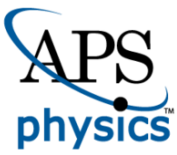

Fundamental Limits on the Capacities of Bipartite Quantum Interactions

Stefan Bäuml, Siddhartha Das, and Mark M. Wilde

Phys. Rev. Lett. **121**, 250504 — Published 19 December 2018

DOI: 10.1103/PhysRevLett.121.250504

Fundamental limits on the capacities of bipartite quantum interactions

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

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[2]*NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands*
[4]*Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA*
[5]*Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

(Dated: October 24, 2018)

Bipartite quantum interactions have applications in a number of different areas of quantum physics, reaching from fundamental areas such as quantum thermodynamics and the theory of quantum measurements to other applications such as quantum computers, quantum key distribution, and other information processing protocols. A particular aspect of the study of bipartite interactions is concerned with the entanglement that can be created from such interactions. In this paper, we present our work on two basic building blocks of bipartite quantum protocols, namely, the generation of maximally entangled states and secret key via bipartite quantum interactions. In particular, we provide a non-trivial, efficiently computable upper bound on the positive-partial-transpose-assisted (PPT-assisted) quantum capacity of a bipartite quantum interaction. In addition, we provide an upper bound on the secret-key-agreement capacity of a bipartite quantum interaction assisted by local operations and classical communication (LOCC). As an application, we introduce a cryptographic protocol for the read-out of a digital memory device that is secure against a passive eavesdropper.

Introduction—Bipartite quantum interactions are a fundamental feature in numerous areas of quantum physics. Any interaction described by a Hamiltonian of an otherwise closed quantum system with a heat bath realizes a bipartite unitary operation that acts on the quantum system and the bath collectively (cf. [1]). Similarly, any noisy evolution or measurement of a quantum system can be described in terms of a bipartite unitary operation acting on the system, as well as an environment or measurement probe system [2, 3]. Quantum computation, error correction, and many more information-theoretical applications of quantum physics rely on bipartite unitary quantum operations known as bipartite quantum gates. Examples include the swap gate, the controlled-NOT (CNOT) gate, or the controlled phase gate [4].

Going beyond unitary bipartite interactions, one can consider noisy interactions between two quantum systems held by separate parties, Alice and Bob, which can be described by a tripartite unitary operation acting on the two quantum systems as well as an uncorrelated environment, or by a completely positive, trace-preserving map, a bidirectional quantum channel [5], acting only on Alice and Bob's systems. Examples of such bidirectional quantum channels are noisy bipartite quantum gates [6], which occur in every realistic implementation of quantum computing, quantum error correction, interactions of two separate quantum systems with a heat bath [1], or joint measurements of two quantum systems, as are performed in teleportation or entanglement swapping [7, 8].

Depending on the kind of bipartite interaction and the input states, entanglement can be created, destroyed, or changed by the interaction [9–11]. Whereas the environment is assumed to be inaccessible to Alice and Bob, it does play a crucial role whenever Alice and Bob are performing bipartite operations in a cryptographic protocol, such as secret key agreement [12–15]. In such a case, it has to be assumed that the eavesdropper can access part of or even the entire environment system.

In this work, we analyse bipartite interactions in terms of their abilities to create entanglement, as well as secret key. In particular, we focus on determining bounds on the non-asymptotic quantum and private capacities of bipartite interactions, i.e., the maximum rates at which maximally entangled states or bits of secret key, respectively, can be distilled when a finite number of interactions are allowed. Previous results in this direction include [5, 16, 17], which introduce capacities for classical and quantum communication via bipartite unitary and non-unitary interactions, respectively, as well as a number of results on the entanglement generating capacities or the entangling power of bipartite unitary interactions [5, 18–23].

What has been an open question since [5] is whether there exists a non-trivial, efficiently computable upper bound on the entanglement generating capacity of a bipartite quantum interaction. The difficulty in addressing this question is that the protocols for entanglement generation are allowed to use local quantum systems of arbitrarily large dimension, and it might not be clear *a priori* whether such bounds would be possible. Another question left open from prior work is that of considering private communication in the bidirectional context, that is, characterizing the rate at which secret key bits can be distilled by Alice and Bob via a bidirectional channel.

