Quantum-locked direct communication at almost the classical capacity rate

Cosmo Lupo¹ and Seth Lloyd¹,²

¹Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA
²Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

We show that, if the accessible information is taken as a security quantifier, a quantum channel can convey private messages at a tremendously high rate, as high as less than one bit below the rate of non-private classical communication. This result is obtained by using the quantum enigma machine, a cipher exploiting the quantum data locking effect. The price to pay to achieve such a high private communication rate is that accessible information-security is in general not composable, yet composable security holds against an eavesdropper with unlimited computation power but having a quantum memory with finite coherence time.

I. INTRODUCTION

One of the most promising contemporary applications of quantum mechanics is within cryptography, where the laws of quantum physics certify the secrecy of a communication protocol. In quantum key distribution, the communication protocol aims at establishing a common key between two legitimate parties, Alice and Bob, in such a way that a third party, say Eve, eavesdropping and tampering the communication line, obtains virtually no information about the key [1]. The key itself it is generated randomly, possibly to serve as a one time pad. On the other hand, in a private communication protocol, the sender, say Alice, aims at sending private messages to Bob [2]. In this case, the content of the messages is under the control of Alice and it is not random from her point of view. Clearly, any private communication protocol can be also used for key distribution.

In this paper we introduce a private communication protocol, based on the phenomenon of quantum data locking (QDL), that allows the highest rate of private communication: as high as less than one bit below the classical capacity for non-private communication (similar ideas were applied to quantum key distribution in [3].) Our protocol is secure according to the accessible information criterion, which is not the standard and widely accepted security criterion in quantum cryptography. For this reason, before proceeding with the description of the protocol, we make a brief detour to clarify in which context the accessible information yields reliable security, as well as to review the phenomenon of QDL [4].
A. Accessible information security

Let us recall that the accessible information is defined as the maximum classical mutual information between Alice’s input and the result of any measurement performed by Eve on her share of the quantum system. Suppose that Alice’s message $x$ is generated with probability $p_X(x)$ by a memoryless source described by the random variable $X$, and the conditional state obtained by Eve is $\rho_{E|x}$. The ensemble state of the joint system of Alice and Eve is hence described by the density matrix $\rho_{AE} = \sum_x p_X(x) |x\rangle_A \langle x| \otimes \rho_{E|x}$.

A local measurement by Eve is described by a map $M_E : E \rightarrow Y$ whose output is the classical variable $Y$. Then the accessible information of the state $\rho_{AE}$ reads

$$I_{\text{acc}} = \max_{M_E} I(X; Y),$$

where $I(X; Y) = H(X) + H(Y) - H(XY)$ is the classical mutual information, and $H$ denotes the Shannon entropy.

To assess the security of our protocol we show that $I_{\text{acc}} \leq \epsilon$ where $\epsilon$ is a security parameter that can be made arbitrarily small under certain conditions. This means that the output of any measurement by Eve is arbitrarily close to be uncorrelated with Alice message. When used as a security quantifier, the accessible information suffers from a major problem: it does not guarantee composable security. Roughly speaking, composable security means that if two communication protocols are secure individually they remain secure when composed. The fact that the accessible information does not ensure composability is intimately related with the very effect of QDL [5]. However, as discussed in [3, 6], the accessible information yields composable security conditioned on certain physical assumptions. For instance, one physical assumption that guarantees composable security is that the eavesdropper does not have access to a quantum memory, that is, she is forced to measure her share of the state as soon as she obtains it. This is a consequence of the fact that the accessible information concerns the output of Eve’s measurement, and not the quantum state itself. A more realistic assumption is that Eve possesses a quantum memory with finite coherence time. In the simplest model, Eve either measures her share of the quantum system within a time $\tau$ or the quantum memory decoheres and becomes classical. Suppose the given communication protocol is used as a subroutine of a larger protocol. In this case composable security is granted if Alice and Bob know the coherence time of Eve’s quantum memory and wait for a time sufficiently longer than $\tau$ before proceeding. Clearly, too large values of $\tau$ would make the protocol unpractical. However, as discussed in [3], in a stationary regime the overall asymptotic communication rate may be independent of $\tau$ and remain finite even in the limit $\tau \rightarrow \infty$. 
B. Quantum data locking

Below we introduce a private communication protocol that is secure according to the accessible information criterion. Such a protocol is a QDL protocol. 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 secret key of $\log K$ bits to select a set of $M$ codewords that they will use for sending information. If an eavesdropper Eve does not know the secret key, then the number of bits, as quantified by the accessible information, that she can obtain about the message by measuring her share of the quantum system is essentially equal to zero for certain choices of codewords. In most of the known QDL protocols, including the protocol we discuss below, codewords are chosen from different bases, and the secret key identifies the basis to which the codewords belong.

A number of works have been devoted to the role of QDL in physics and information theory [4, 7–12]. However, only recently QDL has been considered in the presence of noise [3, 6, 13–15]. Following the idea of the “quantum enigma machine” [13] for applying QDL to cryptography, a formal definition of the locking capacity of a communication channel has been introduced in [6], as the maximum rate at which information can be reliably and securely transmitted through a (noisy) quantum channel $\mathcal{N}_{A \rightarrow B}$ from Alice to Bob, where the security is according to the accessible information criterion. Motivated by QDL protocols, we also allow the assistance of an initial secret key shared by Alice and Bob. In order this key to be inexpensive in the asymptotic limit, we further require that the bits of secret key grow sublinearly with the number of channel uses.

Two notions of locking capacities were defined in [6]: the weak locking capacity and the strong locking capacity. The weak locking capacity is defined by requiring security against an eavesdropper who measures the output of the complementary channel (denoted as $\mathcal{N}_{A \rightarrow E} = \tilde{\mathcal{N}}_{A \rightarrow B}$) of the channel from Alice to Bob. The strong locking capacity is instead defined by requiring 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. It is natural to compare the weak locking capacity with the private capacity [2]. Since the private capacity is defined by a security criterion stronger than the accessible information, it follows that the weak locking capacity is always larger that or at most equal to the private capacity. Finally, both the weak and strong locking capacities cannot exceed the classical capacity, which is the maximum rate of reliable communication allowed by the channel (not requiring any secrecy) [16].

