Locked communication and key generation at (almost) the classical capacity rate

Cosmo Lupo\textsuperscript{1} and Seth Lloyd\textsuperscript{1, 2}

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

Quantum data locking is a protocol that allows for a small secret key to (un)lock an exponentially larger amount of information, hence yielding a strong 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 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 quantum memory is known. Under this condition we introduce protocols for locked communication and key generation through a memoryless qudit channel. For channels with enough symmetry, such as the $d$-dimensional erasure and depolarizing channels, these protocols allow data locking at an asymptotic rate as high as the classical capacity minus one bit.

I. INTRODUCTION

A famous theorem of Shannon theorem 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\textsuperscript{[1]}. When the message is encrypted in quantum bits or qubits, by contrast, the phenomenon of quantum data locking (QDL) shows that the key required for secure encryption of an $n$ bit message can be much less than $n$\textsuperscript{[2]}: in quantum data locking an arbitrarily long message, suitably encoded in a quantum system, is encrypted and decrypted by a secret key of constant length. In the strongest QDL protocols known up to now a key of $O(\log 1/\epsilon)$ bits allows one to lock a message of $n$ bits, in such a way that an eavesdropper measuring the quantum system cannot access more than about $\epsilon n$ bits of information about the message\textsuperscript{[3, 4]}.

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\textsuperscript{[5]}. Suppose that the eavesdropper Eve has access to the state $\rho_{E|x}$ given that the classical message $x$ has been sent by the legitimate sender Alice to the legitimate receiver Bob. The widely accepted security criterion in quantum cryptography requires that Eve’s state is $\epsilon$-close to be a product state in the operator trace norm\textsuperscript{[5]}, that is,

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

where $p_X(x)$ 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 Alicki-Fannes inequality Eq. (1) implies
\[ \chi(E) := S(\rho_E) - \sum_x p_X(x) S(\rho_{E|x}) \leq 4\epsilon \log |X| + 2h_2(\epsilon), \]  
where \( \chi(E) \) is Holevo information of the ensemble of quantum states \( E = \{p_X(x), \rho_{E|x}\} \), \( S(\rho) := -\text{tr} \rho \log \rho \) 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 one (see, e.g., [7]). This criterion requires that the result of any measurement Eve can make on her share of the quantum state is \( \epsilon \)-close to being uncorrelated with the message. Suppose that a measurement operator \( M_{E \rightarrow \hat{X}} \) maps \( \rho_{E|x} \) into the classical variables \( \hat{X} \) with probability distribution \( p_{\hat{X}|X} \). Then one considers the norm
\[ \sup_{M_{E \rightarrow \hat{X}}} \left\| p_{\hat{X}|X} p_X - \hat{p}_{\hat{X}} p_X \right\|_1 := \sup_{M_{E \rightarrow \hat{X}}} \sum_{x,\hat{x}} |p_{\hat{X}|X}(\hat{x}|x)p_X(x) - \hat{p}_{\hat{X}}(\hat{x})p_X(x)|, \]  
where \( p_{\hat{X}}(\hat{x}) = \sum_x p_{\hat{X}|X}(\hat{x}|x)p_X(x) \). If (3) is less than \( \epsilon \), then the Alicki-Fannes inequality implies
\[ I_{\text{acc}}(E) = \sup_{M_{E \rightarrow \hat{X}}} I(X; \hat{X}) \leq 4\epsilon \log |X| + 2h_2(\epsilon), \]  
where \( I_{\text{acc}}(E) \) is the accessible information of the ensemble \( E = \{p_X(x), \rho_{E|x}\} \), \( I(X; \hat{X}) = H(X) + H(\hat{X}) - H(X\hat{X}) \) 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 [8]. Unlike the Holevo information, the accessible information does not obey the property of total proportionality. 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 \( \text{before} \) she measures, then she could use this information to increase the accessible information by a disproportionate amount. As a consequence, accessible information security does not in general imply composable security [5], that is, a protocol that is secure according to the accessible information criterion may not remain so when composed with 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. 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.

Here we exploit the gap between these two security criteria to show that there are communication channels with poor security according to the Holevo information criterion that allow for high rate of secure communication if the accessible information criterion is instead considered. In particular, we show that upon a suitable assumption on the timing of Eve’s measurements, Alice and Bob can generate a secret key through a $d$-dimensional memoryless quantum channel at a rate equal (up to 1 bit) to the classical capacity of the channel. These results can be applied in cryptography under the assumption that Eve is forced to measure her share of the quantum system within a time $\tau$ after she has obtained it. In other words, Alice and Bob must know an upper bound $\tau$ on the coherence time of Eve’s quantum memory. Clearly, any quantum memory device will decohere after a certain time, and then the question is what happens for large coherence time. For any value of $\tau$ Alice and Bob can apply a doubly-blocked communication protocol, where they first send a data packet down the channel, and then wait a time $\tau$ before doing all the required post-processing. In the meanwhile Alice can keep sending to Bob independent data packets that will be processed at a later time. The larger $\tau$ is, the longer Alice and Bob have to wait to guarantee the security of the communication. However, in a stationary regime this doubly-blocked procedure does not depend on $\tau$, that is, the asymptotic communication rate remains finite in the limit $\tau \to \infty$.

II. OVERVIEW

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. If an eavesdropper Eve does not know the private 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 particular, the QDL protocols described in [3, 4] are one-shot protocols defined for a $d$-dimensional noiseless quantum system. Alice and Bob can hence communicate $\log d$ bits of information reliably via a noiseless channel. For $d$ large enough, a pre-shared secret key of $\log K = O(\log 1/\epsilon)$ bits is enough to encrypt the communication, with the guarantee that if Eve intercepts and measures the whole quantum system carrying the message her accessible information will be no more
than $\epsilon \log d$.

