Entropy **2015**, *17*, 3194-3204; doi:10.3390/e17053194

OPEN ACCESS
entropy
ISSN 1099-4300
www.mdpi.com/journal/entropy

Article

Quantum Data Locking for Secure Communication against an Eavesdropper with Time-Limited Storage

Cosmo Lupo

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA; E-Mail: clupo@mit.edu; Tel.:+1-617-324-4886

Received: 6 April 2015 / Accepted: 7 May 2015 / Published: 13 May 2015

Abstract: Quantum cryptography allows for unconditionally secure communication against an eavesdropper endowed with unlimited computational power and perfect technologies, who is only constrained by the laws of physics. We review recent results showing that, under the assumption that the eavesdropper can store quantum information only for a limited time, it is possible to enhance the performance of quantum key distribution in both a quantitative and qualitative fashion. We consider quantum data locking as a cryptographic primitive and discuss secure communication and key distribution protocols. For the case of a lossy optical channel, this yields the theoretical possibility of generating secret key at a constant rate of 1 bit per mode at arbitrarily long communication distances.

Keywords: quantum cryptography; quantum data locking; quantum enigma machine

1. Introduction

Quantum cryptography is a mature and well established research field, at the core of which there is the fact, first noted about 30 years ago, that quantum physics allows for provably secure communication through an insecure communication channel [1]. The most successful application of this core idea is quantum key distribution. In this protocol two honest parties, usually called Alice and Bob, wish to use a communication channel to generate a common bit-string, called a key, which must remain secret to an eavesdropper, usually called Eve, who could intercept the signal and tamper with the communication line (this secret key may be then used as a one-time pad). The security of the generated key is unconditional. That is, it is guaranteed by the laws of quantum physics and holds even if Eve possesses perfect technology and unlimited computational power (including a quantum computer). The price to pay for

unconditional security is that the achievable rates of secret-key generation (measured in bits of secret key per use of the communication channel) are extremely low.

Consider for instance the recent results of [2], which provide upper bounds on the secret-key generation rates of a communication channel. Suppose for example that the communication channel is a lossy single-mode optical fiber that attenuates the input signal by a factor η. For linear loss, η decreases exponentially with the length of the fiber. According to [2], for small values of η (*i.e.*, for long communication distances) the maximum secret-key generation rate through such a channel cannot be larger that about η bits per mode, that is, the key rate decreases exponentially with the communication distance. This upper bound on the key generation rate can be compared with the rates of non-private communication. Unlike secret-key generation, one can in principle send non-private classical information through a lossy fiber at a constant rate across arbitrarily long distances, if sufficient input power is provided.

Here we ask the following question: *Is it possible, by assuming a realistic constraint on Eve's technological capabilities, to substantially improve the rate-loss tradeoff?* We will show that, based on our previous results, a substantial improvement in the secret key can be achieved against an eavesdropper who, although endowed with unlimited computational power (including a quantum computer), can store quantum information only for a finite time. Indeed, any realistic quantum memory is subject to decoherence and can store quantum information only for a time of the order of its coherence time. Given that quantum information is sent at a certain rate, this condition is equivalent to saying that Eve can store only a limited number of qubits of quantum information, which is the assumption of the bounded storage model for quantum cryptography [3]. We have indeed shown that this assumption on the ability of storing quantum information allows us to increase the rate of secret-key generation by a large amount. For quantum systems with finite dimensions, certain communication channels allow for a secret-key rate almost equal to the rate of non-private communication (less than 1 bit below it) [4,5]. Also, for optical lossy channels (as the optical fiber in the example above) it is in principle possible to achieve a constant secret-key rate of 1 bit per mode for arbitrarily long distances [6], that is, the key rate does not decay with the communication distance. We remark that, although no specific restriction is imposed on Alice and Bob, they do not need a perfect quantum memory to run the communication protocol.

