Private States, Quantum Data Hiding, and the Swapping of Perfect Secrecy

Matthias Christandl* and Roberto Ferrara†
QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark
(Received 14 October 2016; revised manuscript received 29 June 2017; published 30 November 2017)

An important contribution to the understanding of quantum key distribution has been the discovery of entangled states from which secret bits, but no maximally entangled states, can be extracted [Horodecki *et al.*, Phys. Rev. Lett. **94**, 200501 (2005)]. The construction of those states was based on an intuition that the quantum mechanical phenomena of data hiding and privacy might be related. In this Letter we firmly connect these two phenomena and highlight three aspects of this result. First, we simplify the definition of the secret key rate. Second, we give a formula for the one-way distillable entanglement of certain private states. Third, we consider the problem of extending the distance of quantum key distribution with help of intermediate stations, a setting called the quantum key repeater. We show that for protocols that first distill private states, it is essentially optimal to use the standard quantum repeater protocol based on entanglement distillation and entanglement swapping.

DOI: 10.1103/PhysRevLett.119.220506

Introduction.—Entanglement distillation [1] is the process of producing high-fidelity maximally entangled states from copies of a noisy entangled state ρ, using only local operations and classical communication (LOCC), between two parties, Alice and Bob. The maximally entangled states can then be used for teleportation, Bell inequality violation, etc. The rate at which they can be distilled from ρ is called the distillable entanglement, $E_D(\rho)$. Because maximally entangled states are pure, they are in product with the environment and, therefore, measuring them leads to perfectly correlated and perfectly secure pairs of bits—perfect secret bits. It turns out that there exist mixed states, the private states, that also lead to perfectly secure bits just by measurement [2]. While the distillable key, $K_D(\rho)$, is defined as the rate at which perfect secret bits can be distilled by local operations and public communication, it was shown that it also equals the rate at which private states can be distilled by LOCC. Proving this equivalence allowed the authors to show that distillable entanglement and distillable key can be very different [2]. There even exists a low-dimensional experimental realization of this separation with photonic states [3].

In light of this, it is natural to ask how much the separation extends to general network scenarios, and in particular whether it persists if we insert a repeater station between the two parties. In [4] the first examples have been produced of states that, while having a high distillable key, do not allow for distillation of significant amounts of the key across the repeater station. This may be an indication that the separation between the distillable key and distillable entanglement does not survive in all general network scenarios.

Here we provide a new perspective on key distillation, and thus quantum key distribution, by relating private states to quantum data hiding [5,6]. This provides a tool for the study of long-distance quantum key distribution involving intermediate repeater stations, where for the first time we are able to show a close connection with entanglement distillation. In this framework [4], noisy entanglement is distributed between the end points and the repeater station and arbitrary noiseless LOCC protocols are allowed. If this setting is used to distill maximally entangled states at the end points, then this is an idealized version of the well-known quantum repeater; if it is used to distill private states, it is called a quantum key repeater. We provide an upper bound on the quantum key repeater rate with one-way classical communication; as such, the bound holds also for noisy protocols that can only lower the rate and thus, if anything, leave room for improvement. Our results go beyond the use of the partial transpose and thus apply to states that are not positive under partial transposition (NPT states) as well as states that are invariant under partial transposition (PPT invariant states), which are out of reach for [4].

The Letter is organized as follows. First, we simplify the class of private states, introducing what we call Bell private states. We show that these states are, for all entanglement-related purposes, equivalent to private states. Second, the simplified structure of Bell private states allows us to confirm the intuition that the separation between the distillable key and distillable entanglement is due to quantum data hiding. More precisely, we show that the states with a separation are those made of a maximally entangled state subject to phase flip error, where the error information is conserved in data-hiding states. Such hidden information of the error preserves the key, but prevents Alice and Bob from correcting the maximally entangled state and distill entanglement. Third, as an application to the quantum key repeater with one-way classical communication from the repeater station, we show that a large class of states and protocols cannot be used to distil more key across a repeater station than by performing entanglement distillation and swapping.