In this paper, we answer the aforementioned questions affirmatively, and our bounds thus serve as benchmarks for assessing the entanglement and secret key agreement capabilities of bipartite interactions. To begin with, we determine an efficiently computable upper bound on the entanglement generating capacity of a bipartite quantum interaction. As examples, we compute this bound for the partial swap operation [24], which is related to how photons interact at a beamsplit-

ter, as well as for the swap gate concatenated with collective dephasing [25], which is a kind of bipartite interaction that can occur in a quantum computer. Next, we introduce the secret-key-agreement capacity of a bipartite quantum interaction and provide a general upper bound on it, based on the max-relative entropy of entanglement [26, 27]. Our upper bounds on the quantum and private capacities involve an optimization over bounded quantum systems having a fixed dimension.

As another contribution, we introduce a cryptographic protocol, which we call private reading, for the read-out of a digital read-only memory device secure against a passive eavesdropper. The protocol of private reading is related to quantum reading [16, 28], in which a classical message is sent to a reader, after being stored in a read-only memory device. Physically, the device contains codewords that are sequences of quantum channels, which are chosen from a memory cell (a collection of quantum channels). The information is stored in the choice of channels, and the reader can retrieve the message by using a quantum state to distinguish the channels. In private quantum reading, the message is assumed to be secret, and the reader has to retrieve it in the presence of an eavesdropper. We determine upper bounds on the performance of any private reading protocol by leveraging the fact that reading digital information stored in a memory device can be understood as a specific kind of bipartite quantum interaction.

Bounds on Quantum and Private Capacities—Let us begin our discussion of entanglement and secret key distillation via bipartite interactions by defining the relevant entanglement measures and capacities. Let A', L_A, and A denote quantum systems held locally by Alice, and let B', L_B, and B denote those held by Bob. Given a bidirectional channel $\mathcal{N}_{A'B'\to AB}$, a completely positive, trace-preserving map from quantum systems $A'B'$ to AB, we define the *bidirectional max-Rains information* of $\mathcal{N}$ as $R_{\max}^{2\to 2}(\mathcal{N}) := \log \Gamma^{2\to 2}(\mathcal{N})$, where $\Gamma^{2\to 2}(\mathcal{N})$ is the solution to the following semi-definite program (SDP):

$$\begin{aligned} &\text{minimize} \quad \| \operatorname{Tr}_{AB}\{V_{L_AABL_B} + Y_{L_AABL_B}\}\|_\infty \\ &\text{subject to} \quad V_{L_AABL_B}, Y_{L_AABL_B} \geq 0, \\ &\qquad \operatorname{T}_{BL_B}(V_{L_AABL_B} - Y_{L_AABL_B}) \geq J^{\mathcal{N}}_{L_AABL_B}, \end{aligned} \tag{1}$$

such that $L_A \simeq A'$, and $L_B \simeq B'$. The notation $V_{L_AABL_A}, Y_{L_AABL_B} \geq 0$ means that $V_{L_AABL_A}$ and $Y_{L_AABL_B}$ are constrained to be positive semidefinite operators acting on the Hilbert space of the composite quantum system L_AABL_B. Furthermore, the notation $L_A \simeq A'$ means that quantum system L_A is isomorphic to system A', which in this case simply means that these systems have the same dimension. Here T_X denotes the partial transposition with respect to subsystem X and $J^{\mathcal{N}} := \mathcal{N}_{A'B'\to AB}(|\Upsilon\rangle\langle\Upsilon|_{L_AL_B:A'B'})$ is the Choi operator of $\mathcal{N}$, with $|\Upsilon\rangle_{L_AL_B:A'B'} := \sum_{ij} |ij\rangle_{L_AL_B}|ij\rangle_{A'B'}$. The SDP is a generalization of the SDP formulation of the max-Rains information of a point-to-point channel [29]. Whereas $R_{\max}^{2\to 2}$ is sufficient to bound entanglement distillation rates, the existence of positive-partial-transpose (PPT) entanglement useful for quantum key distribution [14, 15] motivates the introduction of a second measure of entanglement, the *bidirectional max-relative entropy of entanglement*:

$$E_{\max}^{2\to 2}(\mathcal{N}) := \sup_{\psi_{L_AA'}\otimes\varphi_{B'L_B}} E_{\max}(L_AA; BL_B)_{\mathcal{N}(\psi\otimes\varphi)}, \tag{2}$$

where $\psi_{L_AA'} \otimes \varphi_{B'L_B}$ is a pure product state such that $L_A \simeq A'$, and $L_B \simeq B'$ and $E_{\max}(A;B)_\rho := \inf\{\lambda : \rho_{AB} \leq 2^\lambda \sigma_{AB}, \sigma_{AB} \in \operatorname{SEP}(A:B)\}$ denotes the max-relative entropy of entanglement of a state ρ_{AB} [26, 27], with $\operatorname{SEP}(A:B)$ denoting the set of all separable states of the bipartite system AB.