A number of works have been devoted to the role of QDL in physics and information theory [3, 4, 10–16]. However, only recently QDL has been considered in the presence of noise. Following the idea of the “quantum enigma machine” [14] for applying QDL to cryptography, a formal definition of the locking capacity of a communication channel has been recently introduced in [15], 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. Two notions of capacities were defined in [15]: 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; the strong locking capacity is instead defined by requiring that the eavesdropper is able to measure the output of both the quantum channel and its complementary (this is equivalent to say that the eavesdropper measures the 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 [17], there exist qudit channels with low (1 bit per channel use) or even zero private capacity whose weak locking capacity is larger than $1/2 \log d$. In particular, the examples in [17] refer to channels whose classical capacity is $\log d$ bits, hence showing that the locking capacity can be as high as one half of the classical one.

QDL protocols for noisy quantum channels have been considered in [15] both in the asymptotic and one-shot settings. However, any QDL protocol is inherently a one-shot protocol as it requires that Eve’s measurement takes place at a certain time. Here we exploit this property and make a specific assumption on the timing of Eve’s measurement. Under this assumption, we show examples of qudit channels whose locking capacity can be close to the classical capacity for $d$ large enough. Also, we consider a protocol for secret key generation through a qudit channel, which is secure in the sense of strong locking. We apply this protocol to the case of qudit channels that are covariant under unitary transformations on the input and output, as is the case for the $d$-dimensional depolarizing and erasure channels, for which one can achieve a strong locking secret key generation rate equal to the classical capacity minus 1 bit.

Our starting point is a new QDL protocol for the $d$-dimensional noiseless channel (for any $d \geq 3$). 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. A bootstrap technique then allows for an overall secret key consumption that grows sublinearly in the number of channel uses. We then generalize the protocol to the case of a noisy qudit channel. The crucial property for this generalization to be possible is the fact that our protocol makes use of codewords that are separable among different channel uses. This property allows Alice and Bob to reliably communicate locked information at a rate given by the Holevo information $\chi(\mathcal{E})$ associated to the ensemble of codewords $\mathcal{E}$ used for locking. However, since the required secret key grows linearly in the number of channel use, this protocol does not directly define a strong locking protocol. Nevertheless, one can use it to build a stricto sensu strong locking protocol.

If the channel has non-zero private capacity, one can first use the channel to establish a private key between the two legitimate parties (this key will be secure according to the Holevo information criterion), 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

$$R_{w.l.} = \frac{\chi(\mathcal{E})}{1 + P^{-1}},$$

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 $\chi(\mathcal{E})$ large enough (e.g., the $d$-dimensional depolarizing and erasure channels) $R_{w.l.}$ 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 $\chi(\mathcal{E}) > 1$, this can be done according to the following procedure:

1. Alice and Bob initially share a secret key of $n$ bits;
2. They use the secret key to send about $n\chi(\mathcal{E})$ bits of locked information through $n$ uses of the qudit channel;
3. They wait a time $\tau$ sufficient 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;
4. If $\chi(\mathcal{E}) > 1$, Alice and Bob recycle $n$ of the $n\chi(\mathcal{E})$ 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

$$R_{w.l.} = \chi(\mathcal{E}) - 1$$

bits with a secret key consumption rate of $1/n'$ bits per channel use that goes to zero in
the limit $n' \to \infty$. 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. In this way the communication rate per second remains finite and independent of $\tau$. In particular, we have a weak locking rate of $\chi(E) - 1$ bits also in the limit of $\tau \to \infty$.

In the remainder of the paper, we first define a strong locking protocol for the qudit noiseless channel. Then we extend it to a weak locking protocol for the memoryless qudit channel. Finally, we define a key generation protocol (secure in the strong locking sense) for an arbitrary memoryless qudit channel and we apply it to the case of the qudit depolarizing channel.

III. A PROTOCOL FOR STRONG LOCKING OF A NOISELESS CHANNEL

In this section we define a QDL protocol for locking classical information transmitted through a noiseless channel in $d$-dimensions. The protocol is in a sense similar to the one discussed in [4], though in the present case the QDL codewords are separable among different channel uses. This is indeed a crucial feature that allows us to generalize the protocol to the case of an arbitrary noisy memoryless qudit channels. In this section we assume that the legitimate parties Alice and Bob communicate through $n$ instances of a noiseless qudit channel and that the eavesdropper Eve has also access to the output of the channel to Bob (this is the setup for strong locking of the noiseless channel). We also assume that Alice and Bob initially share a key of $\log K$ bits, unknown to Eve. We require that Alice and Bob are able to communicate reliably at a rate of $\log d$ bits per channel use, and that Eve’s accessible information about the message sent by Alice is less than $\epsilon \log d$ bits per channel use. We will show that $\epsilon$ can be taken to be exponentially small in $n$ with an asymptotic secret key consumption rate of 1 bit per channel use (independently of $d$).

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

$$|m\rangle = \frac{1}{\sqrt{d}} \sum_{\omega=1}^{d} e^{i2\pi m \omega/d} |\omega\rangle. \quad (6)$$

We consider the “phase ensemble” of qudit unitary transformations of the form:

$$U = \sum_{\omega=1}^{d} e^{i \theta(\omega)} |\omega\rangle \langle \omega|, \quad (7)$$

where the angles $\theta(\omega)$, for $\omega = 1, \ldots, d$, are $d$ i.i.d. random variables. We require that these variables are distributed in such a way that $\mathbb{E}[e^{i \theta(\omega)}] = 0$ [18].
Given a collection of \(n\) qudit systems, we consider the product basis vectors \(|m\rangle = \bigotimes_{j=1}^{n} |m^j\rangle\). To encode the message “\(m\)”, Alice prepares the state \(|m\rangle\). The vectors from this basis are then scrambled by applying a unitary transformation \(\bigotimes_{j=1}^{n} U^j\) on the \(n\) qudit system, yielding

\[
|\Psi_m\rangle = \bigotimes_{j=1}^{n} U^j |m^j\rangle = \frac{1}{\sqrt{d^n}} \sum_{|\omega\rangle} e^{i \sum_{j=1}^{n} [2\pi m^j \omega^j / d + \theta^j(\omega^j)]} |\omega\rangle,
\]

(8)

where the \(n\) qudit unitaries \(U^j\), for \(j = 1, \ldots, n\) are chosen i.i.d. from the phase ensemble, and \(|\omega\rangle = \bigotimes_{j=1}^{n} |\omega^j\rangle\). Notice that the vectors \(\{|\Psi_m\rangle\}_m\) define a new basis for the \(n\)-qudit system, which is obtained by locally applying random unitaries chosen i.i.d. from the phase ensemble.