Private states.—Consider two parties, Alice and Bob, sharing a maximally entangled state Φ of two qubit systems A_kB_k—the key systems. Measuring Φ in the computational

basis will produce a perfect secret bit with respect to any adversary; the postmeasurement state of such a measurement is called a key attacked state; this will play an important role in our results and will be denoted by a hat ($\hat{}$),

$$\Phi := \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$$
$$\hat{\Phi} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|). \quad (1)$$

The support of $\hat{\Phi}$ is known as the maximally correlated subspace. Now let Alice and Bob share additional systems A_sB_s—the shield systems. A private state γ is a state on $A_kB_kA_sB_s$ that generalizes the maximally entangled state, in the sense that measuring A_kB_k produces a perfect secret bit with respect to any adversary. γ is a private state if and only if it has the form [2]

$$\gamma := T(\Phi \otimes \sigma)T^\dagger \qquad \hat{\gamma} = T(\hat{\Phi} \otimes \sigma)T^\dagger \quad (2)$$

for some state σ on A_sB_s and controlled unitary T called twisting; with no shield systems, the only private states are maximally entangled states. However, the first example of a private state with low distillable entanglement was constructed as follows [2]:

$$\gamma = p_0\mathcal{Z}^0_{B_k}(\Phi) \otimes \sigma_0 + p_1\mathcal{Z}^1_{B_k}(\Phi) \otimes \sigma_1, \quad (3)$$

where σ_j are the extremal Werner states [7] and $\mathcal{Z}^j(\varrho) := Z^j\varrho Z^{-j}$ is the jth phase flip map, namely, the map that conjugates by the jth power of the Pauli Z. The intuition behind the example is the following: orthogonal data-hiding states σ_j [5,6], like the Werner states [8], should hinder the ability to correct the phase flip locally and, thus, they should suppress the distillable entanglement; nevertheless, because the states are orthogonal, the perfect secret bit is still protected from the environment.

Private states like the ones in Eq. (3) are only a special case (see [9] for different examples); we call them Bell private states. We now show how to convert all private states into Bell private states reversibly using only LOCC. We need two generalizations.

We generalize the maximally entangled state to any key systems of equal finite dimension $|A_k| = |B_k|$. We define the Bell states $\phi_j = |\phi_j\rangle\langle\phi_j| = \mathcal{Z}^j_{B_k}(\Phi)$ for $j = 0, \ldots, |B_k| - 1$. Notice that $\{|\phi_j\rangle\}$ form a basis for the maximally correlated subspace, which brings us to the next generalization. We consider any state supported only on the maximally correlated subspace of A_kB_k, we call such states key correlated. They have no bit-flip error and we can write them as

$$\rho = \sum_{\mu\nu}|\phi_\mu\rangle\langle\phi_\nu| \otimes P_{\mu\nu}, \quad (4)$$

where $P_{\mu\nu}$ are matrices on A_sB_s.

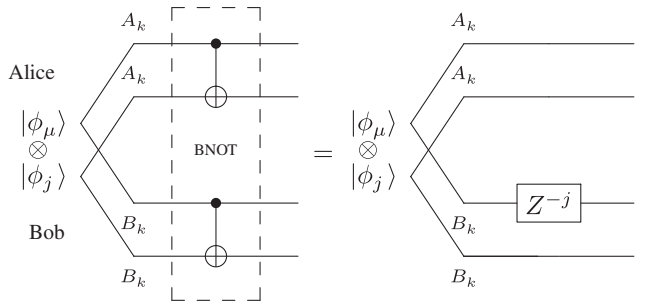

FIG. 1. Quantum circuit for the bilateral CNOT acting on Bell states, the core of the map $\mathcal{E}$ of Lemma 1.

