

## MIT Open Access Articles

*Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement*

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

**Citation:** Zhuang, Quntao, Elton Yechao Zhu, and Peter W. Shor. "Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement." *Physical Review Letters* 118.20 (2017): n. pag. © 2017 American Physical Society

**As Published:** <http://dx.doi.org/10.1103/PhysRevLett.118.200503>

**Publisher:** American Physical Society

**Persistent URL:** <http://hdl.handle.net/1721.1/109828>

**Version:** Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

**Terms of Use:** Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.



# Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement

Quntao Zhuang,<sup>1,2,\*</sup> Elton Yechao Zhu,<sup>1,3</sup> and Peter W. Shor<sup>3,4</sup>

<sup>1</sup>*Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

<sup>2</sup>*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

<sup>3</sup>*Center For Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

<sup>4</sup>*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 14 October 2016; published 19 May 2017)

We give a capacity formula for the classical information transmission over a noisy quantum channel, with separable encoding by the sender and limited resources provided by the receiver’s preshared ancilla. Instead of a pure state, we consider the signal-ancilla pair in a mixed state, purified by a “witness.” Thus, the signal-witness correlation limits the resource available from the signal-ancilla correlation. Our formula characterizes the utility of different forms of resources, including noisy or limited entanglement assistance, for classical communication. With separable encoding, the sender’s signals across multiple channel uses are still allowed to be entangled, yet our capacity formula is additive. In particular, for generalized covariant channels, our capacity formula has a simple closed form. Moreover, our additive capacity formula upper bounds the general coherent attack’s information gain in various two-way quantum key distribution protocols. For Gaussian protocols, the additivity of the formula indicates that the collective Gaussian attack is the most powerful.

DOI: 10.1103/PhysRevLett.118.200503

Communication channels model the physical medium for information transmission between the sender (Alice) and the receiver (Bob). Classical information theory [1,2] says that a channel is essentially characterized by a single quantity—the (classical) channel capacity, i.e., its maximum (classical) information transmission rate. However, quantum channels [3] can transmit information beyond the classical. Formally, a (memoryless) quantum channel is a time-invariant completely positive trace preserving (CPTP) linear map between quantum states. Various types of information lead to various capacities, e.g., classical capacity  $\mathcal{C}$  [4,5] for classical information transmission encoded in quantum states, and quantum capacity  $\mathcal{Q}$  [6–8] for quantum information transmission. For both cases, implicit constraints on the input Hilbert space, e.g., fixed dimension or energy, quantify the resources. Resources can also be in the form of assistance: given unlimited entanglement, one has the entanglement-assisted classical capacity  $\mathcal{C}_E$  [9]. References [10,11] provide a capacity formula for the trade-off of classical and quantum information transmission and entanglement generation (or consumption).

With the trade-off capacity formula in hand, it appears that the picture of communication over quantum channels is complete. However, our understanding about the trade-off is plagued by the “nonadditivity” issue [3], best illustrated by the example of  $\mathcal{C}$ . The Holevo-Schumacher-Westmoreland (HSW) theorem [4,5] gives the one-shot capacity  $\mathcal{C}^{(1)}(\Psi)$  of channel  $\Psi$ , which assumes product-state input in multiple channel uses. Consider the tensor product channel  $\Psi^{\otimes M}$ . It may have one-shot capacity  $\mathcal{C}^{(1)}(\Psi^{\otimes M}) > M\mathcal{C}^{(1)}(\Psi)$  since it allows the input state of  $\Psi^{\otimes M}$  to be entangled across the  $M$  channel uses of  $\Psi$  (the  $M$  shot).  $\mathcal{C}(\Psi)$  is then given by the

regularized expression as  $\lim_{M \rightarrow \infty} \mathcal{C}^{(1)}(\Psi^{\otimes M})/M$ , which is difficult to calculate since the dimension of the input states of  $\Psi^{\otimes M}$  is exponential in  $M$ . If we have the additivity property  $\mathcal{C}^{(1)}(\Psi^{\otimes M}) = M\mathcal{C}^{(1)}(\Psi)$ , the formula of the capacity is greatly simplified, i.e.,  $\mathcal{C}(\Psi) = \mathcal{C}^{(1)}(\Psi)$ . However, both  $\mathcal{C}$  [12] and  $\mathcal{Q}$  [13] are known to be nonadditive. Without additivity, quantification of the trade-off is, in general, infeasible.

