Direct and Reverse Secret-Key Capacities of a Quantum Channel

Stefano Pirandola,[1] Raul García-Patrón,[1] Samuel L. Braunstein,[2] and Seth Lloyd[1,3]
[1]MIT-Research Laboratory of Electronics, Cambridge, Massachusetts 02139, USA
[2]Computer Science, University of York, York YO10 5DD, United Kingdom
[3]MIT-Department of Mechanical Engineering, Cambridge, Massachusetts 02139, USA
(Received 18 September 2008; published 4 February 2009)

We define the direct and reverse secret-key capacities of a memoryless quantum channel as the optimal rates that entanglement-based quantum-key-distribution protocols can reach by using a single forward classical communication (direct reconciliation) or a single feedback classical communication (reverse reconciliation). In particular, the reverse secret-key capacity can be positive for antidegradable channels, where no forward strategy is known to be secure. This property is explicitly shown in the continuous variable framework by considering arbitrary one-mode Gaussian channels.

DOI: 10.1103/PhysRevLett.102.050503 PACS numbers: 03.67.Dd, 42.50.−p, 89.70.Cf

Since the birth of quantum information [1], both the notions of quantum entanglement and memoryless quantum channel have been fundamental in many theoretical investigations. This consideration is particularly true in the field of quantum cryptography. On the one hand, entanglement distribution is a basic process in the formulation of quantum-key-distribution (QKD) protocols [2]. On the other hand, memoryless quantum channels can be seen as the effect of collective attacks, recognized as predominant in quantum cryptography after the recent achievements of Ref. [3]. In this Letter, we consider a generic QKD protocol where two honest parties (Alice and Bob) extract a secret key from the remote correlations that are generated by one of the parties (Alice) after the distribution of a generic entangled state over a memoryless quantum channel. Such a task can be assisted by one-way classical communications (CCs) which can be forward, i.e., from Alice to Bob, or feedback, i.e., from Bob to Alice. Even if the scenario can seem symmetric, it is actually much harder to study the feedback-assisted protocols and optimize the corresponding secret-key rates. The reason relies on the fact that Alice can actively exploit the information already received from Bob for conditioning the subsequent inputs to the quantum channel. In this Letter we simplify this problem by restricting the feedback to a single (and therefore final) CC from Bob. Although we make this restriction on the feedback strategy, the security performance is still remarkable. Under suitable conditions, the corresponding QKD protocols are in fact able to outperform all the known QKD protocols which are based on forward CCs.

In general, we identify the notions of direct and reverse reconciliation [4] with the ones of assistance by a single forward and a single feedback CC, respectively. Then, by optimizing over corresponding protocols, we define the direct and reverse secret-key capacities of a quantum channel. In direct reconciliation, the optimization over a single forward CC is not restrictive at all. In fact, the direct secret-key capacity represents an equivalent entanglement-based formulation of the (forward) secret-key capacity of Ref. [5]. In reverse reconciliation, even if the feedback strategy is limited, the security performance is in any case outstanding. In fact, the reverse secret-key capacity can be positive even if the quantum channel is antidegradable [6]; i.e., an eavesdropper is able to reconstruct completely the output state of the receiver (and no forward protocol is known to be secure). This property is explicitly shown in the most important scenario for the continuous variable QKD: the one-mode Gaussian channel. In order to establish this result in its full generality, we resort to the recent canonical classification of the one-mode Gaussian channels [7] (see also Refs. [8,9]). By assuming an arbitrary one-mode Gaussian channel, we then exploit a general lower bound for the reverse secret-key capacity. This bound corresponds to the additive capacity of Ref. [10], which is connected to the entanglement distillation by feedback CCs. For one-mode Gaussian channels, this additive capacity assumes an analytical formula which is exceptionally simple. Most importantly, it enables us to prove the positivity of the reverse secret-key capacity over a wide range of parameters where the channel is antidegradable. In a final investigation, we also prove that tighter bounds can be derived by exploiting noise effects in the key-distribution process.