To define the reversible LOCC map, consider two copies of systems A_kB_k. Let $V = \mathrm{CNOT}_{A_kA_k} \otimes \mathrm{CNOT}_{B_kB_k}$ be the local unitary illustrated in Fig. 1, namely, the generalization of the qubit BNOT [1]. It holds that

$$V(|\phi_j\rangle_{A_kB_k} \otimes |\phi_\mu\rangle_{A_kB_k}) = |\phi_j\rangle_{A_kB_k} \otimes Z^{-j}_{B_k}|\phi_\mu\rangle_{A_kB_k}. \quad (5)$$

Lemma 1. Define $\mathcal{E}: A_kB_k \to A_kB_kA_kB_k$ as

$$\mathcal{E}(\varrho_{A_kB_k}) := V^\dagger(\hat{\Phi}_{A_kB_k} \otimes \varrho_{A_kB_k})V.$$

Then for any key correlated state ρ (on $A_kB_kA_sB_s$)

$$\mathcal{E}(\rho) \equiv (\mathcal{E}_{A_kB_k} \otimes \mathrm{id}_{A_sB_s})(\rho) = \frac{1}{|B_k|}\sum_j \phi_j \otimes \mathcal{Z}^j_{B_k}(\rho). \quad (6)$$

Because $\hat{\Phi}$ is separable and V is local, $\mathcal{E}$ is one-way LOCC (classical communication only from Alice to Bob or vice versa). $\mathcal{E}$ is reversible by inverting V and tracing out the target, which requires only local operations. Notice that the output key systems are still A_kB_k but the output shield systems are now $A_kA_sB_kB_s$.

Proof.—Using (4), (5) and $\hat{\Phi} = (1/|B_k|)\sum_j \phi_j$ we find

$$\begin{aligned}(\mathcal{E} \otimes \mathrm{id})(\rho) &= \sum_{\mu\nu} V^\dagger(\hat{\Phi} \otimes |\phi_\mu\rangle\langle\phi_\nu|)V \otimes P_{\mu\nu} \\ &= \frac{1}{|B_k|}\sum_{\mu\nu j} V^\dagger(\phi_j \otimes |\phi_\mu\rangle\langle\phi_\nu|)V \otimes P_{\mu\nu} \\ &= \frac{1}{|B_k|}\sum_{\mu\nu j} \phi_j \otimes \mathcal{Z}^j_{B_k}(|\phi_\mu\rangle\langle\phi_\nu|) \otimes P_{\mu\nu}. \quad \square\end{aligned}$$

Bell private states now come as a special case. A Bell private state is any private state of the form

$$\gamma_{\mathrm{Bell}} = \sum_j p_j \cdot \phi_j \otimes \sigma_j,$$

where σ_j are arbitrary orthogonal states of A_sB_s and p_j are arbitrary probabilities. Notice that $\mathcal{Z}^j_{B_k}(\rho)$ are orthogonal, and thus $\mathcal{E}(\rho)$ is a Bell private state only when ρ is a private

state. Because $\mathcal{E}$ is reversible, any property of entanglement monotones (entanglement measures like the distillable entanglement and distillable key) for Bell private states also holds for private states and vice versa. For example, we can always convert the output of a key distillation protocol into an approximate Bell private state, thus simplifying the distillable key to the rate at which Bell private states can be distilled.

Entanglement distillation and quantum data hiding.—We now show that Bell private states with low distillable entanglement are states that hide the phase of the maximally entangled states from local detection. Specifically, we give a lower bound on the one-way distillable entanglement $E_D^{\rightarrow}(\rho)$, where the communication is one way, from Alice to Bob. This lower bound is the rate achieved by the best protocol that starts with a measurement on Alice's shield.

First, for simplicity, let Alice and Bob share a key correlated state of the form

$$\rho = \frac{1}{|B_k|}\sum_j \phi_j \otimes \sigma_j. \tag{7}$$

We now let Alice perform a measurement on her shield and send the outcome to Bob. Then Alice and Bob use the hashing protocol [1,10] and we find (Lemma 18 of Ref. [11])

$$E_D^{\rightarrow}(\rho) \geq \sup_{\mathcal{M}\in LO_A} \frac{1}{|B_k|}\sum_j D(\mathcal{M}(\sigma_j)\|\mathcal{M}(\sigma)), \tag{8}$$