2. Security against an Eavesdropper with Time-Limited Storage

Suppose Alice wishes to use a memoryless quantum channel $\mathcal{N}_{A\to B}$ to send private information to Bob. Upon n uses of the channel, she encodes M messages $x = 1, \ldots, M$, each with probability $p_X(x)$, into the input states $\rho_A(x)$'s. Then Bob will receive the output states $\rho_B(x) = \mathcal{N}_{A\to B}^{\otimes n}(\rho_A(x))$. Let us recall that a quantum channel $\mathcal{N}_{A\to B}$ can always be represented as the reduced dynamics induced by a unitary transformation on a larger space, that is,

$$\mathcal{N}_{A\to B}(\rho_A) = \mathrm{Tr}_E \left[U \left(\rho_A \otimes \omega_E \right) U^\dagger \right] \tag{1}$$

where ω_E is a pure state for a quantum system associated with the environment of the channel, and U is a unitary transformation coupling the system with its environment. In the worst-case scenario the eavesdropper Eve might collect all the information leaking into the channel environment, in which case

the state obtained by Eve reads $\rho_E(x) = \tilde{\mathcal{N}}^{\otimes n}_{A\to E}(\rho_A(x))$, where $\tilde{\mathcal{N}}_{A\to E}$ is the complementary channel, defined as

$$\tilde{\mathcal{N}}_{A\to E}(\rho_A) = \mathrm{Tr}_B\left[U\left(\rho_A \otimes \omega_E\right)U^\dagger\right] \tag{2}$$

Let us consider the state

$$\sigma_{XE} = \sum_{x=1}^{M} p_X(x)|x\rangle\langle x| \otimes \rho_E(x) \tag{3}$$

This state describes the correlations between the classical input x and Eve's quantum system. To quantify the security of the channel one usually considers the trace distance [7]

$$\Delta := \frac{1}{2}\left\|\sigma_{XE} - \sigma_X \otimes \sigma_E\right\|_1 \tag{4}$$

where $\sigma_X = \sum_{x=1}^{M} p_X(x)|x\rangle\langle x|$, $\sigma_E = \sum_{x=1}^{M} p_X(x)\rho_E(x)$ are the reduced states of σ_{XE}, and $\|\cdot\|_1 = \mathrm{Tr}|\cdot|$. If the trace distance is small, this implies that the state σ_{XE} is close to the uncorrelated state $\sigma_X \otimes \sigma_E$. Recall that, from an operational point of view, the trace distance is the bias in distinguishing the states by a measurement. The trace norm is indeed the standard security quantifier used in quantum key distribution: if $\Delta \leq \epsilon$, the communication protocol is secure up to a probability ϵ [7].

The trace norm is the proper security quantifier in a generic setting. However, under certain assumptions on the technological capabilities of the eavesdropper, we can adopt a weaker security criterion. If we know that the eavesdropper cannot store quantum information for longer than a given time τ, then we know that she is forced to make a measurement within a time τ after she received the quantum state. This leads us to consider a post-measurement security quantifier. A measurement Λ on Eve's system defines a classical random variable Y with conditional probability distribution

$$p^{\Lambda}_{Y|x}(y) = \mathrm{Tr}(\rho_E(x)\Lambda(y)) \tag{5}$$

where $\{\Lambda_y\}$ are POVM elements, satisfying $\Lambda_y \geq 0$ and the completeness relation $\sum_y \Lambda_y = \mathbb{I}$. A post-measurement security criterion requires that the joint probability distribution $p^{\Lambda}_{XY}(x,y) = p_X(x)p^{\Lambda}_{Y|x}(y)$ is close to the product of its marginals $p_X(x)p^{\Lambda}_Y(y)$, where $p^{\Lambda}_Y(y) = \sum_x p_X(x)p^{\Lambda}_{Y|x}(y)$, for all measurements Λ. Here we consider the distance

$$\Delta_{\mathrm{acc}} := \max_{\Lambda} \frac{1}{2}\left\|p^{\Lambda}_{XY} - p_X p^{\Lambda}_Y\right\|_1 \tag{6}$$

(the meaning of the subscript "acc" will be clear in the next paragraph) where $\frac{1}{2}\|p^{\Lambda}_{XY} - p_X p^{\Lambda}_Y\|_1 = \frac{1}{2}\sum_{x,y}|p_X(x)p^{\Lambda}_{Y|x}(y) - p_X(x)p^{\Lambda}_Y(y)|$ is the total variation distance. The operational meaning of Δ_{acc} is the bias in distinguishing between the classical distributions p^{Λ}_{XY} and $p_X p^{\Lambda}_Y$. In other words, Δ_{acc} is the bias in distinguishing between the states σ_{XE} and $\sigma_X \otimes \sigma_E$ by a local measurement.