Let us consider an arbitrary quantum channel, i.e., a completely positive trace-preserving (CPT) map $\mathcal{N}$, transforming the input state $\rho_{A'}$ of a sender (Alice) into the output state ρ_B of a receiver (Bob). As depicted in Fig. 1, such a channel can always be represented by an isometric

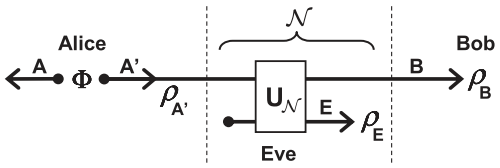

FIG. 1. Quantum channel $\mathcal{N}$ and its dilation.

embedding $U_{\mathcal{N}}:\mathcal{H}_{A'} \to \mathcal{H}_B \otimes \mathcal{H}_E$ followed by a trace over the environment E which we identify with the eavesdropper (Eve). By definition, the original channel $\mathcal{N}$ is called degradable if there exists a CPT map $\mathcal{D}$ such that $\rho_E = \mathcal{D}(\rho_B)$, where ρ_E is the output state of Eve. By contrast, $\mathcal{N}$ is called antidegradable if there exists a CPT map $\tilde{\mathcal{D}}$ such that $\rho_B = \tilde{\mathcal{D}}(\rho_E)$. A further dilation of the quantum channel is provided by the purification of the input $\rho_{A'} = \mathrm{Tr}_A \Phi$ with $\Phi := |\Phi\rangle\langle\Phi|_{AA'}$, involving the introduction of a supplementary system A at Alice's side. Notice that the three output systems A, B, and E are globally described by a pure state $\Psi = |\Psi\rangle\langle\Psi|_{ABE}$, which is given by $\Psi = (I_A \otimes U_{\mathcal{N}})(\Phi)$. A key-distribution protocol can be introduced by extending the scenario of Fig. 1 to n (entangled) uses of the channel and by adding measurements to Alice's and Bob's sides. Restricting the honest users to a single one-way CC, we have a one-way key-distribution protocol which can be direct, if Alice assists Bob, or reverse, if Bob assists Alice.

Let us begin with the direct protocol. In the first step of this protocol, Alice distributes a pure entangled state $\Phi^n := |\Phi\rangle\langle\Phi|_{A^n A'^n}$ sending the A' part through the memoryless quantum channel $\mathcal{N}^{\otimes n} = \mathcal{N} \otimes \cdots \otimes \mathcal{N}$ (see Fig. 2). As a consequence, we have a pure state $\Psi^n = (I_A \otimes \hat{U}_{\mathcal{N}})^{\otimes n}(\Phi^n)$, shared by the output systems of Alice (A^n), Bob (B^n), and Eve (E^n). On her local systems A^n, Alice performs a quantum measurement $\mathcal{M}_A$. This is generally described by a positive operator-valued measure (POVM) $\{\hat{A}_x\}$ with outcomes x. As a result, she gets an output random variable $X = \{x, p(x)\}$ where the values x have probability distribution $p(x) = \mathrm{Tr}(\Psi^n \hat{A}_x)$. After the measurement, Alice processes X via a classical channel $X \to (S_A, L)$, which yields a key variable $S_A = \{s, p(s)\}$ and an assisting variable $L = \{l, p(l)\}$. The assisting variable L contains all the information necessary to Bob for performing error correction and privacy amplification. The value l of L is then broadcast by Alice through a public channel. Using this information, Bob performs a conditional POVM $\mathcal{M}_{B|L} = \{\hat{B}_s^{(l)}\}$ on his systems B^n, and retrieves an estimation of Alice's key S'_A up to an error probability $p(S_A \neq S'_A) \leq \varepsilon$ [11].

In the limit of $n \to +\infty$, Alice and Bob are able to rule out Eve completely and share exactly the same uniform key S_A corresponding to $H(S_A) := nR$ secret bits. The highest secret-key rate R which is achievable by direct protocols over a quantum channel $\mathcal{N}$ is called the direct secret-key capacity $K_{\blacktriangleright}(\mathcal{N})$ of the channel. This quantity is characterized by the formula [12,13]

$$K_{\blacktriangleright}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\substack{\Phi^n, \mathcal{M}_A \\ X \to T}} [I(X{:}B^n|T) - I(X{:}E^n|T)],$$

where the maximum is over all the pure states Φ^n, Alice's POVMs $\mathcal{M}_A$, and all the classical channels $p(t|x){:}X \to T$ generating the conditioning dummy variable T. In this formula, $I(X{:}B^n|T)$ and $I(X{:}E^n|T)$ are the conditional Holevo information of Bob and Eve [14]. In direct reconciliation, one can show [13] that the conditioning by T can actually be avoided in the previous formula, and that $K_{\blacktriangleright}(\mathcal{N})$ is the entanglement-based version of the secret-key capacity $K(\mathcal{N})$ of Ref. [5]. From Ref. [5] it is known that $K(\mathcal{N}) \geq E(\mathcal{N}) = Q(\mathcal{N})$, where $E(\mathcal{N})$ is the entanglement-generation capacity of $\mathcal{N}$ and $Q(\mathcal{N})$ its unassisted quantum capacity [15].