Let us formalize what we mean by entanglement and secret key distillation via a bipartite interaction [30], as depicted in Figure 1. Given a bidirectional channel $\mathcal{N}_{A'B'\to AB}$, we consider entanglement (or key) distillation protocols as follows: an initial PPT-preserving (or LOCC) channel between Alice and Bob creates a state $\rho^{(1)}_{L_{A_1}A_1':B_1'L_{B_1}}$, where subsystems $L_{A_1}A_1'$ and $B_1'L_{B_1}$ are held by Alice and Bob, respectively. Note that a bipartite channel $\mathcal{P}_{A'B'\to AB}$ is PPT-preserving if $\operatorname{T}_B \circ \mathcal{P}_{A'B'\to AB} \circ \operatorname{T}_{B'}$ is a channel [31, 32]. Furthermore, a bipartite channel is PPT-preserving if and only if its Choi operator is a PPT state [32]. An LOCC channel is a particular example of a PPT-preserving channel [31, 32]. The dimensions of the auxiliary systems L_{A_1} and L_{B_1} are finite, but can be arbitrarily large. Subsystems A_1' and B_1' of $\rho^{(1)}_{L_{A_1}A_1':B_1'L_{B_1}}$ are then inserted into the channel $\mathcal{N}$, yielding a state $\sigma^{(1)}_{L_{A_1}A_1:B_1L_{B_1}}$. This is followed by n more PPT-preserving (or LOCC) channels interleaved with n uses of the channel. After n channel uses, the final PPT-preserving (or LOCC) channel should yield a state $\omega_{M_AM_B}$ that has fidelity [33] larger than $1-\varepsilon$ with a maximally entangled state $\Phi_{M_AM_B}$ containing $\log_2 M$ ebits (or a private state containing $\log_2 K$ private bits between Alice and Bob). Such a protocol is called an $(n, M(\text{or } K), \varepsilon)$-protocol. A rate R is achievable if for $\varepsilon \in (0,1)$, $\delta > 0$, and sufficiently large n, there exists an $(n, 2^{n(R-\delta)}, \varepsilon)$ protocol. The largest achievable rate is the PPT-assisted quantum capacity $Q_{\text{PPT}}^{2\to 2}$ (or secret-key agreement capacity $P_{\text{LOCC}}^{2\to 2}$) of $\mathcal{N}$.

By private states containing $\log_2 K$ private bits, we mean states $\gamma_{K_AS_A:K_BS_B}$, such that measurement of the $K_{A,B}$ subsystems, the *key part*, yields $\log K$ bits of secret key as long as the $S_{A,B}$ subsystems, the *shield part*, are kept secure from Eve, who is allowed to be in control of the purification of γ. See the seminal works [14, 15] for further details.

The main results of this paper are *strong converse* bounds on $Q_{\text{PPT}}^{2\to 2}$ and $P_{\text{LOCC}}^{2\to 2}$, in terms of the bidirectional max-Rains information and bidirectional max-relative entropy of entanglement, respectively. The strong-converse nature of the bound means that the error ε tends to one in the limit of many channel uses if the communication rate exceeds the bound. Our first result is as follows:

Theorem 1 *The PPT-assisted quantum communication capacity of a bidirectional channel $\mathcal{N}$ is bounded from above*

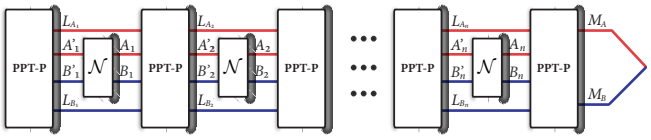

FIG. 1. A model of an adaptive positive-partial-transpose (PPT) assisted entanglement generation protocol using a bidirectional channel $\mathcal{N}$. Secret-key agreement proceeds analogously, if we replace the PPT-preserving channels by LOCC channels.

by its bidirectional max-Rains information: $Q^{2\to 2}_{\mathrm{PPT}}(\mathcal{N}) \leq R^{2\to 2}_{\max}(\mathcal{N})$*, and this upper bound is a strong converse bound.*

