Locking classical information

F. Dupuis, J. . Florjanczyk, P. . Hayden and D. .
Leung

Locking classical information

Frédéric Dupuis[*]   Jan Florjanczyk[†]   Patrick Hayden[†‡]   Debbie Leung[§‡]

4 November 2010

Abstract

It is known that the maximum classical mutual information that can be achieved between measurements on a pair of quantum systems can drastically underestimate the quantum mutual information between those systems. In this article, we quantify this distinction between classical and quantum information by demonstrating that after removing a logarithmic-sized quantum system from one half of a pair of perfectly correlated bitstrings, even the most sensitive pair of measurements might only yield outcomes essentially independent of each other. This effect is a form of information locking but the definition we use is strictly stronger than those used previously. Moreover, we find that this property is generic, in the sense that it occurs when removing a random subsystem. As such, the effect might be relevant to statistical mechanics or black hole physics. Previous work on information locking had always assumed a uniform message. In this article, we assume only a min-entropy bound on the message and also explore the effect of entanglement. We find that classical information is strongly locked almost until it can be completely decoded. As a cryptographic application of these results, we exhibit a quantum key distribution protocol that is "secure" if the eavesdropper's information about the secret key is measured using the accessible information but in which leakage of even a logarithmic number of key bits compromises the secrecy of all the others.

Keywords: information locking, quantum information, encryption, discord, measure concentration, black holes

1 Introduction

One of the most basic and intuitive properties of most information measures is that the amount of information carried by a physical system must be bounded by its size. For example, if one receives ten physical bits, then one's information, regardless of what that information is "about", should not increase by more than ten bits. While this is true for most information measures, in quantum mechanics there exist natural ways of measuring information that violate this principle by a wide margin. In particular, this violation occurs when one defines the information contained in a quantum system as the amount of classical information that can be extracted by the best possible measurement. To construct examples of this effect, we take a classical message and encode it into a two-part quantum message: a *cyphertext*, which is roughly as large as the message, and a much smaller *key*. Given both the cyphertext and the key, the message can be perfectly retrieved. We can then look at the amount of information that can be extracted about the message by a measurement given only access to the cyphertext. Locking occurs if this amount of information is less than the amount of information in the message minus the size of the key.

In previous work on locking [DHL+04, HLSW04], this amount of information was taken to be the accessible information, the maximum (classical) mutual information between the message and the result of a

---
[*]Institute for Theoretical Physics, ETH Zurich, Switzerland

[†]School of Computer Science, McGill University, Montreal, Canada

[‡]Perimeter Institute for Theoretical Physics, Waterloo, Canada

[§]Institute for Quantum Computing, University of Waterloo, Waterloo, Canada

measurement. In [DHL$^+$04], the authors constructed the first example of locking as follows: the cypher-text consists of the uniformly random message, encoded in one of two mutually unbiased bases, and the (one-bit) key reveals the basis in which the encoding was done. In this example, given only the cypher-text, the classical mutual information is only $\frac{n}{2}$ for an n-bit message. Hence, the one-bit key can increase the classical mutual information by another $\frac{n}{2}$ bits. In [HLSW04], the authors considered a protocol in which one encodes a classical message using a fixed basis, and then applies one of k fixed unitaries (where $k = O(\text{polylog } n + \log \frac{1}{\varepsilon})$); the classical key reveals which unitary was applied. If the unitaries are chosen according to the Haar measure, then with high probability, the accessible information was shown to be at most εn when one only has the cyphertext.

In this paper, we present stronger and more general locking results, and show that this effect is generic. Our results will be stronger in the sense that instead of using the accessible information, we will define locking in terms of the trace distance between measurement results on the real state and measurement results on a state completely independent of the message (see Definition 2.4). Unlike the accessible information, this has a very natural operational interpretation: it bounds the largest probability with which we can guess, given a message m and the result x of a measurement done on a cyphertext, whether x comes from a valid cyphertext for m or from a cyphertext generated independently of m. In other words, one could almost perfectly reproduce any measurement results made on a valid cyphertext without having access to the cyphertext at all. Moreover, we recover a strengthened version the earlier statements about the accessible information. Whereas previously the accessible information was shown to be at most 3 bits, our techniques show that the accessible information can be made arbitrarily small. (A follow-up paper further strengthens the definition and explores connections to low-distortion embeddings [FHS10].)

Despite this stronger definition, we will be able to show that the locking phenomenon is generic. Instead of having a classical key reveal the basis in which the information is encoded, as in [DHL$^+$04, HLSW04], we consider the case where there is a single unitary, and the key is simply a small part of the quantum system after the unitary is applied. This means that we can make not only cryptographic statements, but also statements about the dynamics of physical systems, where the unitary represents the evolution of the system. In particular, we will be able to show that locking occurs with high probability in physical systems whose internal dynamics are sufficiently generic to be adequately modelled by a Haar-distributed unitary. This can therefore give interesting results in the context of thermodynamics, or of the black hole information problem.

In that vein, we will also allow the measuring device to share entanglement with the cyphertext-key compound system. While this may not correspond to a very meaningful cryptographic scenario, it allows us to study the behavior of entanglement in physical systems, and to study the extent to which the presence of entanglement interferes with this locking effect.

Finally, in contrast to previous studies, we will not limit the message (or the entanglement) to be uniform; the size of the key will instead depend on the min-entropy of the message. This assumption is easier to justify in cryptographic applications. Indeed, while the locking results we present here can be interpreted as demonstrating the possibility of encrypting classical messages in quantum systems using only very small keys, care must be taking when composing such encryption with other protocols. We use our results to exhibit a quantum key distribution protocol, for example, that appears to be secure if the eavesdropper's information about the secret key is measured using the accessible information, but in which leakage of a logarithmic amount of key causes the entire key to be compromised.

1.1 Transmitting information through a generic unitary

To end the introduction, we introduce the physical scenario that will occupy us throughout the article. The situation is depicted in Figure 1.

Now, let $\{|\psi_m\rangle : 1 \leqslant m \leqslant |M|\}$ be any orthonormal basis for N. The analysis will focus on the
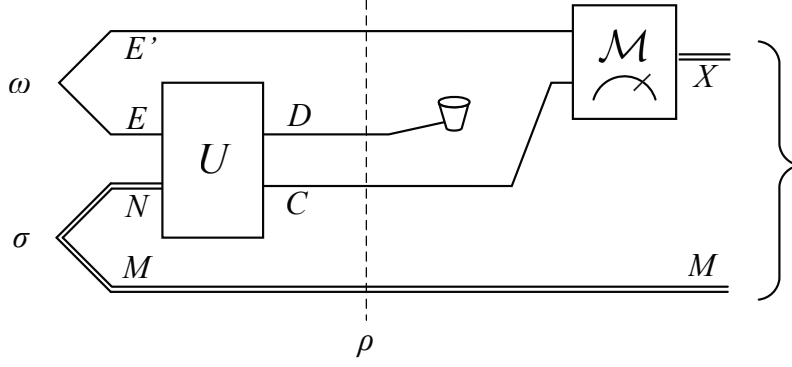
Figure 1: A quantum circuit depicting the physical scenario. The classical message M gets encoded in N, and the unitary then mixes it with the E part of the shared entanglement. If the information is locked, any joint measurement $\mathcal{M}$ on C and E' will yield a result X that is almost independent of the message. On the other hand, if C is large enough, there will be a joint measurement $\mathcal{M}$ reliably decoding M.

properties of the states

$$\sigma^{MN} \quad := \quad \sum_{m=1}^{|M|} p_m |m\rangle\langle m|^M \otimes |\psi_m\rangle\langle\psi_m|^N \quad \text{and} \tag{1.1}$$

$$\rho^{MCDE'} \quad := \quad \left(\mathbb{I}^{ME'} \otimes U^{NE\to CD}\right)\left(\sigma^{MN} \otimes \omega^{EE'}\right)\left(\mathbb{I}^{ME'} \otimes U^{NE\to CD}\right)^\dagger. \tag{1.2}$$

Our objective is to demonstrate that until C is large enough that there exists a measurement on CE' capable of revealing *all* the information about the message M, no measurement will reveal *any* information about the message. This can't quite be true, of course, so what we will demonstrate is that the jump from no information to complete information involves enlarging C by a number of qubits logarithmic in the size of the message M and the amount of entanglement E.