where $\sigma = (1/|B_k|)\sum_j \sigma_j$, $D(\varrho\|\varsigma) = \mathrm{Tr}[\varrho\log\varrho - \rho\log\varsigma]$ is the relative entropy, and $\mathcal{M}$ is a local measurement at Alice ($\mathcal{M} \equiv \mathcal{M}_A \otimes \mathrm{id}_B$). The relative entropy quantifies the distinguishability between states; the relative entropy of the measurement outcomes [23] quantifies how much of this distinguishability is left when Alice and Bob can only act locally. In the particular case of private states, the σ_j state of Eq. (7) are orthogonal; thus, they are perfectly distinguishable and j can be recovered with a global measurement. However, Eq. (8) implies that if the distillable entanglement is low, then the local distinguishability of σ_j is low and j cannot be determined accurately locally: the σ_j are data hiding [5,6].

For general key correlated states ρ we can use Eq. (8) after using Lemma 1; this gives

$$E_D^{\rightarrow}(\rho) \geq \sup_{\mathcal{M}\in LO_A} \frac{1}{|B_k|}\sum_j D(\mathcal{M}\circ\mathcal{Z}_{B_k}^j(\rho)\|\mathcal{M}(\hat{\rho})).$$

Namely, we see that because of the reversible map, we can think of the private state itself as a data-hiding state, where j is encoded using the local phase flip.

We can exploit the measurement being local to simplify our bounds. More precisely, we find that for all local measurements at Alice

$$D(\mathcal{M}\circ\mathcal{Z}_{B_k}^j(\rho)\|\mathcal{M}(\hat{\rho})) = D(\mathcal{M}(\rho)\|\mathcal{M}(\hat{\rho})).$$

Namely, the optimal measurement is independent of the phase flip, which allows us to remove the phase flip in the formula. This is an important feature because it suddenly allows us to regularize [24,25] our lower bound. If $\hat{\rho}$ is separable, then we can combine the regularized lower bound with a known upper bound from [26], and obtain equality with the distillable entanglement as stated in this theorem (Theorem 21 of Ref. [11]).

Theorem 2. *For any key correlated state ρ, it holds*

$$E_D^{\rightarrow}(\rho) \geq D_A(\rho\|\hat{\rho}) \coloneqq \sup_{\mathcal{M}\in LO_A} D(\mathcal{M}(\rho)\|\mathcal{M}(\hat{\rho}))$$

$$E_D^{\rightarrow}(\rho) \geq D_A^{\infty}(\rho\|\hat{\rho}) \coloneqq \lim_{n\to\infty}\frac{1}{n}D_A(\rho^{\otimes n}\|\hat{\rho}^{\otimes n}).$$

If $\hat{\rho}$ is also separable then

$$E_D^{\rightarrow}(\rho) = D_A^{\infty}(\rho\|\hat{\rho}).$$

Quantum key repeaters.—We now apply our findings to long-distance quantum communication, where noise prevents Alice and Bob from sharing entanglement and thus secrecy, and where an intermediate repeater station, Charlie, is necessary to mediate the entanglement.

More precisely, let Alice and Charlie (A and C) share ρ and Charlie and Bob (C' and B) share ρ'. While the goal of a quantum repeater is to distill maximally entangled states between Alice and Bob [27], the goal of a quantum key repeater is to distill perfect secret bits or, equivalently, private states [4]—see Fig. 2. The best rate for this task is called the quantum key repeater rate, $R_D(\rho,\rho')$. Realistic repeaters have multiple stations; however, we reduce to a single station by grouping them into one, which can only increase the rate. The reduction to a single station thus provides upper bounds without loss of generality.