Theorem 1 is a consequence of the observation that the bidirectional max-Rains information of a bidirectional channel $\mathcal{N}$ cannot be enhanced by amortization; i.e., for an input state $\rho_{L_A A' B' L_B}$, the following holds

$$R_{\max}(L_A A; B L_B)_{\mathcal{N}(\rho)} \leq R_{\max}(L_A A'; B' L_B)_{\rho} + R^{2\to 2}_{\max}(\mathcal{N}), \tag{3}$$

where $R_{\max}(A;B)_\rho := \inf\{\lambda : \rho_{AB} \leq 2^\lambda \sigma'_{AB}, \sigma'_{AB} \in \mathrm{PPT}'(A:B)\}$ denotes the max-Rains information of the state ρ_{AB} [34], with $\mathrm{PPT}'(A:B)$ denoting the set of all positive semidefinite operators σ'_{AB} such that the trace norm $\| \mathrm{T}_B(\sigma'_{AB})\|_1 \leq 1$ [35]. This observation was made in the case of point-to-point channels [36] and constitutes a contribution of our companion paper [30]. By successive application of the amortization relation in (3) to every use of $\mathcal{N}$ in an (n, M, ε)-protocol, it follows that $R_{\max}(M_A; M_B)_\omega \leq n R^{2\to 2}_{\max}(\mathcal{N})$, where $|M_A| = |M_B| = M$. As, by assumption, $\mathrm{Tr}[\Phi_{M_A M_B} \omega_{M_A M_B}] \geq 1 - \varepsilon$, whereas by [31, Lemma 2], $\mathrm{Tr}[\Phi_{M_A M_B} \sigma'_{M_A M_B}] \leq \frac{1}{M}$ for any $\sigma'_{M_A M_B} \in \mathrm{PPT}'(A:B)$, it follows by a data-processing argument that $R_{\max}(M_A; M_B)_\omega \geq \log[(1-\varepsilon)M]$. Hence we obtain

$$\frac{1}{n} \log_2 M \leq R^{2\to 2}_{\max}(\mathcal{N}) + \frac{1}{n} \log_2 \left(\frac{1}{1-\varepsilon} \right), \tag{4}$$

which implies Theorem 1. Solving (4) for ε shows that the error increases exponentially fast to one if the rate exceeds $R^{2\to 2}_{\max}(\mathcal{N})$, establishing the strong converse nature of the bound.

As an example, we have numerically computed $R^{2\to 2}_{\max}$ for the qubit partial swap operation [24, 37], which is performed by application of the unitary $U_p = \sqrt{p} I + \iota \sqrt{1-p} S$, where $S = \sum_{ij} |ij\rangle\langle ji|$ is the swap operator. Such an operation can be compared to a beamsplitter [38]. We also consider when the partial swap is followed by a traceout of Alice's subsystem. As another example, we have computed $R^{2\to 2}_{\max}$ for a qubit swap operator with collective dephasing [25], which is a typical model for noise in a quantum computer. In the qubit case, a collective phase rotation acts as $|0\rangle \to |0\rangle$, $|1\rangle \to e^{\iota\phi}|1\rangle$ for some phase ϕ. Hence $|00\rangle \to |00\rangle$, $|01\rangle \to e^{\iota\phi}|01\rangle$, $|10\rangle \to e^{\iota\phi}|10\rangle$, and $|11\rangle \to e^{2\iota\phi}|11\rangle$. The collective phase rotation occurs with probability $1-p$.

Our results are plotted in Figure 2. For the partial swap, the top plot shows the expected decline from two ebits to zero, as

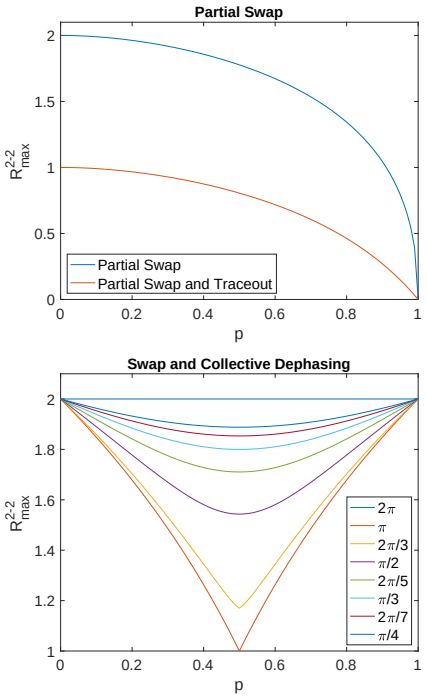

FIG. 2. Our bounds plotted versus the channel parameter p. From top to bottom, they are (i) qubit partial swap operation and qubit partial swap operation followed by traceout of Alice's output and (ii) a qubit swap operation with collective dephasing for various phases ϕ.

