Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate

Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate

Cosmo Lupo[1] and Seth Lloyd[1,2]
[1]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[2]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
(Received 7 July 2014; published 15 October 2014)

Quantum data locking is a protocol that allows for a small secret key to (un)lock an exponentially larger amount of information, hence yielding the strongest violation of the classical one-time pad encryption in the quantum setting. This violation mirrors a large gap existing between two security criteria for quantum cryptography quantified by two entropic quantities: the Holevo information and the accessible information. We show that the latter becomes a sensible security criterion if an upper bound on the coherence time of the eavesdropper's quantum memory is known. Under this condition, we introduce a protocol for secret key generation through a memoryless qudit channel. For channels with enough symmetry, such as the d-dimensional erasure and depolarizing channels, this protocol allows secret key generation at an asymptotic rate as high as the classical capacity minus one bit.

DOI: 10.1103/PhysRevLett.113.160502 PACS numbers: 03.67.Dd, 03.65.-w, 03.67.Hk

Introduction.—A famous theorem of Shannon's assesses the security of one-time pad encryption and shows that the secure encryption of a message of n classical bits requires a key of at least n bits [1]. When the message is encrypted in quantum bits or qubits, by contrast, the phenomenon of quantum data locking (QDL) [2–7] shows that the key required for secure encryption of an n bit message can be much less than n. In a typical QDL protocol, the legitimate parties, Alice and Bob, publicly agree on a set of $N = MK$ codewords in a high-dimensional quantum system. From this set, they then use a short shared private key of $\log K$ bits to select a set of M codewords that they will use for sending information. In the strongest QDL protocols known up to now, a key of *constant* length of about $O(\log 1/\epsilon)$ bits allows one to encrypt a message of n bits, in such a way that if an eavesdropper Eve intercepts and measures the quantum system, then she cannot access more than about ϵn bits of information about the message [6,8].

A number of works have been devoted to the role of QDL in physics and information theory [3–11]. However, only recently has QDL been considered in the presence of noise. Following the idea of the "quantum enigma machine" [10] for applying QDL to cryptography, a formal definition of the locking capacity of a communication channel has been recently introduced in [11] as the maximum rate at which information can be reliably and securely transmitted through a (noisy) quantum channel. Unlike the private capacity (which requires the communication to be secure according to the Holevo information criterion), the locking capacity requires security according to the accessible information criterion, possibly with the assistance of a preshared secret key whose length grows sublinearly in the number of channel uses. Since the Holevo information is an upper bound on the accessible information, the locking capacity is always larger than or equal to the private capacity. Clearly, the locking capacity cannot exceed the classical capacity (that is, the maximum rate for classical communication without any privacy). Two notions of capacity were defined in [11]: the *weak* locking capacity is defined by requiring security against an eavesdropper who measures the output of the complementary channel to the channel from Alice to Bob (that is, she measures the environment of the channel); the *strong* locking capacity is instead defined by assuming that the eavesdropper is able to measure the very input of the channel. In general, the weak locking capacity is larger than or at most equal to the strong locking capacity, as any strong locking protocol also defines a weak locking one. As shown in [12], there exist qudit channels with low (one bit per channel use) or even zero private capacity whose weak locking capacity is larger than $\frac{1}{2}\log d$. In particular, the examples in [12] refer to effectively noiseless channels whose classical capacity is $\log d$ bits.

Here we introduce a protocol that allows high rate QDL over a memoryless (noisy) qudit channel, and we apply it to define a secret key generation protocol which is secure in the sense of strong locking. The protocol allows secret key generation at a rate as high as the classical capacity minus one bit, independently of the channel having any private capacity. This result shows that by using a weaker security criterion (the accessible information) one can increase the secret key generation rate up to almost the classical capacity. As explained below, the accessible information becomes a sensible criterion in a scenario where Alice and Bob know an upper bound on the coherence time of Eve's quantum memory.

