Additive Classical Capacity of Quantum Channels Assisted by Noisy Entanglement

Quntao Zhuang, Elton Yechao Zhu, and Peter W. Shor

Phys. Rev. Lett. **118**, 200503 — Published 19 May 2017

DOI: 10.1103/PhysRevLett.118.200503

The additive classical capacity of quantum channels assisted by noisy entanglement

Quntao Zhuang,[1, 2, *] Elton Yechao Zhu,[1, 3] and Peter W. Shor[3, 4]

[1] *Department of Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[2] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[3] *Center For Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*
[4] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*

(Dated: April 28, 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 pre-shared 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.

PACS numbers: 03.67.Hk,03.67.Dd,03.67.-a,03.67.Bg

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 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]. Ref. 10 and 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 "non-additivity" issue [3], best illustrated by the example of $\mathcal{C}$. The Holevo-Schumacher-Westmoreland (HSW) theorem [4, 5] gives the one-shot capacity $\mathcal{C}^{(1)}\left(\Psi\right)$ of channel Ψ, which assumes product-state input in multiple channel uses. Consider the tensor product channel $\Psi^{\otimes M}$, it may have one-shot capacity $\mathcal{C}^{(1)}\left(\Psi^{\otimes M}\right) > M\mathcal{C}^{(1)}\left(\Psi\right)$, since it allows the input state of Ψ^M to be entangled across M channel uses of Ψ ($M-$shot). $\mathcal{C}\left(\Psi\right)$ is then given by the regularized expression as $\lim_{M\to\infty}\mathcal{C}^{(1)}\left(\Psi^{\otimes M}\right)/M$, 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 $\mathcal{C}^{(1)}\left(\Psi^{\otimes M}\right) = M\mathcal{C}^{(1)}\left(\Psi\right)$, the formula of the capacity is greatly simplified, *i.e.* $\mathcal{C}\left(\Psi\right) = \mathcal{C}^{(1)}\left(\Psi\right)$. However, both $\mathcal{C}$ [12] and $\mathcal{Q}$ [13] are known to be non-additive. 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], noiseless channel assisted by noisy entanglement [23] and noisy channels assisted by limited pure state entanglement [24]. However, all results are in general non-additive as expected [25], since the above imperfect scenarios include the case with zero entanglement assistance—the non-additive $\mathcal{C}$.

In this paper, we obtain an additive classical capacity formula for a noisy quantum channel Ψ assisted by resources such as noisy entanglement. In the most general formalism, Alice sends an optimized ensemble of (possibly mixed) states ρ^i_{SE} to Bob, with signal S through the channel Ψ and an ancilla E pre-shared through the identity channel $\mathcal{I}$. Each ρ^i_{SE} 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 ρ^i_{SE} is obtained by encoding on S from a certain state ρ_{SE}. Moreover, the resource is constrained by the correlation between S and a "witness" W—a purification of (S, E).

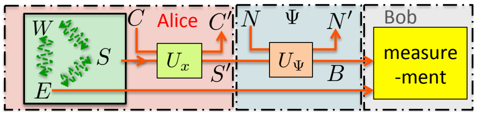

Figure 1. Schematic of a single channel use.

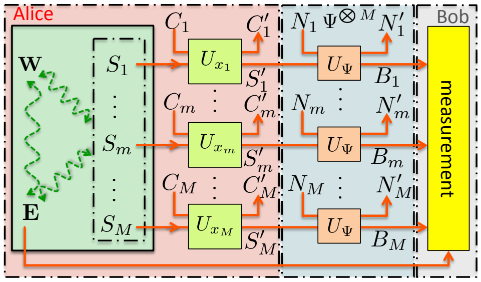

Figure 2. Schematic of M channel uses.