In our protocol Alice locks \(n \log d\) bits of classical information by preparing one of the \(n\)-qudit code-words

\[
|\Psi_{mk}\rangle = \bigotimes_{j=1}^{n} U^j_k |m^j\rangle,
\]

(9)

where the value of the label \(k = 1, \ldots, K\) is determined by the \(\log K\) bits of the pre-shared secret key.

A. Some preliminary results

To characterize our QDL protocol we will make use of two concentration inequalities. The first one is the Maurer tail bound [19]:

**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 \(\mathbb{E}[X], \mathbb{E}[X^2] < \infty\). 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 [20]:

**Theorem 2** Let \(\{X_t\}_{t=1,\ldots,T}\) 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 \(\mathbb{E}[X_t] = \mu I\) (\(I\) is the identity operator). Then, for any \(\tau > 0\) we have that

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

For any given \(d^n\)-dimensional unit vector \(|\Phi\rangle\), \(m\) and \(k\), we define the random variable

\[
q_{mk}(\Phi) = |\langle \Phi | \Psi_{mk} \rangle|^2,
\]

(10)
which is a function of the random codeword $|\Psi_{mk}\rangle$ defined by Eq. (9). To apply Theorems 1 and 2 we compute the first and second moments of $q_{mk}(\Phi)$ with respect to the i.i.d. random unitaries sampled from the phase ensemble. Putting $|\Phi\rangle = \sum_\omega \Phi_\omega |\omega\rangle$, we have

$$
\mathbb{E}[q_{mk}(\Phi)] = \frac{1}{d^n} \sum_{\omega,\omega'} \Phi^*_\omega \Phi_{\omega'} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)}/d \mathbb{E} \left[ e^{i \sum_j=1^d \theta_j (\omega_j - \omega'_j)} \right] \tag{11}
$$

$$
= \frac{1}{d^n} \sum_{\omega,\omega'} \Phi^*_\omega \Phi_{\omega'} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)}/d \prod_{j=1}^n \mathbb{E} \left[ e^{i \theta_j (\omega_j - \omega'_j)} \right] \tag{12}
$$

$$
= \frac{1}{d^n} \sum_{\omega,\omega'} \Phi^*_\omega \Phi_{\omega'} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)}/d \prod_{j=1}^n \delta_{\omega_j,\omega'_j} \tag{13}
$$

$$
= \frac{1}{d^n} \sum_{\omega,\omega'} \Phi^*_\omega \Phi_{\omega'} \prod_{j=1}^n \delta_{\omega_j,\omega'_j} = \frac{1}{d^n}, \tag{14}
$$

and

$$
\mathbb{E}[q_{mk}(\Phi)^2] = \frac{1}{d^{2n}} \sum_{\omega,\omega',\omega'',\omega'''} \Phi^*_\omega \Phi_{\omega'} \Phi^*_\omega' \Phi_{\omega'''} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega''_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'''_j)}/d \mathbb{E} \left[ e^{i \sum_j=1^d \theta_j (\omega_j - \omega'_j) + \theta_j (\omega''_j - \omega'''_j)} \right] \tag{15}
$$

$$
= \frac{1}{d^{2n}} \sum_{\omega,\omega',\omega'',\omega'''} \Phi^*_\omega \Phi_{\omega'} \Phi^*_\omega' \Phi_{\omega'''} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega''_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'''_j)}/d \prod_{j=1}^n \mathbb{E} \left[ e^{i \theta_j (\omega_j - \omega'_j) + i \theta_j (\omega''_j) - i \theta_j (\omega'''_j)} \right] \tag{16}
$$

$$
= \frac{1}{d^{2n}} \sum_{\omega,\omega',\omega'',\omega'''} \Phi^*_\omega \Phi_{\omega'} \Phi^*_\omega' \Phi_{\omega'''} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega''_j)} e^{i \sum_j=1^d \omega_j (\omega_j - \omega'''_j)}/d \prod_{j=1}^n \delta_{\omega_j,\omega'_j} \delta_{\omega''_j,\omega'''_j} + \delta_{\omega_j,\omega''_j} \delta_{\omega'_j,\omega'''_j} \tag{17}
$$

$$
= \frac{1}{d^{2n}} \sum_{\omega,\omega',\omega'',\omega'''} \Phi^*_\omega \Phi_{\omega'} \Phi^*_\omega' \Phi_{\omega'''} \prod_{j=1}^n \delta_{\omega_j,\omega'_j} \delta_{\omega''_j,\omega'''_j} + \delta_{\omega_j,\omega''_j} \delta_{\omega'_j,\omega'''_j} \tag{18}
$$