Assume for simplicity both that M is uniformly distributed and that the state $\omega^{EE'}$ is maximally entangled. As a first step, it is necessary to determine how large C needs to be in order for there to exist a measurement on CE' that will reveal the message M. Begin by purifying the state σ to

$$|\sigma\rangle^{RMN} = \frac{1}{\sqrt{|M|}} \sum_{m=1}^{|M|} |m\rangle^R \otimes |m\rangle^M \otimes |\psi_m\rangle^N. \tag{1.3}$$

Even more demanding than performing a measurement to reveal m is the task of transmitting the quantum information about RM through U, allowing the decoder, who has access only to CE', to recover a high fidelity copy of the state $|\sigma\rangle^{RMN}$. If U is selected according to the Haar measure, then Theorem IV.1 of [ADHW09] implies that there is a quantum operation $\mathcal{D}^{CE'\to N}$ acting only on CE' such that

$$\left\| \mathcal{D}\left(\mathrm{Tr}_D\left[U^{NE\to CD}(\sigma^{RMN} \otimes \omega^{EE'})(U^{NE\to CD})^\dagger\right]\right) - \sigma^{RMN} \right\|_1 \leq 2\sqrt{\frac{M}{C}}. \tag{1.4}$$

Because the trace distance is monotonic under quantum operations, it will not increase by taking the partial trace over R and measuring in the basis $\{|\psi_m\rangle\}$ [NC00]. If we let $p(m'|m)$ be the probability of getting an outcome $|\psi_{m'}\rangle$ when the message was in fact m, Equation (1.4) therefore implies that

$$\frac{1}{M} \sum_m \sum_{m'\neq m} p(m'|m) \leq \sqrt{\frac{M}{C}}. \tag{1.5}$$

3

In words, the probability of the measurement yielding the incorrect outcome, averaged over all messages, is at most $\sqrt{M/C}$, so as soon as C is significantly larger than M, a measurement on CE' can be found that will reveal the message. Our goal in this article will be to demonstrate that until this condition is met, no measurement will reveal any significant information about the message.

1.2   Structure of the paper

The next subsection explains the notation used throughout the paper, and we then move on to the formal definition of locking as well as other important concepts in Section 2. Section 3 will state the main results and give a high-level overview of the proof, and Section 4 will begin the proof with some key lemmas. Section 5 will deal with the proofs of our theorems in the easier case where the measurement device is restricted to making only projective measurements, and Section 6 will deal with the case of general measurements (POVMs). We then show in Section 7 that, in many regimes, as soon as the information is not locked, it is completely decodable. Implications for the security definitions of quantum cryptographic protocols will be presented in Section 8, and we conclude the paper with a discussion in Section 9.

1.3   Notation

General	
$\log$	Logarithm base 2.
$\mathbb{E}_U[f(U)]$	Expectation value of $f(U)$ over the random variable U.
AB	Composite quantum system whose associated Hilbert space is $A \otimes B$. We frequently identify quantum systems with their associated Hilbert spaces.
$\lvert A \rvert$	Dimension of Hilbert space A. However, we will often drop the $\lvert \cdot \rvert$. For example, the dimension of the composite system MCK is denoted by MCK (a scalar value).
$A^{\otimes 2}$	Two identical copies of A the second of which is denoted by $\overline{A}$.
$\lvert\psi\rangle^A, \lvert\varphi\rangle^A, \ldots$	Vectors in A.
$\psi^A, \varphi^A, \ldots$	The "unketted" versions denote their associated density matrices: $\psi^A = \lvert\psi\rangle\langle\psi\rvert$. Furthermore, if we have defined a state ψ^{AB}, then $\psi^A = \mathrm{Tr}_B[\psi^{AB}]$.
π^A	The maximally mixed state $\frac{\mathbb{I}^A}{\lvert A \rvert}$.
$\mathcal{U}(A)$	The unitary group on A.
$\mathrm{Pos}(A)$	The subset of Hermitian operators from A to A consisting of positive semidefinite matrices.
$\mathcal{L}(s, \eta)$	The set of all (s, η)-quasi-measurements, see Definition 2.3.

Operators

$\mathbb{I}^A$	Identity operator on A.
$M^{A \to B}$	Indicates that the operator M is a transformation from states on A to states on B.
$\mathcal{M}^{A \to B}$	Indicates that the superoperator $\mathcal{M}$ is a transformation from operators on A to operators on B. M and $\mathcal{M}$ will be freely identified with their extensions (via tensor product with the identity) to larger systems.
$M \cdot N$	$MNM^\dagger$
$M \leqslant N$	If $M, N \in \mathrm{Herm}(\mathsf{A})$, this means that $N - M \in \mathrm{Pos}(A)$.
$\sqrt{M}$	If $M \in \mathrm{Pos}(A)$ has spectral decomposition $M = \sum_i \lambda_i \lvert\psi_i\rangle\langle\psi_i\rvert$, then $\sqrt{M} = \sum_i \sqrt{\lambda_i}\lvert\psi_i\rangle\langle\psi_i\rvert$.
$\Pi_\pm^A$	Projector onto the symmetric $(+)$ or antisymmetric $(-)$ subspace of $A^{\otimes 2}$.
$\mathrm{op}_{A \to B}(\lvert\psi\rangle^{AB})$	Turns a vector into an operator. See Definition 4.2.

Norms and Entropies

$\lVert M^{A \to B} \rVert_1$	$\mathrm{Tr}\sqrt{M^\dagger M}$
$\lVert \lvert\psi\rangle \rVert_2$	$\sqrt{\lvert\langle\psi\lvert\psi\rangle\rvert}$
$\lVert M^{A \to B} \rVert_2$	$\sqrt{\mathrm{Tr}[M^\dagger M]}$
$\lVert M^{A \to B} \rVert_\infty$	Largest singular value of M, *i.e.* the operator norm of M.
$H_2(A)_\rho$	Renyi 2-entropy of A, defined as $-\log \mathrm{Tr}[\rho^2]$.
$H_{\min}(A)_\rho$	Quantum min-entropy of A, defined as $-\log\min_{\lambda \in \mathbb{R}}\{\lambda : \rho^A \leqslant \lambda\mathbb{I}^A\}$.
$H_{\max}(A)_\rho$	Quantum max-entropy of A, defined as $2\log\mathrm{Tr}\sqrt{\rho^A}$.
$I(A; B)_\rho$	Mutual information of A and B, defined as $H(A)_\rho + H(B)_\rho - H(AB)_\rho$.
$I_{\mathrm{acc}}(A; B)_\rho$	Accessible information, see Definition 2.2.

2 Definitions

This section will present the basic definitions needed to state our results. First, it will be very convenient for us to represent measurements via superoperators in the following manner:

Definition 2.1 (Measurement superoperator). *We call a completely positive, trace-preserving (CPTP) map* $\mathcal{M} : \mathcal{B}(A) \to \mathcal{B}(X)$ *a* measurement superoperator *if it is of the form* $\mathcal{M}(\rho) = \sum_{i=1}^N \lvert i\rangle\langle i\rvert^X \mathrm{Tr}[M_i^A \rho]$, *where* $\{\lvert i\rangle^A : i \in \{1, \ldots, N\}\}$ *is an orthonormal basis for* X, *each* M_i^A *is positive semidefinite, and* $\sum_{i=1}^N M_i^A = \mathbb{I}^A$.