The accessible information is an entropic quantity naturally associated with the distance Δ_{acc}. Let us recall that the accessible information is defined as the maximum classical mutual information that Eve can obtain about the input variable by local measurements on her subsystem, that is,

$$I_{\mathrm{acc}}(X;E) = \max_{\Lambda} I(X;Y) \tag{7}$$

where $I(X;Y) = H(X) + H(Y) - H(XY)$ is the classical mutual information of the variables X and Y. From Alicki-Fannes' inequality [8]:

$$I_{\rm acc}(X;E) \leq 2\Delta_{\rm acc} \log d^n + \eta(2\Delta_{\rm acc}) \tag{8}$$

where $\eta(\,\cdot\,) = -(\,\cdot\,)\log(\,\cdot\,)$. On the other hand, Pinsker's inequality yields [9]

$$\Delta_{\rm acc} \leq \sqrt{\frac{1}{2} I_{\rm acc}(X;E)} \tag{9}$$

These two inequalities imply the effective equivalence of $\Delta_{\rm acc}$ and $I_{\rm acc}(X;E)$ as security quantifiers. If the accessible information is small, Pinsker's inequality implies that the $\Delta_{\rm acc}$ is also small. Viceversa, if $\Delta_{\rm acc}$ is small, then the accessible information is small provided $\Delta_{\rm acc} \ll (\log d^n)^{-1} = n^{-1}/\log d$.

3. Quantum Data Locking

In a quantum data locking protocol [10,11] the legitimate parties Alice and Bob initially share a secret key of $\log K$ bits. They use the key to agree on a code to be used to send classical information through a quantum channel. If they publicly declare a list of K codes, then they can use the shared key to secretly agree on one of them. On the other hand, if an eavesdropper, who does not know the secret key, intercepts and measures the quantum codewords, we require that her accessible information about the input messages must be negligibly small.

Let us first consider the case in which the channel from Alice to Bob is noiseless. In this case Alice can simply encode classical information using a set of orthogonal n-qudit states belonging to a given basis. If Bob knows the basis chosen by Alice, he can reliably decode by measuring in the same basis. Suppose that Eve intercepts the whole set of n qudits. To ensure the security of the quantum data locking protocol, K must be chosen large enough to make Eve's mutual information negligibly small. It was shown in [12] (see also [11,13,14]) that for n large enough, there exist choices of $\log K = 4\log 1/\epsilon + O(\log\log 1/\epsilon)$ bases such that $I_{\rm acc}(X;E) \leq \epsilon \log d^n$.

Notice that for any given (small) ϵ and for n large enough, this implies that a relatively small secret key is sufficient to *lock* an arbitrarily long message. It is worth stressing that this result represents a strong violation of classical information theory in the quantum framework. Indeed, it is well known that in the classical framework the secure encryption of a message of m bits requires at least m bits of secret key (this result is at the basis of the security of the one-time pad). The results of [12] imply that one can lock information through a noiseless qudit channel at a rate of $\log d$ bits per channel use by consuming secret key at a rate (in bits per channel use) of

$$k = \frac{1}{n}\log K \simeq \frac{1}{n}\log 1/\epsilon \tag{10}$$

Such a secret-key consumption rate is asymptotically zero if ϵ is constant or decreases sub-exponentially in n.

While the phenomenon of quantum data locking has been known for more than 10 years, the problem of locking information through noisy channels has been considered only recently in [15], where the notion of locking capacity of a noisy channel was introduced. The latter is defined as the maximum

number of bits per channel use that can be reliably sent through a given channel, in such a way that the eavesdropper's accessible information is negligibly small. Two notions of locking capacities have been defined. The *weak-locking capacity* is defined by requiring security against an eavesdropper who measures the output of the complementary channel of the channel from Alice to Bob. The *strong-locking capacity* instead requires security against an eavesdropper having direct access to the input states prepared by Alice. In an optical setting, a cipher based on the quantum data locking effect is dubbed a *quantum enigma machine* [16]. While the twentieth century's Enigma machine relied on computational security (the presumed difficulty of inverting the complex pattern of electromechanical elements that was used to scramble the inputs of a typing machine), a quantum enigma machine would ensure provable information-theoretical security against an eavesdropper who cannot store quantum information for an arbitrarily long time.