An exception is the (unlimited) entanglement-assisted classical capacity  $\mathcal{C}_E$  [9]. Since it has the form of quantum mutual information [14,15],  $\mathcal{C}_E$  is additive [9,16]. One immediately hopes that the additivity can be extended to classical communication assisted by imperfect entanglement since entanglement is fragile. Many such scenarios have been explored, e.g., superdense coding (SC) over a noisy channel assisted by noisy entanglement [17–22], a noiseless channel assisted by a noisy entanglement [23], and noisy channels assisted by limited pure state entanglement [24]. However, all of the results are, in general, nonadditive, as expected [25], since the above imperfect scenarios include the case with zero entanglement assistance—the nonadditive  $\mathcal{C}$ .

In this Letter, we obtain an additive classical capacity formula for a noisy quantum channel  $\Psi$  assisted by resources such as noisy entanglement. In the most general formalism, Alice sends an optimized ensemble of (possibly mixed) states  $\rho_{SE}^i$  to Bob, with a signal  $S$  through the channel  $\Psi$  and an ancilla  $E$  preshared through the identity channel  $\mathcal{I}$ . Each  $\rho_{SE}^i$  is constrained by some resource, e.g., by the entanglement between  $S$  and  $E$ . Here, similar to SC, we consider a restricted scenario of two-step signal preparation—resource distribution and encoding (see Fig. 1). Each  $\rho_{SE}^i$  is obtained by encoding on  $S$  from a certain state  $\rho_{SE}$ . Moreover, the

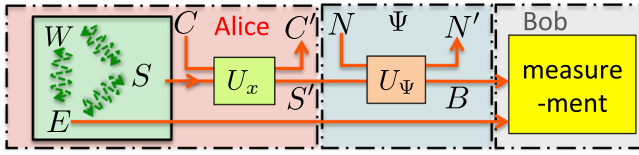


FIG. 1. Schematic of a single channel use.

resource is constrained by the correlation between  $S$  and a “witness”  $W$ —a purification of  $(S, E)$ .

In the resource distribution step,  $W$  is made inaccessible to both Alice and Bob. Instead of explicitly quantifying the available resource (between  $S$  and  $E$ ) as in Ref. [24], we describe the resource implicitly by quantifying the correlation between  $S$  and  $W$ —the unavailable resource—by  $K \geq 1$  inequalities

$$Q_k(\rho_{SW}) \geq y_k, \quad k \in [1, K] \quad (1)$$

on  $\rho_{SW}$ , where each  $Q_k(\cdot)$  is a function on bipartite states. We denote Eq. (1) by  $\mathbf{Q}(\rho_{SW}) \geq \mathbf{y}$ . While Refs. [9,24] considered only pure state entanglement, the form of resources in our case can be arbitrary by choosing different  $Q_k(\cdot)$ 's, e.g., noisy entanglement, cross-correlation [26–28], or quantum discord [29]. However, entanglement measures are more meaningful to consider because (1) they respect the unitary equivalence of the purification  $W$ , and (2) constraints on the entanglement between  $S$  and  $W$  lead to constraints on the entanglement between  $S$  and  $E$ —a property known as monogamy [26,30–32].

Here, we give an example of Eq. (1)—the quantum mutual information [14,15]  $I(S:W) \geq y$ ,  $y \in [0, 2\log_2 d]$  for qudit  $S$ . When  $y = 2\log_2 d$ ,  $\rho_{SW}$  is pure and  $E$  and  $S$  are thus uncorrelated. Since entanglement across multiple channel uses is also excluded here, the additivity of our capacity does not contradict the nonadditivity of  $\mathcal{C}$ . When  $y = 0$ , the optimum has  $W$  and  $S$  in a product state and  $\rho_{SE}$  pure, as in Ref. [24]. This gives the case of Ref. [9]. For intermediate values of  $y$ ,  $\rho_{SE}$  is mixed and signals across multiple channel uses can be entangled; thus, the additivity of our capacity is nontrivial. This example illustrates the desired property of function  $Q_k(\cdot)$ —the correlation between  $S$  and  $W$  increases when  $Q_k(\cdot)$  increases, with the two end points corresponding to  $\rho_{SW}$  pure and product states.

In the encoding step, Alice performs a quantum operation  $\varepsilon_x$  [33] with probability  $P_X(x)$  on  $S$  to encode a message  $x$ , resulting in  $S'$  as the input to  $\Psi$ . In multiple channel uses, the encoding is a set of classically correlated separate operations—local operations and classical communication (LOCC) [34].  $\rho_S$  is constrained to be in  $\mathcal{B}(\mathcal{H}_S)$ —density operators on Hilbert space  $\mathcal{H}_S$ —and the encoding is constrained to be in a certain set, i.e.,  $(P_X(\cdot), \varepsilon) \in \mathbb{G}$ . Upon receiving  $\Psi$ 's output  $B$ , Bob makes a joint measurement on  $B$  and  $E$  to determine  $x$ . The capacity of the above scenario is given as follows.