These play a central role in the definition of accessible information.

Definition 2.2 (Accessible information [Fuc96]). *Let* ρ^{AB} *be a quantum state. Then, the accessible information* $I_{\mathrm{acc}}(A; B)$ *is defined as*

$$I_{\mathrm{acc}}(A; B)_\rho := \sup_{\mathcal{A}, \mathcal{B}} I(X; Y)_{(\mathcal{A} \otimes \mathcal{B})(\rho)},$$

where $\mathcal{A}^{A \to X}$ *and* $\mathcal{B}^{B \to Y}$ *are measurement superoperators, and the supremum is taken over all possible superoperators. In other words, the accessible information is the largest possible mutual information between the results of measurements made on* A *and* B.

The accessible information was originally defined only for states in which the A subsystem was classical. In that case, no measurement on A is necessary in the optimization. This quantity is also known as the classical mutual information of a quantum state [OZ01, HV01].

We also need to introduce the concept of *quasi-measurements* for our analysis. They are, as their name indicates, almost measurements, but differ in three ways: they only contain rank-one elements of equal weight, they have exactly n outcomes, and the sum of all the elements does not necessarily equal the identity, but is instead bounded by $k\mathbb{I}$:

Definition 2.3 (Quasi-measurement). *We call a superoperator $\mathcal{M}^{A \to B}$ an (s, η)-quasi-measurement if it is of the form $\mathcal{M}(\rho) = \frac{|A|}{s} \sum_{i=1}^{s} |i\rangle\langle\chi_i|\rho|\chi_i\rangle\langle i|$ where the $|i\rangle$ index an orthonormal basis for B, and $\frac{|A|}{s} \sum_{i=1}^{s} |\chi_i\rangle\langle\chi_i| \leqslant \eta\mathbb{I}^A$. We call the set of all (s, η)-quasi-measurements on a given system, $\mathcal{L}(s, \eta)$.*

The reason for introducing these, as will soon become apparent, is that they are almost equivalent to POVMs for our purposes while being much easier to handle mathematically. It can easily be seen that projective measurements are simply $(A, 1)$-quasi-measurements.

We now give the formal, strengthened definition of locking. The states in question were introduced in Section 1.1. However, because the cyphertext will always be smaller than or equal to the message when locking occurs, certain identifications become possible. In particular, we can assume without loss of generality that $N \cong C \otimes K$ and $D \cong E \otimes K$. Since the analysis will be performed using only C, K and E, we reproduce the illustration of the physical scenario with the identifications made in Figure 2.
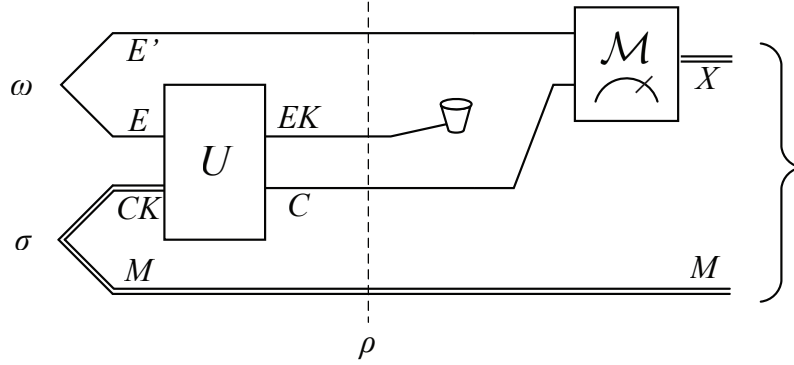
Figure 2: A quantum circuit depicting the physical scenario with the locking-specific identifications $N \cong C \otimes K$ and $D \cong E \otimes K$ made.

Definition 2.4 (ε-locking scheme). *Let M, C, K, E and E' be quantum systems. Let $\rho^{MCKEE'}$ be a quantum state of the form*

$$\rho^{MCKEE'} = \sum_{m} p_m U^{CKE} \left(|m\rangle\langle m|^M \otimes |\psi_m\rangle\langle\psi_m|^{CK} \otimes |\omega\rangle\langle\omega|^{EE'} \right) U^{CKE\dagger}, \qquad (2.1)$$

where the $|\psi_m\rangle$ are orthogonal and U^{CKE} is unitary. Then we call ρ an ε-locking scheme if for any measurement superoperator $\mathcal{M}^{CE' \to X}$, we have that

$$\left\| \mathcal{M} \left(\rho^{MCE'} \right) - \mathcal{M} \left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 \leqslant \varepsilon.$$

Note that this definition of locking is rather different from that used in previous work in the area ([DHL$^+$04, HLSW04]). Their definition involved the *accessible information* between the cyphertext and the message. We can show that our definition implies the older one:

Lemma 2.1. *Let ξ^{MB} be a cq-state such that $\left\| \mathcal{M}(\xi^{MB}) - \xi^M \otimes \mathcal{M}(\xi^B) \right\|_1 \leqslant \varepsilon$ for all measurement superoperators $\mathcal{M}^{B \to X}$. Then,*

$$I_{\mathrm{acc}}(M; B)_\xi \leqslant 4\varepsilon \log M + 2\eta(1 - \varepsilon) + 2\eta(\varepsilon),$$

where $\eta(x) := -x \log x$ and $\eta(0) = 0$.

Proof. This is a direct application of the Alicki-Fannes inequality [AF04]. □

Four quantities will be particularly useful for quantifying variations from uniform messages and maximal entanglement,

$$
\begin{align}
\Delta_{M,\infty} &:= 2^{\log M - H_{\min}(M)_\sigma}, & (2.2) \\
\Delta_{M,2} &:= 2^{\log M - H_2(M)_\sigma}, & (2.3) \\
\Delta_{E,\infty} &:= 2^{\log E - H_{\min}(E)_\omega}, & (2.4) \\
\Delta_{E,2} &:= 2^{\log E - H_2(E)_\omega}. & (2.5)
\end{align}
$$

For a point mass distribution p_m, $\Delta_{M,\infty} = \Delta_{M,2} = |M|$ and for the uniform distribution $\Delta_{M,\infty} = \Delta_{M,2} = 1$. To give an interpretation of the Δ_E quantities, we can note that for a bipartite $|\omega\rangle^{EE'}$ with no entanglement, $\Delta_{E,\infty} = \Delta_{E,2} = |E|$. However, if $|\omega\rangle^{EE'}$ is the maximally entangled state, then $\Delta_{E,\infty} = \Delta_{E,2} = 1$, which we call maximal entanglement. The case of a uniformly distributed message and maximal entanglement will give the simplest expressions for minimum key size. The Δ terms are used in the calculations to provide more general statements relating the entropy of the message and entanglement to the key size.

3   Main results and proof sketch

The locking scheme we study is a scheme where the unitary in Definition 2.4 is chosen according to the Haar measure. Let c, e and n be the logarithms of $|C|, |E|$, and $|M| = |N|$ respectively. In particular, the message is n bits long. Define $K = M/C$ and $k = \log K$. Then $k = n - c$ is the difference in size between the message and cyphertext, that is, the size of the key. Our main theorem is the following:

Theorem 3.1. *If U is chosen according to the Haar measure, then the scheme described in Definition 2.4 is an ε-locking scheme with probability at least $1 - 2^{-9(|C||E|)^2}$ if*

$$k > \frac{1}{2}\Big(n - H_{\min}(M)_\sigma\Big) + \frac{1}{2}\Big(e - H_{\min}(E)_\omega\Big) + \log(c + e) + 2\log(1/\varepsilon) + 11$$

as long as $\varepsilon > 16\Delta_{E,\infty}/\sqrt{|KE|}$.

