# Conditional Quantum One-Time Pad

Kunal Sharma,[1] Eyuri Wakakuwa,[2] and Mark M. Wilde[1]
[1]Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA
[2]Graduate School of Informatics and Engineering, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan

(Received 4 June 2018; accepted 13 January 2020; published 7 February 2020)

Suppose that Alice and Bob are located in distant laboratories, which are connected by an ideal quantum channel. Suppose further that they share many copies of a quantum state $\rho_{ABE}$, such that Alice possesses the $A$ systems and Bob the $BE$ systems. In our model, there is an identifiable part of Bob's laboratory that is insecure: a third party named Eve has infiltrated Bob's laboratory and gained control of the $E$ systems. Alice, knowing this, would like use their shared state and the ideal quantum channel to communicate a message in such a way that Bob, who has access to the whole of his laboratory ($BE$ systems), can decode it, while Eve, who has access only to a sector of Bob's laboratory ($E$ systems) and the ideal quantum channel connecting Alice to Bob, cannot learn anything about Alice's transmitted message. We call this task the conditional one-time pad, and in this Letter, we prove that the optimal rate of secret communication for this task is equal to the conditional quantum mutual information $I(A;B|E)$ of their shared state. We thus give the conditional quantum mutual information an operational meaning that is different from those given in prior works, via state redistribution, conditional erasure, or state deconstruction. We also generalize the model and method in several ways, one of which is a secret-sharing task, i.e., the case in which Alice's message should be secure from someone possessing only the $AB$ or $AE$ systems, but should be decodable by someone possessing all systems $A$, $B$, and $E$.

DOI: 10.1103/PhysRevLett.124.050503

*Introduction.*—This Letter shows that the optimal rate of a communication task, which we call the conditional one-time pad, is equal to a fundamental information quantity called the conditional quantum mutual information. To prove this statement, we operate in the regime of quantum Shannon theory [1–3], supposing that Alice and Bob possess a large number $n$ of copies of a quantum state $\rho_{ABE}$. We suppose that one party, Alice, has access to all of the $A$ systems and another party, Bob, has access to all of the $BE$ systems. We suppose that Bob's laboratory is divided into two parts, one of which is secure (the $B$ part) and the other which is insecure (the $E$ part) and accessible to an eavesdropper Eve. We also suppose that Alice and Bob are connected by an ideal quantum channel, but the eavesdropper Eve can observe any quantum system that is transmitted over the ideal channel if she so desires. The goal of a conditional quantum one-time pad protocol is for Alice to encode a message $m$ into her $A$ systems, in such a way that, if she sends her $A$ systems over the ideal quantum channel, then (i) Bob can decode the message $m$ reliably by performing a measurement on all of the $ABE$ systems, while (ii) an eavesdropper possessing the $AE$ systems has essentially no chance of determining the message $m$ if she tried to figure it out. We prove that the optimal asymptotic rate at which this task can be accomplished is equal to the conditional quantum mutual information of the state $\rho_{ABE}$, defined as

$$I(A;B|E)_\rho \equiv I(A;BE)_\rho - I(A;E)_\rho, \tag{1}$$

where the quantum mutual information of a state $\sigma_{FG}$ is defined as $I(F;G)_\sigma \equiv H(F)_\sigma + H(G)_\sigma - H(FG)_\sigma$, with $H(F)_\sigma \equiv -\mathrm{Tr}\{\sigma_F \log_2 \sigma_F\}$ denoting the quantum entropy of the reduced state $\sigma_F$.

Our main result thus gives an operational meaning to the conditional quantum mutual information (CQMI) that is conceptually different from those appearing in prior works [4–7]. CQMI has previously been interpreted as the optimal rate of quantum communication from a sender to a receiver to accomplish the task of state redistribution [4,5], in which the goal is for a sender to transmit one of her systems to a receiver who possesses a system correlated with the systems of the sender. CQMI has also been interpreted as the optimal rate of noise needed to accomplish the task of conditional erasure or state deconstruction [6,7], in which (briefly) the goal is to apply noise to the $AE$ systems of $\rho_{ABE}^{\otimes n}$ such that the resulting $A$ systems are locally recoverable from the $E$ systems alone, while the marginal state $\rho_{BE}^{\otimes n}$ is negligibly disturbed. Recently, the dynamic counterpart of CQMI has been interpreted as the optimal rate of

 

entanglement-assisted private communication over quantum broadcast channels [8], which is inspired by the conditional one-time pad protocol presented in this Letter.