One can show that (see Appendix A):

$$
\mathbb{E}[q_{mk}(\Phi)^2] \leq \frac{2^n}{d^{2n}}. \tag{19}
$$

For any given $|\Phi\rangle$ and $m$ we define the random variable

$$
Q_m(\Phi) = \frac{1}{K} \sum_{k=1}^K q_{mk}(\Phi). \tag{20}
$$

Notice that for $k \neq k'$, $|\Psi_{mk}\rangle$ and $|\Psi_{mk'}\rangle$ are statistically independent, and so are $q_{mk}(\Phi)$ and $q_{mk'}(\Phi)$. We can hence apply Maurer’s tail bound (Theorem 1). We obtain that for any given $|\Phi\rangle$ and $m$:

$$
Pr \left\{ Q_m(\Phi) < \frac{1}{d^n} \right\} \leq \exp \left( -\frac{K \epsilon^2}{2n+1} \right). \tag{21}
$$
We then apply the operator Chernoff bound (Theorem 2) to the operators $|\Psi_{mk}\rangle\langle\Psi_{mk}|$. Notice that $\mathbb{E}[q_{mk}(\Phi)] = 1/d^n$ [Eq. (14)] implies

$$\mathbb{E}[|\Psi_{mk}\rangle\langle\Psi_{mk}|] = \frac{1}{d^n}. \quad (22)$$

The operator Chernoff bound then yields that for any given $m$

$$Pr\left\{\frac{1}{K} \sum_{k=1}^{K} |\Psi_{mk}\rangle\langle\Psi_{mk}| > (1 - \delta)I\right\} \leq d^n \exp\left(-\frac{K(d^n(1 - \delta) - 1)^2}{d^n 4 \ln 2}\right) \quad (23)$$

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

This result in turn implies that for any given $m$

$$Pr\left\{\max_{|\Phi\rangle} Q_m(\Phi) > 1 - \delta \right\} \leq d^n \exp\left(-\frac{Kd^n(1 - \delta - 1/d^n)^2}{4 \ln 2}\right). \quad (25)$$

Finally, to optimize Eve’s measurement on her share of the quantum state, we will make use of the notion of $\epsilon$-net. An $\epsilon$-net is a finite set of unit vectors $\mathcal{N}_\epsilon = \{|\Phi_i\rangle\}_i$ in a $D$-dimensional Hilbert space such that for any unit vector $|\Phi\rangle$ there exists $|\Phi_i\rangle \in \mathcal{N}_\epsilon$ such that

$$|||\Phi\rangle\langle\Phi| - |\Phi_i\rangle\langle\Phi_i|||_1 \leq \epsilon. \quad (26)$$

As discussed in [10] there exists an $\epsilon$-net such that $|\mathcal{N}_\epsilon| \leq (5/\epsilon)^{2D}$.

### B. Eve’s accessible information

In the strong locking scenario, we assume that Eve intercepts the whole train of qudit systems and measures them. To evaluate the security of the QDL protocol according to the accessible information criterion, we show that there exist choices of the scrambling unitaries $U^j_k$’s that guarantee Eve’s accessible information to be arbitrarily small if $n$ is large enough. To prove that we show that this property is true with a non-zero probability for a random choice of the unitaries $U^j_k$’s. The proof strategy is analogous to the one of [4] and is based on similar ideas already applied to other QDL protocols [3, 10].

Let Eve intercept and measure the train of $n$ qudits sent by Alice. A measurement is described by the 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 $\mathcal{E} = \{p_m, \frac{1}{K} \sum_{k=1}^{K} |\Psi_{mk}\rangle\langle\Psi_{mk}|\}$, where $p_m$ is the probability of the message $m$. For the sake of simplicity here we assume that all the messages have equal probability, that
is, \( p_m = 1/d^n \) (the case of non-uniform distribution was considered in details in [3, 13]). A straightforward calculation then yields

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

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

\[
Q_m(\Phi) = \frac{1}{K} \sum_{k=1}^K |\langle \Phi | \Psi_{mk} \rangle|^2 = \frac{1}{K} \sum_{k=1}^K q_{mk}(\Phi),
\]

and

\[
H[Q(\Phi)] = -\sum_m Q_m(\Phi) \log Q_m(\Phi)
\]

is its Shannon entropy (notice that \( \sum_m Q_m(\Phi) = 1 \)).

Since \( \sum_i \mu_i/d^n = 1 \), the positive coefficients \( \mu_i/d^n \) 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:

\[
I_{acc}(E) \leq \log d^n - \min_{\{\Phi\}} H[Q(\Phi)],
\]

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 \( \min_{\Phi} H[Q(\Phi)] \).

In order to prove that \( I_{acc}(E) \leq \epsilon \log d^n \), we need to show that \( \min_{\Phi} H[Q(\Phi)] \geq (1 - \epsilon) \log d^n \). To do that, for any \( \epsilon > 0 \) and \( d^n \) and \( K \) large enough we bound the probability that

\[
-Q_m(\Phi) \log Q_m(\Phi) < \eta \left( \frac{1 - \epsilon}{d^n} \right),
\]

where \( \eta(x) := -x \log x \). This corresponds to bounding the probability that either \( Q_m(\Phi) < \lambda_- \) or \( Q_m(\Phi) > \lambda_+ \), where \( \lambda_- = (1 - \epsilon)/d^n \) and \( \lambda_+ = 1 - \eta \left( \frac{1 - \epsilon}{d^n} \right) + O \left( \eta \left( \frac{1 - \epsilon}{d^n} \right) \right) \). Notice that for \( d^n \) sufficiently large and/or \( \epsilon \) sufficiently small we have \( \lambda_+ \geq 1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) \).
From Eq. (25) and applying the union bound we obtain

\[ P_r \left\{ \max_{|\Phi,m} Q_m(\Phi) > \lambda_+ \right\} \leq P_r \left\{ \max_{|\Phi,m} Q_m(\Phi) > 1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) \right\} \]

(32)

\[ \leq d^n P_r \left\{ \max_{|\Phi,m} Q_m(\Phi) > 1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) \right\} \]

(33)

\[ \leq d^{2n} \exp \left( - \frac{Kd^n(1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) - 1/d^n)^2}{4\ln 2} \right) \]

(34)

\[ \leq \exp \left( \ln d^{2n} - \frac{Kd^n(1 - 2\eta \left( \frac{1 - \epsilon}{d^n} \right) - 1/d^n)^2}{4\ln 2} \right) \]

(35)

\[ \leq \exp \left( \ln d^{2n} - \frac{Kd^n(1 - 4\eta \left( \frac{1 - \epsilon}{d^n} \right) - 2/d^n)}{4\ln 2} \right) \]

(36)

\[ \leq \exp \left( \ln d^{2n} - \frac{Kd^n(1 - 6\eta \left( \frac{1 - \epsilon}{d^n} \right))}{4\ln 2} \right) =: p_+ \]

(37)

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 that \( K > \frac{\ln d^{2n}}{d^n(1 - 6\eta[(1-\epsilon)/d^n])} \).