Given a quantum channel, it is natural to compare the weak-locking capacity with the private capacity [17,18]. The latter is defined as the maximum rate of secret communication given that the security is defined in terms of the trace distance (4). A private communication protocol allows for unconditional security and does not rely on any assumption on the technological capability of the eavesdropper. While it is easy to see that the weak-locking capacity is at least equal to the private capacity [15], it is non-trivial to show that a (large) gap exist between these two capacities. The first examples of noisy channels with a weak-locking capacity much larger than the private capacity were provided in [19].

Unlike the case of a noiseless channel, in a noisy setting Alice and Bob should use codes that allow for both data locking and error correction. In our recent works we have derived families of random codes that allow for error correction and data locking through noisy channels that have enough symmetry (These channels are covariant under the action of a symmetry group. We expect a lower data locking rate for channels that do not have such a symmetry). Examples include the erasure and depolarizing channels (in finite dimensions) [4,5] and the lossy bosonic channel (for continuous-variable systems) [6]. The price to pay for being able to correct the errors and hence send information reliably through the noisy channel, is a higher rate of secret-key consumption. Assume that Alice encodes M messages into n uses of a memoryless qudit channel. In a strong-locking scenario, in order to guarantee $I_{\text{acc}}(X;E) \leq \epsilon \log d^n$ we need an asymptotic secret-key consumption rate (in bits per channel use) of (assuming that ϵ is either constant or decreases sub-exponentially in n)

$$k = \lim_{n\to\infty} \frac{1}{n} \log K = \max\{\log \gamma, \log d - \chi\} \tag{11}$$

where $\chi = \lim_{n\to\infty} 1/n \log M$ is the asymptotic communication rate, and γ depends on the details of communication channel and of the codes employed.

3.1. Methods

Alice and Bob publicly agree on a set of K codes $\mathcal{C}_1, \ldots \mathcal{C}_K$, where each code contains M equi-probable codewords $\mathcal{C}_k = \{|\psi_k(x)\rangle\}_{x=1,\ldots,M}$, with $|\psi_k(x)\rangle \in \mathbb{C}^{d^n}$. In a strong-locking scenario Eve intercepts the input states $|\psi_k(x)\rangle$'s. Since she does not know the code, the state (3) reads:

$$\sigma_{XE} = \frac{1}{M}\sum_{x=1}^{M} |x\rangle\langle x| \otimes \frac{1}{K}\sum_{k=1}^{K} |\psi_k(x)\rangle\langle\psi_k(x)| \tag{12}$$

Putting $\rho(x) = K^{-1}\sum_{k=1}^{K} |\psi_k(x)\rangle\langle\psi_k(x)|$ and $\rho = M^{-1}\sum_{x=1}^{M}\rho(x)$, the accessible information of σ_{XE} reads

$$I_{\rm acc}(X;E) = \max_{\Lambda}\left\{\log M - \sum_y \mathrm{Tr}(\rho\Lambda_y)\log\mathrm{Tr}(\rho\Lambda_y) + \sum_{xy} M^{-1}\mathrm{Tr}(\rho(x)\Lambda_y)\log\left[M^{-1}\mathrm{Tr}(\rho(x)\Lambda_y)\right]\right\} \tag{13}$$

where the maximum is over POVM's Λ.