**Theorem 1.**—Classical capacity with limited resources and LOCC encoding. With resources constrained by  $V \equiv \{(P_X(\cdot), \varepsilon) \in \mathbb{G}, \rho_S \in \mathcal{B}(\mathcal{H}_S), \mathbf{Q}(\rho_{SW}) \geq \mathbf{y}\}$ , supposing that  $\mathbb{G}$  allows arbitrary phase flips, the classical capacity of the quantum channel  $\Psi$  is

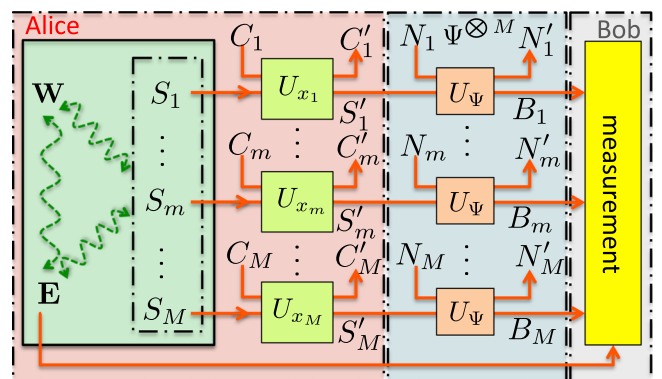
$$\chi_L(\Psi) = \max_V S \left( \sum_x P_X(x) \Psi \circ \varepsilon_x[\rho_S] \right) - \sum_x P_X(x) E_{\Phi_{\varepsilon_x} \otimes I}[\rho_{SW}], \quad (2)$$

where  $\Phi_{\varepsilon_x}$  is the complementary quantum operation to  $\Psi \circ \varepsilon_x$ , the entropy gain  $E_\phi$  [35] of a CPTP map  $\phi$  on state  $\rho$  is defined by  $E_\phi[\rho] \equiv S(\phi[\rho]) - S(\rho)$ , and the maximization is over the encoding  $(P_X(\cdot), \varepsilon)$  and  $\rho_{SW}$ . Equation (2) is additive when the constraint has a separable form on each channel use and the encoding is LOCC.

We make two clarifications about the theorem. First, a schematic of  $\Phi_{\varepsilon_x}$  is given in Fig. 1. The encoding CPTP map  $\varepsilon_x$  is extended to a unitary operation  $U_x$  on  $S$  and an environment  $C$  in the vacuum state, resulting in  $S'$  in state  $\varepsilon_x[\rho_S]$  and  $C'$ .  $S'$  is sent to Bob through  $\Psi$ , whose Stinespring dilation is a unitary operation  $U_\Psi$  on  $S'$  and an environment  $N$  in the vacuum state, producing  $B$  for Bob and an environment  $N'$ . We define  $\Phi_{\varepsilon_x}$  as the CPTP map from  $\rho_S$  to  $\rho_{N'C'}^{(x)}$ , given  $\varepsilon_x$ . Second, by a separable form of constraints on each channel use, we mean constraints expressed by a set of inequalities, each involving states only in a single channel use [see Eq. (3)].

We have given our main result, Theorem 1, in a single channel use scenario. In order to prove additivity, we need to consider multiple channel uses (Fig. 2). Before that, we will make a few more comments. First, for generalized covariant channels, including covariant [36] channels and Weyl-covariant [37] channels, Eq. (2) can be simplified. More details are given in Corollary 2.

Next, we discuss the relationships with other capacities. If  $\mathbb{G}$  allows arbitrary encoding, one can choose to replace the original signal state with an optimal set of

FIG. 2. Schematic of  $M$  channel uses.

pure states, which guarantees that  $\chi_L \geq \mathcal{C}^{(1)}$ . With all encoding operations unitary, we obtain another lower bound,  $\chi_L^{\mathcal{I}}$ . When the  $y_k$ 's are at maximum,  $\chi_L = \mathcal{C}^{(1)}$ ; when the  $y_k$ 's are at minimum,  $\chi_L = \mathcal{C}_E$ . Note that when arbitrary phase flips are not allowed, the rhs of Eq. (2) upper bounds  $\chi_L$  and it is still additive, while  $\chi_L^{\mathcal{I}}$  might not be. We also point out that Ref. [24] and our result are different in the sense that neither of them can be reduced to the other. If the  $\varepsilon_x$ 's are not unitary, then the environment  $\mathcal{C}'$  is never sent to Bob. This is different from Ref. [24], where all purification of the signal is sent to Bob. If we require  $\varepsilon_x$ 's to be unitary, the input states in Ref. [24] do not need to be related by unitary operations, unlike our scenario [42].