Then, for any given \( |\Phi\) we use Eq. (21) and apply again the union bound to obtain

\[ P_r \{ \exists m_1, \ldots, m_\ell \mid \forall i Q_{m_i}(\Phi) < \lambda_- \} = P_r \left\{ \exists m_1, \ldots, m_\ell \mid \forall i Q_{m_i}(\Phi) < \frac{1 - \epsilon}{d^n} \right\} \]

(38)

\[ \leq \left( \frac{d^n}{\ell} \right) P_r \left\{ Q_1(\Phi) < \frac{1 - \epsilon}{d^n} \right\} \]

(39)

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

(40)

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

(41)

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

(42)

Putting \( \ell = \epsilon d^n \) we have

\[ P_r \{ \exists m_1, \ldots, m_\ell \mid \forall i Q_{m_i}(\Phi) < \lambda_- \} \leq \exp \left[ -d^n \left( \frac{K^3}{2^n+1} - \epsilon \ln d^n \right) \right] =: p_- . \]

(43)

Notice that this probability is also exponentially small in \( d^n \), provided that \( K > 2^{n+1} \epsilon^{-2} \ln d^n \).

Inequality (43) implies that with probability greater than \( 1 - p_- \) there are at least \( d^n - \ell = (1 - \epsilon)d^n \) values of \( m \) such that \( Q_m(\Phi) > \lambda_- \). Also, according to Eq. (37), with probability at least equal to \( 1 - p_+ \)
all the $Q_m(\Phi)$’s are larger than $\lambda_+$. Putting these results together we have that

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

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

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

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

with a probability at least equal to $1 - p_--p_+$. For $d^n$ large enough this probability is larger than $1 - 2p$.

The last step is to introduce an $\epsilon$-net $N_\epsilon = \{|\Phi_i\rangle\}_i$. Let us recall that the $\epsilon$-net can be chosen to contain less than $(5/\epsilon)^{2d^n}$ elements. We can hence apply the union bound to obtain:

$$Pr \left\{ \min_{|\Phi_i\rangle \in N_\epsilon} H[Q(\Phi_i)] < (1 - 2\epsilon) \log d^n \right\} \leq (5/\epsilon)^{2d^n} 2p_--p_+$$

$$= 2(5/\epsilon)^{2d^n} \exp \left[ -d^n \left( \frac{K\epsilon^3}{2n+1} - \epsilon \ln d^n \right) \right]$$

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

Finally, we have to replace the minimum over vectors in the $\epsilon$-net with a minimum over all unit vectors. An application of the Fannes inequality \cite{21} yields (see also \cite{10})

$$\left| \min_{|\Phi\rangle} H[Q(\Phi)] - \min_{|\Phi_i\rangle \in N_\epsilon} H[Q(\Phi_i)] \right| \leq \epsilon \log d^n + \eta(\epsilon).$$

This result implies

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

that is,

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

Such a probability is bounded away from one (and goes to zero exponentially in $d^n$) provided

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

In conclusion, we have proven that there exist QDL codes allowing Alice and Bob to lock data through $n$ uses of a noiseless memoryless qudit channel in such a way that Eve’s accessible information is $I_{\text{acc}}(\mathcal{E}) = O(\epsilon \log d^n)$. These codes are defined by codewords that are separable among different channel uses. The rate of locked communication is of $\log d$ bits per channel use and require the pre-shared secret key to be consumed at an asymptotic rate of $\lim_{n \to \infty} \frac{1}{n} \log K = 1$ bit per channel use. Notice that we can put $\epsilon = 2^{-nc}$, with any positive $c < 1$ and still lock data with a secret key consumption rate of 1 bit independently of $d$. 
IV. LOCKING A QUDIT MEMORYLESS CHANNEL

To send locked information through a generic, noisy, qudit memoryless channel $\mathcal{N}$ from Alice to Bob, we apply a suitable modification of the noiseless protocol described above. Over $n$ uses of the channel, Alice encodes the classical messages, $m = 1, \ldots, M$, by preparing the $n$-qudit codewords

$$|\Psi_{mk}\rangle = \bigotimes_{j=1}^{n} |\psi_{mk}^{j}\rangle,$$

where the one-qudit vectors $|\psi_{mk}^{j}\rangle$ are chosen i.i.d. from the “phase ensemble” of vectors

$$|\psi_{mk}\rangle = \frac{1}{\sqrt{d}} \sum_{\omega=1}^{d} e^{i\theta_{mk}(\omega)} |\omega\rangle,$$

and the value of $k = 1, \ldots, K$ is determined by the secret key. As in the noiseless protocol, the angular variables $\theta_{mk}(\omega)$ are sampled i.i.d. from a distribution such that $\mathbb{E}[e^{i\theta_{mk}(\omega)}] = 0$ [18].