ρ and ρ' are usually generated by sharing maximally entangled states through noisy channels (Choi-Jamiołkowski states). While clever channel codes may reach higher

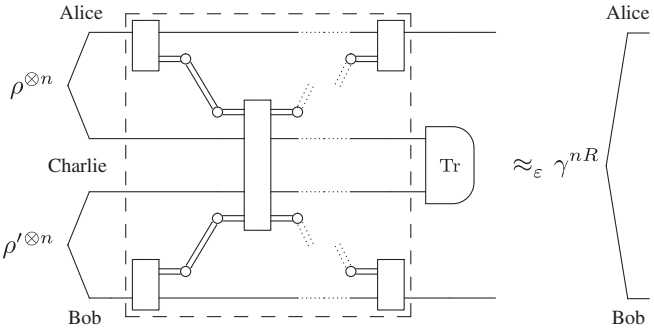

FIG. 2. Quantum circuit for the key repeater protocols in a single node repeater. The dashed box is a tripartite LOCC protocol. The double lines are the classical communication.

rates [28,29], note that the free classical side information allows us in most realistic channels to implement the codes via teleportation from the Choi-Jamiołkowski state (e.g., the depolarizing channel) [1]. Thus, our upper bounds also apply to such codes and channels (see also [30]).

The optimal noise-free protocol for the quantum repeater performs entanglement distillation between Alice and Charlie and Charlie and Bob, followed by entanglement swapping. This results in the rate $\min\{E_D(\rho), E_D(\rho')\}$, but in the quantum key repeater setting the situation is less clear. In alternative to the mentioned protocol, Alice and Charlie can distill private states, and use the maximally entangled states distilled by Charlie and Bob to teleport Charlie's part of the private states. If $E_D(\rho')$ is larger than the private states size at Charlie's, then the rate of this "trivial" protocol equals $K_D(\rho)$ and thus it will be positive even when ρ has zero distillable entanglement [2,9]. In short, while for quantum repeaters the active area of research studies the effect of noisy operations, for quantum key repeaters there are open questions even with perfect operations.

We will consider the one-way key repeater rate variation, also introduced in [4]. In this variation, Alice and Bob's communication with the repeater station Charlie is only one way: Charlie can send messages to Alice and Bob but not vice versa. Alice and Bob can still communicate normally with each other. We denote this rate with $R_D^{CC'\to A:B}$, or simply $R_D^{\rightarrow}$. In [4] the question was posed whether there exist nontrivial protocols beyond distillation and swapping, but only negative examples were found. Here we show that for a large class of states and protocols, the one-way distillable entanglement is an upper bound on the one-way key repeater rate, and thus distillation and swapping are essentially optimal and far from the trivial upper bounds $K_D(\rho)$ and $K_D(\rho')$.

We need a general upper bound which follows from Theorem 4 of Ref. [4],

$$R_D^{CC'\to A:B}(\rho_{AC}, \rho'_{C'B}) \le D^{\infty}_{CC'}(\rho_{AC} \otimes \rho'_{C'B} \| \sigma), \quad (9)$$

for any state σ separable in the $ACC':B$ or $A:CC'B$ cut. So far, this bound could only be estimated via a relaxation that only works for states that have a positive partial transpose (PPT states). Choosing $\sigma = \hat{\rho} \otimes \hat{\rho}'$ and applying Theorem 1 to Eq. (9) now shows the following corollary, independently of the partial transpose.

Corollary 3. *For any key correlated states ρ and ρ' with at least one separable key attacked state, it holds*

$$R_D^{CC'\to A:B}(\rho_{AC}, \rho'_{C'B}) \le E_D^{C\to A}(\rho_{AC} \otimes \rho'_{CA}).$$

Since all private states are NPT (not positive under partial transposition) [31], this gives the first examples of NPT states with a high distillable key but low one-way key repeater rate.

Example. Consider the following Bell private state [see [2] and Eq. (3)]:

$$\gamma = \frac{1}{2}\left(1 + \frac{1}{d}\right)\phi_0 \otimes \sigma_0 + \frac{1}{2}\left(1 - \frac{1}{d}\right)\phi_1 \otimes \sigma_1$$

where σ_0 and σ_1 are, respectively, the symmetric and antisymmetric states in $\mathbb{C}^d \otimes \mathbb{C}^d$—the extreme Werner states [7] which are known to be data-hiding states [8]. Since distillable entanglement is upper bounded by the log-negativity E_N [32], we have the following upper bound which vanishes for large d:

$$R_D^{\rightarrow}(\gamma, \gamma) \le 2E_D^{\rightarrow}(\gamma) \le 2E_N(\gamma) = 2\log\left(1 + \frac{1}{d}\right). \quad (10)$$