A key-distribution protocol in reverse reconciliation, i.e., a reverse protocol, consists of interchanging Alice and Bob in terms of the assisting CC while keeping Alice as dispenser of the quantum state Φ^n. As we have already mentioned, this is a particular case of a more general feedback-assisted protocol, where Alice distributes the entangled state Φ^n in n different rounds, each one conditioned by previous CCs received from Bob. In the first step of a reverse protocol, Alice distributes Φ^n generating Ψ^n as before (see Fig. 3). But now the first measurement is done by Bob, who detects his systems B^n via a POVM $\mathcal{M}_B$, generating an output variable $Y = \{y, p(y)\}$. Again, this variable is processed into a key variable S_B and an assisting variable M, which is broadcast by Bob. Using this information, Alice subjects her local systems A^n to a conditional POVM $\mathcal{M}_{A|M}$, retrieving an estimation of Bob's key S'_B up to a small error probability. The reverse secret-key capacity $K_{\blacktriangleleft}(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is defined as the highest secret-key rate which is achievable by reverse protocols over $\mathcal{N}$. For this capacity we can prove the upper bound [12,13]

$$K_{\blacktriangleleft}(\mathcal{N}) \leq \lim_{n\to\infty} \frac{1}{n} \max_{\substack{\Phi^n, \mathcal{M}_B \\ Y \to T}} [I(Y{:}A^n|T) - I(Y{:}E^n|T)],$$

where the maximum is now over Bob's POVMs $\mathcal{M}_B$ and involves the processing of Bob's variable Y.

In order to find achievable lower bounds for this capacity, let us restrict the process of key distribution to the one of key distillation. A one-way key-distillation protocol over a channel $\mathcal{N}$ (in direct or reverse reconciliation) is defined as a one-way key-distribution protocol where the input state is separable over different uses of the channel, i.e., $\Phi^n = \Phi^{\otimes n}$. Maximizing over these protocols, we can

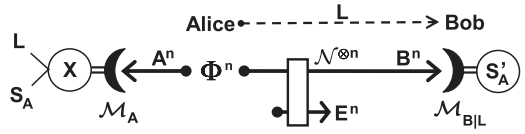

FIG. 2. Key-distribution protocol in direct reconciliation.

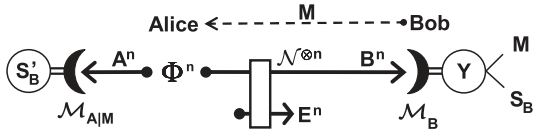

FIG. 3. Key-distribution protocol in reverse reconciliation.

define the direct and reverse key-distillation capacities of a quantum channel, which we denote by $K^{\otimes}_{\blacktriangleright}(\mathcal{N})$ and $K^{\otimes}_{\blacktriangleleft}(\mathcal{N})$. These capacities clearly satisfy $K^{\otimes}_{\blacktriangleright}(\mathcal{N}) \leq K_{\blacktriangleright}(\mathcal{N})$ and $K^{\otimes}_{\blacktriangleleft}(\mathcal{N}) \leq K_{\blacktriangleleft}(\mathcal{N})$. Using the results of Ref. [16], we can easily prove the formulas [12,13]

$$K^{\otimes}_{\blacktriangleright}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\substack{\Phi,\mathcal{M}_A \\ X\to T}} [I(X{:}B^n|T) - I(X{:}E^n|T)],$$

$$K^{\otimes}_{\blacktriangleleft}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\substack{\Phi,\mathcal{M}_B \\ Y\to T}} [I(Y{:}A^n|T) - I(Y{:}E^n|T)],$$

where now the maximization is over the single copy of the state Φ, i.e., over $\Phi^{\otimes n}$. Exploiting the relation with the key distillation, we can prove an important lower bound for $K_{\blacktriangleleft}(\mathcal{N})$. In fact, we have [13]

$$K_{\blacktriangleleft}(\mathcal{N}) \geq K^{\otimes}_{\blacktriangleleft}(\mathcal{N}) \geq E^{(1)}_R(\mathcal{N}) = E_R(\mathcal{N}), \qquad (1)$$