Clearly, for any given $k$, this encoding can be used to send classical information through the quantum channel at a rate given by the Holevo information [22] of the continuous ensemble of qudit states $\mathcal{E} = \{ d\psi = \prod_{\omega=1}^{d} \frac{d\theta(\omega)}{2\pi}, |\psi\rangle = \frac{1}{\sqrt{d}} \sum_{\omega=1}^{d} e^{i\theta(\omega)} |\omega\rangle \}$:

$$\chi(\mathcal{E}) = S[N(\mathbb{I}/d)] - \int d\psi S[N(|\psi\rangle\langle\psi|)],$$

where we have used the fact that $\int d\psi |\psi\rangle\langle\psi| = \mathbb{I}/d$. It is well known that for

$$M = 2^{n(\chi(\mathcal{E}) - \delta \log d)}$$

Bob will be able to decode the message up to a probability of error that is arbitrarily small for $n$ large enough.

In the next sections we consider in detail a protocol for the weak locking of the qudit erasure channel and a protocol for the secret key generation (secret according to the strong locking criterion) through the qudit depolarizing channel.

A. Weak locking of the qudit erasure channel

In this section we consider a weak locking protocol for the qudit erasure channel with erasure probability $p < 1/2$. The Holevo information [22] for this channel is $\chi(\mathcal{E}) = (1 - p) \log d$. Due to the symmetry of the channel this coincides with the classical capacity of the erasure channel. Since we are considering weak locking, we assume that Eve measures the complementary channel. This is also a qudit erasure channel with erasure probability $1 - p > 1/2$. From standard results on typical sequences we have that, for any $\delta > 0$,
there is a probability larger than $1 - \delta$ that at least $n(1 - p - \delta)$ qudits will be erased in the route from Alice to Eve, corresponding to a $\delta$-typical error occurring on the $n$ instances of the memoryless erasure channel to Eve. This implies that, for a given typical error, Eve has to measure no more than $n(p + \delta)$ qudits. These qudits have been transmitted to Eve faultless, while the remaining remaining $n(1 - p - \delta)$ have been erased. We can hence compute the accessible information corresponding to this set of non-erased qudits.

We consider Eve's accessible information conditioned to the occurrence of a typical error. A straightforward calculation (see [4]) yields

$$I_{\text{acc}} \leq \log M - \frac{d^n(p+\delta)}{M} \min_{|\Phi\rangle} \left\{ H[Q(\Phi)] - \eta \left[ \sum_{m=1}^{M} Q_m(\Phi) \right] \right\}. \quad (59)$$

This expression is analogous to the one in (30), with the difference that now we have the additional term $\eta \left[ \sum_{m=1}^{M} Q_m(\Phi) \right]$. By applying the Chernoff bound (Theorem 2) we obtain

$$\Pr \left\{ \max_{|\Phi\rangle} \sum_{m=1}^{M} Q_m(\Phi) > (1 + \epsilon) \frac{M}{d^n(p+\delta)} \right\} \leq d^n(p+\delta) \exp \left( -\frac{K}{4\ln 2} \frac{M}{d^n(p+\delta)} \epsilon^2 \right) \quad (60)$$

$$= \exp \left( \ln d^n(p+\delta) - \frac{K}{4\ln 2} \frac{M}{d^n(p+\delta)} \epsilon^2 \right). \quad (61)$$

We put $M = 2^{n[(1-p)\log d - \delta \log d]} = d^{(1-p-\delta)}$, then this probability is bounded away from one provided

$$K > 4 (\ln 2) \frac{d^{n(2p+2\delta-1)}}{\epsilon^2} \ln d^n(p+\delta). \quad (62)$$

Notice that for $p < 1/2 - \delta$ the right hand side of (62) is exponentially small in $n$. Also, from the noiseless case we expect $K \sim 2^n$, hence the probability in (60) is exponentially small in $2^n$. Finally, we have that

$$\max_{|\Phi\rangle} \sum_{m=1}^{M} Q_m(\Phi) < (1 + \epsilon) \frac{M}{d^n(p+\delta)} \quad (63)$$

implies

$$\frac{d^n(p+\delta)}{M} \max_{|\Phi\rangle} \left[ \sum_{m=1}^{M} Q_m(\Phi) \right] < \frac{d^n(p+\delta)}{M} \eta \left[ (1 + \epsilon) \frac{M}{d^n(p+\delta)} \right]$$

$$= \eta (1 + \epsilon) + (1 + \epsilon) \log \frac{d^n(p+\delta)}{M} \quad (64)$$

$$< (1 + \epsilon) \log \frac{d^n(p+\delta)}{M}. \quad (65)$$

This in turn implies that the bound in Eq. (59) is basically equivalent to

$$I_{\text{acc}} \leq (1 + \epsilon) \log d^n(p+\delta) - \frac{d^n(p+\delta)}{M} \min_{|\Phi\rangle} H[Q(\Phi)] \quad (66)$$
At this point we can proceed as in the noiseless setting. We thus obtain that

\[ Pr \left\{ \exists m_1, \ldots, m_\ell \mid \forall i \ Q_{m_i}(\Phi) < \frac{1 - \epsilon}{d^{n(p+\delta)}} \right\} \leq \left( \frac{M}{\ell} \right) \exp \left( \frac{-\ell K^2}{2^{n+1}} \right) \leq M^\ell \exp \left( \frac{-\ell K^2}{2^{n+1}} \right) = \exp \left( \ell \log M - \frac{\ell K^2}{2^{n+1}} \right), \]  

and putting \( \ell = \epsilon M \)

\[ Pr \left\{ \exists m_1, \ldots, m_\ell \mid \forall i \ Q_{m_i}(\Phi) < \frac{1 - \epsilon}{d^{n(p+\delta)}} \right\} \leq \exp \left[ -M \left( \frac{K^3}{2^{n+1}} - \epsilon \log M \right) \right]. \]  

(70)