The conditional mutual information is an information quantity that plays a central role in quantum information theory. The fact that it is non-negative for any quantum state is nontrivial and known as the strong subadditivity of quantum entropy [9,10]. The strong subadditivity inequality is at the core of nearly every coding theorem in quantum information theory (see, e.g., [1–3]). The CQMI is also the information quantity underlying an entanglement measure called squashed entanglement [11], a quantum correlation measure called quantum discord [12,13] (as shown in [14]), and a steering quantifier called intrinsic steerability [15]. The CQMI is also a witness of Markovianity in the sense that if $I(A;B|E)$ is small, then the correlations between systems $A$ and $B$ are mediated by the system $E$ via a recovery channel from $E$ to $AE$ [16]. Moreover, the CQMI of three regions with a nontrivial topology leads to the topological entanglement entropy of the system, which essentially characterizes irreducible many-body correlation [17–19]. The CQMI is thus an important information quantity to study quantum correlations in condensed matter systems (see, e.g., [20]). Furthermore, in the context of thermodynamics, the CQMI has been used to establish that the free fermion nonequilibrium steady state is an approximate quantum Markov chain [21]. The CQMI also plays an important role in high energy physics [22–24].

The basic intuition for the achievability of the conditional mutual information for the conditional one-time pad task is obtained by inspecting the expansion in (1) and is as follows: the authors of [25] showed that the quantum mutual information of a bipartite state is equal to the optimal rate of a task they called the (unconditional) quantum one-time pad. In our setting, the result of [25] implies that Alice can communicate a message secure against an eavesdropper, who can observe only the $A$ systems, such that Bob, in possession of the $BE$ systems, can decode it reliably, as long as the number of messages is $\approx nI(A;BE)_\rho$ bits. Here, we show that the message of Alice can be secured against an eavesdropper having access to both the $A$ and $E$ systems if Alice sacrifices $\approx nI(A;E)_\rho$ bits of the message, such that the total number of bits of the message is $\approx nI(A;BE)_\rho - nI(A;E)_\rho = nI(A;B|E)_\rho$, where we have employed (1). The main idea for a code construction to accomplish the above task is the same as that for the classical wiretap channel [26], which has been extended in a certain way to the quantum case in [27,28]. To prove the achievability part of the main result of our Letter, we use a coding technique developed in [29] (Sec. III A) and which was rediscovered shortly thereafter in [25] and later used in [30]. We also employ tools known as the quantum packing and covering lemmas (see, e.g., [3]). To establish optimality of the CQMI for the conditional one-time pad task, we employ entropy inequalities. We note that the aforementioned methods also lead to a proof of the main result of [31], which concerns a kind of quantum one-time pad protocol different from that developed in [25] or the present Letter.

A modification of the coding structure for the conditional one-time pad protocol allows us to establish that the following information quantity

$$I(A;BE)_\rho - \max\{I(A;B)_\rho, I(A;E)_\rho\} \tag{2}$$

of a tripartite state $\rho_{ABE}$ is an optimal achievable rate for a particular secret-sharing task that we call "information scrambling." In this modified task, we suppose that Alice, Bob, and Eve are three distinct parties. Alice's laboratory is distant from Bob's and Eve's, but we imagine that Bob's and Eve's laboratories are close together, and an ideal quantum channel connects Alice's laboratory to Bob's and Eve's. The goal of the information scrambling task is for Alice to communicate a message in such a way that it can be decoded only by someone who possesses all three $ABE$ systems. If someone possesses only the $AB$ systems or only the $AE$ systems, then such a person can figure out essentially nothing about the encoded message.