For the cryptographically relevant case in which there is no entanglement shared with the measuring device, we therefore get:

Corollary 3.2. *If U is chosen according to the Haar measure, then the scheme described in Definition 2.4 without shared entanglement is an ε-locking scheme with probability at least $1 - 2^{-9|C|^2}$ if*

$$k > \frac{1}{2}\Big(n - H_{\min}(M)_\sigma\Big) + \log c + 2\log(1/\varepsilon) + 11$$

as long as $\varepsilon > 16/\sqrt{|K|}$.

Hence, the size of the key must be at least as large as half the "min-entropy deficit" $(n - H_{\min}(M)_\sigma)$ of the message plus a term of the order of the logarithm of the size of the message. In particular, for a uniform message, the min-entropy deficit is zero, and a key of size at least $\log c + 2\log(1/\varepsilon) + 11$ is sufficient for locking.

Conversely, we can show that in certain regimes, if the information is not locked, then it is completely decodable, with almost no middle ground. More precisely, we have the following:

Theorem 3.3. *If U is chosen according to the Haar measure, then the information in the scheme described in Figure 1 without shared entanglement is asymptotically almost surely decodable to within ε in trace distance for a receiver with only C as long as*

$$k \leqslant \frac{1}{2}\Big(n - H_{\max}(M)_\sigma\Big) - \frac{1}{2}\Big(e - H_2(E)_\omega\Big) - 2\log(1/\varepsilon) - 4.$$

Note that decoding the message will often require that the cyphertext be longer than the message, in which case k will be negative. Comparing Theorems 3.1 and 3.3 reveals that the difference between being ε-locked and being able to decode quantum information to within ε is determined by at most

$$\frac{1}{2}\left[H_{\max}(M)_\sigma - H_{\min}(M)_\sigma\right] + \left[e - H_{\min}(E)_\omega\right] + \log(c + e) + 4\log(1/\varepsilon) + 15$$

qubits, where the inequality $H_2 \geq H_{\min}$ has been used to simplify the expression.

In other words, if we consider the case of maximal entanglement, then the gap between locking and decodability can only be as wide as the difference between the min- and max-entropy of the message modulo logarithmic terms. One should note that this gap is real, and not only an artifact of our proof technique. To see this, consider an n-bit message distributed such that with probability $\frac{1}{2}$, the first bit is uniform and the rest of the string is always zero, and with probability $\frac{1}{2}$ the whole string is uniform. The max-entropy of such a message is n, but the min-entropy is tiny. Now, to be able to decode, one must be able to decode the entire string in the "worst-case" scenario where the whole string is uniform, so the max-entropy is relevant in this case. But in the locking case, we must be able to lock in the worst-case scenario of only one bit being random, so the min-entropy is the relevant quantity here.

The effect of non-maximal entanglement is not entirely clear, however. There is a fairly large gap between our locking and decodability results here, but the locking side is almost certainly not tight in general. For instance, we can easily set up the system in such a way that there is a part of E' that is clearly useless, but our proof technique forces us to take this part into account, which artificially hurts our bound. This extreme case can be ruled out by restricting E' to the support of $\omega^{E'}$, but it seems likely that more gains could be found in the general case.

Finally, in addition to studying locking for its own sake, we use our results to exhibit a quantum key distribution protocol that appears to be secure if the eavesdropper's information about the secret key is measured using the accessible information, but in which leakage of a logarithmic amount of key causes the entire key to be compromised. This is done in Section 8.

3.1 Proof sketch

We will give here a very high-level overview of the proof. The basic idea is to start from the fact that, given a fixed measurement superoperator, the probability over the choice of unitaries that this measurement yields non-negligible correlations is extremely small. Then, we would like to discretize the space of all measurement superoperators and use the union bound to show that the probability that *any* measurement superoperator yields non-negligible correlations is still very small. For this to work, the "number" of measurements has to be much smaller than the reciprocal of the probability of getting a bad U. However, the set of measurement superoperators cannot be discretized directly, since (among other things) they contain a potentially unbounded number of outputs. Hence, we will instead use the above argument on

(s, η)-quasi-measurements, which *can* be discretized easily (see Lemma 4.4), and then show that the best measurement cannot beat the best (s, η)-quasi-measurement by too much. Along the way, we also prove the special case where the measurement device is constrained to making projective measurements, which can be viewed simply as $(CE', 1)$-quasi-measurements.

The basic ingredient of the proof is the following concentration of measure theorem on Haar-distributed unitaries:

Theorem 3.4 (Corollary 4.4.28 in [AGZ09])**.** *Let* $f : \mathcal{U}(d) \to \mathbb{R}$ *be a function with Lipschitz constant* θ *(see Definition A.1; the Lipschitz constant is taken with respect to the Hilbert-Schmidt distance on unitaries). Then,*

$$\Pr_U \{|f(U) - \mathbb{E}_U f| > \varepsilon\} \leqslant \exp\left(-\frac{d\varepsilon^2}{4\theta^2}\right).$$

We apply the theorem to the function

$$g_{\mathcal{M}}(U) = \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right) \right\|_1$$

for any fixed (s, η)-quasi-measurement $\mathcal{M}$, where ρ depends on U as in Equation (2.1). To do this, we need to bound two quantities from above: the expected value $\mathbb{E}g_{\mathcal{M}}(U)$ and the Lipschitz constant θ. The bounds appear in Lemmas 4.1 and 4.2 respectively, and the resulting concentration statement looks like (see Equation (4.22)):

$$\Pr_U \{g_{\mathcal{M}}(U) > \varepsilon\} \leqslant \exp\left(-\frac{2^{H_{\min}(M)+H_{\min}(E)}CKE}{2^6\eta^2}\left(\varepsilon - \frac{2\Delta_{E,\infty}}{\sqrt{KE}}\right)^2\right).$$

Now we are in a position to use our ε-net over (s, η)-quasi-measurements (Lemma 4.4) and the union bound to get a bound on the probability that there exists an (s, η)-quasi-measurement $\mathcal{M}$ for which $g_{\mathcal{M}}(U) > \varepsilon$; this is done in Theorem 4.5.

At this point, the proof splits into an "easy" and a "hard" branch. The easy branch (Section 5) applies Theorem 4.5 to projective measurements. The result is immediate, since a projective measurement is simply a $(CE', 1)$-quasi-measurement. The hard branch (Section 6) goes for the full prize: showing that $g_{\mathcal{M}}(U)$ is small for every POVM with high probability. For this, we essentially show that a POVM corresponds (for the purposes of this proof) to a distribution over sequences of s states. The operator Chernoff bound can then be used to show that this distribution is almost entirely supported on sequences that are (s, η)-quasi-measurements, for $s = O(CE\log(CE))$ and $\eta = O(1)$. We then apply Theorem 4.5 on these sequences, conditioned on the sequence being an (s, η)-quasi-measurement. A trivial bound is sufficient to cover the other case.

All that is then left to do to get the statements in the theorems stated above is to calculate conditions on the various parameters to make the exponent a reasonably large negative number.

4 Concentration of the distinguishability from independence

To be able to use the general concentration of measure theorem (Theorem 3.4) on $g_{\mathcal{M}}(U)$, we must first be able to upper-bound the expectation of $g_{\mathcal{M}}(U)$ with respect to U. The following lemma does this:

Lemma 4.1 (Distinguishability for a fixed measurement)**.** *If* $\mathcal{M}^{CE' \to X}$ *is an* (s, η)*-quasi-measurement, then*

$$\mathbb{E}_U \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right) \right\|_1 \leqslant \frac{2\Delta_{E,\infty}}{\sqrt{KE}}.$$

Proof. We begin by expanding and simplifying the original expression

$$\mathop{\mathbb{E}}_{U} \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^{M} \otimes \rho^{CE'}\right) \right\|_1 = \mathop{\mathbb{E}}_{U} \left\| \mathcal{M}\left(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'}\right) \right\|_1 \tag{4.1}$$

$$\leqslant \mathop{\mathbb{E}}_{U} \sqrt{s\mathrm{Tr}\left[\left((\sigma^{M})^{-1/4}\,\mathcal{M}\left(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'}\right)\,(\sigma^{M})^{-1/4}\right)^2\right]}$$

$$\leqslant \sqrt{s\mathop{\mathbb{E}}_{U}\mathrm{Tr}\left[\left((\sigma^{M})^{-1/4}\,\mathcal{M}\left(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'}\right)\,(\sigma^{M})^{-1/4}\right)^2\right]}. \tag{4.2}$$

In the manipulations above we have used the linearity of the superoperator $\mathcal{M}$ in the first line. In the second line we have used Lemma A.4 with $\gamma = \mathbb{I}^{X} \otimes \sigma^{M}$, noting that $|X| = s$. The third line follows from the concavity of the square root. We will now use a helpful identity for the trace of an operator squared: $\mathrm{Tr}Z^2 = \mathrm{Tr}(Z \otimes Z)F$, where F is defined as follows.