where $E_R(\mathcal{N})$ is the additive capacity of Ref. [10]. In particular, the single-letter version of this capacity is given by the formula $E^{(1)}_R(\mathcal{N}) := \max_{|\Phi\rangle} I(A\langle B)$, where $I(A\langle B) := H(\rho_A) - H(\rho_{AB})$ is the reverse coherent information computed over Alice and Bob's output state $\rho_{AB} = (I_A \otimes \mathcal{N})(\Phi)$. Remarkably, $E_R(\mathcal{N})$ has a very different behavior with respect to the quantum capacity $Q(\mathcal{N})$. In particular, for an antidegradable channel, we can have $E_R(\mathcal{N}) > 0$ which implies $K_{\blacktriangleleft}(\mathcal{N}) > 0$. In the following this is explicitly shown for a generic Gaussian channel affecting a single bosonic mode.

Recall that a bosonic mode is a quantum system described by a pair of quadrature operators, $\hat{q}$ and $\hat{p}$, with $[\hat{q}, \hat{p}] = 2i$. Then, a Gaussian channel $\mathcal{G}$ acting on this system is a CPT map which preserves the Gaussian statistics of its states. Using the compact formulation of Ref. [8], every $\mathcal{G}$ can be associated with three symplectic invariants: transmission τ, rank r, and temperature $\bar{n}$. These invariants completely characterize the unique canonical form [7] $\mathcal{C}(\tau, r, \bar{n})$ which is unitarily equivalent to $\mathcal{G}$ (see Fig. 4). For a generic one-mode Gaussian channel $\mathcal{G}$ with transmission $\tau \neq 1$, we compute [13]

$$E_R(\mathcal{G}) = \max\left\{0, \log\left|\frac{1}{1-\tau}\right| - g(\bar{n})\right\}, \qquad (2)$$

where $g(x) := (x+1)\log(x+1) - x\log x$. This expression must be compared with

$$Q^{(1,g)}(\mathcal{G}) = \max\left\{0, \log\left|\frac{\tau}{1-\tau}\right| - g(\bar{n})\right\}, \qquad (3)$$

which is the quantum capacity $Q(\mathcal{G})$ restricted to a single use of the channel and pure Gaussian states [17]. It is known that $Q(\mathcal{G}) = Q^{(1,g)}(\mathcal{G})$ for a degradable channel [18], while $Q(\mathcal{G}) = 0$ for an antidegradable channel. In order to analyze and compare the previous quantities, we introduce the scaled thermal noise $\varepsilon := 2\bar{n}|1-\tau|$. For every $\tau \neq 1$, we then consider the minimal noises, ε_Q and ε_R, above which we have $Q^{(1,g)}(\mathcal{G}) = 0$ and $E_R(\mathcal{G}) = 0$, respectively. The corresponding threshold curves $\varepsilon_Q = \varepsilon_Q(\tau)$ and $\varepsilon_R = \varepsilon_R(\tau)$ are shown in Fig. 5. For $\tau \leq 1/2$, the one-mode Gaussian channel is known to be antidegradable [7], and therefore, we have $Q(\mathcal{G}) = 0$. In this case, no forward protocol is known to be secure; i.e., it is not known if $K(\mathcal{G}) = K_{\blacktriangleright}(\mathcal{G}) \neq 0$. However, for $0 < \tau \leq 1/2$ and $\varepsilon < \varepsilon_R(\tau)$, we have a wide region of antidegradability where $E_R(\mathcal{G}) > 0$ and, therefore, $K_{\blacktriangleleft}(\mathcal{G}) > 0$. In other words, even if Eve can reconstruct Bob's state, Alice and

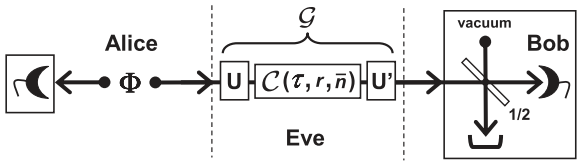

FIG. 4. *Canonical decomposition*. In the center of the figure (Eve), we show the decomposition of a one-mode Gaussian channel $\mathcal{G}$ into a canonical form $\mathcal{C}(\tau, r, \bar{n})$ up to a pair of unitaries $\hat{U}$ and $\hat{U}'$. *Noisy reverse protocol*. The reverse protocol with the rate of Eq. (4) is achieved by applying two inverse unitaries $\hat{U}^{-1}$ and $\hat{U}'^{-1}$ (not shown in the figure), restricting the quantum distribution to a two-mode squeezed vacuum state $\Phi = |\mu\rangle\langle\mu|$, and providing Alice and Bob with homodyne detectors (see boxes in the figure). In particular, Bob's homodyne detector is placed after one of the two output ports of a balanced beam splitter mixing the signal with the vacuum (the output of the other port is discarded).