Overview.—One of the most profound implications of QDL in quantum information theory is the existence of a potentially large gap between two security criteria for quantum cryptography [13]. Suppose that Eve has access

to the state $\rho_{E|x}$ given that the classical message x has been sent by Alice to Bob. The widely accepted security criterion in quantum cryptography requires that Eve's state is ϵ-close to being a product state in the operator trace norm [13], that is,

$$\left\| \sum_x p_X(x)|x\rangle\langle x| \otimes \rho_{E|x} - \sigma \otimes \rho_E \right\|_1 \leq \epsilon, \qquad (1)$$

where $\|\cdot\|_1 = \mathrm{Tr}|\cdot|$, $p_X(x)$ is the probability that the input random variable X takes value x, $\sigma = \sum_x p_X(x)|x\rangle\langle x|$, and $\rho_E = \sum_x p_X(x)\rho_{E|x}$. By application of the Alicki-Fannes inequality [14], Eq. (1) implies

$$\chi(\mathcal{E}) \leq 4\epsilon \log |X| + 2h_2(\epsilon), \qquad (2)$$

where $\chi(\mathcal{E}) := S(\rho_E) - \sum_x p_X(x) S(\rho_{E|x})$ is the Holevo information of the ensemble of quantum states $\mathcal{E} = \{p_X(x), \rho_{E|x}\}$, $S(\rho) := -\mathrm{tr}\rho\log\rho$ denotes the von Neumann entropy, $|X|$ is the cardinality of the input variable X, and $h_2(\epsilon) = -\epsilon\log\epsilon - (1-\epsilon)\log(1-\epsilon)$ denotes the binary Shannon entropy. A fundamental feature of the Holevo information is that it obeys the property of total proportionality [2]. This means that if Eve is given k bits (or $k/2$ qubits) of side information about the message, then her Holevo information cannot increase by more than k bits.

In the early days of quantum cryptography, the accessible information criterion was used instead of the Holevo information (see, e.g., Ref. [15]). This criterion requires that the result of any measurement Eve can make on her share of the quantum state is ϵ-close to being uncorrelated with the message. Suppose that a measurement $\mathcal{M}_{E\to\hat{X}}$ maps $\rho_{E|x}$ into the classical variables $\hat{X}$ with conditional probability distribution $p_{\hat{X}|X}$. Then one considers the norm

$$\sup_{\mathcal{M}_{E\to\hat{X}}} \|p_{\hat{X}|X}p_X - p_{\hat{X}}p_X\|_1 := \sup_{\mathcal{M}_{E\to\hat{X}}} \sum_{x,\hat{x}} |p_{\hat{X}|X}(\hat{x}|x)p_X(x) - p_{\hat{X}}(\hat{x})p_X(x)|, \qquad (3)$$

where $p_{\hat{X}}(\hat{x}) = \sum_x p_{\hat{X}|X}(\hat{x}|x)p_X(x)$. If (3) is less than ϵ, then the Alicki-Fannes inequality implies [16]

$$I_{\mathrm{acc}}(\mathcal{E}) \leq 4\epsilon\log|X| + 2h_2(\epsilon), \qquad (4)$$

where $I_{\mathrm{acc}}(\mathcal{E}) := \sup_{\mathcal{M}_{E\to\hat{X}}} I(X;\hat{X})$ is the accessible information of the ensemble $\mathcal{E} = \{p_X(x), \rho_{E|x}\}$, $I(X;\hat{X}) = H(X) + H(\hat{X}) - H(X\hat{X})$ is the classical mutual information between the message variable X and the measurement result $\hat{X}$, and $H(X) = -\sum_x p_X(x)\log p_X(x)$ denotes the Shannon entropy. Unlike the Holevo information, the accessible information does not obey the property of total proportionality [2]. This implies that the accessible information is, in general, not stable under loss of information to Eve. That is, if Eve obtains k bits of side information about the message, there is no guarantee that her accessible information will increase by a proportionate amount (and indeed it can increase by an arbitrarily large amount according to the QDL effect).

While it is clear that at a certain point Eve has to measure her share of the quantum state, the accessible information criterion is sensitive to the time at which such a measurement takes place. If Eve obtains a small amount of side information *before* she measures her share, then she could use this information to increase her accessible information by a disproportionate amount. As a consequence, accessible information security is not, in general, composable [13]; that is, a protocol that is secure according to the accessible information criterion may not remain so when used as a subroutine of another communication protocol. On the other hand, if Eve obtains k bits of side information *after* the measurement, then (since the classical mutual information obeys total proportionality) her accessible information cannot increase by more than k bits and composable security will be granted [18].