Finally, we emphasize the application of our results. Our capacity formula provides an additive upper bound for the general eavesdropper's coherent attack [38–41] information gain for various two-way quantum key distribution (TW-QKD) protocols [28,51–60]. The constraint in Eq. (1) appears in security checking of TW-QKD protocols, where two parties verify properties of their state  $\rho_{SW}$ 's to constrain the eavesdropper's benefit from  $(S, E)$  (details in Corollary 3). Obtaining upper bounds for eavesdroppers in TW-QKD is more complicated than for one-way protocols due to the simultaneous attack on both the forward and backward channels. Only special attacks [52–57] or general attacks in the absence of loss and noise [58–60] have been considered. Despite this difficulty, a TW-QKD protocol called “floodlight QKD” was recently shown to have the potential of reaching an unprecedented secret key rate (SKR) [28,51]. Consequently, our upper bound is crucial for a high-SKR QKD.

*Multiple channel uses.*—Now we extend the single channel use scenario to  $M \geq 2$  channel uses in a nontrivial way that allows an additive classical capacity (Fig. 2). We keep the same notation for all of the modes except for adding a subscript to index the channel use. For convenience, we introduce the short notation  $\mathbf{S} = \{S_m : m \in [1, M]\}$  for input signals, with its states  $\rho_S \in \mathcal{B}(\mathcal{H}_S^{\otimes M})$ , and also  $\mathbf{W}$  as an arbitrary inaccessible witness and  $\mathbf{E}$  as an arbitrary ancilla. Then the initial state  $(\mathbf{S}, \mathbf{E}, \mathbf{W})$  is pure.

The allowed encoding operations in  $M$  channel uses are LOCC; i.e., they can be classically correlated, satisfying a joint distribution  $P_{\mathbf{X}}(\cdot)$ , where  $\mathbf{X} = (X_1, \dots, X_M)$  denotes the symbols in  $M$  channel uses. Conditioned on the message  $\mathbf{x} \equiv (x_1, \dots, x_M)$ , the encoding operation is  $\varepsilon_{\mathbf{x}} = \otimes_{m=1}^M \varepsilon_{x_m}$ . Again, the CPTP map  $\varepsilon_{\mathbf{x}}$  can be extended as a unitary operation  $\otimes_{m=1}^M U_{x_m}$ , which takes in the signals  $\mathbf{S}$  and the environment  $\mathbf{C} = \{C_m : m \in [1, M]\}$  in the vacuum state and produces the encoded signals  $\mathbf{S}' = \{S'_m : m \in [1, M]\}$  and the environment  $\mathbf{C}' = \{C'_m : m \in [1, M]\}$ . Each encoding operation  $\varepsilon_{x_m}$ , with its own marginal distribution  $P_{X_m}(\cdot)$ , is still constrained to be inside the same set  $\mathbb{G}$ .

After the encoding step, each  $S'_m$  is sent through  $\Psi$  separately. The Stinespring dilation of  $\Psi^{\otimes M}$  takes  $\mathbf{S}'$  and an environment  $\mathbf{N} = \{N_m : m \in [1, M]\}$  in the vacuum state

as inputs and outputs  $\mathbf{B} = \{B_m : m \in [1, M]\}$  for Bob and the environment  $\mathbf{N}' = \{N'_m : m \in [1, M]\}$ . Bob decodes the message by joint measurements on  $(\mathbf{B}, \mathbf{E})$ , where the preshared ancilla  $\mathbf{E}$  provides resources quantified by the constraint  $\mathbf{Q}(\rho_{S_m W_m}) \geq \mathbf{y}$ ,  $m \in [1, M]$ . One can also consider that  $M$  witnesses  $\mathbf{W} = \{W_m : m \in [1, M]\}$ , with constraints on each signal-witness pair,

$$\mathbf{Q}(\rho_{S_m W_m}) \geq \mathbf{y}, \quad m \in [1, M]. \quad (3)$$

Note that both constraints have a separate form on each channel use, allow entanglement between  $S_m$ 's across channel uses when  $\mathbf{y}$  is not at maximum, and give the same additive capacity formula in Theorem 1 [42].