Definition 4.1. *The* swap operator *on $A^{\otimes 2}$, which is written as $A \otimes \overline{A}$, is the unique linear operator F^{A} satisfying*

$$F^{A}\left(|\psi\rangle^{A}|\phi\rangle^{\overline{A}}\right) = |\phi\rangle^{A}|\psi\rangle^{\overline{A}} \qquad \forall|\psi\rangle, |\phi\rangle.$$

Expressing Equation (4.2) using the swap operator gives

$$\mathop{\mathbb{E}}_{U} \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^{M} \otimes \rho^{CE'}\right) \right\|_1 \tag{4.3}$$

$$\leqslant \sqrt{s\mathrm{Tr}\left[\mathop{\mathbb{E}}_{U}\left((\sigma^{M})^{-1/4}\,\mathcal{M}\left(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'}\right)\,(\sigma^{M})^{-1/4}\right)^{\otimes 2} F^{XM}\right]}$$

$$= \sqrt{\frac{(CE')^2}{s}\sum_{i=1}^{s}\mathrm{Tr}\left[\left(F^{M} \otimes \left(\chi_i^{CE'}\right)^{\otimes 2}\right)\mathop{\mathbb{E}}_{U}\left[(\sigma^{M})^{-1/4}(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'})(\sigma^{M})^{-1/4}\right]^{\otimes 2}\right]} \tag{4.4}$$

Equation (4.4) follows from the fact that results of the measurement $\mathcal{M}$ are stored in an orthonormal basis of system X. We will proceed by evaluating $\mathop{\mathbb{E}}_{U}((\sigma^{M})^{-1/4}\left(\rho^{MCE'} - \rho^{M} \otimes \rho^{CE'}\right)(\sigma^{M})^{-1/4})^{\otimes 2}$, but before continuing we absorb the two $\sigma^{-1/4}$ into the operator ρ. That is we define,

$$\tilde{\sigma}^{MCK} \;:=\; \sum_{m=1}^{|M|}\sqrt{p_m}|m\rangle\langle m|^{M} \otimes |\psi_m\rangle\langle\psi_m|^{CK} \quad \text{and} \tag{4.5}$$

$$\tilde{\rho}^{MCKEE'} \;:=\; (\sigma^{M})^{-1/4}\,\rho^{MCKEE'}\,(\sigma^{M})^{-1/4} = \left(\mathbb{I}^{ME} \otimes U^{CKE}\right) \cdot \left(\tilde{\sigma}^{MCK} \otimes \omega^{EE'}\right). \tag{4.6}$$

With these two definitions in hand we can expand $\mathop{\mathbb{E}}_{U}\left(\tilde{\rho}^{MCE'} - \tilde{\rho}^{M} \otimes \rho^{CE'}\right)^{\otimes 2}$ as

$$\mathop{\mathbb{E}}_{U}\left(\tilde{\rho}^{MCE'} - \tilde{\rho}^{M} \otimes \rho^{CE'}\right)^{\otimes 2} \tag{4.7}$$

$$= \mathop{\mathbb{E}}_{U}\left(\mathrm{Tr}_{KE}\left[U^{CKE} \cdot \left(\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^{M} \otimes \sigma^{CK}\right) \otimes \omega^{EE'}\right)\right]\right)^{\otimes 2}$$

$$= \mathrm{Tr}_{KE\overline{KE}}\left[\mathop{\mathbb{E}}_{U}\left(U^{CKE} \cdot \left(\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^{M} \otimes \sigma^{CK}\right) \otimes \omega^{EE'}\right)\right)^{\otimes 2}\right]$$

$$= \mathrm{Tr}_{KE\overline{KE}}\left[\int\left(U^{CKE} \otimes U^{\overline{CKE}} \otimes \mathbb{I}^{ME'\overline{ME'}}\right) \cdot \left(\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^{M} \otimes \sigma^{CK}\right) \otimes \omega^{EE'}\right)^{\otimes 2}\mathrm{d}U\right] \tag{4.8}$$

To evaluate the integral with Lemma A.1, we will need to calculate the projections of our operator onto the symmetric and antisymmetric subspaces of $(CKE)^{\otimes 2}$. Since the projectors onto the symmetric and

antisymmetric subspaces can be written as $\Pi_\pm = \frac{1}{2}(\mathbb{I} \pm F)$, we can arrive at same results by working with $\mathbb{I}$ and F. We begin with $\mathbb{I}$:

$$\text{Tr}_{CKE\overline{CKE}}\left[\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^M \otimes \sigma^{CK}\right)^{\otimes 2} \otimes \left(\omega^{EE'}\right)^{\otimes 2}\mathbb{I}^{CKE\overline{CKE}}\right] \tag{4.9}$$

$$= \sum_m \sqrt{p_m}|m\rangle\langle m|^M \otimes \sum_{m'}\sqrt{p_{m'}}|m'\rangle\langle m'|^{\overline{M}}\text{Tr}_{CK}\left[\psi_m - \sum_{m''}p_{m''}\psi_{m''}\right]^2 \otimes \left(\omega^{E'}\right)^{\otimes 2}$$

$$= (1-1)^2 \cdot (\tilde{\sigma}^M \otimes \omega^{E'})^{\otimes 2} = 0.$$

The projection onto F requires a more subtle calculation,

$$\text{Tr}_{CKE\overline{CKE}}\left[\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^M \otimes \sigma^{CK}\right)^{\otimes 2} \otimes \left(\omega^{EE'}\right)^{\otimes 2} F^{CKE}\right] \tag{4.10}$$

$$= \sum_m \sqrt{p_m}|m\rangle\langle m|^M \otimes \sum_{m'}\sqrt{p_{m'}}|m'\rangle\langle m'|^{\overline{M}}$$

$$\cdot\text{Tr}_{CK}\left[\left(\psi_m - \sum_{m''}p_{m''}\psi_{m''}\right)\left(\psi_{m'} - \sum_{m'''}p_{m'''}\psi_{m'''}\right)\right] \otimes \text{Tr}_{E\overline{E}}\left[\left(\omega^{EE'}\right)^{\otimes 2}F^E\right].$$