the channel tends towards total depolarization. For the partial swap and traceout, the decline is from one ebit to zero. In the example of collective dephasing, as expected, the performance is the worst at $p = 1/2$, where there is the most uncertainty about whether the collective phase rotation has taken place. For $\phi = \pi$, we can have a reduction of a factor of $1/2$. Let us remark that this bound can actually be achieved. To do so, Alice and Bob both locally create two Bell states $\Phi^+_{L_A A'}$ and $\Phi^+_{B' L_B}$, which are maximally entangled. After the swap operation and the collective dephasing, they end up sharing the state $\frac{1}{2}\Phi^+_{AL_B} \otimes \Phi^+_{BL_A} + \frac{1}{2}\Phi^-_{AL_B} \otimes \Phi^-_{BL_A}$. To find out the phase, Alice and Bob can locally measure either A and L_B or L_A and B in the Pauli-X basis, thus sacrificing one ebit. If their results agree, they have Φ^+, and otherwise Φ^-, which can be rotated to Φ^+ via local unitary.

For the generation of secret key, we have the following:

Theorem 2 *The secret-key agreement capacity of a bidirectional channel* $\mathcal{N}$ *is bounded from above by its bidirectional max-relative entropy of entanglement:* $P^{2\to 2}_{\mathrm{LOCC}}(\mathcal{N}) \leq E^{2\to 2}_{\max}(\mathcal{N})$*, and this upper bound is a strong converse bound.*

Theorem 2 is a consequence of the amortization property of the bidirectional max-relative entropy of entanglement, which follows from the *data processed triangle inequality* for the max-relative entropy of entanglement [39]. The proof then follows along the lines of that for Theorem 1, while making use of the relation between tripartite key states and bipartite private states and the privacy test from [40].

If a bidirectional channel has certain symmetries, tighter

bounds than the ones given in Theorems 1 and 2 can be obtained: A bidirectional channel $\mathcal{N}_{A'B'\to AB}$ is said to be PPT-simulable (or teleportation-simulable [41]) with associated resource state $\theta_{D_AD_B}$, for some auxiliary quantum systems D_A and D_B, if there exists a PPT-preserving (or LOCC) channel $\mathcal{P}_{D_AA'B'D_B\to AB}$ such that $\mathcal{N}_{A'B'\to AB}(\rho_{A'B'}) = \mathcal{P}_{D_AA'B'D_B\to AB}(\rho_{A'B'}\otimes\theta_{D_AD_B})$. If a bidirectional channel is PPT-simulable (or teleportation-simulable), then the bounds given in Theorem 1 (or Theorem 2) reduce to the standard Rains relative entropy [31] (or the relative entropy of entanglement [42]) of the resource state.

In particular, it can be shown that any bicovariant bidirectional channel is teleportation-simulable, hence also PPT-simulable, with the normalized Choi state as the associated resource state. By bicovariant, we mean that for finite groups G and H, with representations as unitary one-designs, the following holds for all $g\in G$, $h\in H$ and all input states $\rho_{A'B'}$: $\mathcal{N}_{A'B'\to AB}((\mathcal{U}_{A'}(g)\otimes\mathcal{V}_{B'}(h))(\rho_{A'B'})) = (\mathcal{W}_A(g,h)\otimes\mathcal{T}_B(g,h))(\mathcal{N}_{A'B'\to AB}(\rho_{A'B'}))$, for unitary representations $g\to U_{A'}(g)$, $h\to V_{B'}(h)$, $(g,h)\to W_A(g,h)$ and $(g,h)\to T_B(g,h)$, where we have defined $\mathcal{U}(g)(\cdot) := U(g)(\cdot)(U(g))^\dagger$. An example of a bicovariant channel is the CNOT gate [43, 44], or one that applies the CNOT gate with some probability and replaces with the maximally mixed state with the complementary probability.