Our finding here shows that the quantity in (2) is an optimal achievable rate for information scrambling, such that the message is encoded in the nonlocal degrees of freedom (d.o.f.) of $\rho_{ABE}^{\otimes n}$ and cannot be decoded exclusively from the local d.o.f., which in this case are constituted by systems $AB$ or systems $AE$.

The rest of our Letter proceeds as follows. We first formally define the conditional one-time pad task. We then sketch a proof for the achievability part of our result. We finally discuss variations of the main task, such as the information scrambling task mentioned above and more general tasks, and then we conclude with a brief summary.

The Supplemental Material [32] provides a detailed proof of the achievability part of our main result. It also establishes the optimality part of our main result: that Alice cannot communicate at a rate higher than the conditional mutual information $I(A;B|E)$, while still satisfying the joint demands of reliable decoding for Bob (who gets the $ABE$ systems) and security against an eavesdropper who has access to the $AE$ systems. The optimality proof is based on entropy inequalities and identities.

*Conditional quantum one-time pad.*—We use notation and concepts standard in quantum information theory and point the reader to [3] for further background. Let $n, M \in \mathbb{N}$ and let $\varepsilon, \delta \in [0,1]$. An $(n, M, \varepsilon, \delta)$ conditional one-time pad protocol begins with Alice and Bob sharing $n$ copies of the state $\rho_{ABE}$, so that their state is $\rho_{ABE}^{\otimes n}$. As mentioned previously, Bob has access to the $BE$ systems, but we consider the $E$ systems to be insecure and jointly accessible by an eavesdropper. Alice and Bob are connected by an ideal quantum channel, which Eve has access to as well. [Later, we argue that it suffices for Alice and Bob to use

only $\approx nH(A)_\rho$ ideal qubit channels, but for now, we suppose that the ideal quantum channel can transmit as many qubits as desired.] At the beginning of the protocol, Alice picks a message $m \in \{1, \ldots, M\}$ and applies an encoding channel $\mathcal{E}^m_{A^n \to A'}$ to the $A^n$ systems of $\rho^{\otimes n}_{ABE}$, leading to the state $\omega^m_{A'B^nE^n} \equiv \mathcal{E}^m_{A^n \to A'}(\rho^{\otimes n}_{ABE})$. She transmits the system $A'$ of $\omega^m_{A'B^nE^n}$ over the ideal quantum channel. Bob applies a decoding positive operator-valued measure $\{\Lambda^m_{A'B^nE^n}\}_m$ to the systems $A'B^nE^n$ of $\omega^m_{A'B^nE^n}$ in order to figure out which message was transmitted. The protocol is $\varepsilon$ reliable if Bob can determine the message $m$ with probability not smaller than $1 - \varepsilon$,

$$\forall\ m\colon \operatorname{Tr}\{\Lambda^m_{A'B^nE^n}\omega^m_{A'B^nE^n}\} \geq 1 - \varepsilon. \tag{3}$$

The protocol is $\delta$ secure if the reduced state $\omega^m_{A'E^n}$ on systems $A'E^n$ is nearly indistinguishable from a constant state $\sigma_{A'E^n}$ independent of the message $m$,

$$\forall\ m\colon \frac{1}{2}\|\omega^m_{A'E^n} - \sigma_{A'E^n}\|_1 \leq \delta, \tag{4}$$

where we have employed the normalized trace distance.

We say that a rate $R$ is achievable for the conditional quantum one-time pad if for all $\varepsilon, \delta \in (0,1)$, $\gamma > 0$, and sufficiently large $n$, there exists an $(n, 2^{n[R-\gamma]}, \varepsilon, \delta)$ conditional one-time pad protocol of the above form. The conditional one-time pad capacity of a state $\rho_{ABE}$ is equal to the supremum of all achievable rates.

