetries have played an important role in several quantum information-processing tasks in the context of quantum communication protocols [52,54,55], quantum computing and quantum metrology [96–98], resource theories [99,100], etc.

In this section, we define bidirectional PPT- and teleportation-simulable channels by adapting the definitions of point-to-point PPT- and LOCC-simulable channels [54,55,58] to the bidirectional setting. Then we give upper bounds on the entanglement and secret-key-agreement capacities for communication protocols that employ bidirectional PPT- and teleportation-simulable channels, respectively. These bounds are generally tighter than those given in the previous section, because they exploit the symmetry inherent in bidirectional PPT- and teleportation-simulable channels.

Definition 7 (Bidirectional PPT-simulable). A bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is PPT-simulable with associated resource state $\theta_{D_A D_B} \in \mathcal{D}(\mathcal{H}_{D_A}\otimes\mathcal{H}_{D_B})$ if for all input states $\rho_{A'B'} \in \mathcal{D}(\mathcal{H}_{A'}\otimes\mathcal{H}_{B'})$ the following equality holds:

$$\mathcal{N}_{A'B'\to AB}(\rho_{A'B'}) = \mathcal{P}_{D_A A' B' D_B\to AB}\left(\rho_{A'B'}\otimes\theta_{D_A D_B}\right), \tag{165}$$

with $\mathcal{P}_{D_A A' B' D_B\to AB}$ being a completely PPT-preserving channel acting on $D_A A' : D_B B'$, where the partial transposition acts on the composite system $D_B B'$.

The following definition was given in Ref. [101] for the special case of bipartite unitary channels:

Definition 8 (Bidirectional teleportation-simulable). A bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is teleportation-simulable with associated resource state $\theta_{D_A D_B} \in \mathcal{D}(\mathcal{H}_{D_A}\otimes\mathcal{H}_{D_B})$ if for all input states $\rho_{A'B'} \in \mathcal{D}(\mathcal{H}_{A'}\otimes\mathcal{H}_{B'})$ the following equality holds:

$$\mathcal{N}_{A'B'\to AB}(\rho_{A'B'}) = \mathcal{L}_{D_A A' B' D_B\to AB}\left(\rho_{A'B'}\otimes\theta_{D_A D_B}\right), \tag{166}$$

where $\mathcal{L}_{D_A A' B' D_B\to AB}$ is an LOCC channel acting on $D_A A' : D_B B'$.

Let G and H be finite groups, and for $g \in G$ and $h \in H$, let $g \to U_{A'}(g)$ and $h \to V_{B'}(h)$ be unitary representations. Also, let $(g,h) \to W_A(g,h)$ and $(g,h) \to T_B(g,h)$ be unitary representations. A bidirectional quantum channel $\mathcal{N}_{A'B'\to AB}$ is *bicovariant* with respect to these representations if the following relation holds for all input density operators $\rho_{A'B'}$ and group elements $g \in G$ and $h \in H$:

$$\begin{aligned}&\mathcal{N}_{A'B'\to AB}\{[\mathcal{U}_{A'}(g)\otimes\mathcal{V}_{B'}(h)](\rho_{A'B'})\}\\&\quad = [\mathcal{W}_A(g,h)\otimes\mathcal{T}_B(g,h)][\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})],\end{aligned} \tag{167}$$

where $\mathcal{U}(g)(\cdot) := U(g)(\cdot)[U(g)]^\dagger$ denotes the unitary channel associated with a unitary operator $U(g)$, with a similar convention for the other unitary channels above.

Definition 9 (Bicovariant channel). We define a bidirectional channel to be bicovariant if it is bicovariant with respect to groups that have representations as unitary one-designs, i.e., $\frac{1}{|G|}\sum_g \mathcal{U}_{A'}(g)(\rho_{A'}) = \pi_{A'}$ and $\frac{1}{|H|}\sum_h \mathcal{V}_{B'}(h)(\rho_{B'}) = \pi_{B'}$.

An example of a bidirectional channel that is bicovariant is the controlled-NOT (CNOT) gate [19], for which we have the following covariances [102,103]:

$$\mathrm{CNOT}(X\otimes I) = (X\otimes X)\mathrm{CNOT}, \tag{168}$$

$$\mathrm{CNOT}(Z\otimes I) = (Z\otimes I)\mathrm{CNOT}, \tag{169}$$

$$\mathrm{CNOT}(Y\otimes I) = (Y\otimes X)\mathrm{CNOT}, \tag{170}$$

$$\mathrm{CNOT}(I\otimes X) = (I\otimes X)\mathrm{CNOT}, \tag{171}$$

$$\mathrm{CNOT}(I\otimes Z) = (Z\otimes Z)\mathrm{CNOT}, \tag{172}$$

$$\mathrm{CNOT}(I\otimes Y) = (Z\otimes Y)\mathrm{CNOT}, \tag{173}$$

where $\{I, X, Y, Z\}$ is the Pauli group with the identity element I. A more general example of a bicovariant channel is one that applies a CNOT with some probability and, with the complementary probability, replaces the input with the maximally mixed state.

In Ref. [103] the prominent idea of gate teleportation was developed, wherein one can generate the Choi state for the CNOT gate by sending in shares of maximally entangled states and then simulate the CNOT gate's action on any input state by using teleportation through the Choi state (see also Ref. [104] for earlier related developments). This idea generalized the notion of teleportation simulation of channels [54,55] from the single-sender single-receiver setting to the bidirectional setting. After these developments, Refs. [25,105] generalized the idea of gate teleportation to bipartite quantum channels that are not necessarily unitary channels.

The following result slightly generalizes the developments in Refs. [25,103,105]:

Proposition 3. If a bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is bicovariant, Definition 9, then it is teleportation-simulable with resource state $\theta_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'} \otimes \Phi_{B'L_B})$ (Definition 8).

We give a proof of Proposition 3 in Appendix B.

We now establish an upper bound on the entanglement generation rate of any (n, M, ε) PPT-assisted protocol that employs a bidirectional PPT-simulable channel.

Theorem 3. For a fixed $n,\ M \in \mathbb{N},\ \varepsilon \in (0, 1)$, the following strong converse bound holds for an (n, M, ε) protocol for PPT-assisted bidirectional entanglement generation over a bidirectional PPT-simulable quantum channel $\mathcal{N}$ with associated resource state $\theta_{D_AD_B}$, Definition 7, $\forall\alpha > 1$,

$$\frac{1}{n}\log_2 M \leqslant \widetilde{R}_\alpha(D_A; D_B)_\theta + \frac{\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right), \quad (174)$$

where $\widetilde{R}_\alpha(D_A; D_B)_\theta$ is the sandwiched Rains information (57) of the resource state $\theta_{D_AD_B}$.

Proof. The first few steps are similar to those in the proof of Theorem 1. From Sec. III B 1, we have that

$$\mathrm{Tr}\left\{\Phi_{M_AM_B}\omega_{M_AM_B}\right\} \geqslant 1-\varepsilon, \quad (175)$$

while Ref. [11] (Lemma 2) implies that, $\forall\sigma_{M_AM_B} \in \mathrm{PPT}'(M_A\!:\!M_B)$,

$$\mathrm{Tr}\left\{\Phi_{M_AM_B}\sigma_{M_AM_B}\right\} \leqslant \frac{1}{M}. \quad (176)$$

Under an "entanglement test," which is a measurement with POVM $\{\Phi_{M_AM_B}, I_{M_AM_B} - \Phi_{M_AM_B}\}$, and applying the data processing inequality for the sandwiched Rényi relative entropy, we find that (for details, see Lemma 5 of Ref. [106]), for all $\alpha > 1$,

$$\log_2 M \leqslant \widetilde{R}_\alpha(M_A; M_B)_\omega + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \quad (177)$$

The sandwiched Rains relative entropy is monotonically nonincreasing under the action of completely PPT-preserving channels and vanishing for a PPT state. Applying Lemma 4, we find that

$$\frac{1}{n}\widetilde{R}_\alpha(M_A; M_B)_\omega \leqslant \sup_{\rho_{L_AA'B'L_B}} [\widetilde{R}_\alpha(L_AA; BL_B)_{\mathcal{N}(\rho)} - \widetilde{R}_\alpha(L_AA'; B'L_B)_\rho]. \quad (178)$$

As stated in Definition 7, a PPT-simulable bidirectional channel $\mathcal{N}_{A'B'\to AB}$ with associated resource state $\theta_{D_AD_B}$ is such that, for any input state $\rho'_{A'B'}$,

$$\mathcal{N}_{A'B'\to AB}(\rho'_{A'B'}) = \mathcal{P}_{D_AA'B'D_B\to AB}\big(\rho'_{A'B'} \otimes \theta_{D_AD_B}\big). \quad (179)$$

Then, for any input state $\omega'_{L_AA'B'L_B}$,

$$\begin{aligned}
&\widetilde{R}_\alpha(L_AA; BL_B)_{\mathcal{P}(\omega'\otimes\theta)} - \widetilde{R}_\alpha(L_AA'; B'L_B)_{\omega'}\\
&\quad\leqslant \widetilde{R}_\alpha(D_AL_AA'; B'L_BD_B)_{\omega'\otimes\theta} - \widetilde{R}_\alpha(L_AA'; B'L_B)_{\omega'}\\
&\quad\leqslant \widetilde{R}_\alpha(L_AA'; B'L_B)_{\omega'} + \widetilde{R}_\alpha(D_A; D_B)_\theta\\
&\qquad-\widetilde{R}_\alpha(L_AA'; B'L_B)_{\omega'}\\
&\quad= \widetilde{R}_\alpha(D_A; D_B)_\theta.
\end{aligned} \quad (180)$$

The first inequality follows from monotonicity of $\widetilde{R}_\alpha$ with respect to completely PPT-preserving channels. The second inequality follows because $\widetilde{R}_\alpha$ is subadditive with respect to tensor-product states.

Applying the bound in (180) to (178), we find that

$$\widetilde{R}_\alpha(M_A; M_B)_\omega \leqslant n\widetilde{R}_\alpha(D_A; D_B)_\theta. \quad (181)$$

Combining (177) and (181), we get the desired inequality in (174). ■

Now we establish an upper bound on the secret-key rate of an (n, K, ε) secret-key-agreement protocol that employs a bidirectional teleportation-simulable channel.

Theorem 4. For a fixed $n,\ K \in \mathbb{N},\ \varepsilon \in (0, 1)$, the following strong converse bound holds for an (n, K, ε) protocol for a secret-key agreement over a bidirectional teleportation-simulable quantum channel $\mathcal{N}$ with associated resource state $\theta_{D_AD_B}$: $\forall\alpha > 1$,

$$\frac{1}{n}\log_2 K \leqslant \widetilde{E}_\alpha(D_A; D_B)_\theta + \frac{\alpha}{n(\alpha-1)}\log_2\left(\frac{1}{1-\varepsilon}\right), \quad (182)$$

where $\widetilde{E}_\alpha(D_A; D_B)_\theta$ is the sandwiched relative entropy of entanglement (65) of the resource state $\theta_{D_AD_B}$.

Proof. As stated in Definition 7, a bidirectional teleportation-simulable channel $\mathcal{N}_{A'B'\to AB}$ is such that, for any input state $\rho'_{A'B'}$,

$$\mathcal{N}_{A'B'\to AB}(\rho'_{A'B'}) = \mathcal{L}_{D_AA'B'D_B\to AB}\big(\rho'_{A'B'} \otimes \theta_{D_AD_B}\big). \quad (183)$$

Then, for any input state $\omega'_{L'_AA'B'L'_B}$,

$$\begin{aligned}
&\widetilde{E}_\alpha(L'_AA; BL'_B)_{\mathcal{L}(\omega'\otimes\theta)} - \widetilde{E}_\alpha(L'_AA'; B'L'_B)_{\omega'}\\
&\quad\leqslant \widetilde{E}_\alpha(D_AL'_AA'; B'L'_BD_B)_{\omega'\otimes\theta} - \widetilde{E}_\alpha(L'_AA'; B'L'_B)_{\omega'}\\
&\quad\leqslant \widetilde{E}_\alpha(L'_AA'; B'L'_B)_{\omega'} + \widetilde{E}_\alpha(D_A; D_B)_\theta\\
&\qquad- \widetilde{E}_\alpha(L'_AA'; B'L'_B)_{\omega'}\\
&\quad= \widetilde{E}_\alpha(D_A; D_B)_\theta.
\end{aligned} \quad (184)$$

The first inequality follows from monotonicity of $\widetilde{E}_\alpha$ with respect to LOCC channels. The second inequality follows because $\widetilde{E}_\alpha$ is subadditive.