By convexity of mutual information, the maximum is achieved for a rank-one measurement with POVM elements of the form $\Lambda_y = \mu_y|\phi_y\rangle\langle\phi_y|$ where the $|\phi_y\rangle$'s are unit vectors and $\mu_y > 0$. The condition $\sum_y \mu_y|\phi_y\rangle\langle\phi_y| = \mathbb{I}$ implies $\sum_y \mu_y/d^n = 1$. Putting $Q_x(\phi_y) = \langle\phi_y|\rho(x)|\phi_y\rangle$, we then obtain

$$I_{\rm acc}(X;E) = \log M - \min_{\{\mu_y|\phi_y\rangle\langle\phi_y|\}}\sum_y \frac{\mu_y}{M}\left\{H[Q(\phi_y)] - \eta\left[\sum_x Q_x(\phi_y)\right]\right\} \tag{14}$$

where $H[Q(\phi_y)] = -\sum_x Q_x(\phi_y)\log Q_x(\phi_y)$. Finally, we notice that the positive quantities μ_y/d^n can be interpreted as probability weights. An upper bound on the accessible information is then obtained by the fact that the average cannot exceed the maximum, which yields

$$\begin{aligned} I_{\rm acc}(X;E) &= \log M - \frac{d^n}{M}\min_{\{\mu_y|\phi_y\rangle\langle\phi_y|\}}\sum_y \frac{\mu_y}{d^n}\left\{H[Q(\phi_y)] - \eta\left[\sum_x Q_x(\phi_y)\right]\right\} \\ &\leq \log M - \frac{d^n}{M}\min_{|\phi\rangle}\left\{H[Q(\phi)] - \eta\left[\sum_x Q_x(\phi)\right]\right\}, \end{aligned}$$

where the minimum is over all unit vectors $|\phi\rangle \in \mathbb{C}^{d^n}$.

We now show that for certain choices of the codes $\mathcal{C}_k$'s, the accessible information is smaller than $\epsilon\log d^n$ for n and K large enough. Consider the case of random codes, where the codewords in $\mathcal{C}_k$ are chosen i.i.d. from a certain ensemble of states. Then for any given x and $|\phi\rangle$ the quantity

$$Q_x(\phi) = \frac{1}{K}\sum_{k=1}^{K} |\langle\psi_k(x)|\phi\rangle|^2 \tag{15}$$

is the sum of random variables which, for K large enough, will converge to its average $\mathbb{E}[Q_x(\phi)]$. If the random codewords are chosen from an isotropic ensemble, that is, one satisfying $\mathbb{E}_\psi[|\psi\rangle\langle\psi|] = \mathbb{I}/d^n$, then $\mathbb{E}[Q_x(\phi)] = 1/d^n$. In turn, if $Q_x(\phi) \sim (1\pm\epsilon)/d^n$, then $H[Q(\phi)] \gtrsim (1-\epsilon)M/d^n\log d^n$, and $\eta[\sum_x Q_x(\phi)] \sim \eta[M/d^n] = -M/d^n\log M/d^n$, which finally implies $I_{\rm acc}(X;E) \lesssim \epsilon\log d^n$.

The minimum value of K for which $Q_x(\phi)$ is close enough to its average for all x and $|\phi\rangle$ can be obtained by applying suitable concentration inequalities [20,21]. For n large enough and if ϵ decreases sublinearly with n, we have obtained the following condition on K [5]:

$$\frac{1}{n}\log K \gtrsim \max\{\log\gamma, \log d - \chi\} \tag{16}$$

where $\chi = \frac{1}{n}\log M$ is the communication rate, and

$$\gamma^n = \frac{\mathbb{E}[Q_x(\phi)^2]}{\mathbb{E}[Q_x(\phi)]^2} = \mathbb{E}[Q_x(\phi)^2]\, d^{2n} \tag{17}$$

Notice that the factor γ depends on the ensemble from which the random codewords are drawn.

If the codewords are drawn from the uniform distribution on the unit sphere in $\mathbb{C}^{d^n}$, one obtains $\mathbb{E}[Q_x(\phi)^2] = \frac{2}{d^n(d^n+1)}$, which yields $\gamma^n = \frac{2d^n}{d^n+1}$. If the channel from Alice to Bob is noiseless, we have $\chi = \log d$ and thus obtain an asymptotically vanishing secret-key consumption rate, $\lim_{n\to\infty}\frac{1}{n}\log K = 0$. This result corresponds to the findings of [11,12], which considered random codewords in a high-dimensional Hilbert space and obtained quantum data locking protocols with zero asymptotic secret-key consumption rate through a noiseless channel.