By taking a closer look at Equation (4.10) we can make the simplification

$$\text{Tr}_{CK}\left[\left(\psi_m - \sum_{m''}p_{m''}\psi_{m''}\right)\left(\psi_{m'} - \sum_{m'''}p_{m'''}\psi_{m'''}\right)\right]$$

$$= \text{Tr}_{CK}\left[\psi_m\psi_{m'} - \sum_{m''}p_{m''}\psi_{m''}\psi_{m'} - \sum_{m'''}p_{m'''}\psi_m\psi_{m'''} + \sum_{m'',m'''}p_{m''}p_{m'''}\psi_{m''}\psi_{m'''}\right]$$

$$= \delta_{mm'} - p_{m'} - p_m + \sum_{m''}p_{m''}^2. \tag{4.11}$$

Now we define $\tilde{\sigma}_\circ^{M\overline{M}}$ as the quantity evaluated in Equation (4.10). Substituting the result of Equation (4.11) gives

$$\tilde{\sigma}_\circ^{M\overline{M}} := \text{Tr}_{CK\overline{CK}}\left[\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^M \otimes \sigma^{CK}\right)^{\otimes 2} F^{CK}\right]$$

$$= \left(\sum_m p_m \left(|m\rangle\langle m|\right)^{\otimes 2} - \tilde{\sigma}^M \otimes (\tilde{\sigma}^{\overline{M}})^3 - (\tilde{\sigma}^M)^3 \otimes \tilde{\sigma}^{\overline{M}} + \left(\sum_m p_m^2\right)\tilde{\sigma}^M \otimes \tilde{\sigma}^{\overline{M}}\right).$$

We also define $\Omega^{E'\overline{E'}}$ as the operator acting on system $E'\overline{E'}$ in Equation (4.10), or $\Omega^{E'\overline{E'}} = \text{Tr}_{E\overline{E}}[(\omega^{EE'})^{\otimes 2}F^E]$. At this point, Lemma A.1 can be used to evaluate the integral in Equation (4.8). We can make significant simplifications by first expanding the $\alpha_\pm$ and then using our result from Equation (4.9) to show that

$$\alpha_\pm = \frac{1}{\text{rank}(\Pi_\pm^{CKE})}\text{Tr}_{CKE\overline{CKE}}\left[\left(\tilde{\sigma}^{MCK} - \tilde{\sigma}^M \otimes \sigma^{CK}\right)^{\otimes 2} \otimes \left(\omega^{EE'}\right)^{\otimes 2}\left(\Pi_\pm^{CKE} \otimes \mathbb{I}^{ME'}\right)\right]$$

$$= \frac{\pm\left(\tilde{\sigma}_\circ^{M\overline{M}} \otimes \Omega^{E'\overline{E'}}\right)}{CKE(CKE \pm 1)},$$

where the terms $\Pi_\pm^{CKE}$ are the projectors onto the symmetric and antisymmetric subspaces of $(CKE)^{\otimes 2}$, that is $\frac{1}{2}(\mathbb{I}^{CKE\overline{CKE}} \pm F^{CKE})$. In particular, because α_+ is proportional to α_-, the integral will have the product form

$$\tilde{\sigma}_\circ^{M\overline{M}} \otimes \Omega^{E'\overline{E'}} \otimes \left(\frac{\Pi_+^{CKE}}{CKE(CKE+1)} - \frac{\Pi_-^{CKE}}{CKE(CKE-1)}\right),$$

11

so the calculation of the trace in Equation (4.4) will factor into a product over the systems $(M)^{\otimes 2}$ and $(CKEE')^{\otimes 2}$. Thus,

$$\text{Tr}_{(MKE)^{\otimes 2}} \left[\left(\text{Tr}_{(CE')^{\otimes 2}} \left[\left(\chi_i^{CE'} \right)^{\otimes 2} \underset{U}{\mathbb{E}} \left(\tilde{\rho}^{MCE'} - \tilde{\rho}^M \otimes \rho^{CE'} \right)^{\otimes 2} \right] \right) F^M \right] \tag{4.12}$$

$$= \text{Tr} \left[\tilde{\sigma}_\circ^{M\overline{M}} F^M \right] \cdot \text{Tr} \left[\left(\chi_i^{CE'} \otimes \mathbb{I}^{KE} \right)^{\otimes 2} \left(\frac{\Pi_+^{CKE} \otimes \Omega^{E'\overline{E'}}}{CKE(CKE+1)} - \frac{\Pi_-^{CKE} \otimes \Omega^{E'\overline{E'}}}{CKE(CKE-1)} \right) \right].$$

The first first factor in Equation (4.12) can easily be bounded:

$$\text{Tr}_{M\overline{M}} \left[\tilde{\sigma}_\circ^{M\overline{M}} F^M \right] = \sum_m p_m - \sum_m p_m^{3/2} - \sum_m p_m^{3/2} + \sum_m p_m^2$$

$$\leqslant 2 \sum_m p_m = 2.$$

To estimate the second factor in Equation (4.12) we will need to observe two facts. First, that

$$\text{Tr} \left[(\chi_i^{CE'} \otimes \mathbb{I}^{KE})^{\otimes 2} \, \mathbb{I}^{CKE\overline{CKE}} \otimes \Omega^{E'\overline{E'}} \right] \leqslant (KE)^2 \left\| \Omega^{E'\overline{E'}} \right\|_\infty, \tag{4.13}$$

which follows from the fact that $\chi_i^{CE'}$ is a rank 1 projector. Second, that

$$\text{Tr} \left[(\chi_i^{CE'} \otimes \mathbb{I}^{KE})^{\otimes 2} \, F^{CKE} \otimes \Omega^{E'\overline{E'}} \right] = KE \, \text{Tr}_{E'\overline{E'}} \left[\left(\text{Tr}_{C\overline{C}} \left[(\chi_i^{CE'})^{\otimes 2} F^C \right] \right) \Omega^{E'\overline{E'}} \right]$$

$$\leqslant KE \left\| \Omega^{E'\overline{E'}} \right\|_\infty. \tag{4.14}$$

If we use Equations (4.13) and (4.14) to estimate the second factor of Equation (4.12) we get the bound

$$\text{Tr} \left[\left(\chi_i^{CE'} \otimes \mathbb{I}^{KE} \right)^{\otimes 2} \left(\frac{\Pi_+^{CKE} \otimes \Omega^{E'\overline{E'}}}{CKE(CKE+1)} - \frac{\Pi_-^{CKE} \otimes \Omega^{E'\overline{E'}}}{CKE(CKE-1)} \right) \right]$$

$$\leqslant \left(\frac{(KE)^2 + KE}{2CKE(CKE+1)} - \frac{(KE)^2 - KE}{2CKE(CKE-1)} \right) \cdot \left\| \Omega^{E'\overline{E'}} \right\|_\infty$$

$$\leqslant \frac{2}{C^2 KE} \cdot \left\| \Omega^{E'\overline{E'}} \right\|_\infty. \tag{4.15}$$

This can be rewritten in a more familiar form using

$$\left\| \Omega^{E'\overline{E'}} \right\|_\infty = \left\| \text{Tr}_{E'\overline{E'}} \left[\left(\omega^{EE'} \right)^{\otimes 2} F^E \right] \right\|_\infty$$

$$= \left\| \left(\omega^E \right)^{\otimes 2} F^E \right\|_\infty = \left\| \omega^E \right\|_\infty^2 = 2^{-2H_{\min}(E)_\omega}.$$

In the above, the third equality follows from the fact that the operator norm is right-invariant under unitary transformations and F is a unitary matrix. Combining the results in Equations (4.13) and (4.15), as well as the above identity, we obtain an upper bound for the trace distance through Equation (4.4),

$$\underset{U}{\mathbb{E}} \left\| \mathcal{M} \left(\rho^{MCE'} \right) - \mathcal{M} \left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 \leqslant \sqrt{ s \left(\frac{CE'}{s} \right)^2 \sum_{i=1}^s 2 \frac{2 \cdot 2^{-2H_{\min}(E)_\omega}}{(C)^2 KE} }$$

$$\leqslant \frac{2\Delta_{E,\infty}}{\sqrt{KE}}.$$

$\square$

Lemma 4.2. $g_{\mathcal{M}}(U)$, *the trace distance to independence for a fixed* (s, η)-*quasi-measurement, is Lipschitz continuous on the space* $(\mathcal{U}(CKE), \|\cdot\|_2)$ *with constant* $4\eta\sqrt{\Delta_{M,\infty} \, \Delta_{E,\infty}/ME}$.