*Achievability of CQMI for conditional one-time pad.*—Here we mostly sketch an argument that the CQMI $I(A;B|E)_\rho$ is a lower bound on the conditional one-time pad capacity of $\rho_{ABE}$, while the Supplemental Material [32] contains a detailed proof. First, consider the reduced state $\rho_A$ and a spectral decomposition for it as $\rho_A = \sum_x p_X(x)|x\rangle\langle x|_A$, where $p_X$ is a probability distribution and $\{|x\rangle_A\}_x$ is an orthonormal basis. Let $|\phi\rangle_{AR} = \sum_x \sqrt{p_X(x)}|x\rangle_A|x\rangle_R$ be a purification of $\rho_A$. Let $|\psi\rangle_{ABEF}$ denote a purification of $\rho_{ABE}$, with $F$ playing the role of a purifying system. Since all purifications are related by an isometry acting on the purifying system, there exists an isometry $U_{R\to BEF}$ such that $U_{R\to BEF}|\phi\rangle_{AR} = |\psi\rangle_{ABEF}$. Applying the isometry $U_{R\to BEF}$ followed by a partial trace over $F$ can be thought of as a channel $\mathcal{N}_{R\to BE}$ that realizes the state $\rho_{ABE}$ as $\mathcal{N}_{R\to BE}(\phi_{AR}) = \rho_{ABE}$. Similarly, if we apply the isometry $U_{R\to BEF}$ and trace over $FB$, then this is a channel $\mathcal{M}_{R\to E}$ that realizes the reduced state $\rho_{AE}$ as $\mathcal{M}_{R\to E}(\phi_{AR}) = \rho_{AE}$.

If we take $n$ copies of $\rho_{ABE}$, then the state $\rho^{\otimes n}_{ABE}$ can be thought of as the following state: $\mathcal{N}^{\otimes n}_{R\to BE}(\phi^{\otimes n}_{AR})$. The pure state $|\phi\rangle^{\otimes n}_{AR}$ admits an information-theoretic type decomposition of the following form: $|\phi\rangle^{\otimes n}_{AR} = \sum_t \sqrt{p(t)}|\Phi_t\rangle_{A^nR^n}$, where the label $t$ indicates a type class and $|\Phi_t\rangle_{A^nR^n}$ is a maximally entangled state of Schmidt rank $d_t$ with support on the type class subspace labeled by $t$. We can then consider forming encoding unitaries out of the generalized Pauli shift and phase-shift operators

$$V_{A^n}(x_t, z_t) = X_{A^n}(x_t)Z_{A^n}(z_t), \tag{5}$$

which act on a given type class subspace $t$ and where $x_t, z_t \in \{0, \ldots, d_t - 1\}$. The overall encoding unitary allows for an additional phase $(-1)^{b_t}$ for $b_t \in \{0,1\}$ and has the form

$$U_{A^n}(s) = \bigoplus_t (-1)^{b_t} V_{A^n}(x_t, z_t), \tag{6}$$

where $s$ is a vector $[(b_t, x_t, z_t)]_t$.

The coding scheme is based on random coding, as is usually the case in quantum Shannon theory, and works as follows. Let $M, K \in \mathbb{N}$. Alice has a message variable $m \in \{1, \ldots, M\}$ and a local key variable $k \in \{1, \ldots, K\}$. For each pair $(m,k)$, Alice picks a vector $s$, of the form described previously, uniformly at random and labels it as $s(m,k)$. The set $\mathcal{C} = \{s(m,k)\}_{m,k}$ constitutes the code, and observe that it is initially selected randomly. If Alice wishes to send message $m$, then she picks $k$ uniformly at random from $k \in \{1, \ldots, K\}$, applies the encoding unitary $U_{A^n}[s(m,k)]$ to the state $\rho^{\otimes n}_{ABE}$ and sends the $A^n$ systems to Bob. Bob's goal is to decode both the message variable $m$ and the local key variable $k$. Based on the packing lemma, it follows that if $\log_2 MK \approx nI(A;BE)_\rho$, then there is a decoding measurement $\{\Lambda^{m,k}_{A^nB^nE^n}\}$ for Bob, constructed from typical projectors and corresponding to a particular selected code $\mathcal{C}$, such that