Suppose instead that the codewords are of the form $|\psi_k(x)\rangle = \otimes_{j=1}^n |\psi_{k,j}(x)\rangle$, where for any $j = 1,\ldots,n$, the vectors $|\psi_{k,j}(x)\rangle$'s are drawn i.i.d. from the uniform distribution on the unit sphere in $\mathbb{C}^d$. For these separable codewords we obtain $\mathbb{E}[Q_x(\phi)^2] = \left[\frac{2}{d(d+1)}\right]^n$, which yields $\gamma^n = \left(\frac{2d}{d+1}\right)^n$. This result corresponds to the quantum data locking protocols discussed in [5]. Given a noisy channel allowing a classical communication rate χ, we obtain a secret-key consumption rate of $k = \max\{1 - \log(1+1/d), \log d - \chi\}$ bits per channel use.

We conclude this section by remarking that there is no reason to consider only random codewords generated by spherically symmetric distributions. First, since γ is only determined by the first and second moments of the distribution, quantum data locking protocols with the same performances can be obtained by choosing random codewords from a spherical 2-design. Second, non-uniform distributions can also be used and may lead to similar results (see [4,14]).

3.2. Applications

The results reviewed in the previous section can be applied to achieve secure communication against an eavesdropper with time-limited quantum storage. Suppose Alice and Bob initially share nk bits of secret key. They can use this secret key to lock n uses of the quantum channel. If the channel allows a classical communication rate of χ bits per channel use, they will be able to communicate about $n\chi$ bits of locked information.

After a waiting time sufficiently longer than the coherence time of Eve's quantum memory, Alice and Bob can run a second quantum data locking protocol. If $\chi > k$ they can recycle nk bits of the previous message as a secret key for the new round of quantum data locking. By repeating this procedure many times, they will achieve a net rate of locked communication of $r = \chi - k$ bits per channel use.

A simple non-trivial example of noisy communication is the d-dimensional erasure channel. Upon n uses of the erasure channel, Alice prepares quantum data locking codewords of the form $|\psi_k(x)\rangle = \otimes_{j=1}^n |\psi_{k,j}(x)\rangle$, where $|\psi_{k,j}(x)\rangle$ are random codewords drawn from the uniform distribution on the unit sphere in $\mathbb{C}^d$. Given that the channel from Alice to Bob is a memoryless qudit erasure channel with erasure probability p, they can achieve a classical communication rate (in bits per channel use) of

$$\chi = (1-p)\log d \tag{18}$$

The complementary channel from Alice to Eve is also a qudit erasure channel, with erasure probability $(1-p)$. As discussed in the previous section, a secret-key consumption rate of

$k = \max\{1 - \log(1 + 1/d), \log d - \chi\}$ bits is needed for quantum data locking. In our example, the erasure channel from Alice to Eve will erase all but a fraction p of the qudits sent by Alice. This implies that the secret-key consumption rate will be also reduced by a factor p, leading to $k = \max\{p - p\log(1 + 1/d), p\log d - \chi\}$. Figure 1 shows, for an 8-bit channel ($d = 256$), the net rate of weak locking for the erasure channel,

$$r = \chi - k = (1 - p)\log d - \max\{p - p\log(1 + 1/d), (2p - 1)\log d\} \tag{19}$$

compared with its classical capacity $C = (1 - p)\log d$ and the private capacity $P = (1 - 2p)\log d$. Similar results are obtained for other channels of the form $\tilde{\mathcal{N}}_{A\to E}(\rho) = (1 - p)\rho + p\rho_0$, where ρ_0 is a given density operator [5].

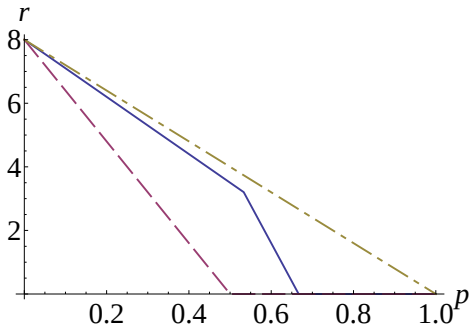

Figure 1. Comparison of several communication rates (in bits per channel use) for the qudit erasure channel with erasure probability p, with $d = 256$. Weak-locking rate (solid line); private capacity (dashed line); classical capacity (dot-dashed line).