This state was implemented experimentally for $d = 2$ [3]. The key was distilled at a rate $K \approx 0.69$, enough to break the bound at $E_N(\gamma) = \log\frac{3}{2} \approx 0.58$. However, because of the factor of 2 in Eq. (10), an implementation with $d = 4$ at the same key rate is required for the same proof of concept. Still, scaling up the implementation should be experimentally feasible, since in $d = 4$ the gate used (swap) is tensor product of qubit gates. In the Supplemental Material we show how to apply Corollary 3 to some PPT invariant states (Example 41 of Ref. [11]). ∎

Conclusions.—Corollary 3 bounds the key repeater rate of a restricted class of states, but it also generalizes to all states if we restrict the protocols to first distil private states with separable key attacked state between the nodes and then try to repeat. In Definition 28 of Ref. [11], we define a new key repeater rate ${}^{\prec}R_D^{\succ\rightarrow}(\rho, \rho')$ from these protocols and prove that for all states, this rate is upper bounded by $E_D^{\rightarrow}(\rho \otimes \rho')$. The restricted protocols still include one-way entanglement distillation and swapping; thus, the new key repeater rate is still lower bounded by the minimum of the one-way distillable entanglements. While being restrictive, we would like to stress that the communication between Alice and Bob is two way, and also that if the two-way step is limited to bipartite distillation between the nodes, we can always apply the result to the outcomes of the distillation. In particular, even if the two-way recurrence protocol is used to distill between the nodes, as in the case of heralded entanglement generation and purification, we can apply the bound on ${}^{\prec}R_D^{\succ\rightarrow}$ to the outputs of the recurrence protocol. The bound also applies to key repeater schemes based on quantum error correction. The link with outgoing communication from the station is trivially covered. For the link with incoming communication, the bound on ${}^{\prec}R_D^{\succ\rightarrow}$ applies to the output of the code (as mentioned above), since usually the code is decoded or corrected at the station, rendering it a bipartite distillation protocol. As such, we can apply our bound in some way to most repeater schemes (see also [29] and references therein for an overview) and where it applies, any attempt to improve the rate of key distillation above that of entanglement distillation will not work. For example, attempting to use

the noisy processing protocol [33] would yield no advantage. We are not aware that there exists any protocol that contains a truly two-way tripartite step.

Finally, we note that, because optimal one-way protocols exist when close to the target states, the optimal two-way protocols are composed of a two-way "lift-off" protocol followed by a one-way "conclusion" protocol [34].

We leave as an open problem whether Corollary 3 generalizes to all states and protocols, including two-way communication. Such a result would show that all entangled states with zero distillable entanglement, including those with distillable key, have zero key repeater rate. Another open problem, called the PPT^2 conjecture [35], asks whether swapping PPT states in all dimensions always yields separable states. If the conjecture is true, then it would imply that all PPT states have zero key repeater rate. In that, the results here presented support the conjecture. Since our results are asymptotic in nature, they give a complementary view on the PPT^2 conjecture to that of the study of swapping specific states in specific dimensions.

The connection made between key distillation, entanglement distillation, and quantum data hiding raises the possibility of finding a rate at which data-hiding states can be distilled, H_D (which we refrain from defining formally). Namely, in performing entanglement distillation on private states, it may be possible to retain the undistillable correlations into data-hiding states with zero distillable entanglement so that they could be used as a resource, such that

$$K_D(\rho) = H_D(\rho) + E_D(\rho).$$

We thank Alexander Müller-Hermes, Cécilia Lancien, and Māris Ozols for helpful discussions. We acknowledge financial support from the European Research Council (ERC Grant No. 337603), the Danish Council for Independent Research (Sapere Aude), and Villum Fonden via the QMATH Centre of Excellence (Grant No. 10059).