Our starting point is a QDL protocol for the $d$-dimensional noiseless channel. It applies to $n$ uses of the channel and locks classical information into codewords that are separable among different channel uses. The
protocol allows QDL (in the strong sense) of the qudit noiseless channel at a rate of $\log d$ bits per channel use, equal to its classical capacity, and consumes secret key at an asymptotic rate of 1 bit per channel use. The crucial property of this protocol is that it makes use of codewords that are separable among different channel uses. This property allows us to generalize the protocol to the case of a noisy memoryless channel.

II. A PROTOCOL FOR STRONG LOCKING OF A NOISELESS CHANNEL

In this section we define a protocol for the strong locking of the qudit noiseless channel. Later we will apply this protocol to the (weak and strong) locking of a noisy memoryless channel.

Let us consider a $d$-dimensional Hilbert space endowed with an orthonormal basis $\{ |\omega\rangle \}_{\omega=0,\ldots,d-1}$ and its Fourier-conjugate basis $\{ |m\rangle \}_{m=0,\ldots,d-1}$,

$$|m\rangle = \frac{1}{\sqrt{d}} \sum_{\omega=0}^{d-1} e^{i2\pi m\omega/d} |\omega\rangle .$$

(2)

To encode classical information in $n$ qudits, Alice uses a code $C : c \in \{1,2,\ldots,M\} \rightarrow (m_1^c, m_2^c, \ldots, m_n^c) \in \{0,1,\ldots,d-1\}^n$. According to this code, she prepares one of the $M^n$ qudit codewords

$$|\psi_c\rangle = \bigotimes_{j=1}^n |m_j^c\rangle .$$

(3)

Alice and Bob publicly agree on a set of $K^n$ qudit unitaries

$$U_k = \bigotimes_{j=1}^n U_j^k ,$$

(4)

for $k = 1, 2, \ldots, K$, where the single-qudit unitary acting on the $j$-th system is of the form

$$U_j^k = \sum_{\omega^j=0}^{d-1} e^{i\theta_j^k(\omega^j)} |\omega^j\rangle \langle \omega^j| .$$

(5)

According to the value of the secret key, Alice applies the unitary transformation $U_k$ on the $n$-qudit codeword, obtaining

$$|\psi_{ck}\rangle = U_k |\psi_c\rangle = \bigotimes_{j=1}^n U_j^k |m_j^c\rangle = \frac{1}{\sqrt{d^n}} \sum_{\omega} e^{i\sum_{j=1}^n [2\pi m_j^k \omega^j / d + \theta_j^k(\omega^j)]} |\omega\rangle ,$$

(6)

where $\omega = (\omega^1, \omega^2, \ldots, \omega^n)$ and $|\omega\rangle = \bigotimes_{j=1}^n |\omega^j\rangle$.

Since Bob knows the unitary $U_k$ chosen by Alice, he can simply apply the inverse transformation $U_k^{-1}$ and then a perform an optimal measurement to discriminate between the codewords. We consider random codewords generated by choosing independently and identically each of the $m_j^c$ according to the uniform
distribution over \( \{0, 1, \ldots, d-1\} \). It is well known that in such a setting Bob can decode reliably in the limit \( n \to \infty \) if \( M < \epsilon d^n \) and \( \epsilon \) vanishes in the limit \( n \to \infty \). For instance, one can take \( \epsilon = 2^{-ns} \) for \( s < 1 \) and obtain an asymptotic rate of communication of \( \log d \) bits.

In the strong locking scenario, we assume that Eve intercepts the whole train of qudit systems and measures them. Since Eve does not have access to the secret key, we have to compute the accessible information of the ensemble of states \( \mathcal{E} = \{ p_c, \frac{1}{K} \sum_{k=1}^{K} |\psi_{c,k}\rangle\langle\psi_{c,k}| \} \), where \( p_c \) is the probability of the codeword \( |\psi_c\rangle \). For the sake of simplicity here we assume that all the messages have equal probability, that is, \( p_c = 1/M \) (the case of non-uniform distribution has been considered in [11, 12]). A straightforward calculation yields (see [14])

\[
I_{\text{acc}} \leq \log M - \frac{d^n}{M} \min_{|\phi\rangle} \left\{ H[Q(\phi)] - \eta \left[ \sum_{c=1}^{M} Q_c(\phi) \right] \right\},
\]

where

\[
Q_c(\phi) = \frac{1}{K} \sum_{k=1}^{K} |\langle\phi|\psi_{c,k}\rangle|^2,
\]

\[
H[Q(\phi)] = -\sum_{c=1}^{M} Q_c(\phi) \log Q_c(\phi), \quad \eta(x) = -x \log x, \quad \text{and the minimization is over all } n\text{-qudit unit vectors } |\phi\rangle.
\]

Below we show that for certain choices of the unitaries \( \{U_k\}_{k=1,\ldots,K} \), and with \( \log K \simeq n \), Alice and Bob also have the guarantee that Eve’s accessible information is exponentially small in \( n \). To show that, we make use of a random coding argument based on random choices of both the codewords and the data locking unitaries. In particular, the set of unitaries \( U^j_k \) is generated randomly by choosing each of the angular variables \( \theta_k^j(\omega^j) \) independently and identically according to a distribution such that \( \mathbb{E}[e^{i\theta_k^j(\omega^j)}] = 0 \). This is the only condition required, any distribution satisfying it will work. For instance, the angles \( \theta_k^j(\omega) \) can be uniformly distributed in \([0, 2\pi]\), or assume the binary values \( \{0, \pi\} \) with equal probabilities.