$$\mathbb{E}_{\mathcal{C}}\left\{\frac{1}{MK}\sum_{m,k}\operatorname{Tr}\{\Lambda^{m,k}_{A^nB^nE^n}U_{A^n}[S(m,k)]\rho^{\otimes n}_{ABE}U^\dagger_{A^n}[S(m,k)]\}\right\} \geq 1 - \varepsilon, \tag{7}$$

for all $\varepsilon \in (0,1)$ and sufficiently large $n$, and where the expectation is with respect to the random choice of code $\mathcal{C}$. On the other hand, from the perspective of someone who does not know the choice of $k$ and who does not have access to the systems $B^n$, the state has the following form:

$$\tau^m_{A^nE^n} \equiv \frac{1}{K}\sum_{k=1}^{K} U_{A^n}[s(m,k)]\rho^{\otimes n}_{AE}U^\dagger_{A^n}[s(m,k)]. \tag{8}$$

The quantum covering lemma and the properties of typical projectors guarantee that

$$\Pr_{\mathcal{C}}\{\|\tau^m_{A^nE^n} - \bar{\tau}_{A^nE^n}\|_1 \leq \delta + 4\sqrt{\delta} + 24\sqrt[4]{\delta}\} \geq 1 - 2D\exp\left(-\frac{\delta^3 K 2^{-n[I(A;E)_\rho + \delta']}}{4}\right), \tag{9}$$

where $D$ is a parameter that is no more than exponential in $n$, $\delta' > 0$ is a small constant, and

$$\bar{\tau}_{A^nE^n} \equiv \mathbb{E}_S\{U_{A^n}(S)\rho_{AE}^{\otimes n}U_{A^n}^\dagger(S)\}. \tag{10}$$

Thus, as long as we pick $\log_2 K \approx nI(A;E)_\rho$, then there is an extremely good chance that the state $\tau_{A^nE^n}^m$ will be nearly indistinguishable from the average state $\bar{\tau}_{A^nE^n}$. Now, we can define the event $E_0$ to be the event that Bob's measurement decodes with high average success probability and the event $E_m$ to be the event that $\|\tau_{A^nE^n}^m - \bar{\tau}_{A^nE^n}\|_1$ is small. The union bound of probability theory then guarantees that there is a nonzero probability for there to be a code $\{s(m,k)\}_{m,k}$ such that the average success probability of Bob's decoder is arbitrarily high and $\|\tau_{A^nE^n}^m - \bar{\tau}_{A^nE^n}\|_1$ is arbitrarily small for all $m$, with these statements holding for sufficiently large $n$. So this means that such a code $\{s(m,k)\}_{m,k}$ exists. A final "expurgation" argument guarantees that Bob can decode each $m$ and $k$ with arbitrarily high probability and that $\|\tau_{A^nE^n}^m - \bar{\tau}_{A^nE^n}\|_1$ is arbitrarily small for all $m$. Therefore, the number of bits that Alice can communicate securely is thus

$$\begin{aligned}\log_2 M &= \log_2 MK - \log_2 K \\ &\approx nI(A;BE)_\rho - nI(A;E)_\rho \\ &= nI(A;B|E)_\rho,\end{aligned} \tag{11}$$

so that $I(A;B|E)_\rho$ is an achievable rate. This concludes the achievability proof sketch. As indicated previously, the optimality proof is given in the Supplemental Material [32].

We note that it actually suffices to use $\approx nH(A)_\rho$ noiseless qubit channels for the communication of the $A$ systems, rather than $n\log|A|$ noiseless qubit channels. This is because Alice can perform Schumacher compression [33] of her $A^n$ systems before transmitting them, and the structure of the encoding unitaries is such that this can be done regardless of which message is being transmitted (see the discussion at the end of [3], Sec. 22.3). The Schumacher compression causes a negligible disturbance to each of the states that is transmitted.