*Proof of Theorem 1.*—With the  $M$ -channel-use scenario established, we now prove Theorem 1. The one-shot classical capacity of the product channel  $\Psi \otimes \mathcal{I}$  for  $(S', E)$  is given by a constrained version of the HSW theorem,

$$\chi_L(\Psi) = \max_V \left\{ S(\rho_{BE}) - \sum_x P_X(x) S(\rho_{BE}^{(x)}) \right\}, \quad (4)$$

where the maximization is over the encoding  $(P_X(\cdot), \varepsilon)$  and the source  $\rho_{SW}$  is constrained by  $V$ , and  $\rho_{BE}^{(x)} = (\Psi \circ \varepsilon_x) \otimes \mathcal{I}[\rho_{SE}]$ , with  $\rho_{BE} = \sum_x P_X(x) \rho_{BE}^{(x)}$ . Because  $(S, E, W)$  and  $N, C$  are pure,  $S(\rho_E) = S(\rho_{SW})$ ; it also follows that  $(B, E, W, N', C')$  is pure, conditioned on  $x$ . Thus,  $S(\rho_{BE}^{(x)}) = S(\rho_{N'C'W}^{(x)})$ . Using the subadditivity of von Neumann entropy on  $S(\rho_{BE})$  and combining the above equalities,

$$\begin{aligned} \chi_L(\Psi) &\leq \chi_L^{\text{UB}}(\Psi) \\ &\equiv \max_V \left\{ S(\rho_B) - \sum_x P_X(x) [S(\rho_{N'C'W}^{(x)}) - S(\rho_{SW})] \right\}. \end{aligned} \quad (5)$$

Noticing that  $\Phi_{\varepsilon_x}$  maps  $S$  to  $N'C'$ , Eq. (5) can be expressed as  $\chi_L^{\text{UB}}(\Psi) = \max_V F[\rho_{SW}, (P_X(\cdot), \varepsilon)]$ , where

$$F[\rho_{SW}, (P_X(\cdot), \varepsilon)] \equiv S(\rho_B) - \sum_x P_X(x) E_{\Phi_{\varepsilon_x} \otimes \mathcal{I}}[\rho_{SW}]. \quad (6)$$

It is subadditive since  $E_{\phi}$  is superadditive [42].

Now we switch to the  $M$ -channel-use scenario to prove additivity. If we adopt constraint (3), the overall constraint  $V^{(M)}$  is in a separable form of  $\{V_m, m \in [1, M]\}$ , where  $V_m \equiv \{(P_{X_m}(\cdot), \varepsilon) \in \mathbb{G}, \rho_{S_m} \in \mathcal{B}(\mathcal{H}_S), \mathbf{Q}(\rho_{S_m W_m}) \geq \mathbf{y}\}$ . This separable form and the LOCC encoding allow the upper bound [42]  $\chi_L^{\text{UB}}(\Psi^{\otimes M}) \leq \sum_{m=1}^M \max_{V_m} F[\rho_{S_m W_m}, (P_{X_m}(\cdot), \varepsilon)]$ , which can be achieved [42] by block encoding [24], leading to Eq. (2) since  $\rho_B = \sum_x P_X(x) \Psi \circ \varepsilon_x[\rho_S]$ .

*Special case: Generalized covariant channels.*—Considering a  $d$ -dimensional channel  $\Psi$ , we define its covariant group  $G(\Psi) := \{U \in U(d) : \forall \text{ density matrix } \rho, \exists V \in U(d), \text{ such that } \Psi(U\rho U^\dagger) = V\Psi(\rho)V^\dagger\}$ , where  $U(d)$  is the  $d$ -dimensional unitary group. If there exists a subset  $G_U(\Psi) \subset G(\Psi)$  of size  $d^2$  such that  $\sum_{U_x \in G_U(\Psi)} U_x M U_x^\dagger = 0$  for all  $d \times d$  traceless matrices  $M$  [23], we call  $\Psi$  *generalized covariant*. Generalized covariant channels include covariant channels [36] and Weyl-covariant channels [37], and they allow a simplification of Theorem 1 [42].

*Corollary 2.*—With an arbitrary qudit state as input and arbitrary encoding, and resources constrained by  $\mathbf{Q}(\rho_{SW}) \geq \mathbf{y}$ , the classical capacity of a  $d$ -dimensional generalized covariant channel  $\Psi$  is

$$\chi_L(\Psi) = S[\Psi(I/d)] - \min_{\substack{\epsilon, \rho_{SW} \\ \mathbf{Q}(\rho_{SW}) \geq \mathbf{y}}} E_{\Phi_\epsilon \otimes \mathcal{I}}[\rho_{SW}]. \quad (7)$$

It is additive when the constraint has a separable form on each channel use and the encoding is LOCC.

Note that the encoding being considered is  $\epsilon$  plus unitaries in  $G_U(\Psi)$ . The lower bounds of  $\chi_L(\Psi)$  are obtained by choosing a special  $\epsilon$ ; if  $\epsilon = \mathcal{I}$  (unitary encoding),  $\Phi_\epsilon$  is  $\Psi$ 's complementary channel  $\Psi^c$  and we recover  $\chi_L^\mathcal{I}(\Psi)$ ; if  $\epsilon = \mathcal{R}$ , the map from all states to a pure state inside  $\mathcal{H}_S$ , we recover  $\mathcal{C}^{(1)}$ . Note here that we do not require phase flips to guarantee achievability.