Proof. We wish to analyze the behaviour of the trace distance with respect to the unitary matrix defining the channel. Recall the definition of function $g_{\mathcal{M}}(U)$,

$$g_{\mathcal{M}}(U) = \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right)\right\|_1.$$

If we denote by ρ_U and ρ_V the states $\mathrm{Tr}_K\left[U \cdot \sigma\right]$ and $\mathrm{Tr}_K\left[V \cdot \sigma\right]$ respectively, we can bound the deviation of $g_{\mathcal{M}}$ using the triangle inequality by

$$
\begin{aligned}
\left|g_{\mathcal{M}}(U) - g_{\mathcal{M}}(V)\right| &\leqslant \left\| \mathcal{M}\left(\rho_U^{MCE'}\right) - \mathcal{M}\left(\rho_V^{MCE'}\right)\right\|_1 \\
&\qquad + \left\| \mathcal{M}\left(\rho_U^M \otimes \rho_U^{CE'}\right) - \mathcal{M}\left(\rho_V^M \otimes \rho_V^{CE'}\right)\right\|_1 \\
&= \left\| \mathcal{M}\left(\rho_U^{MCE'} - \rho_V^{MCE'}\right)\right\|_1 + \left\| \mathcal{M}\left(\sigma^M \otimes \left(\rho_U^{CE'} - \rho_V^{CE'}\right)\right)\right\|_1,
\end{aligned}
\tag{4.16}
$$

where the second line follows from the linearity of the superoperator. We note that for any hermitian operator ζ,

$$
\begin{aligned}
\left\| \mathcal{M}\left(\zeta\right)\right\|_1 &= \left\| \frac{CE'}{s} \sum_{i=1}^{s} |i\rangle\langle\chi_i|\zeta|\chi_i\rangle\langle i| \right\|_1 \\
&= \frac{CE'}{s} \sum_{i=1}^{s} |\langle\chi_i|\zeta|\chi_i\rangle| \leqslant \frac{CE'}{s} \sum_{i=1}^{s} \langle\chi_i||\zeta||\chi_i\rangle \\
&= \frac{CE'}{s} \sum_{i=1}^{s} \mathrm{Tr}\left[\chi_i|\zeta|\right] \leqslant \eta\left\|\zeta\right\|_1,
\end{aligned}
$$

where the last inequality follows from the definition of (s, η)-quasi-measurements. Applying this new fact, our bound in Equation (4.16) becomes,

$$
\begin{aligned}
\left|g_{\mathcal{M}}(U) - g_{\mathcal{M}}(V)\right| &\leqslant \eta\left\| \rho_U^{MCE'} - \rho_V^{MCE'}\right\|_1 + \eta\left\| \sigma^M \otimes \left(\rho_U^{CE'} - \rho_V^{CE'}\right)\right\|_1 \\
&\leqslant 2\eta\left\| \rho_U^{MCKEE'} - \rho_V^{MCKEE'}\right\|_1 \\
&= 2\eta\left\| (U - V)\cdot\sigma\otimes\omega\right\|_1,
\end{aligned}
\tag{4.17}
$$

where the second line follows from monotonicity. We introduce a purification of σ^{MCK} in a new but temporary system N such that $\dim(N) = \dim(M)$. We also recall that ω is pure. This permits us to use Lemma A.3 and arrive at the following consequence of Equation (4.17),

$$\left|g_{\mathcal{M}}(U) - g_{\mathcal{M}}(V)\right| \leqslant 4\eta\left\| \left(U^{CKE} - V^{CKE}\right) \otimes \mathbb{I}_{MNE'}|\sigma\rangle^{MNCK}|\omega\rangle^{EE'}\right\|_2. \tag{4.18}$$

We now introduce a helpful operation.

Definition 4.2 (Vector-operator correspondence). *Endow systems A and B with fixed orthonormal bases $\{|a_i\rangle^A\}_i$ and $\{|b_i\rangle^B\}_i$ respectively, and let $\mathrm{op}_{A\to B} : A \otimes B \to \mathrm{L}(A, B)$, the space of linear transformations from A to B, be defined as*

$$\mathrm{op}_{A\to B}\left(|a_i\rangle|b_j\rangle\right) = |b_j\rangle\langle a_i| \qquad \forall i, j$$

This operation depends on the choice of basis; therefore, whenever it is used, a particular choice of basis is implied. Since this choice will never matter in our calculations, we shall not explicitly define these bases.

Useful properties of the correspondence can be found in [Dup09].

13

We can think of the operator $(U^{CKE} - V^{CKE}) \otimes \mathbb{I}^{MNE'}$ as bipartite over composite systems MNE' and CKE. Since the 2-norm depends only on the Schmidt coefficients of the states, it will be invariant under the op operation defined in Definition 4.2. Our bound from Equation (4.18) then becomes,

$$
\begin{aligned}
|g_{\mathcal{M}}(U) - g_{\mathcal{M}}(V)| &\leqslant 4\eta \left\| \mathrm{op}_{MNE' \to CKE} \left((U^{CKE} - V^{CKE}) \otimes \mathbb{I}^{MNE'} |\sigma\rangle^{MNCK} |\omega\rangle^{EE'} \right) \right\|_2 \\
&= 4\eta \left\| (U - V) \, \mathrm{op}_{MNE' \to CKE} (|\sigma\rangle |\omega\rangle) \right\|_2 ,
\end{aligned}
$$

where the second line follows from the fact that $\mathrm{op}_{MNE' \to CKE}$ is linear and commutes with unitary transformations on CKE. We are left with a few easy steps to bound the Lipschitz constant.

$$
\begin{aligned}
|g_{\mathcal{M}}(U) - g_{\mathcal{M}}(V)| &\leqslant 4\eta \left\| U - V \right\|_2 \left\| \mathrm{op}_{MNE' \to CKE} (|\sigma\rangle |\omega\rangle) \right\|_\infty \\
&= 4\eta \left\| U - V \right\|_2 \sqrt{ \left\| \sigma^{CK} \otimes \omega^E \right\|_\infty } \\
&= 4\eta \left\| U - V \right\|_2 \sqrt{ \left\| \sum_m p_m |\psi_m\rangle\langle\psi_m|^{CK} \right\|_\infty \left\| \omega^E \right\|_\infty } \\
&= 4\eta \left\| U - V \right\|_2 \sqrt{ \max p_m \cdot 2^{-H_{\min}(E)_\omega} } \\
&= 4\eta \left\| U - V \right\|_2 \, 2^{-\frac{1}{2} H_{min}(M)_\sigma} 2^{-\frac{1}{2} H_{\min}(E)_\omega} \\
&= \frac{4\eta \sqrt{\Delta_{M,\infty} \, \Delta_{E,\infty}}}{\sqrt{ME}} \left\| U - V \right\|_2 .
\end{aligned}
$$

A proof of the inequality can be found, for example, in [Dup09]. The second line follows from the fact the Schmidt coefficients of $|\sigma\rangle^{MNCK}$ are the square roots of the eigenvalues of σ^{CK}. The last line follows from the definition of $\Delta_{\min}$. $\qquad \square$

In order to discretize the set of all (s, η)-quasi-measurements, we require a distance measure for the set.