*Conditional one-time pad of a quantum message.*—We note that it is possible to define a conditional quantum one-time pad of a quantum message, in which the goal is to transmit one share $\hat{M}$ of a quantum state $|\varphi\rangle_{M''\hat{M}}$ securely in such a way that Bob, possessing systems $A'B^nE^n$, can decode the quantum message in $\hat{M}$, while someone possessing the systems $A'E^n$ cannot learn anything about the quantum system $\hat{M}$. Our result here is that $I(A;B|E)_\rho/2$ is the optimal rate for this task of a conditional one-time pad of a quantum message. The optimality proof is nearly identical to the optimality proof given previously, except that we start with the assumption that the initial state $|\varphi\rangle_{M''\hat{M}}$ is a maximally entangled state $|\Phi\rangle_{M''\hat{M}}$, such that the quantum information in system $\hat{M}$ can be decoded well. Then, the proof starts with the condition that $\log_2 M = I(M'';\hat{M})_\Phi/2$ and proceeds identically from there. For the achievability part, we perform a coherent version of the above protocol, as reviewed in [3] (Sec. 22.4), and we find that it generates coherent bits [34], which are secure from someone possessing the $A^nE^n$ systems, at a rate equal to $I(A;B|E)_\rho$. By the coherent communication identity from [34], it follows that qubits can be transmitted securely at a rate equal to $I(A;B|E)_\rho/2$.

*Generalizations.*—We note that the coding scheme outlined above in the achievability proof can be generalized in several interesting ways. Suppose that Alice shares a state with "many Bobs," i.e., one of the form $\rho_{AB_1,\ldots,B_\ell}$ for some positive integer $\ell \geq 2$. Then Alice might wish to encode a message $m$ in her $A$ systems of $\rho_{AB_1,\ldots,B_\ell}^{\otimes n}$ in such a way that only someone possessing all of the systems $AB_1,\ldots,B_\ell$ would be able to decode it, but someone possessing system $A$ and some subset $\mathcal{B}_i \in \{B_1,\ldots,B_\ell\}$ would not be able to determine anything about the message $m$. Alice might wish to protect the message against several different subsets $\mathcal{B}_i$, for $i \in \{1,\ldots,p\}$, as in secret sharing. Then we could structure a coding scheme similar to our achievability proof to have a message variable $m \in \{1,\ldots,M\}$ and a local key variable $k \in \{1,\ldots,K\}$, such that

$$\log_2 MK \approx nI(A;B_1,\ldots,B_\ell), \tag{12}$$

$$\log_2 K \approx n[\max\{I(A;\mathcal{B}_1),\ldots,I(A;\mathcal{B}_p)\}]. \tag{13}$$

Given that

$$I(A;B_1,\ldots,B_\ell)_\rho - \max\{I(A;\mathcal{B}_1)_\rho,\ldots,I(A;\mathcal{B}_p)_\rho\} \tag{14}$$

is always non-negative, the coding scheme guarantees that this information difference is an achievable rate that accomplishes the desired task. We note that the secret-sharing task discussed above is different from the previously considered protocols in [35,36] and references therein.

A particular case of interest is the scenario mentioned earlier in this Letter and which we called information scrambling. There, Alice, Bob, and Eve share a state $\rho_{ABE}$, and the goal is for Alice to encode a message in the $A$ system such that someone possessing the $ABE$ systems can decode it, but someone possessing the $AB$ systems or the $AE$ systems cannot determine anything about the message $m$ (i.e., the message $m$ has been scrambled in the nonlocal d.o.f. of the state $\rho_{ABE}$ and is not available in $\rho_{AB}$ or $\rho_{AE}$). According to the above reasoning, an achievable rate for this task is the information quantity $I(A;BE)_\rho - \max\{I(A;B)_\rho, I(A;E)_\rho\}$. This rate is also optimal.

We note also that our methods give a concrete and transparent approach to prove the results of [31], as discussed in the Supplemental Material [32]. In particular, we have established an information-theoretic converse of that result using entropy identities and inequalities along the lines presented previously, and the achievability part of that result can be accomplished by using the encoding unitaries discussed earlier, along with the quantum packing and covering lemmas.