From Sec. IV B 2, the following inequality holds for an (n, K, ε) protocol:

$$F\left(\omega_{S_A K_A K_B S_B}, \gamma_{S_A K_A K_B S_B}\right) \geqslant 1 - \varepsilon, \tag{185}$$

for some bipartite private state $\gamma_{S_A K_A K_B S_B}$ with key dimension K. From Sec. II G, $\omega_{S_A K_A K_B S_B}$ passes a γ-privacy test with probability at least $1-\varepsilon$, whereas any $\tau_{S_A K_A K_B S_B} \in \mathrm{SEP}(S_A K_A : K_B S_B)$ does not pass with probability greater than $\frac{1}{K}$ [15]. Making use of the results in Ref. [88] (Sec. 5.2), we conclude that

$$\log_2 K \leqslant \widetilde{E}_\alpha(S_A K_A; K_B S_B)_\omega + \frac{\alpha}{\alpha - 1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{186}$$

Now we can follow steps similar to those in the proof of Theorem 3 in order to arrive at (182). ■

We can also establish the following weak converse bounds, by combining the above approach with that in Ref. [58] (Sec. 3.5):

Remark 7. The following weak converse bound holds for an (n, M, ε) PPT-assisted bidirectional quantum communication protocol (Sec. III B 1) that employs a bidirectional PPT-simulable quantum channel $\mathcal{N}$ with associated resource state $\theta_{L_A L_B}$:

$$(1-\varepsilon)\frac{\log_2 M}{n} \leqslant R(L_A; L_B)_\theta + \frac{1}{n}h_2(\varepsilon), \tag{187}$$

where $R(L_A; L_B)_\theta$ is defined in (55) and $h_2(\varepsilon) := -\varepsilon \log_2 \varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$.

Remark 8. The following weak converse bound holds for an (n, K, ε) LOCC-assisted bidirectional secret-key-agreement protocol (Sec. IV B 2) that employs a bidirectional teleportation-simulable quantum channel $\mathcal{N}$ with associated resource state $\theta_{D_A D_B}$:

$$(1-\varepsilon)\frac{\log_2 K}{n} \leqslant E(D_A; D_B)_\theta + \frac{1}{n}h_2(\varepsilon), \tag{188}$$

where $E(D_A; D_B)_\theta$ is defined in (66).

Since every LOCC channel $\mathcal{L}_{D_A A' B' D_B \to AB}$ acting with respect to the bipartite cut $D_A A' : D_B B'$ is also a completely PPT-preserving channel with the partial transposition action on $D_B B'$, it follows that bidirectional teleportation-simulable channels are also bidirectional PPT-simulable channels. Based on Proposition 3, Theorem 3, Theorem 4, and the limits $n \to \infty$ and then $\alpha \to 1$ (in this order) [107], we can then conclude the following strong converse bounds:

Corollary 5. If a bidirectional quantum channel $\mathcal{N}$ is bicovariant (Definition 9), then

$$\widetilde{Q}^{2\to 2}_{\mathrm{PPT}}(\mathcal{N}) \leqslant R(L_A A; B L_B)_\theta, \tag{189}$$

$$\widetilde{P}^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N}) \leqslant E(L_A A; B L_B)_\theta, \tag{190}$$

where $\theta_{L_A A B L_B} = \mathcal{N}_{A'B' \to AB}(\Phi_{L_A A'} \otimes \Phi_{B' L_B})$, and $\widetilde{Q}^{2\to 2}_{\mathrm{PPT}}(\mathcal{N})$ and $\widetilde{P}^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N})$ denote the strong converse PPT-assisted bidirectional quantum capacity and strong converse LOCC-assisted bidirectional secret-key-agreement capacity, respectively, of a bidirectional channel $\mathcal{N}$.

VI. PRIVATE READING OF A READ-ONLY MEMORY DEVICE

Devising a communication or information-processing protocol that is secure against an eavesdropper is an area of primary interest in information theory. In this section, we introduce the task of private reading of information stored in a memory device. A secret message can either be encrypted in a computer program with circuit gates or in a physical storage device, such as a CD-ROM, DVD, etc. Here we limit ourselves to the case in which these computer programs or physical storage devices are used for read-only tasks; for simplicity, we refer to such media as memory devices.

In Ref. [22] a communication setting was considered in which a memory cell consists of unitary operations that encode a classical message. This model was generalized and studied under the name “quantum reading” in Ref. [42], and it was applied to the setting of an optical memory. In subsequent works [59,108,109], the model was extended to a memory cell consisting of arbitrary quantum channels. In Ref. [59] the most natural and general definition of the reading capacity of a memory cell was given, and this work also determined the reading capacities for some broad classes of memory cells. Quantum reading can be understood as a direct application of quantum channel discrimination [106,110–117]. In many cases, one can achieve performance better than what can be achieved when using a classical strategy [108,109,118–120]. In Ref. [121] the author discussed the security of a message encoded using a particular class of optical memory cells against readers employing classical strategies.

In a reading protocol, it is assumed that the reader has a description of a memory cell, which is a set of quantum channels. The memory cell is used to encode a classical message in a memory device. The memory device containing the encoded message is then delivered to the interested reader, whose task is to read out the message stored in it. To decode the message, the reader can transmit a quantum state to the memory device and perform a quantum measurement on the output state. In general, since quantum channels are noisy, there is a loss of information to the environment, and there is a limitation on how well information can be read out from the memory device.

To motivate the task of private reading, consider that once reading devices equipped with quantum systems are built, the readers can use these devices to transmit quantum states as a probe and then perform a joint measurement for reading the memory device. There could be a circumstance in which an individual would have to access a reading device in a public library under the surveillance of a librarian or other parties, whom we suppose to be a passive eavesdropper Eve. In such a situation, an individual would want information in a memory device not to be leaked to Eve, who has access to the environment, for security and privacy reasons. This naturally gives rise to the question of whether there exists a protocol for reading out a classical message that is secure from a passive eavesdropper.

In what follows, we introduce the details of private reading: briefly, it is the task of reading out a classical message (key) stored in a memory device, encoded with a memory cell, by the reader such that the message is not leaked to Eve. We

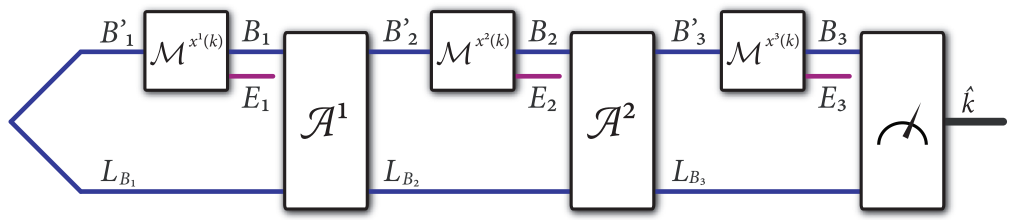

FIG. 3. The figure depicts a private reading protocol that calls a memory cell three times to decode the key k as $\hat{k}$. See the discussion in Sec. VI A for a detailed description of a private reading protocol.

also mention here that private reading can be understood as a particular kind of secret-key-agreement protocol that employs a particular kind of bipartite interaction, and thus, there is a strong link between the developments in Sec. IV and what follows (we elaborate on this point in what follows).

A. Private reading protocol

In a private reading protocol, we consider an encoder and a reader (decoder). Alice, an encoder, is one who encodes a secret classical message onto a read-only memory device that is delivered to Bob, a receiver, whose task is to read the message. We also refer to Bob as the reader. The private reading task comprises the estimation of the secret message encoded in the form of a sequence of quantum wiretap channels chosen from a given set $\{\mathcal{M}^x_{B'\to BE}\}_{x\in\mathcal{X}}$ of quantum wiretap channels (called a wiretap memory cell), where $\mathcal{X}$ is an alphabet, such that there is negligible leakage of information to Eve, who has access to the system E. A special case of this is when each wiretap channel $\mathcal{M}^x_{B'\to BE}$ is an isometric channel. In the most natural and general setting, the reader can use an adaptive strategy when decoding, as considered in Ref. [59].

Consider a set $\{\mathcal{M}^x_{B'\to BE}\}_{x\in\mathcal{X}}$ of wiretap quantum channels, where the size of B', B, and E are fixed and independent of x. The memory cell from the encoder Alice to the reader Bob is as follows: $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{M}^x_{B'\to B}\}_x$, where

$$\forall x\in\mathcal{X}\colon \mathcal{M}^x_{B'\to B}(\cdot) := \mathrm{Tr}_E\left\{\mathcal{M}^x_{B'\to BE}(\cdot)\right\}, \tag{191}$$

which may also be known to Eve, before executing the reading protocol. We assume only the systems E are accessible to Eve for all channels $\mathcal{M}^x$ in a memory cell. Thus, Eve is a passive eavesdropper in the sense that all she can do is to access the output of the channels

$$\forall x\in\mathcal{X}\colon \mathcal{M}^x_{B'\to E}(\cdot) = \mathrm{Tr}_B\left\{\mathcal{M}^x_{B'\to BE}(\cdot)\right\}. \tag{192}$$

We consider a classical message set $\mathcal{K} = \{1, 2, \dots, K\}$, and let K_A be an associated system denoting a classical register for the secret message. In general, Alice encodes a message $k \in \mathcal{K}$ using a codeword $x^n(k) = x_1(k)x_2(k)\cdots x_n(k)$ of length n, where $x_i(k)\in\mathcal{X}$ for all $i\in\{1, 2, \dots, n\}$. Each codeword identifies with a corresponding sequence of quantum channels chosen from the wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$:

$$\left(\mathcal{M}^{x_1(k)}_{B'_1\to B_1E_1}, \mathcal{M}^{x_2(k)}_{B'_2\to B_2E_2}, \dots, \mathcal{M}^{x_n(k)}_{B'_n\to B_nE_n}\right). \tag{193}$$

An adaptive decoding strategy makes n calls to the memory cell, as depicted in Fig. 3. It is specified in terms of a transmitter state $\rho_{L_{B_1}B'_1}$, a set of adaptive, interleaved channels $\{\mathcal{A}^i_{L_{B_i}B_i\to L_{B_{i+1}}B'_{i+1}}\}_{i=1}^{n-1}$, and a final quantum measurement $\{\Lambda^{(\hat{k})}_{L_{B_n}B_n}\}_{\hat{k}}$ that outputs an estimate $\hat{k}$ of the message k. The strategy begins with Bob preparing the input state $\rho_{L_{B_1}B'_1}$ and sending the B'_1 system into the channel $\mathcal{M}^{x_1(k)}_{B'_1\to B_1E_1}$. The channel outputs the system B_1 for Bob. He adjoins the system B_1 to the system L_{B_1} and applies the channel $\mathcal{A}^1_{L_{B_1}B_1\to L_{B_2}B'_2}$. The channel $\mathcal{A}^i_{L_{B_i}B_i\to L_{B_{i+1}}B'_{i+1}}$ is called adaptive because it can take an action conditioned on the information in the system B_i, which itself might contain partial information about the message k. Then he sends the system B'_2 into the channel $\mathcal{M}^{x_2(k)}_{B'_2\to B_2E_2}$, which outputs systems B_2 and E_2. The process of successively using the channels interleaved by the adaptive channels continues $n-2$ more times, which results in the final output systems L_{B_n} and B_n with Bob. Next, he performs a measurement $\{\Lambda^{(\hat{k})}_{L_{B_n}B_n}\}_{\hat{k}}$ on the output state $\rho_{L_{B_n}B_n}$, and the measurement outputs an estimate $\hat{k}$ of the original message k. It is natural to assume that the outputs of the adaptive channels and their complementary channels are inaccessible to Eve and are instead held securely by Bob.

The physical model that we assume, as is standard in QKD protocols, is that Bob's local laboratory is secure. So Bob can perform whatever local operations that he would like to in his laboratory. Furthermore, without loss of generality, Bob can perform all of these local steps as isometric channels, sending the original output as output and keeping the former environment to himself, thus ensuring that the new complement of each isometric channel is trivial so that Eve gets no information from these steps. So the task does not change even if we assume that Eve has access to the complements of each of the adaptive channels since it is possible to do things in this way without loss of generality.