*christandl@math.ku.dk
†roberto@math.ku.dk

[1] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).
[2] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (2005).
[3] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzań-ski, K. Banaszek, and P. Horodecki, Experimental Extraction of Secure Correlations from a Noisy Private State, Phys. Rev. Lett. **106**, 030501 (2011).
[4] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, Limitations on quantum key repeaters, Nat. Commun. **6**, 6908 (2014).
[5] B. Terhal, D. DiVincenzo, and D. Leung, Hiding Bits in Bell States, Phys. Rev. Lett. **86**, 5807 (2001).
[6] D. DiVincenzo, B. Terhal, and D. Leung, Quantum data hiding, IEEE Trans. Inf. Theory **48**, 580 (2002).
[7] R. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).
[8] T. Eggeling and R. Werner, Hiding Classical Data in Multipartite Quantum States, Phys. Rev. Lett. **89**, 097905 (2002).
[9] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, Low-dimensional bound entanglement with one-way distillable cryptographic key, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[10] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[11] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.119.220506 for the details of the section on private states, for the PPT-invariant example, and for the definition of key repeater rate from private-state-swapping protocols, which includes [12–22].
[12] V. Vedral, M. Plenio, M. Rippin, and P. Knight, Quantifying Entanglement, Phys. Rev. Lett. **78**, 2275 (1997).
[13] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?, Phys. Rev. Lett. **80**, 5239 (1998).
[14] M. Donald and M. Horodecki, Continuity of relative entropy of entanglement, Phys. Lett. A **264**, 257 (1999).
[15] K. Audenaert, B. De Moor, K. Vollbrecht, and R. Werner, Asymptotic relative entropy of entanglement for orthogonally invariant states, Phys. Rev. A **66**, 032310 (2002).
[16] P. Badziag, M. Horodecki, A. Sen, and U. Sen, Locally Accessible Information: How Much Can the Parties Gain by Cooperating?, Phys. Rev. Lett. **91**, 117901 (2003).
[17] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A **37**, L55 (2004).
[18] T. Hiroshima and M. Hayashi, Finding a maximally correlated state: Simultaneous Schmidt decomposition of bipartite pure states, Phys. Rev. A **70**, 030302 (2004).
[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Locking Entanglement with a Single Qubit, Phys. Rev. Lett. **94**, 200501 (2005).
[20] A. Winter, Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints, Commun. Math. Phys. **347**, 291 (2016).
[21] M. Berta, O. Fawzi, and M. Tomamichel, Exploiting variational formulas for quantum relative entropy, in *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, Barcelona, 2016) pp. 2844–2848.
[22] D. Petz, Sufficient subalgebras and the relative entropy of states of a von Neumann algebra, Commun. Math. Phys. **105**, 123 1986.
[23] M. Piani, Relative Entropy of Entanglement and Restricted Measurements, Phys. Rev. Lett. **103**, 160504 (2009).
[24] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, Math. Z. **17**, 228 (1923).
[25] P. Hayden, M. Horodecki, and B. Terhal, The asymptotic entanglement cost of preparing a quantum state, J. Phys. A **34**, 6891 (2001).

[26] K. Li and A. Winter, Relative entropy and squashed entanglement, Commun. Math. Phys. **326**, 63 (2014).
[27] H. Briegel, W. Dür, J. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. **81**, 5932 (1998).
[28] E. Knill and R. Laflamme, Concatenated quantum codes, arXiv:quant-ph/9608012.
[29] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. Lukin, and L. Jiang, Optimal architectures for long distance quantum communication, Sci. Rep. **6**, 20463 (2016).
[30] M. Christandl and A. Müller-Hermes, Relative entropy bounds on quantum, private and repeater capacities, Commun. Math. Phys. **353**, 821 (2017).
[31] 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).
[32] G. Vidal and R. Werner, Computable measure of entanglement, Phys. Rev. A **65**, 032314 (2002).
[33] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).
[34] D. Kretschmann and R. Werner, Tema con variazioni: quantum channel capacity, New J. Phys. **6**, 26 (2004).
[35] M. Christandl, PPT square conjecture (problem G), in *Banff International Research Station Workshop: Operator Structures in Quantum Information Theory* (2012), https://www.birs.ca/workshops/2012/12w5084/report12w5084.pdf.