A. Some preliminary results

To characterize our QDL protocol we will make use of two concentration inequalities. The first one is the tail bound [17]:

**Theorem 1** Let \( \{X_t\}_{t=1,\ldots,T} \) be \( T \) i.i.d. non-negative real-valued random variables, with \( X_t \sim X \) and finite first and second moments, \( \mathbb{E}[X], \mathbb{E}[X^2] < \infty \). Then, for any \( \tau > 0 \) we have that

\[
\Pr \left\{ \frac{1}{T} \sum_{t=1}^{T} X_t < \mathbb{E}[X] - \tau \right\} \leq \exp \left( -\frac{T\tau^2}{2\mathbb{E}[X^2]} \right).
\]
(Pr\{x\} denotes the probability that the proposition \(x\) is true.)

The second one is the operator Chernoff bound [18]:

**Theorem 2** Let \(\{X_t\}_{t=1,...,T}\) be \(T\) i.i.d. random variables taking values in the algebra of hermitian operators in dimension \(D\), with \(0 \leq X_t \leq I\) and \(E[X_t] = \mu I\) (\(I\) is the identity operator). Then, for any \(\tau > 0\) we have that

\[
Pr\left\{ \frac{1}{T} \sum_{t=1}^{T} X_t > (1 + \tau)\mu I \right\} \leq D \exp\left( -\frac{T\tau^2 \mu^2}{4 \ln 2} \right).
\]

For any given \(d^n\)-dimensional unit vector \(|\phi\rangle\) and codeword \(|\psi_{ck}\rangle\), we define the quantity

\[
q_{ck}(\phi) = \left| \langle \phi | \psi_{ck} \rangle \right|^2.
\]

(9)

Clearly, the latter is a random variable if the unitary \(U_k\) and/or the codeword \(c\) are chosen randomly. Also, since \(|\psi_{ck}\rangle\) and \(|\psi_{ck'}\rangle\) are statistically independent, so are \(q_{ck}(\phi)\) and \(q_{ck'}(\phi)\). To apply Theorems 1 and 2, we compute the first and second moments of \(q_{ck}(\phi)\), for given \(|\phi\rangle\) and \(c\), with respect to the i.i.d. random locking unitaries (the same results are obtained if also \(c\) is chosen randomly). As shown in [3], we have

\[
E[q_{ck}(\phi)] = \frac{1}{d^n},
\]

(10)

and

\[
E[q_{ck}(\phi)^2] \leq \frac{2^n}{d^{2n}}.
\]

(11)

For any given \(|\phi\rangle\) and \(c\), we also consider the quantity

\[
Q_c(\phi) = \frac{1}{K} \sum_{k=1}^{K} q_{ck}(\phi).
\]

(12)

We now derive several concentration inequalities by applying Theorems 1 and 2:

- Applying Maurer’s tail bound (Theorem 1), we obtain that for any given \(|\phi\rangle\) and \(c\)

\[
Pr\left\{ Q_c(\phi) < \frac{1 - \epsilon}{d^n} \right\} \leq \exp\left( -\frac{K\epsilon^2}{2n+1} \right).
\]

(13)

We then use this inequality to bound the probability that there exist \(\ell\) codewords such that \(Q_c(\phi) < \frac{1 - \epsilon}{d^n}\). Applying the union bound we obtain

\[
Pr\left\{ \exists c_1, \ldots, c_\ell \mid \forall i \ Q_{c_i}(\phi) < \frac{1 - \epsilon}{d^n} \right\} \leq \left( \frac{M}{\ell} \right)^\ell \left( Pr\left\{ Q_c(\phi) < \frac{1 - \epsilon}{d^n} \right\} \right)^\ell
\]

(14)

\[
\leq \left( \frac{M}{\ell} \right) \exp\left( -\frac{\ell K\epsilon^2}{2n+1} \right)
\]

(15)

\[
\leq M^\ell \exp\left( -\frac{\ell K\epsilon^2}{2n+1} \right)
\]

(16)

\[
= \exp\left( \ell \ln M - \frac{\ell K\epsilon^2}{2n+1} \right).
\]

(17)
Let us consider the operators $|\psi_{ck}\rangle\langle\psi_{ck}|$ and apply the operator Chernoff bound (Theorem 2). Notice that Eq. (10) implies

$$E[|\psi_{ck}\rangle\langle\psi_{ck}|] = \frac{I}{d^n}. \quad (18)$$

Putting $\mu = 1/d^n$ and $(1 + \tau)\mu = (1 - \delta)$, the operator Chernoff bound then yields that for any given $c$

$$P_r \left\{ \frac{1}{K} \sum_{k=1}^{K} |\psi_{ck}\rangle\langle\psi_{ck}| > (1 - \delta)I \right\} \leq d^n \exp \left( -\frac{K(d^n(1 - \delta) - 1)^2}{d^n 4 \ln 2} \right) \quad (19)$$

$$= d^n \exp \left( -\frac{Kd^n(1 - \delta - 1/d^n)^2}{4 \ln 2} \right). \quad (20)$$

This in turn implies that

$$P_r \left\{ \max_{|\phi\rangle} Q_c(\phi) > 1 - \delta \right\} \leq d^n \exp \left( -\frac{Kd^n(1 - \delta - 1/d^n)^2}{4 \ln 2} \right). \quad (21)$$

We bound the probability that there exists a codeword $c$ and a vector $|\phi\rangle$ such that $Q_c(\phi) > 1 - \delta$. Applying the union bound we obtain

$$P_r \left\{ \max_{|\phi\rangle,c} Q_c(\phi) > 1 - \delta \right\} \leq M P_r \left\{ \max_{|\phi\rangle} Q_c(\phi) > 1 - \delta \right\} \quad (22)$$

$$\leq M d^n \exp \left( -\frac{Kd^n(1 - \delta - 1/d^n)^2}{4 \ln 2} \right) \quad (23)$$

$$\leq \exp \left( \ln M d^n - \frac{Kd^n(1 - \delta - 1/d^n)^2}{4 \ln 2} \right). \quad (24)$$