In the resource distribution step, W is made inaccessible to both Alice and Bob. Instead of explicitly quantifying the available resource (between S, 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

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

on ρ_{SW}, where each $Q_k(\cdot)$ is a function on bipartite states. We denote Eqn. 1 by $\mathbf{Q}\left(\rho_{SW}\right) \geq \mathbf{y}$. While Ref. 9 and 24 only considered pure state entanglement, the form of resources in our case can be arbitrary by choosing different $Q_k(\cdot)$, *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; (2) constraints on the entanglement between S and W leads to constraints on the entanglement between S and E—a property known as monogamy [26, 30–32].

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

In the encoding step, Alice performs a quantum operation ε_x [33] with probability $P_X(x)$ on S to encode a message x, resulting in S' as the input to Ψ. In multiple channel uses, the encoding is a set of classically correlated separate operations—local operations and classical communication (LOCC) [34]. ρ_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 $V \equiv \{(P_X(\cdot), \varepsilon.) \in \mathbb{G}, \rho_S \in \mathcal{B}(\mathcal{H}_S), \mathbf{Q}(\rho_{SW}) \geq \mathbf{y}\}$, suppose $\mathbb{G}$ allows arbitrary phase flips, the classical capacity of the quantum channel Ψ is*

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

where Φ_{ε_x} is the complementary quantum operation to $\Psi \circ \varepsilon_x$, the entropy gain E_ϕ [35] of a CPTP map ϕ on state ρ is defined by $E_\phi[\rho] \equiv S(\phi[\rho]) - S(\rho)$, and the maximization is over the encoding $(P_X(\cdot), \varepsilon.)$ and ρ_{SW}. Eqn. 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 Φ_{ε_x} is given in Fig. 1. The encoding CPTP map ε_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 Ψ, whose Stinespring's dilation is a unitary operation U_Ψ on S' and an environment N in the vacuum state, producing B for Bob and an environment N'. We define Φ_{ε_x} as the CPTP map from ρ_S to $\rho^{(x)}_{N'C'}$, given ε_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 Eqn. 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 make a few more comments. First, for generalized covariant channels, including covariant [36] channels and Weyl-covariant [37] channels, Eqn. 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 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 y_k's are maximum, $\chi_L = \mathcal{C}^{(1)}$; when y_k's are minimum, $\chi_L = \mathcal{C}_E$; Note when arbitrary phase flips are not allowed, the r.h.s. of Eqn. 2 upper bounds χ_L, and it is still additive while χ_L 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 ε_x's are not unitary, then the environment C' is never sent to

Bob. This is different from Ref. 24, where all purification of the signal is sent to Bob. If we restrict ε_x's to be unitary, the input states in Ref. 24 do not need to be related by unitary operations, different from 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 Eqn. 1 appears in security checking of TW-QKD protocols, where two parties verify properties of their state ρ_{SW} 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 the 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" has recently been shown to have the potential of reaching unprecedented secret key rate (SKR) [28, 51]. Consequently, our upper bound is crucial for high-SKR QKD.

Multiple channel uses.—Now we extend the single channel use scenario to $M \geq 2$ channel uses in a non-trivial way that allows an additive classical capacity (Fig. 2). We keep the same notation for all 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 $\rho_{\mathbf{S}} \in \mathcal{B}\left(\mathcal{H}_S^{\otimes M}\right)$, and also $\mathbf{W}$ for arbitrary inaccessible witness and $\mathbf{E}$ for 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 some joint distribution $P_{\mathbf{X}}(\cdot)$, where $\mathbf{X} = (X_1, \cdots, X_M)$ denotes the symbols in M channel uses. Conditioned on the message $\mathbf{x} \equiv (x_1, \cdots, x_M)$, 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 environment $\mathbf{C'} = \{\, C'_m : m \in [1, M]\,\}$. Each encoding operation ε_{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 Ψ separately. The Stinespring's 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 pre-shared ancilla $\mathbf{E}$ provides resources quantified by the constraint $\mathbf{Q}\left(\rho_{S_m\mathbf{W}}\right) \geq \mathbf{y}, m \in [1, M]$. One can also consider M witnesses $\mathbf{W} = \{\, W_m : m \in [1, M]\,\}$, with constraints on each signal-witness pair,

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

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 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 the constrained version of the HSW theorem

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

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

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

Noticing that Φ_{ε_x} maps S to $N'C'$, Eqn. 5 can be expressed as $\chi_L^{\mathrm{UB}}(\Psi) = \max_V F\left[\rho_{SW}, \left(\, P_X(\cdot), \varepsilon_\cdot\, \right)\right]$, where

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

It's subadditive since E_ϕ is superadditive [42].