We now apply quantum data locking to a continuous-variable quantum system. In [6] we have considered the case of a lossy bosonic channel with transmissivity η, where the input codewords are multimode coherent states drawn from a Gaussian distribution with N mean photons per mode. Although the quantum system has infinite dimensions, it is sufficient to consider the typical subspace spanned by these random codewords. For n-mode coherent states, such a typical subspace has dimension $d^n \sim 2^{ng(N)}$, with $g(N) = (N + 1)\log(N + 1) - N\log N$. Here we consider a weak-locking scenario where Eve measures the complementary channel, which in this case is also a lossy bosonic channel with transmissivity $(1 - \eta)$. Inspired by [22] we have introduced a reverse-reconciliation protocol for secret-key generation by quantum data locking. In this protocol Alice and Bob publicly agree on a collection of measurements Λ_k, for $k = 1, \ldots, K$. Then Alice locally prepares a bipartite entangled state and sends one subsystems to Bob through the quantum channel. According to the value of the pre-shared secret key, Bob makes the measurement Λ_k. This induces a virtual backward quantum channel from Bob to Alice. As shown in [6], this protocol may achieve an asymptotic classical communication rate of $\chi = g(N) - g[(1 - \eta)N']$ bits per mode, with $N' = N/(1 + \eta N)$. On the other hand, weak locking can be obtained with a secret-key consumption rate of $k = 2g[(1 - \eta)N] - g[(1 - \eta)N'] - g[(1 - \eta)N'']$, with $N'' = (1 + 2\eta N)N'$. In this way we achieve a net weak-locking rate of $r = \chi - k$ bits per mode which, in the limit of $N \to \infty$ yields, for any $\eta > 0$,

$$r = \log\left(\frac{1}{1 - \eta}\right) + 1 \tag{20}$$

This yields a rate larger than 1 bit per mode for any non-zero transmissivity, *i.e.*, a constant rate of secret-key generation across arbitrarily long communication distances.

The obtained rate of weak-locking can be compared with the secret-key rate achievable assuming the standard security criterion quantified by the trace distance. For the lossy channel a lower and an upper bound on this rate are respectively given by $r_{\mathrm{lb}} = \log\left(\frac{1}{1-\eta}\right)$ [22] and $r_{\mathrm{ub}} = \log\left(\frac{1+\eta}{1-\eta}\right)$ [2]. Figure 2 shows a comparison between these three rates versus the channel transmissivity η. Our result shows that secure communication against an eavesdropper with time-limited quantum storage not only allows for a quantitative enhancement in the private communication rate, but also yields striking qualitative changes in the rate-loss tradeoff.

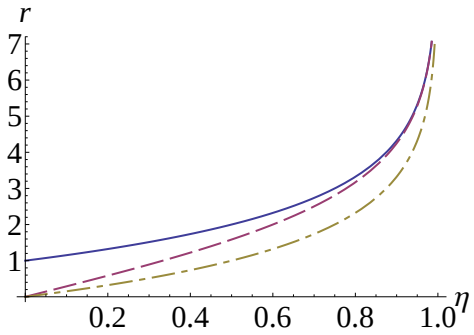

Figure 2. Secret-key rate (in bits per transmitted mode) vs channel transmissivity. Blue solid line: Achievable secret-key rate by quantum data locking (20). Red dashed line: Upper bound for the secret-key rate (assisted by two-way public communication) according to the standard security definition [2]. Yellow dash-dotted line: Achievable secret-key rate according to the standard security definition as given by the reverse coherent information [22].

4. Conclusions

We have reviewed recent results on quantum data locking, speculating on applications of this intriguing quantum phenomenon to secret communication and key distribution through an insecure quantum channel. As quantum data locking relies on a post-measurement security criterion, it protects against an eavesdropper who can store quantum information only for a finite time.

Since a quantum memory is always limited by its coherence time, our assumption may be justified in some cases. We have seen that under this assumption one obtains not only a quantitative enhancement in the secret-key generation rate, but also a qualitative improvement in the rate-loss tradeoff. In the most important case of a lossy channel, we have seen that this assumption allows us to achieve a constant secret-key generation rate at any distance. This result must be compared with the performance of standard quantum key distribution, which yields a rate that decays exponentially with the communication distance.