It is apparent that a nonadaptive strategy is a special case of an adaptive strategy. In a nonadaptive strategy, the reader does not perform any adaptive channels and instead uses $\rho_{L_BB'^n}$ as the transmitter state with each B'_i system passing through the corresponding channel $\mathcal{M}^{x_i(k)}_{B'_i\to B_iE_i}$ and L_B being a reference system. The final step in such a nonadaptive strategy is to perform a decoding measurement on the joint system L_BB^n.

As argued in Ref. [59], based on the physical setup of quantum reading, in which the reader assumes the role of both a transmitter and receiver, it is natural to consider the use of an adaptive strategy when defining the private reading capacity of a memory cell.

Definition 10 (Private reading protocol). An $(n, K, \varepsilon, \delta)$ private reading protocol for a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is defined by an encoding map $\mathcal{K}\to\mathcal{X}^{\otimes n}$, an adaptive strategy with measurement $\{\Lambda^{(\hat{k})}_{L_{B_n}B_n}\}_{\hat{k}}$, such that the average success probability is at least $1-\varepsilon$ where $\varepsilon \in (0,1)$:

$$1-\varepsilon \leqslant 1-p_{\mathrm{err}} := \frac{1}{K}\sum_k \operatorname{Tr}\left\{\Lambda^{(k)}_{L_{B_n}B_n}\rho^{(k)}_{L_{B_n}B_n}\right\}, \tag{194}$$

where

$$\rho^{(k)}_{L_{B_n}B_nE^n} = \left(\mathcal{M}^{x_n(k)}_{B'_n\to B_nE_n}\circ\mathcal{A}^{n-1}_{L_{B_{n-1}}B_{n-1}\to L_{B_n}B'_n}\right.$$
$$\left.\circ\cdots\circ\mathcal{A}^{1}_{L_{B_1}B_1\to L_{B_2}B'_2}\circ\mathcal{M}^{x_1(k)}_{B'_1\to B_1E_1}\right)\left(\rho_{L_{B_1}B'_1}\right). \tag{195}$$

Furthermore, the security condition is that

$$\frac{1}{K}\sum_{k\in\mathcal{K}}\frac{1}{2}\left\|\rho^{(k)}_{E^n}-\tau_{E^n}\right\|_1 \leqslant \delta, \tag{196}$$

where $\rho^{(k)}_{E^n}$ denotes the state accessible to the passive eavesdropper when message k is encoded. Also, τ_{E^n} is some fixed state. The rate $P := \frac{1}{n}\log_2 K$ of a given $(n, K, \varepsilon, \delta)$ private reading protocol is equal to the number of secret bits read per channel use.

Based on the discussions in Ref. [88] (Appendix B), there are connections between the notions of private communication given in Sec. IV B 2 and Definition 10, and we exploit these in what follows.

To arrive at a definition of the private reading capacity, we demand that there exists a sequence of private reading protocols, indexed by n, for which the error probability $p_{\mathrm{err}} \to 0$ and security parameter $\delta \to 0$ as $n\to\infty$ at a fixed rate P.

A rate P is called achievable if for all $\varepsilon, \delta \in (0,1]$, $\delta' > 0$, and sufficiently large n, there exists an $(n, 2^{n(P-\delta')}, \varepsilon, \delta)$ private reading protocol. The private reading capacity $P^{\mathrm{read}}(\overline{\mathcal{M}}_{\mathcal{X}})$ of a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is defined as the supremum of all achievable rates.

An $(n, K, \varepsilon, \delta)$ private reading protocol for a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is a nonadaptive private reading protocol when the reader abstains from employing any adaptive strategy for decoding. The nonadaptive private reading capacity $P^{\mathrm{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}})$ of a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is defined as the supremum of all achievable rates for a private reading protocol that is limited to nonadaptive strategies.

B. Nonadaptive private reading capacity

In what follows we restrict our attention to reading protocols that employ a nonadaptive strategy, and we now derive a regularized expression for the nonadaptive private reading capacity of a general wiretap memory cell.

Theorem 5. The nonadaptive private reading capacity of a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is given by

$$P^{\mathrm{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}}) = \sup_n \max_{p_{X^n},\sigma_{L_BB'^n}} \frac{1}{n}[I(X^n;L_BB^n)_\tau - I(X^n;E^n)_\tau], \tag{197}$$

where

$$\tau_{X^nL_BB^nE^n} := \sum_{x^n} p_{X^n}(x^n)|x^n\rangle\langle x^n|_{X^n}\otimes\mathcal{M}^{x^n}_{B'^n\to B^nE^n}\left(\sigma_{L_BB'^n}\right), \tag{198}$$

and it suffices for $\sigma_{L_BB'^n}$ to be a pure state such that $L_B \simeq B'^n$.

Proof. Let us begin by defining a cq-state corresponding to the task of private reading. Consider a wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{M}^x_{B'\to BE}\}_{x\in\mathcal{X}}$. The initial state $\rho_{K_AL_BB'^n}$ of a nonadaptive private reading protocol takes the form

$$\rho_{K_AL_BB'^n} := \frac{1}{K}\sum_k |k\rangle\langle k|_{K_A}\otimes\rho_{L_BB'^n}. \tag{199}$$

The action of the encoding is to apply an instrument that measures the K_A register and, conditioned on the outcome, presents Bob with a channel codeword sequence $\mathcal{M}^{x^n(k)}_{B'^n\to B^nE^n} := \bigotimes_{i=1}^n \mathcal{M}^{x_i(k)}_{B'_i\to B_iE_i}$. Bob then passes the transmitter state $\rho_{L_BB'^n}$ through $\mathcal{M}^{x^n(k)}_{B'^n\to B^nE^n}$. Then the resulting state is

$$\rho_{K_AL_BB^nE^n} = \frac{1}{K}\sum_k |k\rangle\langle k|_{K_A}\otimes\mathcal{M}^{x^n(k)}_{B'^n\to B^nE^n}\left(\rho_{L_BB'^n}\right). \tag{200}$$

Let $\rho_{K_AK_B} = \mathcal{D}_{L_BB^n\to K_B}(\rho_{K_AL_BB^n})$ be the output state at the end of the protocol after the decoding channel $\mathcal{D}_{L_BB^n\to K_B}$ is performed by Bob. The privacy criterion introduced in Definition 10 requires that

$$\frac{1}{K}\sum_{k\in\mathcal{K}}\frac{1}{2}\left\|\rho^{x^n(k)}_{E^n}-\tau_{E^n}\right\|_1 \leqslant \delta, \tag{201}$$

where $\rho^{x^n(k)}_{E^n} := \operatorname{Tr}_{L_BB^n}\{\mathcal{M}^{x^n(k)}{}_{B'^n\to B^nE^n}(\rho_{L_BB'^n})\}$ and τ_{E^n} is some arbitrary constant state. Hence

$$\delta \geqslant \frac{1}{2}\sum_k \frac{1}{K}\left\|\rho^{x^n(k)}_{E^n}-\tau_{E^n}\right\|_1 \tag{202}$$

$$= \frac{1}{2}\left\|\rho_{K_AE^n}-\pi_{K_A}\otimes\tau_{E^n}\right\|_1, \tag{203}$$

where π_{K_A} denotes maximally mixed state, i.e., $\pi_{K_A} := \frac{1}{K}\sum_k |k\rangle\langle k|_{K_A}$. We note that

$$I(K_A;E^n)_\rho = S(K_A)_\rho - S(K_A|E^n)_\rho \tag{204}$$

$$= S(K_A|E^n)_{\pi\otimes\tau} - S(K_A|E^n)_\rho \tag{205}$$

$$\leqslant \delta\log_2 K + g(\delta), \tag{206}$$

which follows from an application of Lemma 2.

We are now ready to derive a weak converse bound on the private reading rate:

$$\begin{aligned}
\log_2 K &= S(K_A)_\rho \\
&= I(K_A;K_B)_\rho + S(K_A|K_B)_\rho \\
&\leqslant I(K_A;K_B)_\rho + \varepsilon\log_2 K + h_2(\varepsilon) \\
&\leqslant I(K_A;L_BB^n)_\rho + \varepsilon\log_2 K + h_2(\varepsilon) \\
&\leqslant I(K_A;L_BB^n)_\rho - I(K_A;E^n)_\rho + \varepsilon\log_2 K \\
&\quad + h_2(\varepsilon) + \delta\log_2 K + g(\delta) \\
&\leqslant \max_{p_{X^n},\sigma_{L_BB'^n}} [I(X^n;L_BB^n)_\tau - I(X^n;E^n)_\tau] \\
&\quad + \varepsilon\log_2 K + h_2(\varepsilon) + \delta\log_2 K + g(\delta),
\end{aligned} \tag{207}$$

where $\tau_{X^nL_BB^nE^n}$ is a state of the form in (198). The first inequality follows from Fano's inequality [122]. The second inequality follows from the monotonicity of mutual information under the action of a local quantum channel by Bob (Holevo bound). The final inequality follows because the maximization is over all possible probability distributions and input states. Then

$$\frac{\log_2 K}{n}(1-\varepsilon-\delta) \leqslant \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}[I(X^n;L_B B^n)_\tau - I(X^n;E^n)_\tau] + \frac{h_2(\varepsilon)+g(\delta)}{n}. \tag{208}$$

Now considering a sequence of nonadaptive $(n, K_n, \varepsilon_n, \delta_n)$ protocols with $\lim_{n\to\infty} \frac{\log_2 K_n}{n} = P$, $\lim_{n\to\infty} \varepsilon_n = 0$, and $\lim_{n\to\infty} \delta_n = 0$, the converse bound on nonadaptive private reading capacity of memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$ is given by

$$P \leqslant \sup_n \max_{p_{X^n},\sigma_{L_B B'^n}} \frac{1}{n}[I(X^n;L_B B^n)_\tau - I(X^n;E^n)_\tau], \tag{209}$$

which follows by taking the limit as $n \to \infty$.

It follows from the results of Refs. [12,13] that right-hand side of (209) is also an achievable rate in the limit $n \to \infty$. Indeed, the encoder and reader can induce the cq wiretap channel $x \to \mathcal{M}^x_{B'\to BE}(\sigma_{L_B B'})$, to which the results of Refs. [12,13] apply. A regularized coding strategy then gives the general achievability statement. Therefore, the nonadaptive private reading capacity is given as stated in the theorem. ■

C. Purifying private reading protocols

As observed in Refs. [14,15] and reviewed in Sec. II G, any protocol of the above form, discussed in Sec. VI B, can be purified in the following sense. In this section, we assume that each wiretap memory cell consists of a set of isometric channels, written as $\{\mathcal{U}^{\mathcal{M}^x}_{B'\to BE}\}_x$. Thus, Eve has access to system E, which is the output of a particular isometric extension of the channel $\mathcal{M}^x_{B'\to B}$, i.e., $\widehat{\mathcal{M}}^x_{B'\to E}(\cdot) = \mathrm{Tr}_B\{\mathcal{U}^{\mathcal{M}^x}_{B'\to BE}(\cdot)\}$, for all $x \in \mathcal{X}$. We refer to such memory cell as an isometric wiretap memory cell.