Private Reading—Consider the task of reading a message stored in a memory device, while under the surveillance of a passive eavesdropper Eve. The read-out of the stored message should be private, under the assumption that Eve has complete access to the environment but no direct access to the device. Such a private reading protocol is a private version of the quantum reading protocol from [45] (see also [16, 28]). Formally, in a private reading protocol, the encoder, Alice, encodes a secret classical message $k\in\mathcal{K}$ into a sequence of wiretap channels chosen from a set $\mathcal{M}_{\mathcal{X}} := \{\mathcal{N}^x_{B'\to BE}\}_{x\in\mathcal{X}}$, by means of codewords $x^n(k) = x_1(k)\cdots x_n(k)$. We call the set of wiretap channels a *wiretap memory cell*, where the dimensions of the systems B', B, and E are independent of x. It is assumed that Eve has access to the E systems only, but her computational power may be unbounded. As a special case, we can consider isometric memory cells, which map the input space B' reversibly into the output space BE. The memory device containing the channels is then delivered to the reader, Bob, as a read-only device.

Bob can use quantum inputs, channels, and measurements to read out the message encoded in the device. In particular, he can apply an adaptive strategy consisting of creating an initial state $\rho^{(1)}_{B'_1S_{B_1}}$, inserting B'_1 into the channel $\mathcal{N}^{x_1}$, applying a quantum channel on the output $B_1L_{B_1}$, which results in a new state $\rho^{(2)}_{B'_2L_{B_2}}$, the B'_2 subsystem of which is then entered into $\mathcal{N}^{x_2}$ and so on. After using all n channels, interleaved by quantum channels, Bob then performs a final measurement, yielding an estimate $\hat{k}$ of the encoded message.

As mentioned above, the channels are wiretapped by an eavesdropper Eve. As is the case for Bob, the device is assumed to be read-only for Eve as well. So she assumes the role of a passive eavesdropper and only has access to the output systems $E_1,\ldots,E_n$ of the channels $\mathcal{N}^{x_1},\ldots,\mathcal{N}^{x_n}$, respectively. The goal is to maximize Bob's success probability of guessing the message, while restricting Eve to obtain negligible information about the message.

In the case of an isometric wiretap memory cell $\mathcal{M}_{\mathcal{X}} = \{\mathcal{U}^x_{B'\to BE}\}_{x\in\mathcal{X}}$, Theorem 2 provides a (strong converse) upper bound on the maximum achievable rate of a private reading protocol. This follows from the observation that in a *purified* setting [14, 15, 40], in which purifications of all input states are considered and for every operation the ancillary subsystems are being considered as well, a private reading protocol can be used to create a private state, containing $K = |\mathcal{K}|$ bits of secret key, between Alice and Bob. To do so, Alice prepares a purification $\frac{1}{\sqrt{K}}\sum_{k\in\mathcal{K}}|k,k,k\rangle_{K_A\hat{K}C}$ of a maximally classically correlated state $\frac{1}{K}\sum_{k\in\mathcal{K}}|k,k\rangle\langle k,k|_{K_AC}$ and encodes subsystem C by means of an isometry $|k\rangle_C\to|x^n(k)\rangle_{X^n}$. For every letter $x_i(k)$ of the codeword, the combined operation of Alice's writing and Bob's readout of the memory device is then described by a controlled isometry

$$U^{\mathcal{M}_{\mathcal{X}}}_{X_iB'_i\to X_iB_iE_i} := \sum_{x\in\mathcal{X}}|x\rangle\langle x|_{X_i}\otimes U^x_{B'_i\to B_iE_i}. \tag{5}$$

In an adaptive protocol, the U_i's are interleaved with Bob's operations. This is then followed by a decoding channel on Bob's side, after which Alice and Bob's state should be ε-close to a private state $\gamma_{K_AS_A:K_BS_B}$, where S_A and S_B denote the shield parts containing all ancillary systems that Alice and Bob have created during the purified protocol (see [30, Section 6.3]). Defining a bidirectional channel $\mathcal{N}^{\mathcal{M}_{\mathcal{X}}}_{XB'\to XB}(\cdot) := \mathrm{Tr}_E[U^{\mathcal{M}_{\mathcal{X}}}_{XB'\to XBE}(\cdot)(U^{\mathcal{M}_{\mathcal{X}}}_{XB'\to XBE})^\dagger]$, it is straightforward to conclude that the purified reading protocol is an example of a bidirectional secret-key-agreement protocol. Hence by Theorem 2, its capacity is bounded from above by $E^{2\to2}_{\max}(\mathcal{N}^{\mathcal{M}_{\mathcal{X}}}_{XB'\to XB})$.