For the quantum erasure channel (QEC) [61], Eq. (7) can be further simplified to  $\chi_L(\Psi) = \max_{\epsilon, \rho_{SW}} (1 - \epsilon)(\log_2 d - E_{\epsilon \otimes \mathcal{I}}[\rho_{SW}])$ , where  $\epsilon$  is the erasure probability [42]. Let the quantum mutual information be the bipartite correlation measure in  $\mathbf{Q}(\rho_{SW}) \geq \mathbf{y}$ . One can further obtain the lower bound [42]  $\chi_L^\mathcal{I} = \mathcal{C}_E[1 - y/(2\log_2 d)]$ , where  $\mathcal{C}_E = (1 - \epsilon)2\log_2 d$  [14]. The other lower bound is  $\mathcal{C}^{(1)} = \mathcal{C} = \mathcal{C}_E/2$  [62]. We observe that, at  $y = 2\log_2 d$ ,  $\rho_{SW}$  is maximally entangled and thus  $\rho_S = I/d$ ,  $\chi_L = \mathcal{C}^{(1)}$ , while  $\chi_L^\mathcal{I} = 0$ ; at  $y = 0$ ,  $\chi_L = \chi_L^\mathcal{I} = \mathcal{C}_E$ . These two points are generic for all channels; when  $0 < y < 2\log_2 d$ , it is an open question as to which  $\epsilon$  allows  $\chi_L(\Psi)$  to exceed  $\max[\chi_L^\mathcal{I}, \mathcal{C}^{(1)}]$ . Numerical results of the quantum depolarizing channel [15] suggest similar scaling behavior with  $y$  [42].

*Application in quantum cryptography.*—We apply Theorem 1 in TW-QKD protocols to bound the general eavesdropper Eve's (coherent attack) information gain. Figure 3 shows a general TW-QKD protocol [59]. First, party 1 prepares a pure signal-reference pair  $(R, W)$ . Reference  $W$  is kept by party 1, and a portion of it is used for security checking [63]. Then the signal  $R$  goes through the forward channel controlled by Eve to party 2. Eve performs a unitary operation on  $R$  and the pure mode  $V$ , producing her ancilla  $E$  and  $S$  for party 2. Note that, in multiple channel uses, Eve's unitary operation can act on all signals jointly. Upon receiving  $S$ , party 2 uses a portion of the  $S$  for security checking [63] and encodes a secret key on

the rest of  $S$  by a chosen scheme  $(P_X(\cdot), \epsilon)$ . The security checking by party 1 and party 2 jointly, measures certain functions  $\mathbf{Q}(\rho_{SW})$  of the state  $\rho_{SW}$ . Then the encoded signal goes through channel  $\Psi$  in party 2 (e.g., device loss, amplification), leading to the output mode  $B$ , which is sent back to party 1 through the backward channel controlled by Eve. Finally, party 1 makes a measurement on the received mode and reference  $W$  to obtain the secret key.

*Corollary 3.*—In the TW-QKD protocol given above, the information gain per channel use of the eavesdropper's coherent attack is upper bounded by  $\chi_L(\Psi) = \max_{\rho_{SW}} F[\rho_{SW}, (P_X(\cdot), \epsilon)]$ , where  $F[\cdot]$  is defined in Eq. (6), and the maximization is constrained by security checking measurement result  $\mathbf{Q}(\rho_{SW}) = \mathbf{y}$  and keeping  $\rho_W$  fixed.

*Proof.*—To upper bound Eve's information gain, we give Eve all of  $B$ . This concession to Eve will not substantially increase Eve's information gain in long-distance QKD since the return fiber loss  $\ll 1$  (e.g.,  $\sim 0.01$  at 100 km), which means almost all of the light is leaked to Eve. Eve makes an optimal measurement on all  $(B, E)$  pairs in multiple channel uses.

In a single run of the QKD protocol,  $(S, E, W)$  is pure after Eve's unitary operation, the same scenario as for Theorem 1. Here,  $W$  is the witness—kept locally by party 1 and inaccessible to Eve;  $E$  provides the resource as the preshared ancilla. The multiple QKD protocol runs also fit in our scenario. Moreover, party 1 and party 2 perform security checking to obtain constraints in the form of Eqs. (1) and (3) on  $\rho_{SW}$ . Controlled by party 2, the encoding operations are always LOCC. Equation (2) upper bounds the information gain per channel use of Eve's coherent attack.