We begin by considering nonadaptive private reading protocols. A nonadaptive purified secret-key-agreement protocol that uses an isometric wiretap memory cell begins with Alice preparing a purification of the maximally classically correlated state:

$$\frac{1}{\sqrt{K}}\sum_{k\in\mathcal{K}} |k\rangle_{K_A}|k\rangle_{\hat{K}}|k\rangle_C, \tag{210}$$

where $\mathcal{K} = \{1,2,\dots,K\}$, and K_A, $\hat{K}$, and C are classical registers. Alice coherently encodes the value of the register C using the memory cell, the codebook $\{x^n(k)\}_k$, and the isometric mapping $|k\rangle_C \to |x^n(k)\rangle_{X^n}$. Alice makes two coherent copies of the codeword $x^n(k)$ and stores them safely in coherent classical registers X^n and $\hat{X}^n$. At the same time, she acts on Bob's input state $\rho_{L_B B'^n}$ with the following isometry:

$$\sum_{x^n} |x^n\rangle\langle x^n|_{X^n} \otimes U^{\mathcal{M}^{x^n}}_{B'^n\to B^n E^n} \otimes |x^n\rangle_{\hat{X}^n}. \tag{211}$$

For the task of reading, Bob inputs the state $\rho_{L_B B'^n}$ to the channel sequence $\mathcal{M}^{x^n(k)}$, with the goal of decoding k. In the purified setting, the resulting output state is $\psi_{K_A\hat{K}X^n L'_B L_B B^n E^n \hat{X}^n}$, which includes all concerned coherent classical registers or quantum systems accessible by Alice, Bob, and Eve:

$$|\psi\rangle_{K_A\hat{K}X^n L'_B L_B B^n E^n \hat{X}^n} := \frac{1}{\sqrt{K}}\sum_k |k\rangle_{K_A}|k\rangle_{\hat{K}} \otimes |x^n(k)\rangle_{X^n} \times U^{\mathcal{M}^{x^n}}_{B'^n\to B^n E^n}|\psi\rangle_{L'_B L_B B'^n}|x^n(k)\rangle_{\hat{X}^n}, \tag{212}$$

where $\psi_{L'_B L_B B'^n}$ is a purification of $\rho_{L_B B'^n}$ and the systems L'_B, L_B, and B^n are held by Bob, whereas Eve has access only to E^n. The final global state is $\psi_{K_A\hat{K}X^n L'_B K_B E^n \hat{X}^n}$ after Bob applies the decoding channel $\mathcal{D}_{L_B B^n\to K_B}$, where

$$|\psi\rangle_{K_A\hat{K}X^n L'_B L''_B K_B E^n \hat{X}^n} := U^{\mathcal{D}}_{L_B B^n\to L''_B K_B}|\psi\rangle_{K_A\hat{K}X^n L'_B L_B B^n E^n \hat{X}^n}, \tag{213}$$

$U^{\mathcal{D}}$ is an isometric extension of the decoding channel $\mathcal{D}$, and L''_B is part of the shield system of Bob.

At the end of the purified protocol, Alice possesses the key system K_A and the shield systems $\hat{K}X^n\hat{X}^n$, Bob possesses the key system K_B and the shield systems $L'_B L''_B$, and Eve possesses the environment system E^n. The state $\psi_{K_A\hat{K}X^n L'_B L''_B K_B \hat{X}^n E^n}$ at the end of the protocol is a pure state.

For a fixed n, $K \in \mathbb{N}$, $\varepsilon \in [0,1]$, the original protocol is an $(n, 2^{nP}, \sqrt{\varepsilon}, \sqrt{\varepsilon})$ private reading protocol if the memory cell is called n times as discussed above, and if

$$F\left(\psi_{K_A\hat{K}X^n L'_B L''_B K_B \hat{X}^n}, \gamma_{S_A K_A K_B S_B}\right) \geqslant 1-\varepsilon, \tag{214}$$

where γ is a private state such that $S_A = \hat{K}X^n\hat{X}^n$, $K_A = K_A$, $K_B = K_B$, $S_B = L'_B L''_B$. See Ref. [88] (Appendix B) for further details.

Similarly, it is possible to purify a general adaptive private reading protocol, but we omit the details.

D. Converse bounds on private reading capacities

In this section, we derive different upper bounds on the private reading capacity of an isometric wiretap memory cell. The first is a weak converse upper bound on the nonadaptive private reading capacity in terms of the squashed entanglement. The second is a strong converse upper bound on the (adaptive) private reading capacity in terms of the bidirectional max-relative entropy of entanglement. Finally, we evaluate the private reading capacity for an example: a qudit erasure memory cell.

We derive the first converse bound on nonadaptive private reading capacity by making the following observation, related to the development in Ref. [88] (Appendix B): any nonadaptive $(n, 2^{nP}, \varepsilon, \delta)$ private reading protocol of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$, for reading out a secret key, can be realized by an $(n, 2^{nP}, \varepsilon'(2-\varepsilon'))$ nonadaptive purified secret-key-agreement reading protocol, where $\varepsilon' := \varepsilon + 2\delta$. As such, a converse bound for the latter protocol implies a converse bound for the former.

First, we derive an upper bound on the nonadaptive private reading capacity in terms of the squashed entanglement [90]:

Proposition 4. The nonadaptive private reading capacity $P^{\mathrm{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}})$ of an isometric wiretap memory cell

$\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{U}^{\mathcal{M}^x}_{B'\to BE}\}_{x\in\mathcal{X}}$ is bounded from above as

$$P^{\text{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}}) \leqslant \sup_{p_X,\psi_{LB'}} E_{\text{sq}}(XL_B;B)_{\omega}, \tag{215}$$

where $\omega_{XL_BB} = \text{Tr}_E\{\omega_{XL_BBE}\}$, such that $\psi_{L_BB'}$ is a pure state and

$$|\omega\rangle_{XLBE} = \sum_{x\in\mathcal{X}} \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B'\to BE}|\psi\rangle_{L_BB'}. \tag{216}$$

Proof. For the discussed purified nonadaptive secret-key-agreement reading protocol, when (214) holds, the dimension of the secret-key system is upper bounded as [123] (Theorem 2)

$$\log_2 K \leqslant E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A;K_BL_BL''_B)_{\psi} + f_1(\sqrt{\varepsilon},K), \tag{217}$$

where

$$f_1(\varepsilon,K_A) := 2\varepsilon\log_2 K + 2g(\varepsilon). \tag{218}$$

We can then proceed as follows:

$$\log_2 K \leqslant E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A;K_BL''_BL'_B)_{\psi} + f_1(\sqrt{\varepsilon},K) \tag{219}$$

$$= E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A;B^nL_BL'_B)_{\psi} + f_1(\sqrt{\varepsilon},K), \tag{220}$$

where the first equality is due to the invariance of E_{sq} under isometries.

For any five-partite pure state $\phi_{B'B_1B_2E_1E_2}$, the following inequality holds [93] (Theorem 7):

$$E_{\text{sq}}(B';B_1B_2)_{\phi} \leqslant E_{\text{sq}}(B'B_2E_2;B_1)_{\phi} + E_{\text{sq}}(B'B_1E_1;B_2)_{\phi}. \tag{221}$$

Choosing $B' = \hat{K}X^n\hat{X}^nK_A$, $B_1 = B_n$, $B_2 = L_BL'_BB^{n-1}$, $E_1 = E_n$ and $E_2 = E^{n-1}$, this implies that

$$\begin{aligned}
&E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A;B^nL_BL'_B)_{\psi}\\
&\quad\leqslant E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AL_BL'_BB^{n-1}E^{n-1};B_n)_{\psi}\\
&\qquad + E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AB_nE_n;L_BL'_BB^{n-1})_{\psi}\\
&\quad= E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_AL_BL'_BB^{n-1}E^{n-1};B_n)_{\psi}\\
&\qquad + E_{\text{sq}}(\hat{K}X^n\hat{X}^{n-1}K_AB'_n;L_BL'_BB^{n-1})_{\psi},
\end{aligned} \tag{222}$$

where the equality holds by considering an isometry with the following uncomputing action:

$$\begin{aligned}
&|k\rangle_{K_A}|k\rangle_{\hat{K}}|x^n(k)\rangle_{X^n}U^{\mathcal{M}^{x^n}}_{B'^n\to B^nE^n}|\psi\rangle_{L'_BL_BB'^n}|x^n(k)\rangle_{\hat{X}^n}\\
&\quad\to |k\rangle_{K_A}|k\rangle_{\hat{K}}|x^n(k)\rangle_{X^n}U^{\mathcal{M}^{x^{n-1}}}_{B'^{n-1}\to B^{n-1}E^{n-1}}|\psi\rangle_{L'_BL_BB'^n}\\
&\quad\times|x^{n-1}(k)\rangle_{\hat{X}^{n-1}}.
\end{aligned} \tag{223}$$

Applying the inequality in (221) and uncomputing isometries like the above repeatedly to (222), we find that

$$\begin{aligned}
&E_{\text{sq}}(\hat{K}X^n\hat{X}^nK_A;B^nL_BL'_B)_{\psi}\\
&\qquad\leqslant \sum_{i=1}^n E_{\text{sq}}(\hat{K}X^n\hat{X}_iK_AL_BL'_BB'^{n\setminus\{i\}};B_i),
\end{aligned} \tag{224}$$

where the notation $B'^{n\setminus\{i\}}$ indicates the composite system $B'_1B'_2\cdots B'_{i-1}B'_{i+1}\cdots B'_n$, i.e., all $n-1$ B'-labeled systems except B'_i. Each summand above is equal to the squashed entanglement of some state of the following form: a bipartite state is prepared on some auxiliary system Z and a control system X, a bipartite state is prepared on systems L_B and B', a controlled isometry $\sum_x |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}$ is performed from X to B', and then E is traced out. By applying the development in Ref. [41] (Appendix A), we conclude that the auxiliary system Z is not necessary. Thus, the state of systems X, L_B, B', and E can be taken to have the form in (216). From (220) and the above reasoning, since $\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{f_1(\sqrt{\varepsilon},K)}{n} = 0$, we conclude that

$$\widetilde{P}^{\text{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}}) \leqslant \sup_{p_X,\psi_{L_BB'}} E_{\text{sq}}(XL;B)_{\omega}, \tag{225}$$

where $\omega_{XL_BB} = \text{Tr}_E\{\omega_{XL_BBE}\}$, such that $\psi_{L_BB'}$ is a pure state and

$$|\omega\rangle_{XL_BBE} = \sum_{x\in\mathcal{X}} \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B'\to BE}|\psi\rangle_{L_BB'}. \tag{226}$$

This concludes the proof. ■

We now bound the strong converse private reading capacity of an isometric wiretap memory cell in terms of the bidirectional max-relative entropy.

Theorem 6. The strong converse private reading capacity $\widetilde{P}^{\text{read}}(\overline{\mathcal{M}}_{\mathcal{X}})$ of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{U}^{\mathcal{M}^x}_{B'\to BE}\}_{x\in\mathcal{X}}$ is bounded from above by the bidirectional max-relative entropy of entanglement $E^{2\to 2}_{\max}(\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{X'B'\to XB})$ of the bidirectional channel $\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{X'B'\to XB}$,

$$\widetilde{P}^{\text{read}}(\overline{\mathcal{M}}_{\mathcal{X}}) \leqslant E^{2\to 2}_{\max}(\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XB}), \tag{227}$$

where

$$\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XB}(\cdot) := \text{Tr}_E\left\{U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE}(\cdot)\left(U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE}\right)^{\dagger}\right\}, \tag{228}$$

such that

$$U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE} := \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}. \tag{229}$$

Proof. First we recall, as stated previously, that a $(n, 2^{nP}, \varepsilon, \delta)$ (adaptive) private reading protocol of a memory cell $\overline{\mathcal{M}}_{\mathcal{X}}$, for reading out a secret key, can be realized by an $(n, 2^{nP}, \varepsilon'(2-\varepsilon'))$ purified secret-key-agreement reading protocol, where $\varepsilon' := \varepsilon + 2\delta$. Given that a purified secret-key-agreement reading protocol can be understood as particular case of a bidirectional secret-key-agreement protocol (as discussed in Sec. IV B 2), we conclude that the strong converse private reading capacity is bounded from above by

$$\widetilde{P}^{\text{read}}_{\text{n-a}}(\overline{\mathcal{M}}_{\mathcal{X}}) \leqslant E^{2\to 2}_{\max}(\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XB}), \tag{230}$$

where the bidirectional channel is

$$\mathcal{N}^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XB}(\cdot) = \text{Tr}_E\left\{U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE}(\cdot)\left(U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE}\right)^{\dagger}\right\}, \tag{231}$$

such that

$$U^{\overline{\mathcal{M}}_{\mathcal{X}}}_{XB'\to XBE} := \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}. \tag{232}$$

The reading protocol is a particular instance of an LOCC-assisted bidirectional secret-key-agreement protocol in which classical communication between Alice and Bob does not occur. The local operations of Bob in the bidirectional secret-key-agreement protocol are equivalent to adaptive operations by Bob in reading. Therefore, applying Theorem 2, we conclude that (227) holds, where the strong converse in this context means that $\varepsilon + 2\delta \to 1$ in the limit as $n \to \infty$ if the reading rate exceeds $E_{\max}^{2\to 2}(\mathcal{N}_{XB'\to XB}^{\overline{\mathcal{M}}_{\mathcal{X}}})$ [124]. ■

1. Qudit erasure wiretap memory cell

The main goal of this section is to evaluate the private reading capacity of the qudit erasure wiretap memory cell [59].