As is customary in quantum key distribution, our secret key generation protocol is divided into two parts. The first part is a QDL protocol in which Alice encodes her share of the raw key into quantum states and sends them to Bob via an insecure quantum channel. After Bob measures the output of the channel, he obtains his own share of the raw key that has to be reconciled with Alice's one. The security of this part of the protocol is granted by the QDL effect and is quantified by the accessible information. In the second part of the protocol, Alice sends error correcting information to Bob through a public channel (in our case there is no need for privacy amplification since the raw key is already secure due to QDL [19]). We are hence in a situation where the QDL protocol is used as a subroutine of the key distribution protocol. This implies that the latter will be secure only if the former is secure in the composable sense. As discussed above, this is, in general, true only under the assumption that Eve has already measured her share of the quantum state when the second part of the protocol takes place. If Alice knows that Eve's quantum memory has a coherence time not larger than τ, then she can simply wait for a sufficiently long time before sending error correcting information to Bob through the public channel. After such a time, Eve has either made a measurement or her quantum memory has completely decohered. In both cases the security of the QDL protocol will be composable.

For any value of τ Alice and Bob can apply a doubly blocked communication protocol, where they first send a data packet down the quantum channel and then wait a time τ before doing all the required classical post-processing. In the meantime Alice can keep sending Bob independent data packets that will be processed at a later time. The larger τ is, the longer Alice and Bob have to wait to guarantee the security of the protocol. Clearly, too large values of τ would make the protocol unpractical. However, it is worth

remarking that, from an abstract point of view, in a stationary regime the asymptotic communication rate is independent of τ, and it remains finite even in the limit $\tau \to \infty$.

Accessible information security.—Our starting point is a new QDL protocol defined for a memoryless d-dimensional channel (for any $d \geq 3$). Upon n uses of the qudit channel $\mathcal{N}$, the protocol allows one to lock classical information using an ensemble of input codewords $\mathcal{E}$ that are separable among different channel uses. The protocol requires Alice and Bob to initially share a secret key of $\log K_n$ bits, which is consumed at an asymptotic rate of $\lim_{n\to\infty}(1/n)\log K_n = 1$ bit per channel use.

Let us fix a qudit basis $\{|\omega\rangle\}_{\omega=1,\ldots,d}$ and its Fourier conjugate $\{|m\rangle\}_{m=1,\ldots,d}$, with

$$|m\rangle = \frac{1}{\sqrt{d}}\sum_{\omega=1}^{d} e^{i2\pi m\omega/d}|\omega\rangle. \tag{5}$$

We consider the "phase ensemble" of qudit unitary transformations of the form

$$U = \sum_{\omega=1}^{d} e^{i\theta(\omega)}|\omega\rangle\langle\omega|, \tag{6}$$

where the angles $\theta(\omega)$, for $\omega = 1, \ldots, d$, are d i.i.d. (independent and identically distributed) random variables. We require that these variables are distributed in such a way that $\mathbb{E}[e^{i\theta(\omega)}] = 0$ [21]. To define the QDL protocol upon n uses of the channel, Alice and Bob publicly agree on a set of K_n n-qudit unitaries of the form $\{\otimes_{j=1}^{n} U_k^j\}_{k=1,\ldots,K_n}$. The value of the index k plays the role of a secret key of $\log K_n$ bits initially shared by Alice and Bob. Alice prepares, with equal probability, one of the d^n orthogonal vectors $|\boldsymbol{m}\rangle = \otimes_{j=1}^{n}|m^j\rangle$ (the $n\log d$ bits string $\boldsymbol{m}$ will serve as a raw key for Alice) and then *scrambles* it by applying one of the unitary transformations, yielding

$$|\Psi_{\boldsymbol{m}k}\rangle = \otimes_{j=1}^{n} U_k^j|m^j\rangle = \sum_{\boldsymbol{\omega}} \frac{e^{i\sum_{j=1}^{n}[2\pi m^j\omega^j/d+\theta_k^j(\omega^j)]}}{\sqrt{d^n}}|\boldsymbol{\omega}\rangle. \tag{7}$$

We prove that if Eve (who does not know the value of the index k) intercepts the whole train of qudit systems and measures them, then she can only retrieve a negligible amount of information about the input variable $\boldsymbol{m}$. In particular, we show that there exist choices of the scrambling unitaries U_k^j that guarantee that Eve's accessible information is arbitrarily small if n is large enough. To prove this, we show that this property is almost certainly true if each U_k^j is sampled i.i.d. from the phase ensemble of unitaries [22].