Proceeding as in the noiseless setting, we introduce an \( \epsilon \)-net for the \( d^{n(p+\delta)} \)-dimensional Hilbert space and apply the Fannes-Audenaert inequality [21] (see [4]). We then obtain

\[ Pr \left\{ \max_{\{\Phi\}} I_{\text{acc}} > 4 \epsilon \log d^{n(p+\delta)} + \eta(\epsilon) \right\} \leq 2 \exp \left[ -M \left( \frac{K^3}{2^{n+1}} - \epsilon \ln M - \frac{2d^{n(p+\delta)}}{M} \log \frac{5}{\epsilon} \right) \right]. \]  

(71)

Putting \( M = d^{n(1-p-\delta)} \) we obtain that such a probability is exponentially small in \( M \) provided that

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

(72)

In conclusion, the erasure channel with \( p < 1/2 \) can be locked (in the weak sense) by using secret key at a rate of 1 bit per channel use. We can use this result to define two \textit{stricto sensu} weak locking protocols for the erasure channel (recall that for a weak locking protocol we require that the secret key consumption increases sublinearly with the number of channel uses):

1. For the first protocol Alice and Bob do not need a preshared secret key. Since for \( p < 1/2 \) the erasure channel has a non-zero quantum capacity of \( (1 - 2p) \log d \) bits, they can use the first \( n \) instances of the channel to establish a secret key of about \( n(1 - 2p) \log d \) bits. Then they use such a key to lock the successive \( n' = n(1 - 2p) \log d \) uses of the channel. In this way they achieve a weak locking communication rate of

\[ R_{w.l.} = \frac{(1 - p) \log d}{1 + [(1 - 2p) \log d]} = \frac{C}{1 + P^{-1}}, \]  

(73)

where \( C \) and \( P \) denote respectively the classical and private capacity of the qudit erasure channel with \( p < 1/2 \). Notice that for any given \( p \in (0, 1/2) \) and \( d \) large enough, \( R_{w.l.} \) is bigger than the private capacity \( (1 - 2p) \log d \) and arbitrarily close to the classical capacity \( (1 - p) \log d \).

2. If Alice and Bob know an upper bound \( \tau \) on the coherence time of Eve’s quantum memory, then they can make QDL at high rate following the strategy outlined in Section III for the noiseless channel.
Upon $n$ uses of the channel Alice can send to Bob about $n(1 - p) \log d$ bits of locked information. A fraction of $n$ bits can be recycled and used as a secret key to lock another sequence of $n$ channel uses. To do that, Alice and Bob has to wait a time greater than $\tau$ to ensure that Eve’s quantum memory has completely decohered. In this way, they will finally achieve a weak locking rate of

$$R_{w,l} = (1 - p) \log d - 1 = C - 1 \quad (74)$$

bits per channel use for the qudit erasure channel with $p < 1/2$. As already discussed in III this procedure allows in principle a finite communication rate even in the limit $\tau \to \infty$.

A comparison of the asymptotic rates of these weak locking protocols with other capacities of the erasure channel is shown in Fig. 1.

B. Secret key generation in a strong locking scenario

In this section we describe a protocol for secret key generation through a generic qudit memoryless channel. Such a protocol is secure in the strong locking sense and is obtained by direct application of the QDL protocol for the strong locking of the noiseless channel discussed in Section III.

Upon $n$ uses of the qudit channel Alice prepares input states of the form $|\Psi_{mk}\rangle = \otimes_{j=1}^{n} U_{jk}^j |m^j\rangle$, encoding the message variable $m$. As detailed in Section III the local qudit unitaries $U_{jk}^j$ are chosen i.i.d. from the phase ensemble of qudit unitaries [Eq. (7)], and the label $k$ is determined by the value of the secret key.

According to the discussion of Section III if Eve measures the input of the channel she will get an accessible information smaller than $\epsilon \log d^n$ with an asymptotic secret key consumption rate of 1 bit per
channel use. On the other hand, to extract secret key from the raw data Alice has to send error correcting information to Bob. Since this transmission will take place on a public communication channel, the protocol will remain secure if Alice knows an upper bound $\tau$ on the coherence time of Eve’s quantum memory. If so, Alice must wait for a time larger that $\tau$ before being able to safely send error correcting information to Bob via the public channel. After such a time Eve has either made a measurement or her quantum memory has completely decohered. We remark that this setting corresponds to the one detailed in Section 4.1 of Ref. [23], where Eve is unable to eavesdrop 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. In this way Alice and Bob can establish a secret key (secure in the strong locking sense) at a rate equal to the Holevo information of the phase ensemble $\chi(E)$ [see Eq. (57)]. Applying the general key recycling strategy outlined in Section II, the final asymptotic rate of secret (in the strong locking sense) key generation is of

$$S_{s,1} = \chi(E) - 1$$  \hspace{1cm} (75)

bits per channel use.

For a unitarily covariant channel $N$, that is, satisfying $N(U\rho U^\dagger) = UN(\rho)U^\dagger$, the Holevo information $\chi(E)$ may be equal to the classical capacity $C$. For example, this is the case of the qudit erasure channel and the qudit depolarizing channel:

$$N(\rho) = (1 - p)\rho + p\frac{I}{d}. \hspace{1cm} (76)$$

For these channels our protocol achieves a secret key generation rate of $S_{s,1} = C - 1$, just one bit below the channel classical capacity.

Figure 2 shows a comparison of the strong locking rate for secret key generation with the classical capacity and a secret key generation rate (secure according to the Holevo information criterion) achieved by the protocol in [24] (we notice incidentally that this rate achieves the Hashing bound).

V. CONCLUSION

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. In this paper we have shown that this gap may persist when information is transmitted through a noisy environment, as formalized by the notions of weak and strong locking capacities of a quantum channel. In particular, for channels with enough symmetry, the locking capacity can be as large as the classical capacity minus one bit. To show that we have employed a new QDL protocol that makes use of separable input states over $n$ uses of a memoryless qudit channel.
This represents a novelty with respect to previously know QDL protocols that are based on codewords that are entangled in a large-dimension Hilbert space (in principle those previous protocols required to take the limit of $d \to \infty$).