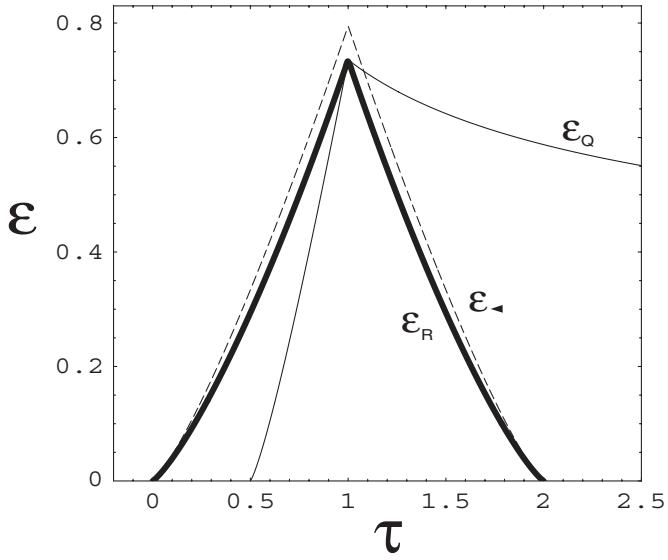

FIG. 5. Scaled thermal noise ε versus transmission $\tau \neq 1$. The thin solid curve $\varepsilon_Q = \varepsilon_Q(\tau)$ refers to $Q^{(1,g)}(\mathcal{G})$, while the thick solid curve $\varepsilon_R = \varepsilon_R(\tau)$ refers to $E_R(\mathcal{G})$. Above (below) these curves the corresponding capacities are zero (positive). Notice that $E_R(\mathcal{G})$ is positive in the region $0 < \tau \leq 1/2$ and $\varepsilon < \varepsilon_R(\tau)$, where the channel is antidegradable. The dashed curve $\varepsilon_{\blacktriangleleft} = \varepsilon_{\blacktriangleleft}(\tau)$ corresponds to $R_{\blacktriangleleft} = 0$, where $R_{\blacktriangleleft}$ is the rate given in Eq. (4).

Bob are still able to extract a secret key using a reverse protocol. This result is a remarkable feature of the reverse reconciliation, which is here stated in its full generality by considering arbitrary one-mode Gaussian channels.

As a final investigation, we prove an effective separation between $K_{\blacktriangleleft}$ and E_R, i.e., the existence of tighter lower bounds for $K_{\blacktriangleleft}$. In particular, we show a reverse key-distillation protocol whose rate $R_{\blacktriangleleft}$ can outperform $E_R(\mathcal{G})$, so that we have $K_{\blacktriangleleft}^{\otimes}(\mathcal{G}) \neq E_R(\mathcal{G})$ and, therefore, $K_{\blacktriangleleft}(\mathcal{G}) \neq E_R(\mathcal{G})$. This protocol exploits a noisy decoding measurement as in Ref. [19] and works as follows. For every $\mathcal{G}$, Alice and Bob can in principle apply two input-output unitaries that put $\mathcal{G}$ in canonical form. Assuming this reduction, Alice distributes n copies of a two-mode squeezed vacuum state $|\mu\rangle\langle\mu|$ with variance μ [20]. At the output of the channel, Bob's measurement setup consists of a balanced beam splitter followed by a random homodyne detection of $\hat{q}$ or $\hat{p}$, as shown in Fig. 4. The corresponding outcomes are classically processed to provide the two variables S_B and M. Then, Bob broadcasts the value of the assisting variable M, containing also the correct sequence of $\hat{q}$ and $\hat{p}$ detections. As a consequence, Alice performs the same sequence of homodyne detections on her systems A^n and then applies error correction and privacy amplification to get her estimation of the key S_B'. In the limits for $n \to +\infty$ and $\mu \to +\infty$ (and for $\tau \neq 1$), the honest users achieve the secret-key rate

$$R_{\blacktriangleleft} = \max\left\{0, \frac{1}{2}\log\frac{\lambda}{|1-\tau|} + g\left(\sqrt{\frac{w}{4\lambda}} - \frac{1}{2}\right) - g(\bar{n})\right\}, \quad (4)$$