Let Eve intercept and measure the train of n qudits sent by Alice. A measurement is described by a collection of positive operator-valued measurement (POVM) elements $\{\mu_i|\Phi_i\rangle\langle\Phi_i|\}_i$, where $\sum_i\mu_i = d^n$, $\mu_i > 0$, and $|\Phi_i\rangle$ are unit vectors (possibly entangled over the n qudit systems). Since Eve does not have access to the secret key, we have to compute the accessible information of the ensemble of states $\mathcal{E} = \{p_{\boldsymbol{m}}, \frac{1}{K_n}\sum_{k=1}^{K_n}|\Psi_{\boldsymbol{m}k}\rangle\langle\Psi_{\boldsymbol{m}k}|\}$, averaged over the values of the secret key, where $p_{\boldsymbol{m}} = 1/d^n$ is the probability of the message $\boldsymbol{m}$. A straightforward calculation then yields

$$I_{acc}(\mathcal{E}) = \log d^n - \min_{\{\mu_i|\Phi_i\rangle\langle\Phi_i|\}}\sum_i \frac{\mu_i}{d^n}H[Q(\Phi_i)], \tag{8}$$

where $Q(\Phi)$ denotes the d^n-dimensional real vector with non-negative entries

$$Q_{\boldsymbol{m}}(\Phi) = \frac{1}{K_n}\sum_{k=1}^{K_n}|\langle\Phi|\Psi_{\boldsymbol{m}k}\rangle|^2, \tag{9}$$

and

$$H[Q(\Phi)] = -\sum_{\boldsymbol{m}} Q_{\boldsymbol{m}}(\Phi)\log Q_{\boldsymbol{m}}(\Phi) \tag{10}$$

is its Shannon entropy [notice that $\sum_{\boldsymbol{m}}Q_{\boldsymbol{m}}(\Phi) = 1$].

Since $\sum_i\mu_i/d^n = 1$, the positive coefficients μ_i/d^n can be interpreted as probability weights. We can then apply a standard convexity argument (the minimum is never larger than the average) to obtain an upper bound on Eve's accessible information:

$$I_{acc}(\mathcal{E}) \leq \log d^n - \min_{|\Phi\rangle} H[Q(\Phi)], \tag{11}$$

where the minimum is over all n-qudit unit vectors. According to this expression, an upper bound on the accessible information follows from a lower bound on the minimum Shannon entropy $\min_{|\Phi\rangle}H[Q(\Phi)]$.

To show that $I_{acc}(\mathcal{E})$ can be made arbitrarily small, we apply concentration inequalities [23,24] to the quantities $Q_{\boldsymbol{m}}(\Phi)$'s. Notice that the latter are random variables if the unitaries U_k^j are chosen randomly from the phase ensemble. The main idea is that the $Q_{\boldsymbol{m}}(\Phi)$'s will concentrate around their mean value $1/d^n$. We prove (see [25]) that the probability of a deviation larger than ϵ/d^n is exponentially suppressed. This property will be used to show that $I_{acc}(\mathcal{E}) \lesssim \epsilon\log d^n$ (up to a probability exponentially small in d^n). In order for this to be true, the number of different scrambling unitaries has to satisfy [27]

$$K_n > 2^{n+1}\left(\frac{1}{\epsilon^2}\ln d^n + \frac{2}{\epsilon^3}\log\frac{5}{\epsilon}\right). \tag{12}$$

This implies an asymptotic secret key consumption rate of $\lim_{n\to\infty}(1/n)\log K_n = 1$ bit per channel use. We remark that we can put $\epsilon = 2^{-n^c}$, for any $c < 1$, and still lock data

with a secret key consumption rate of one bit independently of d.