Finally, we consider random choices of the codewords $c$ and apply the Chernoff bound with $\tau = \epsilon$. We then obtain

$$P_r \left\{ \max_{|\phi\rangle} \sum_{c=1}^{M} Q_c(\phi) > (1 + \epsilon)\frac{M}{d^n} \right\} \leq d^n \exp \left( -\frac{K \frac{M}{d^n} \epsilon^2}{4 \ln 2} \right) \quad (25)$$

$$= \exp \left( \ln d^n - \frac{K \frac{M}{d^n} \epsilon^2}{4 \ln 2} \right). \quad (26)$$

**B. Eve’s accessible information**

Let Eve intercept and measure the train of $n$ qudits sent by Alice. To evaluate the security of the QDL protocol according to the accessible information criterion, we show that there exist choices of the scrambling unitaries $U_k^j$’s that guarantee Eve’s accessible information to be negligibly small. To prove that we show that this property is true with an arbitrary high probability for a random choice of the unitaries $U_k^j$’s if $n$ is large enough.
We consider a random choice of the code $C$. From Eq. (26), we have that for all $|\phi\rangle$, $\sum_{c=1}^{M} Q_c(\phi)$ is smaller than $(1 + \epsilon) \frac{M}{d^n}$ up to a probability which is bounded away from one provided

$$K > \frac{d^n}{M} \frac{4 \ln 2 \ln d^n}{\epsilon^2}.$$  \hfill (27)

Assuming $\max_{|\phi\rangle} \sum_{c=1}^{M} Q_c(\phi) < (1 + \epsilon) \frac{M}{d^n}$ and $M/d^n \ll 1$, then we have

$$\frac{d^n}{M} \max_{|\phi\rangle} \eta \left[ \sum_{c=1}^{M} Q_c(\phi) \right] < \frac{d^n}{M} \eta \left[ (1 + \epsilon) \frac{M}{d^n} \right]$$

$$= \eta(1 + \epsilon) \log \frac{d^n}{M}$$

$$< (1 + \epsilon) \log \frac{d^n}{M}.$$  \hfill (30)

This in turn implies that, for $K$ large enough, Eq. (7) is equivalent, up to a negligibly small probability, to

$$I_{acc} \leq (1 + \epsilon) \log d^n - \frac{d^n}{M} \min_{|\phi\rangle} H[Q(\phi)].$$  \hfill (31)

According to the latter expression, an upper bound on the accessible information follows from a lower bound on the minimum Shannon entropy, $\min_{|\phi\rangle} H[Q(\phi)]$. That is, to prove that $I_{acc} \leq \epsilon \log d^n$, we need to show that $\frac{d^n}{M} \min_{|\phi\rangle} H[Q(\phi)] \geq (1 - \epsilon) \log d^n$. To do that, for any $\epsilon > 0$ and $d^n$ and $K$ large enough we bound the probability that

$$- Q_c(\phi) \log Q_c(\phi) < \eta \left( \frac{1 - \epsilon}{d^n} \right).$$  \hfill (32)

This corresponds to bounding the probability that either $Q_c(\phi) > \lambda_+ = 1 - \eta \left( \frac{1 - \epsilon}{d^n} \right) + O \left( \eta \left( \frac{1 - \epsilon}{d^n} \right) \right)$ or $Q_c(\phi) < \lambda_- = (1 - \epsilon)/d^n$. Notice that for $d^n$ sufficiently large and/or $\epsilon$ sufficiently small we have $\lambda_+ \geq 1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right)$.

First, we bound the probability that there exists a codeword $c$ and a vector $|\phi\rangle$ such that $Q_c(\phi) > \lambda_+$. We apply Eq. (24) with $\delta = 2\eta \left( \frac{1 - \epsilon}{d^n} \right)$ to obtain

$$P \left\{ \max_{|\phi\rangle, c} Q_c(\phi) > \lambda_+ \right\} \leq P \left\{ \max_{|\phi\rangle, c} Q_c(\phi) > 1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) \right\}$$

$$\leq \exp \left( \ln M d^n - \frac{K d^n (1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) - 1/d^n)^2}{4 \ln 2} \right)$$

$$\leq \exp \left( \ln M d^n - \frac{K d^n (1 - 4\eta \left( \frac{1 - \epsilon}{d^n} \right) - 2/d^n)}{4 \ln 2} \right)$$

$$\leq \exp \left( \ln M d^n - \frac{K d^n (1 - 6\eta \left( \frac{1 - \epsilon}{d^n} \right))}{4 \ln 2} \right) =: p_+,$$  \hfill (36)

where we have also used the fact that $\frac{1}{d^n} < \eta \left( \frac{1 - \epsilon}{d^n} \right)$ for $n$ large enough. This probability vanishes exponentially with $d^n$ provided $K$ is not too small, that is, $K > \frac{\ln M d^n}{d^n} + 4 \ln 2$. 


Second, we bound the probability that there exist $\ell \ll M$ codewords such that $Q_c(\phi) < \lambda_-$. We apply Eq. (17) and obtain

$$Pr \{ \exists c_1, \ldots, c_\ell \mid \forall i \ Q_{c_i}(\phi) < \frac{1 - \epsilon}{d^n} \} = Pr \left\{ \exists c_1, \ldots, c_\ell \mid \forall i \ Q_{c_i}(\phi) < \frac{1 - \epsilon}{d^n} \right\} \leq \exp \left( \ell \ln M - \frac{\ell K \epsilon^2}{2^{n+1}} \right).$$

(37)

Putting $\ell = \epsilon M$ we have

$$Pr \{ \exists c_1, \ldots, c_\ell \mid \forall i \ Q_{c_i}(\phi) < \lambda_- \} \leq \exp \left[ -M \left( \frac{K \epsilon^3}{2^{n+1}} - \epsilon \ln M \right) \right] =: p_-.$$

(38)

(39)

Notice that this probability is also exponentially small in $M$, provided that $K > 2^{n+1} e^{-2} \ln M$.