Finally, it is worth remarking that the assumption of limited quantum memory is also at the basis of the bounded storage model for quantum cryptography. We argue that our results can also be applied to obtain achievable secret-key rates within this model.

Acknowledgments

The results reviewed here have been obtained in collaboration with Seth Lloyd, as part of a research program also involving Mark M. Wilde, Saikat Guha, Patrick Hayden, Hari Krovi, Jeffrey H. Shapiro, and Masahiro Takeoka. This research has been supported by the DARPA Quiness Program through US Army Research Office No. W31P4Q-12-1-0019. We acknowledge numerous discussions with Andreas Winter, Pierre Desjardins, Zheshen Zhang, Jake Mower, and Dirk Englund. All these discussions have greatly contributed to push forward this research program.

Conflicts of Interest

The author declares no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; Volume 175, p. 8.
2. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, doi:10.1038/ncomms6235.
3. Damgard, I.B.; Fehr, S.; Renner, R.; Salvail, L.; Schaffner, C. A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. In *Advances in Cryptology—CRYPTO 2007*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4622, pp. 360–378.
4. Lupo, C.; Lloyd, S. Quantum-locked key distribution at nearly the classical capacity rate. *Phys. Rev. Lett.* **2014**, *113*, 160502 .
5. Lupo, C.; Lloyd, S. Quantum data locking for high-rate private communication. *New J. Phys.* **2015**, *17*, 033022.
6. Lupo, C.; Lloyd, S. How to pull yourself up by your adversary's quantum discord. **2015**, arXiv:1501.07212.
7. Koenig, R.; Renner, R.; Bariska, A.; Maurer, U. Small Accessible Quantum Information Does Not Imply Security. *Phys. Rev. Lett.* **2007**, *98*, 140502.
8. Alicki, R.; Fannes, M. Continuity of Quantum Conditional Information. *J. Phys. A* **2004**, *98*, L55.
9. Fedotov, A.A.; Harremoës, P.; Topsøe, F. Refinements of Pinsker's inequality. *IEEE Trans. Inf. Theory* **2003**, *49*, 1491–1498.
10. DiVincenzo, D.P.; Horodecki, M.; Leung, D.W.; Smolin, J.A.; Terhal, B.M. Locking classical correlations in quantum states. *Phys. Rev. Lett.* **2004**, *92*, 067902.
11. Hayden, P.; Leung, D.; Shor, P.W.; Winter, A. Randomizing quantum states: Constructions and applications. *Comm. Math. Phys.* **2004**, *250*, 371–391.
12. Fawzi, O.; Hayden, P.; Sen, P. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. *J. ACM* **2013**, *60*, doi:10.1145/2518131.
13. Dupuis, F.; Florjanczyk, J.; Hayden, P.; Leung, D. The locking-decoding frontier for generic dynamics. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **2013**, *469*, 20130289.

14. Lupo, C.; Wilde, M.M.; Lloyd, S. Robust quantum data locking from phase modulation. *Phys. Rev. A* **2014**, *90*, 022326.
15. Guha, S.;Hayden, P.; Krovi, H.; Lloyd, S.; Lupo, C.; Shapiro, J.H.; Takeoka, M.; Wilde, M.M. Quantum enigma machines and the locking capacity of a quantum channel. *Phys. Rev. X* **2014**, *4*, 011016.
16. Lloyd, S. Quantum enigma machines. **2013**, arXiv:1307.0380.
17. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **2005**, *51*, 44–55.
18. Cai, N.; Winter, A.; Yeung, R.W. Quantum privacy and quantum wiretap channels. *Probl. Inf. Transm.* **2004**, *40*, 318–336.
19. Winter, A. Weak locking capacity of quantum channels can be much larger than private capacity. **2014**, arXiv:1403.6361.
20. Maurer, A. A bound on the deviation probability for sums of non-negative random variables. *J. Inequal. Pure Appl. Math.* **2003**, *4*, Article 15.
21. Ahlswede, R.; Winter, A. Strong converse for identication via quantum channels. *IEEE Trans. Inf. Theory* **2002**, *48*, 569–579.
22. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503.