Secret key generation.—As an example, we consider the case of a collective attack by Eve, which induces the memoryless qudit channel $\mathcal{N}$ from Alice to Bob. (Since our QDL is secure in the strong locking sense, it will be secure also in the case of general coherent attacks.) For any given value of k, Bob receives one of the d^n equiprobable n-qudit states $\mathcal{N}^{\otimes n}(|\Psi_{\boldsymbol{m}k}\rangle\langle\Psi_{\boldsymbol{m}k}|)$ at the output of the channel. For the sake of simplicity, we consider the case of unitarily covariant channels, that is, satisfying $\mathcal{N}(U\rho U^\dagger) = U\mathcal{N}(\rho)U^\dagger$ for any qudit unitary U. (For example, this is the case of the erasure and depolarizing channels.) To decrypt the message, Bob can apply the inverse unitary $\otimes_{j=1}^n U_k^{j-1}$. After the decryption, Bob obtains n independent instances of the qudit ensemble of output states $\{1/d, \mathcal{N}(|m\rangle\langle m|)\}$. To decode this, Bob applies a measurement on these states, obtaining a raw key $\hat{\boldsymbol{m}}$ given by the measurement outcomes. Finally, to distill a perfectly correlated key, Alice should send error correcting information to Bob. If Bob makes the optimal measurement, they will asymptotically achieve about $n\chi_{\mathcal{N}}(\mathcal{E})$ bits of common randomness, where $\chi_{\mathcal{N}}(\mathcal{E}) = S[(1/d)\sum_m \mathcal{N}(|m\rangle\langle m|)] - (1/d)\sum_m S[\mathcal{N}(|m\rangle\langle m|)]$ is the Holevo information of the channel [28]. At this stage we make use of the assumption that Alice knows an upper bound τ on the coherence time of Eve's quantum memory. Since the error correcting information will be transmitted on a public communication channel, Alice must wait for a time larger than τ before being able to safely send error correcting information to Bob. In this way Alice and Bob establish a secret key of about $n\chi_{\mathcal{N}}(\mathcal{E})$ bits starting from one of about n bits. If $\chi_{\mathcal{N}}(\mathcal{E}) > 1$, they can then run the protocol again by recycling part of the obtained secret key and achieve an overall asymptotic rate of secret key generation of $R = \chi_{\mathcal{N}}(\mathcal{E}) - 1$ bits per channel use.

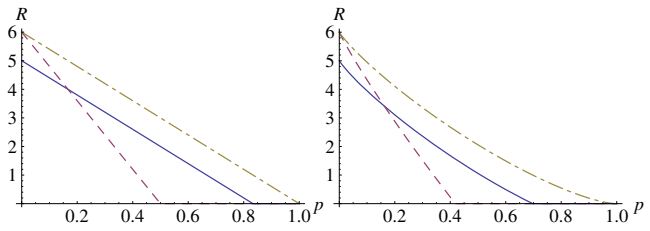

FIG. 1 (color online). Comparison of several communication rates (in bits per channel use). Left panel: Asymptotic rates for the qudit erasure channel as a function of the erasure probability p. We show the QDL secret key generation rate (solid line), private capacity $P = (1-2p)\log d$ (dashed line), and classical capacity $C = (1-p)\log d$ (dash-dotted line). Right panel: Asymptotic rates for the qudit depolarizing channel as a function of the depolarizing probability p. We show the QDL secret key generation rate (solid line), the asymptotic secret key generation rate achieved by the protocol in [29] (we notice, incidentally, that this rate achieves the Hashing bound) (dashed line), and classical capacity (dash-dotted line).

In particular, for a unitarily covariant channel, such as the qudit erasure channel and the qudit depolarizing channel, the Holevo information $\chi_{\mathcal{N}}(\mathcal{E})$ equals the classical capacity $C_{\mathcal{N}}$; hence, QDL allows for a secret key generation rate of $R = C_{\mathcal{N}} - 1$ bits, just one bit below the channel's classical capacity.

Figure 1 shows a comparison of the secret key generation rates of our protocol $R = C_{\mathcal{N}} - 1$ with the classical capacity and the private capacity (which equals the secret key generation rate with the assistance of one-way public communication from Alice to Bob) for the qudit erasure and depolarizing channels.

Conclusions.—According to the QDL effect, a large gap exists between two natural security definitions, one related to the Holevo information and the other to the accessible information (the difference between these two entropic quantities is known as quantum discord [30]). In this Letter we have shown that, if the latter criterion is assumed, one can generate a secret key through a memoryless noisy channel at a rate as high as the classical capacity minus one bit, independently of the channel's private capacity. The price to pay for such a high rate of secret key generation is that the accessible information criterion does not guarantee unconditional and composable security. Our protocol guarantees composable security under the assumption that Alice and Bob know that the coherence time of Eve's quantum memory is no larger than τ. Interestingly enough, the key generation rate is independent of the value of τ, as long as Alice and Bob know this value (though large values of τ would make the protocol unpractical).

One should also ensure that the QDL is robust under leakage to Eve of a small fraction of the key or the message. Indeed, as a small key allows one to (un)lock a disproportionate amount of information, it could very well happen that the leakage to Eve of a few bits may allow her to uncover a much larger portion of the message. This problem has been recently addressed in [8], where it is shown that there exist QDL protocols that can be made resilient to loss of a given amount of information by increasing the secret key consumption by a proportional amount. The conclusions of [8] may be straightforwardly generalized to the protocol discussed here and hence applied to guarantee the robustness of our QDL protocol for noisy channels.