Now we switch to the M channel uses 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 $V_m \equiv \{\, \left(P_{X_m}(\cdot), \varepsilon_\cdot\right) \in \mathbb{G},\ \rho_{S_m} \in \mathcal{B}\left(\mathcal{H}_S\right),\ \mathbf{Q}\left(\rho_{S_m W_m}\right) \geq \mathbf{y}\,\}$. This separable form and the LOCC encoding allows the upper bound [42] $\chi_L^{\mathrm{UB}}\left(\Psi^{\otimes M}\right) \leq \sum_{m=1}^M \max_{V_m} F\left[\rho_{S_m W_m}, \left(\, P_{X_m}(\cdot), \varepsilon_\cdot\, \right)\right]$, which can be achieved [42] by block encoding [24], leading to Eqn. 2 since $\rho_B = \sum_x P_X(x)\, \Psi \circ \varepsilon_x\left[\rho_S\right]$.

Special case: generalized covariant channels.— Consider a d-dimensional channel Ψ, we define its covariant group $G(\Psi) := \{U \in U(d) : \forall\, \text{density matrix}\, \rho, \exists\, V \in U(d), s.t.\, \Psi\left(U\rho U^\dagger\right) = V\Psi(\rho)V^\dagger\}$, 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 Ψ *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 arbitrary qudit state as input and arbitrary encoding, and resources constrained by $\mathbf{Q}\left(\rho_{SW}\right)\geq\mathbf{y}$, the classical capacity of a d-dimensional generalized covariant channel Ψ is*

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

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

For the QEC [61], Eqn. 7 can be further simplified to $\chi_L\left(\Psi\right)=\max_{\varepsilon,\rho_{SW}}\left(1-\epsilon\right)\left(\log_2 d-E_{\varepsilon^c\otimes\mathcal{I}}\left[\rho_{SW}\right]\right)$, where ϵ is the erasure probability [42]. Let the quantum mutual information be the bipartite correlation measure in $Q\left(\rho_{SW}\right)\geq y$. One can further obtain the lower bound [42] $\chi_L^{\mathcal{I}}=\mathcal{C}_E\left(1-y/\left(2\log_2 d\right)\right)$, where $\mathcal{C}_E=\left(1-\epsilon\right)2\log_2 d$ [14]. The other lower bound is $\mathcal{C}^{(1)}=\mathcal{C}=\mathcal{C}_E/2$ [62]. We observe that: at $y=2\log_2 d$, ρ_{SW} is maximally entangled 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 open what ε allows $\chi_L\left(\Psi\right)$ to exceed $\max\left[\chi_L^{\mathcal{I}},\mathcal{C}^{(1)}\right]$. Numerical results of quantum depolarizing channel [15] suggest similar scaling behaviour 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. Fig. 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 $\left(P_X\left(\cdot\right),\ \varepsilon.\right)$. The security checking by party-1 and party-2 jointly measures some functions $\mathbf{Q}\left(\rho_{SW}\right)$ of the state ρ_{SW}. Then the encoded signal goes through channel Ψ 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.

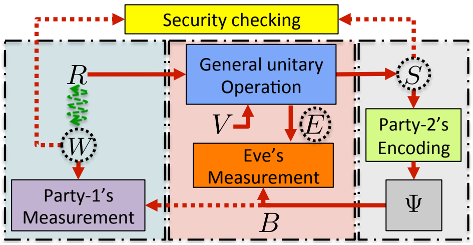

Figure 3. Schematic of two-way QKD. The dotted circles highlight the three modes in the resource distribution step.