Our operational interpretation of the conditional mutual information also leads to an interesting operational interpretation of the squashed entanglement of a bipartite state $\rho_{AB}$: we can consider squashed entanglement to be the optimal rate of secure communication in the conditional one-time pad if an eavesdropper has the $E$ system of the worst possible extension $\rho_{ABE}$ of the state $\rho_{AB}$, given that squashed entanglement is defined as $1/2 \inf_{\rho_{ABE}}\{I(A;B|E)_\rho : \mathrm{Tr}_E\{\rho_{ABE}\} = \rho_{AB}\}$ [11]. This is analogous to the interpretations from [37] and the follow-up one in [7].

*Conclusion.*—In this Letter, we proved that the conditional mutual information $I(A;B|E)_\rho$ of a tripartite state $\rho_{ABE}$ is equal to the optimal rate of secure communication for a task that we call the conditional one-time pad. This represents a fundamentally different operational interpretation of conditional mutual information that is conceptually simple at the same time. Furthermore, due to the fact that the optimal rate is given by conditional mutual information, the conditional one-time pad is an example of a communication task in which non-Markov quantum states are used as a resource [38,39]. In the continuing quest to understand a refined generalization of conditional mutual information, as has been attempted previously in [40–43], the protocol of a conditional one-time pad might end up being helpful in this effort.

We thank David Ding, Rahul Jain, and Andreas Winter for discussions related to the topic of this Letter. M. M. W. acknowledges support from the Office of Naval Research and the National Science Foundation. K. S. acknowledges support from the Department of Physics and Astronomy at LSU and the National Science Foundation under Grant No. 1714215.

[1] M. Hayashi, *Quantum Information: An Introduction* (Springer, New York, 2006).
[2] A. S. Holevo, *Quantum systems, channels, information*, de Gruyter Studies in Mathematical Physics (Book 16) (de Gruyter, Berlin, 2012).
[3] M. M. Wilde, *Quantum Information Theory*, 2nd ed. (Cambridge University Press, Cambridge, England, 2017).
[4] I. Devetak and J. Yard, Exact Cost of Redistributing Multipartite Quantum States, Phys. Rev. Lett. **100**, 230501 (2008).
[5] J. Yard and I. Devetak, Optimal quantum source coding with quantum side information at the encoder and decoder, IEEE Trans. Inf. Theory **55**, 5339 (2009).
[6] M. Berta, F. G. S. L. Brandao, C. Majenz, and M. M. Wilde, Conditional Decoupling of Quantum Information, Phys. Rev. Lett. **121**, 040504 (2018).
[7] M. Berta, F. G. S. L. Brandao, C. Majenz, and M. M. Wilde, Deconstruction and conditional erasure of quantum correlations, Phys. Rev. A **98**, 042320 (2018).
[8] H. Qi, K. Sharma, and M. M. Wilde, Entanglement-assisted private communication over quantum broadcast channels, J. Phys. A **51**, 374001 (2018).
[9] E. H. Lieb and M. B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy, J. Math. Phys. **14**, 1938 (1973).
[10] E. H. Lieb and M. B. Ruskai, A Fundamental Property of Quantum-Mechanical Entropy, Phys. Rev. Lett. **30**, 434 (1973).
[11] M. Christandl and A. Winter, Squashed entanglement—an additive entanglement measure, J. Math. Phys. **45**, 829 (2004).
[12] W. H. Zurek, Einselection and decoherence from an information theory perspective, Ann. Phys. **9**, 855 (2000).
[13] H. Ollivier and W. H. Zurek, Quantum discord: A measure of the quantumness of correlations, Phys. Rev. Lett. **88**, 017901 (2001).
[14] M. Piani, Problem with geometric discord, Phys. Rev. A **86**, 034101 (2012).
[15] E. Kaur, X. Wang, and M. M. Wilde, Conditional mutual information and quantum steering, Phys. Rev. A **96**, 022332 (2017).
[16] O. Fawzi and R. Renner, Quantum conditional mutual information and approximate Markov chains, Commun. Math. Phys. **340**, 575 (2015).
[17] A. Kitaev and J. Preskill, Topological Entanglement Entropy, Phys. Rev. Lett. **96**, 110404 (2006).
[18] M. Levin and X.-G. Wen, Detecting Topological Order in a Ground State Wave Function, Phys. Rev. Lett. **96**, 110405 (2006).
[19] I. H. Kim, Perturbative analysis of topological entanglement entropy from conditional independence, Phys. Rev. B **86**, 245116 (2012).
[20] B. Zeng, X. Chen, D.-L. Zhou, and X.-G. Wen, Quantum information meets quantum matter, arXiv: 1508.02595.
[21] R. Mahajan, C. Daniel Freeman, S. Mumford, N. Tubman, and B. Swingle, Entanglement structure of non-equilibrium steady states, arXiv:1608.05074.
[22] B. Czech, L. Lamprou, S. McCandlish, and J. Sully, Integral geometry and holography, J. High Energy Phys. 10 (2015) 175.
[23] D. Ding, P. Hayden, and M. Walter, Conditional mutual information of bipartite unitaries and scrambling, J. High Energy Phys. 20 (2016) 145.
[24] F. Pastawski, J. Eisert, and H. Wilming, Towards Holography via Quantum Source-Channel Codes, Phys. Rev. Lett. **119**, 020501 (2017).
[25] B. Schumacher and M. D. Westmoreland, Quantum mutual information and the one-time pad, Phys. Rev. A **74**, 042305 (2006).