Definition 11 (Erasure wiretap memory cell). The qudit erasure wiretap memory cell $\overline{\mathcal{Q}}_{\mathcal{X}}^{q} = \{\mathcal{Q}_{B'\to BE}^{q,x}\}_{x\in\mathcal{X}}$, $|\mathcal{X}| = d^2$, consists of the following qudit channels:

$$\mathcal{Q}^{q,x}(\cdot) = \mathcal{Q}^{q}[\sigma^{x}(\cdot)(\sigma^{x})^{\dagger}], \tag{233}$$

where $\mathcal{Q}^q$ is an isometric channel extending the qudit erasure channel [125]:

$$\mathcal{Q}^{q}(\rho_{B'}) = U^{q}\rho_{B'}(U^{q})^{\dagger}, \tag{234}$$

$$U^{q}|\psi\rangle_{B'} = \sqrt{1-q}|\psi\rangle_{B}|e\rangle_{E} + \sqrt{q}|e\rangle_{B}|\psi\rangle_{E}, \tag{235}$$

such that $q \in [0, 1]$, $\dim(\mathcal{H}_{B'}) = d$, $|e\rangle\langle e|$ is some state orthogonal to the support of input state ρ, and $\forall x \in \mathcal{X} : \sigma^{x} \in \mathbf{H}$ are the Heisenberg-Weyl operators as reviewed in (C5) of Appendix C. Observe that $\mathcal{Q}_{\mathcal{X}}^{q}$ is jointly covariant with respect to the Heisenberg-Weyl group $\mathbf{H}$ because the qudit erasure channel $\mathcal{Q}^q$ is covariant with respect to $\mathbf{H}$.

Now we establish the private reading capacity of the qudit erasure wiretap memory cell.

Proposition 5. The private reading capacity and strong converse private reading capacity of the qudit erasure wiretap memory cell $\overline{\mathcal{Q}}_{\mathcal{X}}^{q}$ are given by

$$P^{\text{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^{q}) = \widetilde{P}^{\text{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^{q}) = 2(1-q)\log_2 d. \tag{236}$$

Proof. To prove the proposition, consider that $\mathcal{N}^{\overline{\mathcal{Q}}_{\mathcal{X}}^{q}}$ as defined in (228) is bicovariant and $\mathcal{Q}_{B'\to B}^{q}$ is covariant. Thus, to get an upper bound on the strong converse private reading capacity, it is sufficient to consider the action of a coherent use of the memory cell on a maximally entangled state (see Corollary 5). We furthermore apply the development in Ref. [41] (Appendix A) to restrict to the following state:

$$\begin{aligned}
&\phi_{XL_BBE}\\
&:= \frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x\in\mathcal{X}}|x\rangle_{X}\otimes U_{B'\to BE}^{\mathcal{Q}^{q,x}}|\Phi\rangle_{L_BB'}\\
&= \sqrt{\frac{1-q}{d|\mathcal{X}|}}\sum_{i=0}^{d}\sum_{x}|x\rangle_{X}\otimes\sigma^{x}|i\rangle_{B}|i\rangle_{L_B}|e\rangle_{E}\\
&\quad+\sqrt{\frac{q}{d|\mathcal{X}|}}\sum_{i=0}^{d}\sum_{x}|x\rangle_{X}\otimes|e\rangle_{B}|i\rangle_{L_B}\otimes\sigma^{x}|i\rangle_{E}.
\end{aligned} \tag{237}$$

Observe that $\sum_{i=0}^{d-1}\sum_{x}|x\rangle_{X}\otimes|e\rangle_{B}|i\rangle_{L_B}\otimes\sigma^{x}|i\rangle_{E}$ and $\sum_{i=0}^{d-1}\sum_{x}|x\rangle_{X}\otimes\sigma^{x}|i\rangle_{B}|i\rangle_{L_B}|e\rangle_{E}$ are orthogonal. Also, since, $|e\rangle$ is orthogonal to the input Hilbert space, the only term contributing to the relative entropy of entanglement is $\sqrt{1-q}\frac{1}{d}\sum_{i=0}^{d}\sum_{x}|x\rangle_{X}\otimes\sigma^{x}|i\rangle_{B}|i\rangle_{L_B}$. Let

$$|\psi\rangle_{XL_BB} = \frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x=0}^{d^2-1}|x\rangle_{X}\otimes\sigma^{x}|\Phi\rangle_{BL_B}. \tag{238}$$

$\{\sigma^{x}|\Phi\rangle_{BL_B}\}_{x\in\mathcal{X}}$ forms an orthonormal basis in $\mathcal{H}_B\otimes\mathcal{H}_{L_B}$ (see Appendix C), so

$$|\psi\rangle_{XL_BB} = |\Phi\rangle_{X:BL_B} = \frac{1}{d}\sum_{x=0}^{d^2-1}|x\rangle_{X}\otimes|x\rangle_{BL_B}, \tag{239}$$

and $E(X;LB)_{\Phi} = 2\log_2 d$. Applying Corollary 5 and convexity of relative entropy of entanglement, we conclude that

$$\widetilde{P}^{\text{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^{q}) \leqslant 2(1-q)\log_2 d. \tag{240}$$

From Theorem 5, the following bound holds:

$$\begin{aligned}
P^{\text{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^{q}) &\geqslant P_{\text{n-a}}^{\text{read}}(\overline{\mathcal{Q}}_{\mathcal{X}}^{q}) &(241)\\
&\geqslant I(X;L_BB)_{\rho} - I(X;E)_{\rho}, &(242)
\end{aligned}$$

where

$$\rho_{XL_BBE} = \frac{1}{d^2}\sum_{x=0}^{d^2-1}|x\rangle\langle x|_{X}\otimes\mathcal{U}_{B'\to BE}^{\mathcal{Q}^{q,x}}(\Phi_{X:L_BB'}). \tag{243}$$

After a calculation, we find that $I(X;E)_{\rho} = 0$ and $I(X;L_BB)_{\rho} = 2(1-q)\log_2 d$. Therefore, from (240) and the above, we conclude the statement of the theorem.

From the above and Ref. [59] (Corollary 4), we conclude that there is no difference between the private reading capacity of the qudit erasure memory cell and its reading capacity.

VII. ENTANGLEMENT GENERATION FROM A COHERENT MEMORY CELL OR CONTROLLED ISOMETRY

In this section, we consider an entanglement distillation task between two parties Alice and Bob holding systems X and B, respectively. The set up is similar to purified secret-key generation when using a memory cell (see Sec. VI C). The goal of the protocol is as follows: Alice and Bob, who are spatially separated, try to generate a maximally entangled state between them by making coherent use of an isometric wiretap memory cell $\overline{\mathcal{M}}_{\mathcal{X}} = \{\mathcal{U}_{B'\to BE}^{\mathcal{M}^x}\}_{x\in\mathcal{X}}$ known to both parties. That is, Alice and Bob have access to the following controlled isometry:

$$U_{XB'\to XBE}^{\overline{\mathcal{M}}_{\mathcal{X}}} := \sum_{x\in\mathcal{X}}|x\rangle\langle x|_{X}\otimes U_{B'\to BE}^{\mathcal{M}^x}, \tag{244}$$

such that X and E are inaccessible to Bob. Using techniques from Ref. [13], we can state an achievable rate of entanglement generation by coherently using the memory cell.

Theorem 7. The following rate is achievable for entanglement generation when using the controlled isometry in (244):

$$I(X\rangle L_BB)_{\omega}, \tag{245}$$

where $I(X\rangle L_BB)_{\omega}$ is the coherent information of state ω_{XL_BB} (32) such that

$$|\omega\rangle_{XL_BBE} = \sum_{x}\sqrt{p_X(x)}|x\rangle_{X}\otimes U_{B'\to BE}^{\mathcal{M}^x}|\psi\rangle_{L_BB'}. \tag{246}$$

Proof. Let $\{x^n(m,k)\}_{m,k}$ denote a codebook for private reading, as discussed in Sec. VI B, and let $\psi_{L_BB'}$ denote a pure state that can be fed into each coherent use of the memory cell. The codebook is such that for each m and k, the codeword $x^n(m,k)$ is unique. The rate of private reading is given by

$$I(X;L_BB)_\rho - I(X;E)_\rho, \tag{247}$$

where

$$\rho_{XB'BE} = \sum_x p_X(x)|x\rangle\langle x|_X \otimes \mathcal{U}^{\mathcal{M}^x}_{B'\to BE}(\psi_{L_BB'}). \tag{248}$$

Note that the following equality holds:

$$I(X;L_BB)_\rho - I(X;E)_\rho = I(X\rangle L_BB)_\omega, \tag{249}$$

where

$$|\omega\rangle_{XL_BBE} = \sum_x \sqrt{p_X(x)}|x\rangle_X \otimes U^{\mathcal{M}^x}_{B'\to BE}|\psi\rangle_{L_BB'}. \tag{250}$$

The code is such that there is a measurement $\Lambda^{m,k}_{L_B^nB^n}$ for all m,k, for which

$$\mathrm{Tr}\left\{\Lambda^{m,k}_{L_B^nB^n}\mathcal{M}^{x^n(m,k)}_{B'^n\to B^n}\left(\psi^{\otimes n}_{L_BB'}\right)\right\} \geqslant 1-\varepsilon, \tag{251}$$

and

$$\frac{1}{2}\left\|\frac{1}{K}\sum_k \widehat{\mathcal{M}}^{x^n(m,k)}_{B'^n\to E^n}\left(\psi^{\otimes n}_{B'}\right) - \sigma_{E^n}\right\|_1 \leqslant \delta. \tag{252}$$

From this private reading code, we construct a coherent reading code as follows. Alice begins by preparing the state

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}. \tag{253}$$

Alice performs a unitary that implements the following isometry:

$$|m\rangle_{M_A}|k\rangle_{K_A} \to |m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}, \tag{254}$$

so that the state above becomes

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}. \tag{255}$$

Bob prepares the state $|\psi\rangle^{\otimes n}_{L_BB'}$, so that the overall state is

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}|\psi\rangle^{\otimes n}_{L_BB'}. \tag{256}$$

Now Alice and Bob are allowed to access n instances of the controlled isometry,

$$\sum_x |x\rangle\langle x|_X \otimes U^{\mathcal{M}^x}_{B'\to BE}, \tag{257}$$

and the state becomes

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n}U^{\mathcal{M}^{x^n(m,k)}}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'}. \tag{258}$$

Bob now performs the isometry

$$\sum_{m,k}\sqrt{\Lambda^{m,k}_{L_B^nB^n}} \otimes |m\rangle_{M_1}|k\rangle_{K_1}, \tag{259}$$

and the resulting state is close to

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}|x^n(m,k)\rangle_{X^n} \otimes U^{x^n(m,k)}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'}|m\rangle_{M_1}|k\rangle_{K_1}. \tag{260}$$

At this point, Alice locally uncomputes the unitary from (254) and discards the X^n register, leaving the following state:

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}|k\rangle_{K_A}U^{\mathcal{M}_A{}^{x^n(m,k)}}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'} \otimes |m\rangle_{M_1}|k\rangle_{K_1}. \tag{261}$$

Following the scheme of Ref. [13] for entanglement distillation, she then performs a Fourier transform on the register K_A and measures it, obtaining an outcome $k' \in \{0,\dots,K-1\}$, leaving the following state:

$$\frac{1}{\sqrt{MK}}\sum_{m,k}e^{2\pi ik'k/K}|m\rangle_{M_A} \otimes U^{\mathcal{M}_A{}^{x^n(m,k)}}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'} \otimes |m\rangle_{M_1}|k\rangle_{K_1}. \tag{262}$$

She communicates the outcome to Bob, who can then perform a local unitary on system K_1 to bring the state to

$$\frac{1}{\sqrt{MK}}\sum_{m,k}|m\rangle_{M_A}U^{\mathcal{M}^{x^n(m,k)}}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'}|m\rangle_{M_1}|k\rangle_{K_1}. \tag{263}$$

Now consider that, conditioned on a value m in register M, the local state of Eve's register E^n is given by

$$\frac{1}{K_A}\sum_k \widehat{\mathcal{M}}^{x^n(m,k)}_{B'^n\to E^n}\left(\psi^{\otimes n}_{B'}\right). \tag{264}$$

Thus, by invoking the security condition in (252) and Uhlmann's theorem [44], there exists a isometry $V^m_{L_B^nB^nK_1\to\widetilde{B}}$ such that

$$V^m_{L_B^nB^nK_1\to\widetilde{B}}\left[\frac{1}{\sqrt{K_A}}\sum_k U^{\mathcal{M}^{x^n(m,k)}}_{B'^n\to B^nE^n}|\psi\rangle^{\otimes n}_{L_BB'}|k\rangle_{K_1}\right] \approx |\varphi^\sigma\rangle_{E^n\widetilde{B}}. \tag{265}$$

Thus, Bob applies the controlled isometry

$$\sum_m |m\rangle\langle m|_{M_1} \otimes V^m_{L_B^nB^nK_1\to\widetilde{B}}, \tag{266}$$

and then the overall state is close to

$$\frac{1}{\sqrt{M}}\sum_m |m\rangle_{M_A}|\varphi^\sigma\rangle_{E^n\widetilde{B}}|m\rangle_{M_1}. \tag{267}$$

Bob now discards the register $\widetilde{B}$ and Alice and Bob are left with a maximally entangled state that is locally equivalent to approximately $n[I(X;L_BB)_\rho - I(X;E)_\rho] = nI(X\rangle L_BB)_\omega$ ebits.