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* $\chi_L\left(\Psi\right)=\max_{\rho_{SW}}F\left[\rho_{SW},\left(P_X\left(\cdot\right),\varepsilon.\right)\right]$, *where* $F\left[\cdot\right]$ *is defined in Eqn. 6,and the maximization is constrained by security checking measurement result* $\mathbf{Q}\left(\rho_{SW}\right)=\mathbf{y}$ *and* ρ_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.*, ~ 0.01 at 100 kilometers), which means almost all 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 as the scenario for theorem 1. Here W is the witness—kept locally by party-1 and inaccessible to Eve; E provides the resource as the pre-shared 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 Eqn. 1 and Eqn. 3 on ρ_{SW}. Controlled by party-2, the encoding operations are always LOCC. Eqn. 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 Ψ covariant with the unitary encoding, similar to corollary 2, $\chi_L\left(\Psi\right)$ in corollary 3 has

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

For Gaussian protocols, the source (R,W) and the channel Ψ are Gaussian. The security checking functions are the mean photon number of S, and the cross-correlation between S and W—both are functions of the covariance matrix Λ_{SW} of ρ_{SW}. As a simplified form of Eqn. 6, Eqn. 8 is subadditive. Moreover, W is Gaussian and passive symplectic transforms [27] over S preserve Eqn. 8 [28], so the Gaussian extremality theorem [64] applies. With all constraints on Λ_{SW}, Eqn. 8 is maximum when ρ_{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.* $\mathbb{E}\left[Q_k\left(\rho_{SW}\right)\right]\geq y_k$, extension of corollary. 2 to infinite dimensional systems and explicit evaluation of the capacity of QEC are of interest.

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

* quntao@mit.edu

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 379-423 (1948).

[2] T. M. Cover and J. A. Thomas, Elements of information theory,John Wiley & Sons, (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), ISSN 0018-9448.

[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 *lecture notes, MSRI Workshop on Quantum Computation* (2002).

[8] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005), ISSN 0018-9448.

[9] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002), ISSN 0018-9448.

[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:quant-ph/1106.1445 (2011).

[15] M. Nielsen and I. L. Chuang, Quantum computation and quantum information,Cambridge university press, (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 Measurements and Quantum Metrology **1**, 21-23 (2013)

[23] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, Quantum Inf. Comput. **1**, 70–78(2001); arXiv:quant-ph/0106080.

[24] P. W. Shor, Quantum Inf. Comput. **4**, 537(2004); arXiv:quant-ph/0402129.

[25] E. Y. Zhu, Q. Zhuang, and P. W. Shor, arXiv:quant-ph/1704.06955.(2017)

[26] L. Lami, C. Hirche, G. Adesso, and A. Winter, arXiv:quant-ph/1607.05285v1.(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 of her state, measurement is not necessary, thus it's adequate to consider CPTP maps.

[34] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[35] R. Alicki, arXiv:quant-ph/0402080 (2004).

[36] A. S. Holevo, arXiv:quant-ph/0212025 (2002).

[37] N. Datta, M. Fukuda, and A. S. Holevo, Quant. Inf. Process. **5**, 179 (2006).

[38] R. Renner, Int. J. Quantum Inf. **6**, 1–127 (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. 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 materials, which includes Refs. 43–50.

[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), ISSN 0018-9448.

[46] D. Leung, and J. Watrous, arXiv:1510.01366 (2015).

[47] A. S. Holevo, Theory Probab. Appl. **51**, 92 (2007),

[48] R. Ahlswede, and P. Lober, IEEE Trans. Inf. Theory **47**, 474 (2001), ISSN 0018-9448.

[49] A. Uhlmann, Comm. Math. Phys. **54**, 21 (1977).

[50] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Comm. Math. Phys. **246**, 359 (2004), ISSN 1432-0916.

[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 EP (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, andS. 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. Henao, 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).