Inequality (24) implies that, with probability at least equal to $1 - p_-$, all the $Q_c(\phi)$’s are larger than $\lambda_+$. Also, according to Eq. (39), for a given $|\phi\rangle$ there exist, with probability greater than $1 - p_-$ at least $M - \ell = (1 - \epsilon) M$ values of $c$ such that $Q_c(\phi) > \lambda_-$. Putting these results together we have that for any given $|\phi\rangle$

$$H[Q(\phi)] > -M (1 - \epsilon) \left( \frac{1 - \epsilon}{d^n} \log \frac{1 - \epsilon}{d^n} \right)$$

(40)

$$= -M (1 - \epsilon)^2 \log \frac{1 - \epsilon}{d^n}$$

(41)

$$> M d^n (1 - 2\epsilon) \log d^n - M d (1 - 2\epsilon) \log (1 - \epsilon)$$

(42)

$$> M d^n (1 - 2\epsilon) \log d^n,$$

(43)

that is,

$$\frac{d^n}{M} H[Q(\phi)] > (1 - 2\epsilon) \log d^n,$$

(44)

with a probability at least equal to $1 - p_- - p_+$, which is in turn larger than $1 - 2p_-$ for $M$ large enough.

To bound the right hand side of Eq. (31) we have to show that a relation similar to (44) holds for all vectors $|\phi\rangle$. To do that we introduce an $\epsilon$-net. Let us recall that an $\epsilon$-net is a finite set of unit vectors $N_\epsilon = \{|\phi_i\rangle\}$ in a $D$-dimensional Hilbert space such that for any unit vector $|\phi\rangle$ there exists $|\phi_i\rangle \in N_\epsilon$ such that

$$\| |\phi\rangle \langle \phi | - |\phi_i\rangle \langle \phi_i | \|_1 \leq \epsilon.$$

(45)

As discussed in [7] there exists an $\epsilon$-net such that $|N_\epsilon| \leq (5/\epsilon)^{2D}$. Below, we first extend the bound (44) on all the $\epsilon$-net, and then, for $\epsilon$ sufficiently small, to all the manifold of unit vectors.
By applying the union bound we obtain:

\[
\Pr \left\{ \min_{|\phi_i\rangle \in \mathcal{N}_\varepsilon} H[Q(\phi_i)] < (1 - 2\varepsilon) \log d^n \right\} \leq \frac{5}{\varepsilon} 2^d \exp \left[ -M \left( \frac{K\varepsilon^3}{2^n+1} - \varepsilon \ln M \right) \right]
\]

\[
= 2\exp \left[ -M \left( \frac{K\varepsilon^3}{2^n+1} - \varepsilon \ln M - 2\frac{d^n}{M} \ln \frac{5}{\varepsilon} \right) \right].
\]

Finally, we have to replace the minimum over vectors in the \(\varepsilon\)-net with a minimum over all unit vectors. An application of the Fannes inequality \([19]\) yields (see also \([7]\))

\[
\left| \min_{|\phi \rangle} H[Q(\phi)] - \min_{|\phi_i\rangle \in \mathcal{N}_\varepsilon} H[Q(\phi_i)] \right| \leq \varepsilon \log d^n + \eta(\varepsilon),
\]

which implies

\[
\Pr \left\{ \min_{|\phi \rangle} H[Q(\phi)] < (1 - 3\varepsilon) \log d^n - \eta(\varepsilon) \right\} \leq 2 \exp \left[ -M \left( \frac{K\varepsilon^3}{2^n+1} - \varepsilon \ln M - 2\frac{d^n}{M} \ln \frac{5}{\varepsilon} \right) \right],
\]

that is,

\[
\Pr \left\{ I_{\text{acc}} > 3\varepsilon \log d^n + \eta(\varepsilon) \right\} \leq 2 \exp \left[ -M \left( \frac{K\varepsilon^3}{2^n+1} - \varepsilon \ln M - 2\frac{d^n}{M} \ln \frac{5}{\varepsilon} \right) \right].
\]

Such a probability is bounded away from one (and goes to zero exponentially in \(M\)) provided

\[
K > 2^{n+1} \left( \frac{1}{\varepsilon^2} \ln M + \frac{2}{\varepsilon^3} \frac{d^n}{M} \ln \frac{5}{\varepsilon} \right).
\]

If we put \(\varepsilon = 2^{-ns}\), with \(s \in (0, 1)\), Eve’s accessible information will be exponentially small in \(n\), with an asymptotic secret key consumption rate equal to

\[
\lim_{n \to \infty} \frac{\log K}{n} = 1 + \lim_{n \to \infty} \frac{\log d^n}{n}. \tag{53}
\]

By increasing \(n\) we want Bob to be able to decode reliably. As noted above, for the case of a noiseless channel we can choose \(M = \varepsilon d^n\), which finally yields a secret consumption rate of 1 bit per channel use.

In conclusion, we have proven that there exist QDL codes allowing Alice and Bob to data lock classical information through \(n\) uses of a noiseless memoryless qudit channel in such a way that Eve’s accessible information is \(I_{\text{acc}}(E) = O(\varepsilon \log d^n)\), where \(\varepsilon\) can be taken to approach zero exponentially in \(n\). The strong locking rate equals \(\log d\) bits per channel use and require the pre-shared secret key to be consumed at an asymptotic rate of 1 bit per channel use (independently on \(d\)).
III. STRONG LOCKING A QUUDIT MEMORYLESS CHANNEL

The noiseless protocol can be applied for the strong locking of a noisy qudit channels $\mathcal{N}_{A \rightarrow B}$ connecting Alice to Bob. The point is that in a strong locking setting we require that the communication is secure against an eavesdropper having access to the very input of the channel. In other words, the security of the protocol is independent on how the channel acts on the input, and hence it applies to both the noiseless and noisy settings. That is, the bound on the accessible information in Eq. (51) and the condition on the number of key values in Eq. (52) apply for a generic qudit channel.