The QDL states and unitaries in Eqs. (5) and (6) are particularly suitable for quantum optics applications, where a qudit can be encoded by coherently splitting a single photon over d modes (e.g., path, temporal, linear momentum, orbital angular momentum) and then by applying i.i.d. random phases to the different modes by modulating an array of phase shifters. For example, this kind of transformation can be implemented by group velocity dispersion, and our protocol can be realized by a simple modification of standard d-dimensional quantum key

distribution protocols; see, e.g., [31]. As discussed in [10], this requires passive linear optical transformations and photodetection. In the unary encoding of a single photon over d modes, linear losses are modeled by a qudit erasure channel, and the depolarizing channel model provides a standard benchmark for assessing the performance of quantum key distribution. Different channel models reflect different collective attacks conducted by the eavesdropper. While the final key generation rate may depend on the channel model, the security of our QDL protocol (which holds in the strong locking sense) does not depend on the details of the channel, and it also holds in the case of coherent attacks. Finally, let us remark that unlike previous QDL protocols, the one presented here does not require d to be arbitrarily large. Instead, our protocol requires an increasing number of channel uses (as typical of i.i.d. information theory), while it is sufficient to assume $d \geq 3$.

We are grateful to Frédéric Dupuis, Andreas Winter, and especially to Mark M. Wilde for helpful discussions and comments. This research was supported by the DARPA Quiness Program through U.S. Army Research Office Grant No. W31P4Q-12-1-0019.

[1] C. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[2] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[3] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[4] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Phys. Rev. A **78**, 022316 (2008).
[5] D. Leung, J. Phys. Conf. Ser. **143**, 012008 (2009).
[6] O. Fawzi, P. Hayden, and P. Sen, J. ACM **60**, 44 (2013).
[7] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, Proc. R. Soc. Edinburgh, Sect. A **469**, 20130289 (2013).
[8] C. Lupo, M. M. Wilde, and S. Lloyd, Phys. Rev. A **90**, 022326 (2014).
[9] J. A. Smolin and J. Oppenheim, Phys. Rev. Lett. **96**, 081302 (2006).
[10] S. Lloyd, arXiv:1307.0380.
[11] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Phys. Rev. X **4**, 011016 (2014).
[12] A. Winter, arXiv:1403.6361.
[13] R. König, R. Renner, A. Bariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502 (2007).
[14] R. Alicki and M. Fannes, J. Phys. A **37**, L55 (2004).
[15] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[16] Vice versa, the Pinsker inequality (see, e.g., Ref. [17] and references therein) implies that if $I_{\mathrm{acc}}(\mathcal{E}) \leq \epsilon$, then the norm in Eq. (3) is smaller than $\sqrt{(2\ln 2)\epsilon}$.
[17] A. A. Fedotov, P. Harremoës, and F. Topsøe, IEEE Trans. Inf. Theory **49**, 1491 (2003).
[18] The Holevo information does not suffer from this dependence on external variables, such as the timing of the measurement. This is the reason why the latter is the preferred and widely accepted security criterion for quantum cryptography.
[19] We remark that this setting corresponds to the one detailed in Sec. 4.1 of Ref. [20], where Eve is unable to eavesdrop on any information from the quantum channel (due to the QDL effect in our case), but transmission errors may occur in the communication from Alice to Bob (due to the noise introduced by the channel).
[20] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[21] For instance, the angles $\theta(\omega)$ can be uniformly distributed in $[0, 2\pi[$, or assume the binary values $\theta(\omega) \in \{0, \pi\}$ with equal probabilities.
[22] The proof strategy is analogous to the one of [8] and is based on similar ideas already applied to other QDL protocols [3,6].
[23] A. Maurer, JIPAM **4**, 15 (2003).
[24] R. Ahlswede and A. J. Winter, IEEE Trans. Inf. Theory **48**, 569 (2002).
[25] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.160502, which contains the proof and includes Ref. [26].
[26] M. Fannes, Commun. Math. Phys. **31**, 291 (1973); K. M. R. Audenaert, J. Phys. A **40**, 8127 (2007).
[27] It could, in principle, be possible to improve this bound.
[28] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[29] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).
[30] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[31] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87**, 062322 (2013).