VIII. DISCUSSION

In this work, we mainly focused on two different information-processing tasks: entanglement distillation and secret-key distillation using bipartite quantum interactions or bidirectional channels. We determined several bounds on the entanglement and secret-key-agreement capacities of bipartite quantum interactions. In deriving these bounds, we described communication protocols in the bidirectional setting, related to those discussed in Ref. [4] and which generalize related point-to-point communication protocols. We introduced an entanglement measure called the bidirectional max-Rains information of a bidirectional channel and showed that it is a strong converse upper bound on the PPT-assisted quantum capacity of the given bidirectional channel. We also introduced a related entanglement measure called the bidirectional max-relative entropy of entanglement and showed that it is a strong converse bound on the LOCC-assisted secret-key-agreement capacity of a given bidirectional channel. When the bidirectional channels are either teleportation- or PPT-simulable, the upper bounds on the bidirectional quantum and bidirectional secret-key-agreement capacities depend only on the entanglement of an underlying resource state. If a bidirectional channel is bicovariant, then the underlying resource state can be taken to be the Choi state of the bidirectional channel.

Next, we introduced a private communication task called private reading. This task allows for secret-key agreement between an encoder and a reader in the presence of a passive eavesdropper. Observing that access to an isometric wiretap memory cell by an encoder and the reader is a particular kind of bipartite quantum interaction, we were able to leverage our bounds on the LOCC-assisted bidirectional secret-key-agreement capacity to determine bounds on its private reading capacity. We also determined a regularized expression for the nonadaptive private reading capacity of an arbitrary wiretap memory cell. For particular classes of memory cells obeying certain symmetries, such that there is an adaptive-to-nonadaptive reduction in a reading protocol, as in Ref. [59], the private reading capacity and the nonadaptive private reading capacity are equal. We derived a single-letter, weak converse upper bound on the nonadaptive private reading capacity of an isometric wiretap memory cell in terms of the squashed entanglement. We also proved a strong converse upper bound on the private reading capacity of an isometric wiretap memory cell in terms of the bidirectional max-relative entropy of entanglement. We applied our results to show that the private reading capacity and the reading capacity of the qudit erasure memory cell are equal. Finally, we determined an achievable rate at which entanglement can be generated between two parties who have coherent access to a memory cell.

We have left open the question of determining a relation between the bidirectional max-Rains information and the bidirectional max-relative entropy of entanglement for an arbitrary bidirectional channel. However, we strongly suspect that the bidirectional max-Rains information can never exceed the bidirectional max-relative entropy of entanglement. It would also be interesting to derive an upper bound on the bidirectional secret-key-agreement capacity in terms of the squashed entanglement. Another future direction would be to determine classes of memory cells for which the regularized expressions of the nonadaptive private reading capacities reduce to single-letter expressions. For this, one could consider memory cells consisting of degradable channels [126,127]. More generally, determining the private reading capacity of an arbitrary wiretap memory cell is an important open question.

ACKNOWLEDGMENTS

We thank Koji Azuma, Aram Harrow, Cosmo Lupo, Bill Munro, Mio Murao, and George Siopsis for helpful discussions. S.D. acknowledges support from the LSU Graduate School Economic Development Assistantship and the LSU Coates Conference Travel Award. M.M.W. acknowledges support from the U.S. Office of Naval Research and the National Science Foundation.

APPENDIX A: COVARIANT CHANNEL

Proof of Lemma 1. Given is a group G and a quantum channel $\mathcal{M}_{A\to B}$ that is covariant in the following sense:

$$\mathcal{M}_{A\to B}\big(U_A^g \rho_A U_A^{g\dagger}\big) = V_B^g \mathcal{M}_{A\to B}(\rho_A) V_B^{g\dagger}, \tag{A1}$$

for a set of unitaries $\{U_A^g\}_{g\in G}$ and $\{V_B^g\}_{g\in G}$.

Let a Kraus representation of $\mathcal{M}_{A\to B}$ be given as

$$\mathcal{M}_{A\to B}(\rho_A) = \sum_j L^j \rho_A L^{j\dagger}. \tag{A2}$$

We can rewrite (A1) as

$$V_B^{g\dagger} \mathcal{M}_{A\to B}\big(U_A^g \rho_A U_A^{g\dagger}\big) V_B^g = \mathcal{M}_{A\to B}(\rho_A), \tag{A3}$$

which means that for all g, the following equality holds

$$\sum_j L^j \rho_A L^{j\dagger} = \sum_j V_B^{g\dagger} L^j U_A^g \rho_A \big(V_B^{g\dagger} L^j U_A^g\big)^\dagger. \tag{A4}$$

Thus, the channel has two different Kraus representations $\{L^j\}_j$ and $\{V_B^{g\dagger} L^j U_A^g\}_j$, and these are necessarily related by a unitary with matrix elements w_{jk}^g [94,128]:

$$V_B^{g\dagger} L^j U_A^g = \sum_k w_{jk}^g L^k. \tag{A5}$$

A canonical isometric extension $U_{A\to BE}^{\mathcal{M}}$ of $\mathcal{M}_{A\to B}$ is given as

$$U_{A\to BE}^{\mathcal{M}} = \sum_j L^j \otimes |j\rangle_E, \tag{A6}$$

where $\{|j\rangle_E\}_j$ is an orthonormal basis. Defining W_E^g as the following unitary:

$$W_E^g |k\rangle_E = \sum_j w_{jk}^g |j\rangle_E, \tag{A7}$$

where the states $|k\rangle_E$ are chosen from $\{|j\rangle_E\}_j$, consider that

$$\begin{aligned} U_{A\to BE}^{\mathcal{M}} U_A^g &= \sum_j L^j U_A^g \otimes |j\rangle_E &\text{(A8)}\\ &= \sum_j V_B^g V_B^{g\dagger} L^j U_A^g \otimes |j\rangle_E &\text{(A9)}\\ &= \sum_j V_B^g \left[\sum_k w_{jk}^g L^k\right] \otimes |j\rangle_E &\text{(A10)}\\ &= V_B^g \sum_k L^k \otimes \sum_j w_{jk}^g |j\rangle_E &\text{(A11)} \end{aligned}$$

$$= V_B^g \sum_k L^k \otimes W_E^g |k\rangle_E \tag{A12}$$

$$= \left(V_B^g \otimes W_E^g\right) U_{A\to BE}^{\mathcal{M}}. \tag{A13}$$

This concludes the proof. ∎

APPENDIX B: BICOVARIANT CHANNELS AND TELEPORTATION SIMULATION

Proof of Proposition 3. Let $\mathcal{N}_{A'B'\to AB}$ be a bidirectional quantum channel, and let G and H be groups with unitary representations $g \to \mathcal{U}_{A'}(g)$ and $h \to \mathcal{V}_{B'}(h)$ and $(g,h) \to \mathcal{W}_A(g,h)$ and $(g,h) \to \mathcal{T}_B(g,h)$, such that

$$\frac{1}{|G|}\sum_g \mathcal{U}_{A'}(g)(X_{A'}) = \mathrm{Tr}\{X_{A'}\}\pi_{A'}, \tag{B1}$$

$$\frac{1}{|H|}\sum_h \mathcal{V}_{B'}(h)(Y_{B'}) = \mathrm{Tr}\{Y_{B'}\}\pi_{B'}, \tag{B2}$$

and

$$\mathcal{N}_{A'B'\to AB}\{[\mathcal{U}_{A'}(g)\otimes\mathcal{V}_{B'}(h)](\rho_{A'B'})\} = [\mathcal{W}_A(g,h)\otimes\mathcal{T}_B(g,h)][\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})], \tag{B3}$$

where $X_{A'} \in \mathcal{B}(\mathcal{H}_{A'})$, $Y_{B'} \in \mathcal{B}(\mathcal{H}_{B'})$, and π denotes the maximally mixed state. Consider that

$$\frac{1}{|G|}\sum_g \mathcal{U}_{A''}(g)(\Phi_{A''A'}) = \pi_{A''}\otimes\pi_{A'}, \tag{B4}$$

where Φ denotes a maximally entangled state and A'' is a system isomorphic to A'. Similarly,

$$\frac{1}{|H|}\sum_h \mathcal{V}_{B''}(h)(\Phi_{B''B'}) = \pi_{B''}\otimes\pi_{B'}. \tag{B5}$$

Note that in order for $\{U_{A'}^g\}$ to satisfy (B1), it is necessary that $|A'|^2 \leqslant |G|$ [129]. Similarly, it is necessary that $|B'|^2 \leqslant |H|$. Consider the POVM $\{E_{A''L_A}^g\}_g$, with each element $E_{A''L_A}^g$ defined as

$$E_{A''L_A}^g := \frac{|A'|^2}{|G|} U_{A''}^g \Phi_{A''L_A}\left(U_{A''}^g\right)^\dagger. \tag{B6}$$

It follows from the fact that $|A'|^2 \leqslant |G|$ and (B4) that $\{E_{A''L_A}^g\}_g$ is a valid POVM. Similarly, we define the POVM $\{F_{B''L_B}^h\}_h$ as

$$F_{B''L_B}^h := \frac{|B'|^2}{|H|} V_{B''}^h \Phi_{B''L_B}\left(V_{B''}^h\right)^\dagger. \tag{B7}$$

The simulation of the channel $\mathcal{N}_{A'B'\to AB}$ via teleportation begins with a state $\rho_{A''B''}$ and a shared resource $\theta_{L_AABL_B} = \mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'}\otimes\Phi_{B'L_B})$. The desired outcome is for the receivers to receive the state $\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})$ and for the protocol to work independently of the input state $\rho_{A'B'}$. The first step is for the senders to locally perform the measurement $\{E_{A''L_A}^g \otimes F_{B''L_B}^h\}_{g,h}$ and then send the outcomes g and h to the receivers. Based on the outcomes g and h, the receivers then perform $W_A^{g,h}$ and $T_B^{g,h}$. The following analysis demonstrates that this protocol works, by simplifying the form of the postmeasurement state:

$$
\begin{aligned}
&|G||H|\,\mathrm{Tr}_{A''L_AB''L_B}\left\{\left(E_{A''L_A}^g\otimes F_{B''L_B}^h\right)\left(\rho_{A''B''}\otimes\theta_{L_AABL_B}\right)\right\}\\
&= |A'|^2|B'|^2\,\mathrm{Tr}_{A''L_AB''L_B}\left\{\left[U_{A''}^g\Phi_{A''L_A}\left(U_{A''}^g\right)^\dagger\otimes V_{B''}^h\Phi_{B''L_B}\left(V_{B''}^h\right)^\dagger\right]\left(\rho_{A''B''}\otimes\theta_{L_AABL_B}\right)\right\} &\text{(B8)}\\
&= |A'|^2|B'|^2\langle\Phi|_{A''L_A}\otimes\langle\Phi|_{B''L_B}\left(U_{A''}^g\otimes V_{B''}^h\right)^\dagger\left(\rho_{A''B''}\otimes\theta_{L_AABL_B}\right)\left(U_{A''}^g\otimes V_{B''}^h\right)|\Phi\rangle_{A''L_A}\otimes|\Phi\rangle_{B''L_B} &\text{(B9)}\\
&= |A'|^2|B'|^2\langle\Phi|_{A''L_A}\otimes\langle\Phi|_{B''L_B}\left[\left(U_{A''}^g\otimes V_{B''}^h\right)^\dagger\rho_{A''B''}\left(U_{A''}^g\otimes V_{B''}^h\right)\right]\\
&\quad\otimes\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'}\otimes\Phi_{B'L_B})|\Phi\rangle_{A''L_A}\otimes|\Phi\rangle_{B''L_B} &\text{(B10)}\\
&= |A'|^2|B'|^2\langle\Phi|_{A''L_A}\otimes\langle\Phi|_{B''L_B}\left[\left(U_{L_A}^g\otimes V_{L_B}^h\right)^\dagger\rho_{L_AL_B}\left(U_{L_A}^g\otimes V_{L_B}^h\right)\right]^*\\
&\quad\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'}\otimes\Phi_{B'L_B})|\Phi\rangle_{A''L_A}\otimes|\Phi\rangle_{B''L_B}. &\text{(B11)}
\end{aligned}
$$