*Special case: Gaussian protocol.*—If party 2 chooses the Gaussian channel to be  $\Psi$  covariant with the unitary encoding, similar to Corollary 2,  $\chi_L(\Psi)$  in Corollary 3 has

$$F[\rho_{SW}, (P_X(\cdot), \epsilon)] = S(\rho_B) - E_{\Psi^c \otimes \mathcal{I}}[\rho_{SW}]. \quad (8)$$

For Gaussian protocols, the source  $(R, W)$  and the channel  $\Psi$  are Gaussian. The security checking functions are the mean photon number of  $S$ , and the cross-correlation

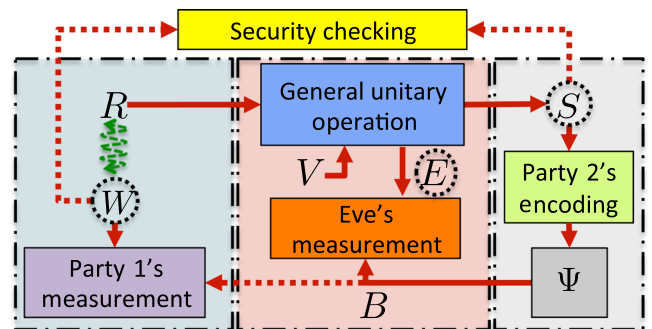


FIG. 3. Schematic of two-way QKD. The dotted circles highlight the three modes in the resource distribution step.

between  $S$  and  $W$ —both are functions of the covariance matrix  $\Lambda_{SW}$  of  $\rho_{SW}$ . As a simplified form of Eq. (6), Eq. (8) is subadditive. Moreover,  $W$  is Gaussian and passive symplectic transforms [27] over  $S$  preserve Eq. (8) [28], so the Gaussian extremality theorem [64] applies. With all of the constraints on  $\Lambda_{SW}$ , Eq. (8) is maximum when  $\rho_{SW}$  is Gaussian. Thus, for Gaussian protocols, the collective Gaussian attack is the most powerful.

*Discussion.*—In future work, constraints in expectation value forms, i.e.,  $\mathbb{E}[Q_k(\rho_{SW})] \geq y_k$ , an extension of Corollary 2 to infinite dimensional systems, and an explicit evaluation of the capacity of the QEC are of interest.

Q. Z. is supported by the Claude E. Shannon Research Assistantship and AFOSR Grant No. FA9550-14-1-0052. E. Y. Z. is supported by the National Science Foundation under Grant Contract No. CCF-1525130. P. W. S. is supported by the National Science Foundation under Grant Contract No. CCF-1525130, and by the NSF through the STC for Science of Information under Grant No. CCF0-939370. The authors thank Zheshen Zhang, Jeffrey Shapiro, Aram Harrow, and Zi-Wen Liu for the helpful discussion. The authors also thank the anonymous referees for their helpful feedback.