As a concrete example, let us consider a *qudit erasure wiretap memory cell* [45]. It is defined as $\bar{\mathcal{Q}}^p_{\mathcal{X}} = \{\mathcal{Q}^{p,x}_{B'\to BE}\}_{x\in\mathcal{X}}$, where $\mathcal{Q}^{p,x}(\cdot) = U^p\sigma^x(\cdot)(\sigma^x)^\dagger(U^p)^\dagger$, with Heisenberg–Weyl operators σ^x and $U^p|\psi\rangle_{B'} = \sqrt{1-p}|\psi\rangle_B|e\rangle_E + \sqrt{p}|e\rangle_B|\psi\rangle_E$. is the isometric extension of the erasure channel. Using a covariance argument, we reduce the upper bound in Theorem 2 to the relative entropy of entanglement of the Choi state, which provides a strong converse upper bound of $2(1-p)\log_2 d$ on the private reading capacity of $\bar{\mathcal{Q}}^p_{\mathcal{X}}$.

Summary and Outlook—We have provided strong converse upper bounds on the PPT-assisted quantum capacity and the LOCC-assisted private capacity of a bidirectional quantum channel. The bound on the quantum capacity is related to the Rains bound [31, 32], as well as that in [29], and can be efficiently computed by SDP solvers. We have provided examples that demonstrate the applicability of our bound. The bound on the private capacity is in terms of the max-relative entropy of entanglement [26, 27, 39]. As an application, we have considered the task of private reading in the presence of

a passive eavesdropper. Both bounds can be improved in the case of a bicovariant bidirectional channel. As an example, we have upper bounded the private reading capacity of a qudit erasure wiretap memory cell. Future directions from here include generalising our results from bi- to multipartite quantum interactions, which could be effectively applied in the theory of quantum networks.

We thank K. Azuma, A. Harrow, M. Huber, C. Lupo, B. Munro, M. Murao, and G. Siopsis for discussions. SD acknowledges support from the LSU Graduate School Economic Development Assistantship and the LSU Coates Conference Travel Award. MMW acknowledges support from the US Office of Naval Research and the National Science Foundation. Part of this work was completed during the workshop "Beyond i.i.d. in Information Theory," hosted by the Institute for Mathematical Sciences, NUS Singapore, 24-28 July 2017.

* stefanbaeuml@gmx.de
† sdas21@lsu.edu
‡ mwilde@lsu.edu

[1] John Goold, Marcus Huber, Arnau Riera, Lídia del Rio, and Paul Skrzypczyk. The role of quantum information in thermodynamics—a topical review. *Journal of Physics A: Mathematical and Theoretical*, 49(14):143001, 2016.

[2] William F. Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6:211–216, 1955.

[3] Asher Peres. *Quantum theory: concepts and methods*, volume 57. Springer Science & Business Media, 2006.

[4] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[5] Charles H. Bennett, Aram W. Harrow, Debbie W. Leung, and John A. Smolin. On the capacities of bipartite Hamiltonians and unitary gates. *IEEE Transactions on Information Theory*, 49(8):1895–1911, August 2003. arXiv:quant-ph/0205057.

[6] Peter W Shor. Fault-tolerant quantum computation. In *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on*, pages 56–65. IEEE, 1996.

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

[8] Marek Zukowski, Anton Zeilinger, Michael A Horne, and Aarthur K Ekert. "event-ready-detectors"bell experiment via entanglement swapping. *Physical Review Letters*, 71:4287–4290, 1993.

[9] Martin B. Plenio and Shashank Virmani. An introduction to entanglement measures. *Quantum Information & Compution*, 7(1):1–51, January 2007. arXiv:quant-ph/0504163.

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

[11] Marcus Huber, Martí Perarnau-Llobet, Karen V Hovhannisyan, Paul Skrzypczyk, Claude Klöckl, Nicolas Brunner, and Antonio Acín. Thermodynamic cost of creating correlations. *New Journal of Physics*, 17(6):065008, 2015.

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

[13] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, January 2005. arXiv:quant-ph/0306078.

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

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

[16] Sougato Bose, Luke Rallan, and Vlatko Vedral. Communication capacity of quantum computation. *Physical Review Letters*, 85(25):5448–5451, December 2000. arXiv:quant-ph/0003072.

[17] Andrew M. Childs, Debbie W. Leung, and Hoi-Kwong Lo. Two-way quantum communication channels. *International Journal of Quantum Information*, 04(01):63–83, February 2006. arXiv:quant-ph/0506039.

[18] Paolo Zanardi, Christof Zalka, and Lara Faoro. Entangling power of quantum evolutions. *Physical Review A*, 62(3):030301, August 2000. arXiv:quant-ph/0005031.