The first three equalities follow by substitution and some rewriting. The fourth equality follows from the fact that

$$\langle\Phi|_{A'A}M_{A'} = \langle\Phi|_{A'A}M_A^* \tag{B12}$$

for any operator M and where $*$ denotes the complex conjugate, taken with respect to the basis in which $|\Phi\rangle_{A'A}$ is defined. Continuing, we have that

$$
\begin{aligned}
\text{Eq. (B11)} &= |A'||B'|\,\mathrm{Tr}_{L_AL_B}\left\{\left[\left(U_{L_A}^g\otimes V_{L_B}^h\right)^\dagger\rho_{L_AL_B}\left(U_{L_A}^g\otimes V_{L_B}^h\right)\right]^*\mathcal{N}_{A'B'\to AB}(\Phi_{L_AA'}\otimes\Phi_{B'L_B})\right\} &\text{(B13)}\\
&= |A'||B'|\,\mathrm{Tr}_{L_AL_B}\left(\mathcal{N}_{A'B'\to AB}\left\{\left[\left(U_{A'}^g\otimes V_{B'}^h\right)^\dagger\rho_{A'B'}\left(U_{A'}^g\otimes V_{B'}^h\right)\right]^\dagger\left(\Phi_{L_AA'}\otimes\Phi_{B'L_B}\right)\right\}\right) &\text{(B14)}\\
&= \mathcal{N}_{A'B'\to AB}\left\{\left[\left(U_{A'}^g\otimes V_{B'}^h\right)^\dagger\rho_{A'B'}\left(U_{A'}^g\otimes V_{B'}^h\right)\right]^\dagger\right\} &\text{(B15)}\\
&= \mathcal{N}_{A'B'\to AB}\left[\left(U_{A'}^g\otimes V_{B'}^h\right)^\dagger\rho_{A'B'}\left(U_{A'}^g\otimes V_{B'}^h\right)\right] &\text{(B16)}\\
&= \left(W_A^{g,h}\otimes T_B^{g,h}\right)^\dagger\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})\left(W_A^{g,h}\otimes T_B^{g,h}\right). &\text{(B17)}
\end{aligned}
$$

The first equality follows because $|A|\langle\Phi|_{A'A}(I_{A'}\otimes M_{AB})|\Phi\rangle_{A'A}=\mathrm{Tr}_A\{M_{AB}\}$ for any operator M_{AB}. The second equality follows by applying the conjugate transpose of (B12). The final equality follows from the covariance property of the channel.

Thus, if the receivers finally perform the unitaries $W_A^{g,h}\otimes T_B^{g,h}$ upon receiving g and h via a classical channel from the senders, then the output of the protocol is $\mathcal{N}_{A'B'\to AB}(\rho_{A'B'})$, so that this protocol simulates the action of the channel $\mathcal{N}$ on the state ρ. ■

APPENDIX C: QUDIT SYSTEM AND HEISENBERG-WEYL GROUP

Here we introduce some basic notations and definitions related to qudit systems. A system represented with a d-dimensional Hilbert space is called a *qudit* system. Let $J_{B'}=\{|j\rangle_{B'}\}_{j\in\{0,\dots,d-1\}}$ be a computational orthonormal basis of $\mathcal{H}_{B'}$ such that $\dim(\mathcal{H}_{B'})=d$. There exists a unitary operator called *cyclic shift operator* $X(k)$ that acts on the orthonormal states as follows:

$$\forall|j\rangle_{B'}\in J_{B'}:\ X(k)|j\rangle=|k\oplus j\rangle, \tag{C1}$$

where $\oplus$ is a cyclic addition operator, i.e., $k\oplus j:=(k+j)\bmod d$. There also exists another unitary operator called the *phase operator* $Z(l)$ that acts on the qudit computational basis states as

$$\forall|j\rangle_{B'}\in J_{B'}:\ Z(l)|j\rangle=\exp\left(\frac{\iota 2\pi l j}{d}\right)|j\rangle. \tag{C2}$$

The d^2 operators $\{X(k)Z(l)\}_{k,l\in\{0,\dots,d-1\}}$ are known as the Heisenberg-Weyl operators. Let $\sigma(k,l):=X(k)Z(l)$. The maximally entangled state $\Phi_{R:B'}$ of qudit systems RB' is given as $|\Phi\rangle_{RB'}:=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_R|j\rangle_{B'}$, and we define $|\Phi^{k,l}\rangle_{RB'}:=(I_R\otimes\sigma_{B'}^{k,l})|\Phi\rangle_{R:B'}$. The d^2 states $\{|\Phi^{k,l}\rangle_{RB'}\}_{k,l\in\{0,\dots,d-1\}}$ form a complete, orthonormal basis:

$$\langle\Phi^{k_1,l_1}|\Phi^{k_2,l_2}\rangle=\delta_{k_1,k_2}\delta_{l_1,l_2}, \tag{C3}$$

$$\sum_{k,l=0}^{d-1}|\Phi^{k,l}\rangle\langle\Phi^{k,l}|_{RB'}=I_{RB'}. \tag{C4}$$

Let $\mathcal{W}$ be a discrete set such that $|\mathcal{W}|=d^2$. There exists one-to-one mapping $\{(k,l)\}_{k,l\in\{0,d-1\}}\leftrightarrow\{w\}_{w\in\mathcal{W}}$. For example, we can use the following map: $w=k+d\cdot l$ for $\mathcal{W}=\{0,\dots,d^2-1\}$. This allows us to define $\sigma^w:=\sigma(k,l)$ and $\Phi^w_{RB'}:=\Phi^{k,l}_{RB'}$. Let the set of d^2 Heisenberg-Weyl operators be denoted as

$$\mathbf{H}:=\{\sigma^w\}_{w\in\mathcal{W}}=\{X(k)Z(l)\}_{k,l\in\{0,\dots,d-1\}}, \tag{C5}$$

and we refer to $\mathbf{H}$ as the Heisenberg-Weyl group.

[1] P. A. M. Dirac, *The Principles of Quantum Mechanics,* 4th ed., International Series of Monographs on Physics Vol. 27 (Clarendon Press, Oxford, 1981).

[2] J. J. Sakurai, *Modern Quantum Mechanics*, revised ed. (Addison Wesley, Boston, 1993)

[3] W. F. Stinespring, Positive functions on C*-algebras, Proc. Am. Math. Soc. **6**, 211 (1955).

[4] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, On the capacities of bipartite Hamiltonians and unitary gates, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[5] M. B. Plenio and S. S. Virmani, An introduction to entanglement theory, *Quantum Information and Coherence* (Springer, Cham, 2014), pp. 173–209.

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[7] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935).

[8] E. Schrödinger, Discussion of probability relations between separated systems, Math. Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[9] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

[10] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation Via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[11] E. M. Rains, Bound on distillable entanglement, Phys. Rev. A **60**, 179 (1999).

[12] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, IEEE Trans. Inf. Theory **51**, 44 (2005).

[13] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. London A **461**, 207 (2005).

[14] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[15] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, General paradigm for distilling classical key from quantum states, IEEE Trans. Inf. Theory **55**, 1898 (2009).

[16] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State Via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **70**, 1895 (1993).

[17] C. H. Bennett and S. J. Wiesner, Communication Via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett. **69**, 2881 (1992).

[18] C. E. Shannon, Two-way communication channels, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics* (University of California Press, Berkeley, 1961), pp. 611–644.

[19] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa, Conditional Quantum Dynamics and Logic Gates, Phys. Rev. Lett. **74**, 4083 (1995).

[20] P. Zanardi, C. Zalka, and L. Faoro, Entangling power of quantum evolutions, Phys. Rev. A **62**, 030301(R) (2000).

[21] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Optimal local implementation of nonlocal quantum gates, Phys. Rev. A **62**, 052317 (2000).

[22] S. Bose, L. Rallan, and V. Vedral, Communication Capacity of Quantum Computation, Phys. Rev. Lett. **85**, 5448 (2000).

[23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[24] D. Collins, N. Linden, and S. Popescu, Nonlocal content of quantum operations, Phys. Rev. A **64**, 032302 (2001).

[25] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Entangling Operations and their Implementation Using a Small Amount of Entanglement, Phys. Rev. Lett. **86**, 544 (2001).

[26] A. M. Childs, D. W. Leung, and G. Vidal, Reversible simulation of bipartite product Hamiltonians, IEEE Trans. Inf. Theory **50**, 1189 (2004).

[27] B. Jonnadula, P. Mandayam, K. Życzkowski, and A. Lakshminarayan, Impact of local dynamics on entangling power, Phys. Rev. A **95**, 040302(R) (2017).

[28] S. Das, G. Siopsis, and C. Weedbrook, Continuous-variable quantum Gaussian process regression and quantum singular value decomposition of non-sparse low rank matrices, Phys. Rev. A **97**, 022315 (2018).

[29] Y. Sekino and L. Susskind, Fast scramblers, J. High Energy Phys. 10 (2008) 065.

[30] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, Chaos in quantum channels, J. High Energy Phys. 02 (2016) 004.

[31] D. Ding, P. Hayden, and M. Walter, Conditional mutual information of bipartite unitaries and scrambling, J. High Energy Phys. 12 (2016) 145.

[32] P. Hayden and J. Preskill, Black holes as mirrors: Quantum information in random subsystems, J. High Energy Phys. 09 (2007) 120.

[33] S. W. Hawking, Breakdown of predictability in gravitational collapse, Phys. Rev. D **14**, 2460 (1976).

[34] A. M. Childs, D. W. Leung, and H.-K. Lo, Two-way quantum communication channels, Int. J. Quantum. Inform. **04**, 63 (2006).

[35] S. Bravyi, Upper bounds on entangling rates of bipartite Hamiltonians, Phys. Rev. A **76**, 052319 (2007).

[36] S. Das, S. Khatri, G. Siopsis, and M. M. Wilde, Fundamental limits on quantum dynamics based on entropy change, J. Math. Phys. **59**, 012205 (2018).

[37] M. S. Leifer, L. Henderson, and N. Linden, Optimal entanglement generation from quantum operations, Phys. Rev. A **67**, 012306 (2003).

[38] A. W. Harrow and D. W. Leung, Bidirectional coherent classical communication, Quantum Inf. Comput. **5**, 380 (2005), arXiv:quant-ph/0412126.

[39] N. Linden, J. A. Smolin, and A. Winter, Entangling and Disentangling Power of Unitary Transformations are Not Equal, Phys. Rev. Lett. **103**, 030501 (2009).

[40] E. Wakakuwa, A. Soeda, and M. Murao, A coding theorem for bipartite unitaries in distributed quantum computation, IEEE Trans. Inf. Theory **63**, 5372 (2017).

[41] L. Chen and L. Yu, Entangling and assisted entangling power of bipartite unitary operations, Phys. Rev. A **94**, 022307 (2016).