[26] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 1355 (1975).
[27] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, IEEE Trans. Inf. Theory **51**, 44 (2005).
[28] N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, Probl. Inf. Transm. **40**, 318 (2004).
[29] M.-H. Hsieh, I. Devetak, and A. Winter, Entanglement-assisted capacity of quantum multiple-access channels, IEEE Trans. Inf. Theory **54**, 3078 (2008).
[30] N. Datta, M. Tomamichel, and M. M. Wilde, On the second-order asymptotics for entanglement-assisted communication, Quantum Inf. Process. **15**, 2569 (2016).
[31] F. G. S. L. Brandao and J. Oppenheim, Quantum One-Time Pad in the Presence of an Eavesdropper, Phys. Rev. Lett. **108**, 040504 (2012).
[32] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.124.050503 for detailed mathematical proofs of the claims in the main text.
[33] B. Schumacher, Quantum coding, Phys. Rev. A **51**, 2738 (1995).
[34] A. Harrow, Coherent Communication of Classical Messages, Phys. Rev. Lett. **92**, 097902 (2004).
[35] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).
[36] K. Senthoor and P. K. Sarvepalli, Communication efficient quantum secret sharing, Phys. Rev. A **100**, 052313 (2019).
[37] J. Oppenheim, A paradigm for entanglement theory based on quantum communication, arXiv:0801.0458.
[38] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Structure of states which satisfy strong subadditivity of quantum entropy with equality, Commun. Math. Phys. **246**, 359 (2004).
[39] E. Wakakuwa, Operational resource theory of non-Markovianity, arXiv:1709.07248.
[40] M. Berta, K. Seshadreesan, and M. M. Wilde, Rényi generalizations of the conditional quantum mutual information, J. Math. Phys. **56**, 022205 (2015).
[41] N. Datta, M.-H. Hsieh, and J. Oppenheim, An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution, J. Math. Phys. **57**, 052203 (2016).
[42] M. Berta, M. Christandl, and D. Touchette, Smooth entropy bounds on one-shot quantum state redistribution, IEEE Trans. Inf. Theory **62**, 1425 (2016).
[43] A. Anshu, V. K. Devabathini, and R. Jain, Quantum Communication Using Coherent Rejection Sampling, Phys. Rev. Lett. **119**, 120506 (2017).