---

\*quntao@mit.edu

- [1] C. E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
- [2] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 2012).
- [3] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, *Rev. Mod. Phys.* **86**, 1203 (2014).
- [4] A. S. Holevo, *IEEE Trans. Inf. Theory* **44**, 269 (1998).
- [5] B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).
- [6] S. Lloyd, *Phys. Rev. A* **55**, 1613 (1997).
- [7] P. W. Shor, in *Proceedings of the MSRI Workshop in Quantum Computation, Berkeley, 2002* (Mathematical Sciences Research Institute, Berkeley, 2002).
- [8] I. Devetak, *IEEE Trans. Inf. Theory* **51**, 44 (2005).
- [9] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *IEEE Trans. Inf. Theory* **48**, 2637 (2002).
- [10] M. Wilde and M.-H. Hsieh, *Quantum Inf. Process.* **11**, 1431 (2012).
- [11] M. M. Wilde, P. Hayden, and S. Guha, *Phys. Rev. A* **86**, 062306 (2012).
- [12] M. B. Hastings, *Nat. Phys.* **5**, 255 (2009).
- [13] W. Dür, J. I. Cirac, and P. Horodecki, *Phys. Rev. Lett.* **93**, 020503 (2004).
- [14] M. M. Wilde, [arXiv:1106.1445](https://arxiv.org/abs/1106.1445).
- [15] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).
- [16] C. Adami and N. J. Cerf, *Phys. Rev. A* **56**, 3470 (1997).
- [17] S. Mozes, J. Oppenheim, and B. Reznik, *Phys. Rev. A* **71**, 012311 (2005).
- [18] M. R. Beran and S. M. Cohen, *Phys. Rev. A* **78**, 062337 (2008).
- [19] P. S. Bourdon, E. Gerjuoy, J. P. McDonald, and H. T. Williams, *Phys. Rev. A* **77**, 022305 (2008).
- [20] S. Wu, S. M. Cohen, Y. Sun, and R. B. Griffiths, *Phys. Rev. A* **73**, 042311 (2006).
- [21] Z. Ji, Y. Feng, R. Duan, and M. Ying, *Phys. Rev. A* **73**, 034307 (2006).
- [22] Z. Shadman, H. Kampermann, C. Macchiavello, and D. Bruß, *Quantum Meas. Quantum Metrol.* **1**, 21 (2013).
- [23] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, *Quantum Inf. Comput.* **1**, 70 (2001).
- [24] P. W. Shor, *Quantum Inf. Comput.* **4**, 537 (2004); [arXiv:quant-ph/0402129](https://arxiv.org/abs/quant-ph/0402129).
- [25] E. Y. Zhu, Q. Zhuang, and P. W. Shor, [arXiv:1704.06955](https://arxiv.org/abs/1704.06955).
- [26] L. Lami, C. Hirche, G. Adesso, and A. Winter, *Phys. Rev. Lett.* **117**, 220502 (2016).
- [27] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [28] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, *Phys. Rev. A* **94**, 012322 (2016).
- [29] H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **88**, 017901 (2001).
- [30] V. Coffman, J. Kundu, and W. K. Wootters, *Phys. Rev. A* **61**, 052306 (2000).
- [31] T. J. Osborne and F. Verstraete, *Phys. Rev. Lett.* **96**, 220503 (2006).
- [32] T. Hiroshima, G. Adesso, and F. Illuminati, *Phys. Rev. Lett.* **98**, 050503 (2007).
- [33] Because Alice has all the information on her state, measurement is not necessary; thus, it is adequate to consider CPTP maps.
- [34] M. A. Nielsen, *Phys. Rev. Lett.* **83**, 436 (1999).
- [35] R. Alicki, [arXiv:quant-ph/0402080](https://arxiv.org/abs/quant-ph/0402080).
- [36] A. S. Holevo, [arXiv:quant-ph/0212025](https://arxiv.org/abs/quant-ph/0212025).
- [37] N. Datta, M. Fukuda, and A. S. Holevo, *Quantum Inf. Process.* **5**, 179 (2006).
- [38] R. Renner, *Int. J. Quantum. Inform.* **06**, 1 (2008).
- [39] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [40] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, *Phys. Rev. Lett.* **109**, 100502 (2012).
- [41] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, *Phys. Rev. Lett.* **110**, 030502 (2013).
- [42] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.118.200503>, which includes Refs. [43–50], for details of proofs and calculations.
- [43] Z. Shadman, H. Kampermann, C. Macchiavello, and D. Bruß, *New J. Phys.* **12**, 073042 (2010).
- [44] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [45] C. King, *IEEE Trans. Inf. Theory* **49**, 221 (2003).
- [46] D. Leung and J. Watrous, [arXiv:1510.01366](https://arxiv.org/abs/1510.01366).
- [47] A. S. Holevo, *Theory Probab. Appl.* **51**, 92 (2007).
- [48] R. Ahlswede and P. Lober, *IEEE Trans. Inf. Theory* **47**, 474 (2001).
- [49] A. Uhlmann, *Commun. Math. Phys.* **54**, 21 (1977).
- [50] P. Hayden, R. Jozsa, D. Petz, and A. Winter, *Commun. Math. Phys.* **246**, 359 (2004).

- [51] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, *Phys. Rev. A* **95**, 012332 (2017).
- [52] Y.-G. Han, Z.-Q. Yin, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, *Sci. Rep.* **4**, 4936 (2014).
- [53] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nat. Phys.* **4**, 726 (2008).
- [54] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, *J. Phys. B* **47**, 035501 (2014).
- [55] C. Weedbrook, C. Ottaviani, and S. Pirandola, *Phys. Rev. A* **89**, 012309 (2014).
- [56] C. Ottaviani, S. Mancini, and S. Pirandola, *Phys. Rev. A* **92**, 062323 (2015).
- [57] C. Ottaviani and S. Pirandola, *Sci. Rep.* **6**, 22225 (2016).
- [58] K. Boström and T. Felbinger, *Phys. Rev. Lett.* **89**, 187902 (2002).
- [59] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, *Phys. Rev. A* **88**, 062302 (2013).
- [60] C. I. Henaö and R. M. Serra, *Phys. Rev. A* **92**, 052317 (2015).
- [61] M. Grassl, Th. Beth, and T. Pellizzari, *Phys. Rev. A* **56**, 33 (1997).
- [62] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *Phys. Rev. Lett.* **83**, 3081 (1999).
- [63] This is realized either by a beam splitter or a switch between security checking and key generation.
- [64] M. M. Wolf, G. Giedke, and J. I. Cirac, *Phys. Rev. Lett.* **96**, 080502 (2006).