The crucial difference, however, is that the presence of noise reduces the rate at which Alice and Bob can communicate reliably. Let us suppose that, using the codewords described above, Alice and Bob can achieve a reliable communication rate of $R$ bits per channel use $[20]$. Then we can put, for $n$ large enough, $M = \epsilon 2^{nR}$, which yields the following condition on the key (from Eq. (52)):

$$K > 2^{n+1} \left( \frac{1}{\epsilon^2} \ln (\epsilon 2^{nR}) + \frac{2}{\epsilon^4} 2^{n(\log d - R)} \ln \frac{5}{\epsilon} \right).$$

These condition implies an asymptotic key consumption rate of

$$\lim_{n \to \infty} \frac{\log K}{n} = 1 + \log d - R.$$ (55)

Since $R$ cannot exceed $\log d$, this implies an increase in the secret key consumption rate of $\log d - R$ bits with respect of the noiseless setting. We can say that the latter equation represents a trade off between communication rate and secret key consumption. In order to achieve strong locking, the secret key consumption rate should increase to compensate the reduced communication rate.

IV. WEAK LOCKING A QUUDIT MEMORYLESS CHANNEL

Our analysis of the strong locking of a noisy channel showed that a longer secret key, which means more randomness, has to be employed to compensate the reduction in the communication rate. On the other hand, in the weak locking scenario the eavesdropper has access to the output of the complementary channel, that is, also the eavesdropper signal is distorted by noise. One can hence expect that the randomness introduced by the noise can produce a QDL effect. If this is true, then one can exploit the randomness due to the noise to reduce the length of the required secret key. Below we show that this intuition is true by examining a family of channels of a specific form. We define these channels through their conjugates, which are of the form

$$\tilde{\mathcal{N}}_{A \rightarrow B}(\rho) = \mathcal{N}_{A \rightarrow E}(\rho) = p \rho + (1 - p)\sigma,$$ (56)
where \( p \in [0, 1] \) and \( \sigma \) is a given density matrix (notable examples of channels belonging to this family are the erasure channel and the conjugate of the depolarizing channel).

The results on the noiseless case can be easily applied to these channels. To do that, it is sufficient to notice that, with probability \( p \), the channel \( \mathcal{N}_{A \rightarrow E} \) is noiseless. In other words, for \( n \) uses of the channel, one expects that the channel \( \mathcal{N}_{A \rightarrow E} \) will act as an effective noiseless channel over a fraction of about \( pn \) qudits. It is sufficient to require that the protocol data locks the information contained in these qudits, since the remaining \( (1 - p)n \) qudits do not convey any information at all about the message as the output is independent on the input.

More formally, upon \( n \) uses of the channel Eve receives (with probability arbitrarily close to 1 for \( n \) large enough) no more than \( n(p + \delta) \) qudits without any distortion. Let us hence fix a subset of \( n(p + \delta) \) qudits and apply the same reasoning of the noiseless channel given above with \( d^n \) replaced by \( d^{n(p+\delta)} \). This yields a bound on Eve’s accessible information conditioned on the choice of the subset:

\[
\Pr\left\{ I_{\text{acc}} > 3\epsilon \log d^{n(p+\delta)} + \eta(\epsilon) \right\} \leq 2 \exp\left[ -M \left( \frac{K\epsilon^3}{2^{n(p+\delta)+1}} - \epsilon \ln M - 2 \frac{d^{n(p+\delta)}}{M} \ln \frac{5}{\epsilon} \right) \right].
\]

Finally, we apply the union bound to account for all possible \( \binom{n}{n(p+\delta)} \) choices of the subset of \( n(p + \delta) \) qudits:

\[
\Pr\left\{ I_{\text{acc}} > 3\epsilon \log d^{n(p+\delta)} + \eta(\epsilon) \right\} \leq 2 \binom{n}{n(p+\delta)} \exp\left[ -M \left( \frac{K\epsilon^3}{2^{n(p+\delta)+1}} - \epsilon \ln M - 2 \frac{d^{n(p+\delta)}}{M} \ln \frac{5}{\epsilon} \right) \right]
\]

\[
\leq 2^n(n(p+\delta)) \exp\left[ -M \left( \frac{K\epsilon^3}{2^{n(p+\delta)+1}} - \epsilon \ln M - 2 \frac{d^{n(p+\delta)}}{M} \ln \frac{5}{\epsilon} \right) \right]
\]

\[
\leq 2^n(p+\delta) \ln n - M \left( \frac{K\epsilon^3}{2^{n(p+\delta)+1}} - \epsilon \ln M - 2 \frac{d^{n(p+\delta)}}{M} \ln \frac{5}{\epsilon} \right).
\]

This probability goes to zero exponentially in \( M \) — we can always assume that \( M = e^{2^nR} \) where \( R \) is the communication rate — under the following condition on the secret key:

\[
K > 2^{n(p+\delta)+1} \left( \frac{1}{\epsilon^2} \ln M + \frac{2}{\epsilon^4} \frac{d^{n(p+\delta)}}{2^nR} \ln \frac{5}{\epsilon} \right),
\]

which requires an asymptotic secret key consumption of (we can assume \( \lim_{n \to \infty} \delta = 0 \))

\[
\lim_{n \to \infty} \frac{\log K}{n} = p + \max \{0, p \log d - R\}.
\]
This example shows that the presence of noise in the channel to Eve allows Alice and Bob to consume secret key at a reduced rate. We now compute a lower bound on the maximum achievable communication rate for the class of channels considered here. To compute $R$, we first write an isometric extension of the channel. We introduce four quantum systems: systems 1, 2, and 3 are qudits and system 4 is a qubit. In input, system 1 is assigned to Alice and systems 2, 3, and 4 to Eve. In output, system 1 is assigned to Eve and the others to Bob. We put

$$U_{1234} = I_{123} \otimes |0\rangle_4 \langle 0| + S_{12} \otimes I_3 \otimes |1\rangle_4 \langle 1|,$$

(63)

where $S_{12}$ is the swap operation between qudits 1 and 2. As initial state of the environment we put

$$|\phi_E\rangle = |\phi\rangle_{23} \otimes \left(\sqrt{p}|0\rangle_4 \langle 0| + \sqrt{1-p}|1\rangle_4 \langle 1|\right),$$

(64)

where $\text{Tr}_3(|\phi\rangle_{23} \langle \phi|) = \sigma_2$ (without loss of generality we can also assume $\text{Tr}_3(|\phi\rangle_{23} \langle \phi|) = \sigma_3$).