[19] Mathew S. Leifer, Leah Henderson, and Noah Linden. Optimal entanglement generation from quantum operations. *Physical Review A*, 67(1):012306, January 2003. arXiv:quant-ph/0205055.

[20] Aram W. Harrow and Debbie W. Leung. Bidirectional coherent classical communication. *Quantum Information & Computation*, 5(4):380–395, July 2005. arXiv:quant-ph/0412126v3.

[21] Noah Linden, John A. Smolin, and Andreas Winter. Entangling and disentangling power of unitary transformations are not equal. *Physical Review Letters*, 103(3):030501, July 2009. arXiv:quant-ph/0511217.

[22] Eyuri Wakakuwa, Akihito Soeda, and Mio Murao. A coding theorem for bipartite unitaries in distributed quantum computation. *IEEE Transactions on Information Theory*, 63(8):5372–5403, August 2017. arXiv:1505.04352.

[23] Lin Chen and Li Yu. Entangling and assisted entangling power of bipartite unitary operations. *Physical Review A*, 94(2):022307, August 2016. arXiv:1604.05788.

[24] Koenraad Audenaert, Nilanjana Datta, and Maris Ozols. Entropy power inequalities for qudits. *Journal of Mathematical Physics*, 57(5):052202, 2016.

[25] G Massimo Palma, Kalle-Antti Suominen, and Artur K Ekert. Quantum computers and dissipation. In *Proc. R. Soc. Lond. A*, volume 452, pages 567–584. The Royal Society, 1996.

[26] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, June 2009. arXiv:0803.2770.

[27] Nilanjana Datta. Max-relative entropy of entanglement, alias log robustness. *International Journal of Quantum Information*, 7(02):475–491, January 2009. arXiv:0807.2536.

[28] Stefano Pirandola. Quantum reading of a classical digital memory. *Physical Review Letters*, 106(9):090504, March 2011. arXiv:1103.3478.

[29] Xin Wang, Kun Fang, and Runyao Duan. Semidefinite programming converse bounds for quantum communication. September 2017. arXiv:1709.00200.

[30] Siddhartha Das, Stefan Bäuml, and Mark M. Wilde. Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices. December 2017. arXiv:1712.00827.

[31] Eric M. Rains. Bound on distillable entanglement. *Physical Review A*, 60(1):179–184, July 1999. arXiv:quant-ph/9809082.

[32] Eric M. Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47(7):2921–2933, November 2001. arXiv:quant-ph/0008047.

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

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

[35] Koenraad Audenaert, Bart De Moor, Karl Gerd H. Vollbrecht, and Reinhard F. Werner. Asymptotic relative entropy of entanglement for orthogonally invariant states. *Physical Review A*, 66(3):032310, September 2002. arXiv:quant-ph/0204143.

[36] Mario Berta and Mark M. Wilde. Amortization does not enhance the max-Rains information of a quantum channel. *New Journal of Physics*, 20:053044, May 2018. arXiv:1709.04907.

[37] Omar Fawzi, Patrick Hayden, Ivan Savov, Pranab Sen, and Mark M. Wilde. Classical communication over a quantum interference channel. *IEEE Transactions on Information Theory*, 58(6):3670–3691, June 2012. arXiv:1102.2624.

[38] Robert König and Graeme Smith. Limits on classical communication from quantum entropy power inequalities. *Nature Photonics*, 7(2):142, 2013.

[39] Matthias Christandl and Alexander Müller-Hermes. Relative entropy bounds on quantum, private and repeater capacities. *Communications in Mathematical Physics*, 353(2):821–852, July 2017. arXiv:1604.03448.

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

[41] Akihito Soeda, Peter S. Turner, and Mio Murao. Entanglement cost of implementing controlled-unitary operations. *Physical Review Letters*, 107(18):180501, October 2011. arXiv:1008.1128.

[42] Vlatko Vedral and Martin B Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619, 1998.

[43] Daniel Gottesman. The Heisenberg representation of quantum computers. In Peter D. Jarvis S. P. Corney, Robert Delbourgo, editor, *Group Theoretical Methods in Physics: Proceedings*, 22. Cambridge, USA: International Press, July 1999. arXiv:quant-ph/9807006.

[44] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, November 1999. arXiv:quant-ph/9908010.

[45] Siddhartha Das and Mark M. Wilde. Quantum reading capacity: General definition and bounds. March 2017. arXiv:1703.03706.