We have explicitly considered the case of the memoryless erasure channel in $d$-dimension. For erasure probability $p < 1/2$ the channel has non-zero private capacity. One can then exploit this feature to established a certain amount of secret key between the legitimate parties, and then use this key to lock the future uses of the channel. Alternatively, if Alice and Bob know an upper bound on the coherence time of Eve’s quantum memory, they can apply a bootstrap technique to recycle part of the locked message to be used as a fresh secret key. While the calculation for the erasure channel is straightforward, the extension to general communication channels, though natural, remains an open problem.

We have also described a protocol for secret key generation (secret in the strong locking sense) for a generic qudit channel, under the assumption that Alice and Bob know an upper bound $\tau$ on Eve’s quantum memory coherence time. The timing assumption is indeed crucial for QDL, as confirmed by the fact that it allows Alice and Bob to generate secret key at an asymptotic rate only one bit below the channel capacity. Interestingly enough, the key generation rate is independent on the value of $\tau$, as long as Alice and Bob know such a value.

In view of cryptographic applications, one should also consider if 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 discussed in [4], where it was 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 [4] may be straightforwardly generalized to the protocol discussed in the present paper, and hence applied to guarantee the robustness of our QDL protocols for noisy channels.

The QDL states and unitaries in Eqs. (6)-(7) are particularly suitable for quantum optics applications, where a qudit can be encoded by coherently split a single photon over $d$ modes (e.g., path, temporal, linear momentum, orbital angular momentum) and then i.i.d. random phases can be applied to the modes by modulating an array of phase-shifters. For example, this kind of transformation can be realized by group velocity dispersion [25]. As discussed in [14] this requires passive linear optical transformations and photodetection. In the unary encoding of a single photon over $d$ modes, linear losses are modeled as a qudit erasure channel and the depolarizing channel model provides a standard benchmark for 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 QDL (in the strong sense) does not depend on the details of the channel and holds also in the case of coherent attacks. Finally, let us remark that differently to previous QDL protocols the one presented here does not require $d$ to be arbitrarily large. In our case, one requires an increasing number of channel uses (as typical of i.i.d. information theory) while it is sufficient to assume $d \geq 3$.

Appendix A: Second moment of $q_{mk}(\Phi)$

Let us put

$$g_{\omega \omega' \omega'' \omega'''} = \prod_{j=1}^{n} \frac{\delta_{\omega_j \omega_j'} \delta_{\omega_j'' \omega_j'''} + \delta_{\omega_j \omega_j'''} \delta_{\omega_j' \omega_j''}}{1 + \delta_{\omega_j \omega_j''}}. \quad (A1)$$

Notice $g_{\omega \omega' \omega'' \omega'''}$ takes values in $\{0, 1\}$ and that the number of times it is equal to 1 is $(2d^2 - d)^n$. Then we have (summation over repeated indexes is assumed)

$$f(\Phi) = d^{2n} \mathbb{E}[q_{mk}(\Phi)^2] = g_{\omega \omega' \omega'' \omega'''} \Phi_* \Phi \Phi_* \Phi \Phi_* \Phi \Phi'''. \quad (A2)$$

Let us define the $d^{2n} \times d^{2n}$ matrix $G$ with entries:

$$G^{(n)}_{\omega \omega'', \omega' \omega'''} := g_{\omega \omega' \omega'' \omega'''} , \quad (A3)$$

where $\omega$ and $\omega'$ are respectively row and column indexes. Then we have

$$f(\Phi) \leq \|G^{(n)}\|_{\infty} , \quad (A4)$$
where $\|G^{(n)}\|_\infty$ denotes the maximum eigenvalue of the matrix $G^{(n)}$. We then notice that $G^{(n)} = G^\otimes n$, where $G$ is the $d^2 \times d^2$ matrix with entries (no summation over repeated indexes)

$$G_{\omega'\omega''\omega'} = \frac{\delta_{\omega'\omega'}\delta_{\omega''\omega''} + \delta_{\omega''\omega''}\delta_{\omega'\omega'}}{1 + \delta_{\omega''\omega''}} = \delta_{\omega'\omega'}\delta_{\omega''\omega''} + \delta_{\omega''\omega''}\delta_{\omega'\omega'} - \delta_{\omega'\omega'}\delta_{\omega''\omega''}\delta_{\omega'\omega''}.$$

(A5)

We have

$$G = I + S - P \leq I + S - P\,,$$

(A6)

where $I$ is the $d^2 \times d^2$ identity matrix, $S$ is the swap matrix, and $P$ is the positive semidefinite matrix with entries $P_{\omega''\omega'\omega''} = \delta_{\omega'\omega'}\delta_{\omega''\omega''}\delta_{\omega'\omega''}$.

Since $I$ and $S$ are unitary (and hermitian) their eigenvalues are not greater than 1, which implies $\|G\|_\infty \leq 2$ and $\|G^{(n)}\|_\infty \leq 2^n$. In conclusion we obtain $f(\Phi) \leq 2^n$ and $E[q_{mk}(\Phi)^2] \leq 2^n/d^{2n}$.
[18] 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.

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

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

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

[22] A. S. Holevo, IEEE Trans. Inf. Theory 44, 269 (1998); B. Schumacher and W. D. Westmoreland, Phys. Rev. A 56, 131 (1997).

[23] C. H. Bennett, G. Brassard, J.-M. Robert, SIAM J. Comput. 17, 210 (1988).

[24] L. Sheridan and V. Scarani, Phys. Rev. A 82, 030301(R) (2010).

[25] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, D. Englund, Phys. Rev. A 87, 062322 (2013).