One can easily check that

$$\text{Tr}_{234} \left(U_{1234} \rho_1 \otimes |\phi_E\rangle_{234} \langle \phi_E| U_{1234}^\dagger\right) = p \rho_1 + (1-p) \sigma.$$

(65)

Taking the trace over the output systems 1 we obtain the output of the channel to Bob:

$$\text{Tr}_1 \left(U_{1234} \rho_1 \otimes |\phi_E\rangle_{234} \langle \phi_E| U_{1234}^\dagger\right) = p |\phi\rangle_{23} \langle \phi| \otimes |0\rangle_4 \langle 0| + (1-p) \rho_2 \otimes \sigma_3 \otimes |1\rangle_4 \langle 1|

+ \sqrt{p(1-p)} [\text{Tr}_1 (S_{12} \rho_1 \otimes |\phi\rangle_{23} \langle \phi|) \otimes |1\rangle_4 \langle 0| + \text{h.c.}].$$

(66)

We notice that the action on the channel from Alice and Bob depends on $\sigma$ through the last two terms proportional to $|0\rangle_4 \langle 1|$ and $|1\rangle_4 \langle 0|$. If we apply a completely dephasing channel on qubit 4 the channel to Bob becomes an erasure channel with erasure probability $p$ independently of $\sigma$. This implies that the classical capacity of the erasure channel is an achievable rate for classical communication, hence we can put $R = (1-p) \log d$. Moreover, this bound holds for any choice of the locking unitary, since the erasure channel is covariant under unitary transformations.

A. Erasure channel

If $\sigma$ is orthogonal to the input space, the channel in Eq. (56) is a qudit erasure channel with erasure probability $1-p$, whose complement is an erasure channel with erasure probability $p$. In this case, the maximum communication rate equals the classical capacity of the erasure channel, $R = (1-p) \log d$, and the secret key consumption rate is of $p - (1 - 2p) \log d$ bits if $p \geq 1/2$ and of $p$ bits if $p \leq 1/2$. 
B. Conjugate of the depolarizing channel

If $\sigma = \mathbb{I}/d$, the channel in Eq. (56) is a qudit depolarizing channel with depolarizing probability $1 - p$. We can rewrite the action of the depolarizing channel as

$$\mathcal{N}_{A\to E}(\rho) = p \rho + \frac{1-p}{d^2} \sum_{a,b=0}^{d-1} X^a Z^b \rho Z^{-b} X^{-a},$$

(67)

where $X = \sum_{j=0}^{d-1} |j \oplus 1 \rangle \langle j|$ (\(\oplus\) denotes summation modulo $d$) and $Z = \sum_{j=0}^{d-1} e^{ij2\pi/d} |j \rangle \langle j|$ are the $d$-dimensional generalization of the Pauli matrices, and $\{|j\rangle\}_{j=0,...,d-1}$ is a qudit basis. This representation of the channel to Eve induces a representation for the isometric extension, which is given by the bipartite conditional unitary:

$$U = \sum_{a,b=0}^{d-1} |ab\rangle \langle ab| \otimes X^a Z^b,$$

(68)

where the first system, assigned to Eve’s input, is represented by a $d^2$-dimensional Hilbert space (spanned by the basis vectors $\{|ab\rangle\}$), and the second is the input qudit system. As initial state of Eve’s system we take

$$|\phi_E\rangle = \sum_{a,b=0}^{d-1} \sqrt{q_{ab}} |ab\rangle,$$

(69)

where $q_{00} = p + (1-p)/d^2$ and $q_{ab} = (1-p)/d^2$ for $ab \neq 00$. Taking the partial trace over Eve’s output system, we finally obtain the following expression for the channel to Bob:

$$\mathcal{N}_{A\to B}(\rho) = \sum_{a,b,a',b'=0}^{d-1} \sqrt{q_{ab} q_{a'b'}} |ab\rangle \langle a'b'| \text{Tr} \left( X^a Z^b \rho Z^{-b'} X^{-a'} \right).$$

(70)

A straightforward calculation yields that the maximum achievable rate using our ensemble of input states is

$$R = f(p,d^2) - f(p,d),$$

(71)

where

$$f(p,D) = -\left( p + \frac{1-p}{D} \right) \log \left( p + \frac{1-p}{D} \right) - (D-1) \frac{1-p}{D} \log \left( \frac{1-p}{D} \right).$$

(72)

As in the case of the erasure channel, this rate is independent of the choice of encoding basis.

In conclusion, Eq. (71) gives the maximum reliable communication rate from Alice to Bob. The secret key consumption rate is hence equal to $p + \max \{p \log d - f(p,d^2) + f(p,d)\}$. 
V. CONCLUSIONS

Our QDL protocols yield achievable rates of strong and weak locking through a noisy qudit channel. Consider the case of weak locking at a rate $R$ with a secret consumption rate of $k$ bits per channel use (analogous results are obtained for strong locking). If the channel $N_{A \rightarrow B}$ has non-zero private capacity, one can first use the channel to establish a private key between the two legitimate parties, then use such a key to lock the subsequent uses of the channel. In this way Alice and Bob will achieve a weak locking rate of

$$R_{wl} = \frac{R}{1 + k/P},$$

(73)

where $P$ is the private capacity of the communication channel. In this way any channel with non-zero private capacity allows us to lock data in the weak locking sense. For qudit channels having $R$ and $P$ large enough, $R_{wl}$ can be much larger than the private capacity and arbitrarily close to the classical capacity.