[42] S. Pirandola, Quantum Reading of a Classical Digital Memory, Phys. Rev. Lett. **106**, 090504 (2011).

[43] S. Bäuml, S. Das, and M. M. Wilde, Fundamental Limits on the Capacities of Bipartite Quantum Interactions, Phys. Rev. Lett. **121**, 250504 (2018).

[44] A. Uhlmann, The "transition probability" in the state space of a *-algebra, Rep. Math. Phys. **9**, 273 (1976).

[45] G. T. Horowitz and J. Maldacena, The black hole final state, J. High Energy Phys. 02 (2004) 008.

[46] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996).

[47] A. Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[48] K. Audenaert, B. De Moor, K. G. H. Vollbrecht, and R. F. Werner, Asymptotic relative entropy of entanglement for orthogonally invariant states, Phys. Rev. A **66**, 032310 (2002).

[49] E. M. Rains, A semidefinite program for distillable entanglement, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[50] E. Chitambar, J. I. de Vicente, M. W. Girard, and G. Gour, Entanglement manipulation and distillability beyond LOCC (2017).

[51] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, Everything you always wanted to know about LOCC (but were afraid to ask), Commun. Math. Phys. **328**, 303 (2014).

[52] A. S. Holevo, Remarks on the classical capacity of quantum channel, arXiv:quant-ph/0212025.

[53] A. S. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction*, Vol. 16 (Walter de Gruyter, Berlin, 2012).

[54] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[55] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, Phys. Rev. A **60**, 1888 (1999).

[56] R. F. Werner, All teleportation and dense coding schemes, J. Phys. A **34**, 7081 (2001).

[57] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Realization schemes for quantum instruments in finite dimensions, J. Math. Phys. **50**, 042101 (2009).

[58] E. Kaur and M. M. Wilde, Amortized entanglement of a quantum channel and approximately teleportation-simulable channels, J. Phys. A **51**, 035303 (2017).

[59] S. Das and M. M. Wilde, Quantum reading capacity: General definition and bounds, IEEE Trans. Inf. Theory **65**, 7566 (2019).

[60] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Verlag von Julius Springer, Berlin, 1932).

[61] B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, Phys. Rev. A **54**, 2629 (1996).

[62] H. Umegaki, Conditional expectations in an operator algebra, IV (entropy and information), Kodai Math. Sem. Rep. **14**, 59 (1962).

[63] A. Mueller-Hermes and D. Reeb, Monotonicity of the quantum relative entropy under positive maps, Ann. Henri Poincaré **18**, 1777 (2017).

[64] G. Lindblad, Completely positive maps and entropy inequalities, Commun. Math. Phys. **40**, 147 (1975).
[65] E. H. Lieb and M. B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy, J. Math. Phys. **14**, 1938 (1973).
[66] E. H. Lieb and M. B. Ruskai, A Fundamental Property of Quantum-Mechanical Entropy, Phys. Rev. Lett. **30**, 434 (1973).
[67] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A **37**, L55 (2004).
[68] A. Winter, Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints, Commun. Math. Phys. **347**, 291 (2016).
[69] Y. Polyanskiy and S. Verdú, Arimoto channel coding converse and Rényi divergence, in *Proceedings of the 48th Annual Allerton Conference on Communication, Control, and Computation, Allerton, IL, USA* (IEEE, Piscataway, NJ, 2010), pp. 1327–1333.
[70] N. Sharma and N. A. Warsi, On the strong converses for the quantum channel capacity theorems, arXiv:1205.1712.
[71] M. M. Wilde, A. Winter, and D. Yang, Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy, Commun. Math. Phys. **331**, 593 (2014).
[72] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, On quantum Rényi entropies: A new definition and some properties, J. Math. Phys. **54**, 122203 (2013).
[73] R. L. Frank and E. H. Lieb, Monotonicity of a relative Rényi entropy, J. Math. Phys. **54**, 122201 (2013).
[74] M. M. Wilde, Optimized quantum f-divergences and data processing, J. Phys. A **51**, 374002 (2018).
[75] S. Beigi, Sandwiched Rényi divergence satisfies data processing inequality, J. Math. Phys. **54**, 122202 (2013).
[76] N. Datta, Min- and max-relative entropies and a new entanglement monotone, IEEE Trans. Inf. Theory **55**, 2816 (2009).
[77] N. Datta, Max-relative entropy of entanglement, alias log robustness, Int. J. Quantum. Inform. **7**, 475 (2009).
[78] F. Buscemi and N. Datta, The quantum capacity of channels with arbitrarily correlated noise, IEEE Trans. Inf. Theory **56**, 1447 (2010).
[79] L. Wang and R. Renner, One-Shot Classical-Quantum Capacity and Hypothesis Testing, Phys. Rev. Lett. **108**, 200501 (2012).
[80] M. Christandl and A. Müller-Hermes, Relative entropy bounds on quantum, private and repeater capacities, Commun. Math. Phys. **353**, 821 (2017).
[81] K. Ben Dana, M. García Díaz, M. Mejatty, and A. Winter, Resource theory of coherence: Beyond states, Phys. Rev. A **95**, 062327 (2017).
[82] L. Rigovacca, G. Kato, S. Bäuml, M. Kim, W. J. Munro, and K. Azuma, Versatile relative entropy bounds for quantum networks, New J. Phys. **20**, 013033 (2018).
[83] M. Tomamichel, M. M. Wilde, and A. Winter, Strong converse rates for quantum communication, IEEE Trans. Inf. Theory **63**, 715 (2017).
[84] X. Wang and R. Duan, A semidefinite programming upper bound of quantum capacity, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, New York, 2016).
[85] X. Wang, K. Fang, and R. Duan, Semidefinite programming converse bounds for quantum communication, IEEE Trans. Inf. Theory **65**, 2583 (2019).
[86] M. Berta and M. M. Wilde, Amortization does not enhance the max-Rains information of a quantum channel, New J. Phys. **20**, 053044 (2018).
[87] X. Wang and R. Duan, Improved semidefinite programming upper bound on distillable entanglement, Phys. Rev. A **94**, 050301(R) (2016).
[88] M. M. Wilde, M. Tomamichel, and M. Berta, Converse bounds for private communication over quantum channels, IEEE Trans. Inf. Theory **63**, 1792 (2017).
[89] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, Phys. Rev. A **57**, 1619 (1998).
[90] M. Christandl and A. Winter, "Squashed entanglement": An additive entanglement measure, J. Math. Phys. **45**, 829 (2004).
[91] R. R. Tucci, Quantum entanglement and conditional information transmission, arXiv:quant-ph/9909041.
[92] R. R. Tucci, Entanglement of distillation and conditional mutual information, arXiv:quant-ph/0202144.
[93] M. Takeoka, S. Guha, and M. M. Wilde, The squashed entanglement of a quantum channel, IEEE Trans. Inf. Theory **60**, 4987 (2014).
[94] J. Watrous, Theory of Quantum Information, https://cs.uwaterloo.ca/~watrous/TQI/ (2015).
[95] R. Bhatia, *Matrix Analysis* (Springer, New York, 1997).
[96] G. M. D'Ariano and P. Perinotti, Programmable quantum channels and measurements, arXiv:quant-ph/0510033.
[97] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, Parameter estimation of quantum channels, IEEE Trans. Inf. Theory **54**, 5172 (2008).
[98] R. Demkowicz-Dobrzański and L. Maccone, Using Entanglement Against Noise in Quantum Metrology, Phys. Rev. Lett. **113**, 250801 (2014).
[99] T. Fritz, Resource convertibility and ordered commutative monoids, Math. Struct. Comput. Sci. **27**, 850 (2015).
[100] F. G. S. L. Brandão and G. Gour, Reversible Framework for Quantum Resource Theories, Phys. Rev. Lett. **115**, 070503 (2015).
[101] A. Soeda, P. S. Turner, and M. Murao, Entanglement Cost of Implementing Controlled-Unitary Operations, Phys. Rev. Lett. **107**, 180501 (2011).
[102] D. Gottesman, The Heisenberg Representation of Quantum Computers, in *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
[103] D. Gottesman and I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature (London) **402**, 390 (1999).
[104] M. A. Nielsen and I. L. Chuang, Programmable Quantum Gate Arrays, Phys. Rev. Lett. **79**, 321 (1997).
[105] W. Dür, M. J. Bremner, and H. J. Briegel, Quantum simulation of interacting high-dimensional systems: The influence of noise, Phys. Rev. A **78**, 052325 (2008).
[106] T. Cooney, M. Mosonyi, and M. M. Wilde, Strong converse exponents for a quantum channel discrimination problem and

quantum-feedback-assisted communication, Commun. Math. Phys. **344**, 797 (2016).

[107] One could also set $\alpha = 1 + 1/\sqrt{n}$ and then take the limit $n \to \infty$.

[108] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, Quantum reading capacity, New J. Phys. **13**, 113012 (2011).

[109] C. Lupo and S. Pirandola, Super-additivity and entanglement assistance in quantum reading, Quantum Inf. Comput. **17**, 611 (2017).

[110] A. Kitaev, Quantum computations: Algorithms and error correction, Russ. Math. Surv. **52**, 1191 (1997).

[111] A. Fujiwara, Quantum channel identification problem, Phys. Rev. A **63**, 042304 (2001).

[112] G. M. D'Ariano, P. L. Presti, and M. G. A. Paris, Using Entanglement Improves the Precision of Quantum Measurements, Phys. Rev. Lett. **87**, 270404 (2001).

[113] A. Acin, Statistical Distinguishability Between Unitary Operations, Phys. Rev. Lett. **87**, 177901 (2001).

[114] G. Wang and M. Ying, Unambiguous discrimination among quantum operations, Phys. Rev. A **73**, 042301 (2006).

[115] R. Duan, Y. Feng, and M. Ying, Perfect Distinguishability of Quantum Operations, Phys. Rev. Lett. **103**, 210501 (2009).

[116] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, Adaptive versus nonadaptive strategies for quantum channel discrimination, Phys. Rev. A **81**, 032339 (2010).

[117] R. Duan, C. Guo, C.-K. Li, and Y. Li, Parallel distinguishability of quantum operations, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, NJ, 2016), pp. 2259–2263.

[118] S. Guha, Z. Dutton, R. Nair, J. Shapiro, and B. Yen, Information capacity of quantum reading, in *Laser Science* (Optical Society of America, Washington DC, 2011), p. LTuF2.

[119] S. Guha and M. M. Wilde, Polar coding to achieve the Holevo capacity of a pure-loss optical channel, in *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)* (IEEE, Piscataway, NJ, 2012), pp. 546–550.

[120] M. M. Wilde, S. Guha, S.-H. Tan, and S. Lloyd, Explicit capacity-achieving receivers for optical communication and quantum reading, in *2012 IEEE International Symposium on Information Theory Proceedings (ISIT)* (IEEE, Piscataway, NJ, 2012), pp. 551–555.

[121] G. Spedalieri, Cryptographic aspects of quantum reading, Entropy **17**, 2218 (2015).

[122] R. M. Fano, Fano inequality, Scholarpedia **3**, 6648 (2008).

[123] M. M. Wilde, Squashed entanglement and approximate private states, Quant. Info. Proc. **15**, 4563 (2016).

[124] Such a bound might be called a "pretty strong converse," in the sense of Ref. [130]. However, we could have alternatively defined a private reading protocol to have a single parameter characterizing reliability and security, as in Ref. [88], and with such a definition, we would get a true strong converse.

[125] M. Grassl, T. Beth, and T. Pellizzari, Codes for the quantum erasure channel, Phys. Rev. A **56**, 33 (1997).

[126] I. Devetak and P. W. Shor, The capacity of a quantum channel for simultaneous transmission of classical and quantum information, Commun. Math. Phys. **256**, 287 (2005).

[127] G. Smith, Private classical capacity with a symmetric side channel and its application to quantum cryptography, Phys. Rev. A **78**, 022306 (2008).

[128] M. M. Wilde, *Quantum Information Theory,* 2nd ed. (Cambridge University Press, Cambridge, 2017).

[129] A. Ambainis, M. Mosca, A. Tapp, and R. Wolf, Private quantum channels, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Piscataway, NJ, 2000), pp. 547–553.

[130] C. Morgan and A. Winter, "Pretty strong" converse for the quantum capacity of degradable channels, IEEE Trans. Inf. Theory **60**, 317 (2014).