where $\lambda := (|1-\tau| + w)/(1 + |1-\tau|w)$ and $w := 2\bar{n} + 1$. Let us denote by $\varepsilon_{\blacktriangleleft} = \varepsilon_{\blacktriangleleft}(\tau)$ the security threshold corresponding to $R_{\blacktriangleleft} = 0$. As shown in Fig. 5, there is a whole region for $0 < \tau < 2$ and $\varepsilon_R < \varepsilon < \varepsilon_{\blacktriangleleft}$, where $R_{\blacktriangleleft} > E_R(\mathcal{G}) = 0$. As a consequence, we generally have $K_{\blacktriangleleft}^{\otimes}(\mathcal{G}) \neq E_R(\mathcal{G})$ and, therefore, $K_{\blacktriangleleft}(\mathcal{G}) \neq E_R(\mathcal{G})$. Notice that when $\mathcal{G}$ is just a canonical form, the previous protocol can be implemented in practice, without the help of any quantum memory. Alice and Bob can in fact perform their detections step-by-step and then keep only the data measured in the same basis ($\hat{q}$ or $\hat{p}$). In this case the rate $R_{\blacktriangleleft}$ of Eq. (4) refers to the sifted key after the basis reconciliation.

In conclusion, we have introduced the notions of direct and reverse secret-key capacities of a quantum channel, specifying these notions for key-distillation too. In particular, the reverse capacities $K_{\blacktriangleleft}$ and $K_{\blacktriangleleft}^{\otimes}$ extend the concept of reverse reconciliation to a completely general scenario, where this procedure must be intended as a classical assistance by means of a single feedback CC. Such reverse capacities are lower bounded by an additive quantity E_R, which is connected with entanglement distillation and has been explicitly computed for one-mode Gaussian channels. For these channels, we have shown that the property of antidegradability does not necessarily preclude the possibility to extract a secret key. This is proven in full generality without any restriction on the Gaussian model. In other words, we have not restricted the one-mode Gaussian channel to any specific description like, e.g., a beam splitter with a thermal input. In this general scenario, we have also shown an explicit protocol which proves an effective separation between $K_{\blacktriangleleft}$ and E_R. In future works, our results can be exploited for exploring the ultimate cryptographic properties of arbitrary quantum channels.

The research of S. P. was supported by a Marie Curie Action within the 6th European Community Framework Programme. R. G. P. and S. L. were supported by the W. M. Keck foundation center for extreme quantum information theory (xQIT).

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] R. Renner, Ph.D. thesis, ETH Zürich, 2005; R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005); R. Renner and J. I. Cirac, arXiv:0809.2243.
[4] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[5] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[6] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[7] A. S. Holevo, Probl. Inf. Transm. **43**, 1 (2007); F. Caruso *et al.*, New J. Phys. **8**, 310 (2006).
[8] S. Pirandola *et al.*, Phys. Rev. Lett. **101**, 200504 (2008).
[9] A. Serafini *et al.*, Phys. Rev. A **71**, 012320 (2005).
[10] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, arXiv:0808.0210.
[11] For simplicity, we include error correction and privacy amplification (which correspond to a classical channel) into the decoding POVM.
[12] In the formulas for $K_{\blacktriangleright}(\mathcal{N})$, $K_{\blacktriangleleft}(\mathcal{N})$, $K_{\blacktriangleright}^{\otimes}(\mathcal{N})$, and $K_{\blacktriangleleft}^{\otimes}(\mathcal{N})$, we implicitly assume $\max x = \max\{0, x\}$.
[13] Detailed derivations will be presented elsewhere.
[14] In the formulas for $K_{\blacktriangleright}(\mathcal{N})$ and $K_{\blacktriangleright}^{\otimes}(\mathcal{N})$, the information quantities refer to the classical-quantum state $\omega_{XTB^nE^n} = \sum_{t,x} p(t|x)p(x)|x\rangle\langle x|_X \otimes |t\rangle\langle t|_T \otimes \rho_{B^nE^n}(x)$, where $\rho_{B^nE^n}(x)$ is Bob and Eve's state conditioned to the outcome x. A corresponding state $\omega_{YTA^nE^n}$ must be considered for $K_{\blacktriangleleft}(\mathcal{N})$ and $K_{\blacktriangleleft}^{\otimes}(\mathcal{N})$.
[15] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996); S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[16] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); Proc. R. Soc. A **461**, 207 (2005).
[17] A. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[18] M. M. Wolf *et al.*, Phys. Rev. Lett. **98**, 130501 (2007).
[19] R. García-Patrón and N. Cerf, arXiv:0806.3954.
[20] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).