Alternatively, for generic channels, including those with zero private capacity, one can define a QDL protocol under the assumption that Alice and Bob know an upper bound $\tau$ on the coherence time of Eve’s quantum memory. For $R > k$, a weak locking protocol is then defined according to the following procedure:

1. Alice and Bob initially share a secret key of $nk$ bits;
2. They use the secret key to send about $nR$ bits of locked information through $n$ uses of the qudit channel;
3. They wait a time $\tau$ sufficiently long to guarantee that Eve’s quantum memory decoheres. After such a time the locked information Alice has sent to Bob can be considered secure in the composable sense (see Sec. II and Ref. [3]);
4. Alice and Bob recycle $nk$ of the $nR$ bits as a secret key for the next round of the communication protocol;
5. They repeat the above procedure for $n'$ times.

Using this bootstrap technique, Alice and Bob will asymptotically achieve a weak locking rate of

$$R_{wl} = R - k = R - p - \max \{0, p \log d - R\}$$

(74)

bits per channel use, with a secret key consumption rate of $k/n'$ bits that goes to zero in the limit $n' \rightarrow \infty$. While the rate per channel use is finite and independent of $\tau$, one may object that the communication rate per second will become arbitrarily small if $\tau$ is large enough. To solve this problem, Alice and Bob can run
two or more independent instances of the protocol in parallel (each using an independent secret key) taking advantage of the dead times between one protocol and the other. It follows that the communication rate per second remains finite and independent of $\tau$ even in the limit of $\tau \to \infty$. (Clearly, the protocol can become unpractical if $\tau$ is too large.)

For the erasure channel, the latter procedure achieves a weak locking rate of $R_{wl} = (1 - p) \log d - p$ bits for $p \leq 1/2$, and of $R_{wl} = (2 - 3p) \log d - p$ bits for $p \geq 1/2$. For the conjugate of the depolarizing channel, it achieves a weak locking rate of $R_{wl} = f(p, d^2) - f(p, d^2) - p - \max \{0, p \log d - f(p, d^2) + f(p, d^2)\}$. Figure 1 shows the weak locking rate compared with the classical capacity [16] and the private capacity [2] of the erasure channel. Figure 2 shows the weak locking rate for the conjugate of the depolarizing channel, compared with its classical capacity and the Hashing bound for private communication.

FIG. 1: Comparison of several communication rates (in bits per channel use) for the qudit erasure channel, with $d = 64$ and $p \in [0, 1]$. Weak locking rate (solid line); classical capacity (dashed line); private capacity (dot-dashed line).

FIG. 2: Comparison of several communication rates (in bits per channel use) for the conjugate of the depolarizing channel, with $d = 64$ and $p \in [0, 1]$. Weak locking rate (solid line); classical capacity (dashed line); hashing bound for private communication (dot-dashed line).
In conclusion, we have presented protocols that achieve a weak locking rate as high as less than one bit below the classical capacity. These results, together with [3, 15], further deepen our understanding of the QDL effect as well as of the notion of locking capacities recently introduced in [6]. A few natural questions remain open. It is not clear whether our strong locking protocol for the noiseless channel is optimal in terms of secret key consumption. The secret key consumption rate of 1 bit per channel use could very well not be a fundamental limit, but just an artifact of our proof technique. Also, one would like to find good locking protocols for general channels beyond the restricted class considered here. Finally, since the most important realizations of quantum communication channels are infinite dimensional, it is urgent to discover QDL that are not restricted to the finite dimensional setting.

**Acknowledgment.** We are grateful to Giuseppe Vallone, Frédéric Dupuis, Andreas Winter, and 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] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
[2] I. Devetak, IEEE Trans. Inf. Theory 51, 44 (2005); N. Cai, A. Winter, and R. W. Yeung, Probl. Inf. Transm. 40, 318 (2004).
[3] C. Lupo and S. Lloyd, Phys. Rev. Lett 113, 160502 (2014).
[4] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, B. M. Terhal, Phys. Rev. Lett. 92, 067902 (2004).
[5] R. König, R. Renner, A. Baris, U. Maurer, Phys. Rev. Lett. 98, 140502 (2007).
[6] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, M. M. Wilde, Phys. Rev. X 4 011016 (2014).
[7] P. Hayden, D. Leung, P. W. Shor, A. Winter, Comm. Math. Phys. 250, 371 (2004).
[8] J. A. Smolin and J. Oppenheim, Phys. Rev. Lett. 96, 081302 (2006).
[9] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, S. Wehner, Phys. Rev. A 78, 022316 (2008).
[10] D. Leung, International Workshop on Statistical-Mechanical Informatics 2008 (IW-SMI 2008), J. Phys.: Conference Series 143, 012008 (2009).
[11] O. Fawzi, P. Hayden, P. Sen, Journal of the ACM 60, 44 (2013).
[12] F. Dupuis, J. Florjanczyk, P. Hayden, D. Leung, Proc. Royal Soc. A 469, 20130289 (2013).
[13] S. Lloyd, ‘Quantum enigma machines,’ arXiv:1307.0380 (2013).
[14] C. Lupo, M. M. Wilde, S. Lloyd, Phys. Rev. A 90, 022326 (2014).
[15] A. Winter, ‘Weak locking capacity of quantum channels can be much larger than private capacity,’ arXiv:1403.6361 (2014).
[16] A. S. Holevo, IEEE Trans. Inf. Theory 44, 269 (1998); B. Schumacher and M. D. Westmoreland, Phys. Rev. A 56, 131 (1997).

[17] A. Maurer, JIPAM, 4, 15 (2003).

[18] R. Ahlswede, A. J. Winter, IEEE Trans. Inf. Theory, 48 569, (2002).

[19] M. Fannes, Comm. Math. Phys. 31, 291 (1973); K. M. R. Audenaert, J. Phys. A 40, 8127 (2007).

[20] In general, this rate could depend on the choice of bases used by Alice for encoding, that is, on the value of the secret key. To obtain a key-independent value one should consider the minimum rate.