Definition 4.3 (Metric on the set of (s, η)-quasi-measurements, $\mathcal{L}(s, \eta)$). *Consider $\mathcal{M}, \mathcal{N} \in \mathcal{L}(s, \eta)$ defined as*

$$
\mathcal{M}(\sigma) = \frac{|CE'|}{s} \sum_{i=1}^{s} |i\rangle\langle\chi_i|\sigma|\chi_i\rangle\langle i|, \qquad \mathcal{N}(\sigma) = \frac{|CE'|}{s} \sum_{i=1}^{s} |i\rangle\langle\nu_i|\sigma|\nu_i\rangle\langle i|.
$$

We define the distance between these two elements as

$$
d(\mathcal{M}, \mathcal{N}) := \sum_{i=1}^{s} \left\| \chi_i - \nu_i \right\|_2 .
$$

Now letting $\mathcal{M}$ vary instead of U, we define a new function $h_U(\mathcal{M})$ by

$$
h_U(\mathcal{M}) = \left\| \mathcal{M}\left(\rho^{MCE'} \right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 .
$$

Lemma 4.3. $h_U(\mathcal{M})$ *is Lipschitz continuous on the space $(\mathcal{L}(s, \eta), d)$ with constant $\frac{2\sqrt{CE'}}{s} \sqrt{\Delta_{M,2} \Delta_{E,2}}$.*

Proof. As for Lemma 4.2, we can use the triangle inequality to rewrite the variation of the trace distance

as follows,

$$
\begin{aligned}
&|h_U(\mathcal{M}) - h_U(\mathcal{N})| \\
&\leqslant \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{N}\left(\rho^{MCE'}\right) \right\|_1 + \left\| \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right) - \mathcal{N}\left(\rho^M \otimes \rho^{CE'}\right) \right\|_1 \\
&= \frac{CE'}{s} \sum_{i=1}^n \left(\left\| \mathrm{Tr}_{CE'}\left[\left(\chi_i^{CE'} - \nu_i^{CE'}\right) \rho^{MCE'} \right] \right\|_1 + \left\| \mathrm{Tr}_{CE'}\left[\left(\chi_i^{CE'} - \nu_i^{CE'}\right) \rho^M \otimes \rho^{CE'} \right] \right\|_1 \right) \\
&\leqslant \frac{CE'}{s} \sum_{i=1}^s \left\| \left(\chi_i^{CE'} - \nu_i^{CE'}\right) \rho^{MCE'} \right\|_1 + \frac{CE'}{s} \sum_{i=1}^s \left\| \left(\chi_i^{CE'} - \nu_i^{CE'}\right) \rho^M \otimes \rho^{CE'} \right\|_1 \\
&\leqslant \frac{CE'}{s} \sum_{i=1}^s \left\| \chi_i^{CE'} - \nu_i^{CE'} \right\|_2 \left\| \rho^{MCE'} \right\|_2 + \frac{CE'}{s} \sum_{i=1}^s \left\| \chi_i^{CE'} - \nu_i^{CE'} \right\|_2 \left\| \rho^M \otimes \rho^{CE'} \right\|_2, \quad (4.19)
\end{aligned}
$$

where the last line follows from the operator version of the Cauchy-Schwarz inequality (see Equation (IX.32) in [Bha96]). Consider momentarily the second factor in the first term in Equation (4.19),

$$
\begin{aligned}
\left\| \rho^{MCE'} \right\|_2 &= \left\| \mathrm{Tr}_{KE}\left[U_{CKE} \cdot \left(\sigma^{MCK} \otimes \omega^{EE'} \right) \right] \right\|_2 \\
&= \sqrt{ \mathrm{Tr}\left[\left(U_{CKE}^{\otimes 2} \cdot (\sigma^{MCK} \otimes \omega^{EE'})^{\otimes 2} \right) F^{MCE'} \right] } \\
&= \sqrt{ \mathrm{Tr}\left[\left(U_{CKE}^{\otimes 2} F^C U_{CKE}^{\dagger \otimes 2} \right) \left(\sum_m p_m^2 (|\psi_m\rangle\langle\psi_m|^{CK})^{\otimes 2} \otimes (\omega^{EE'})^{\otimes 2} \right) F^{E'} \right] } \\
&\leqslant \sqrt{ \mathrm{Tr}\left[\sum_m p_m^2 (|\psi_m\rangle\langle\psi_m|^{CK})^{\otimes 2} \otimes (\omega^{EE'})^{\otimes 2} F^{E'} \right] } \\
&= \sqrt{ \mathrm{Tr}\left[(\omega^{EE'})^{\otimes 2} F^{E'} \right] \sum_m p_m^2 } = 2^{-\frac{1}{2} H_2(M)_\sigma - \frac{1}{2} H_2(E)_\omega}. \quad (4.20)
\end{aligned}
$$

The third line is true by the cyclic property of the trace. The inequality, however, is true by the following observation: since $F^2 = \mathbb{I}$ we know that F has eigenvalues ± 1 and so $F \leq \mathbb{I}$. We can make a similar evaluation for the last factor in Equation (4.19),

$$
\left\| \rho^M \otimes \rho^{CE'} \right\|_2 \leqslant 2^{-\frac{1}{2} H_2(M)_\sigma - \frac{1}{2} H_2(E)_\omega}, \quad (4.21)
$$

since this inequality is a just a special case of the calculations leading to Equation (4.20). If we apply Equations (4.20) and (4.21) to Equation (4.19), we can extract a very simple bound on the variation of the trace distance

$$
\begin{aligned}
|h_U(\mathcal{M}) - h_U(\mathcal{N})| &\leqslant \frac{2CE'}{s} 2^{-\frac{1}{2} H_2(M)_\sigma - \frac{1}{2} H_2(E)_\omega} \sum_{i=1}^s \left\| \chi_i^C - \nu_i^C \right\|_2 \\
&\leqslant \frac{2\sqrt{CE'}}{s} \sqrt{\Delta_{M,2} \Delta_{E,2}}\, d(\mathcal{M}, \mathcal{N}),
\end{aligned}
$$

where the last line follows from the definition of our metric on $\mathcal{L}(s, \eta)$. We have also ignored a factor of $1/\sqrt{K}$ above when expressing the bound in terms of $\Delta_{M,2}$. We do this to simplify future calculations and it only gives a slightly less tight bound here. $\square$

Lemma 4.4. *Given system A, there exists a ε-net $\mathcal{J}$ over the set $\mathcal{L}(s, \eta)$ of all (s, η)-quasi-measurements on A, such that each element $L \in \mathcal{L}(s, \eta)$ is at most ε-distant from an element of $J \in \mathcal{J}$ with respect to the metric $d(\cdot, \cdot)$. The size of this net can be taken to be*

$$
|\mathcal{J}| \leqslant \left(\frac{10s}{\varepsilon} \right)^{2s|A|}.
$$

Proof. We begin by consider an ε-net $\mathcal{K}$ over $\mathbb{S}_{2|A|}^{\times s}$ (s-tuples of $2|A|$-dimensional Euclidean unit spheres). First, there exists a ε-net over $\mathbb{S}_{2|A|}$ of size no more than $(5/\varepsilon)^{2|A|}$. (See, for example, Lemma II.4 in [HLSW04].) $\mathcal{K}$ can then be constructed by assembling the direct product of all the nets on the individual unit spheres. This produces a new net on the set of s-tuples of $2|A|$-dimensional unit spheres. Recall the distance measure $d(\cdot, \cdot)$ over $\mathcal{L}(s, \eta)$, the set of all (s, η)-quasi-measurements. This metric can be extended to s-tuples. If it is then evaluated for any s-tuple x and its representative in the net y,

$$d(x, y) = \sum_{i=1}^{s} \|\chi_i - \nu_i\|_2 \le s\varepsilon.$$

Thus the spacing of the net $\mathcal{K}$ over s-tuples is at most $s\varepsilon$ with respect to the desired metric. Consider the following set:

$$\mathcal{K}' := \{y \in \mathcal{K} : \exists\, x \in \mathcal{L}(s, \eta), \|x - y\|_2 \le s\varepsilon\}.$$

This is the set of all elements of the net $\mathcal{K}$ which are close to (s, η)-quasi-measurements. In other words, all (s, η)-quasi-measurements use an element of $\mathcal{K}'$ as their "representative" in the net. Now, divide $\mathcal{L}(s, \eta)$ into subsets of elements which share the same representation in $\mathcal{K}'$ and construct $\mathcal{J}$ by choosing one $L \in \mathcal{L}$ from each subset. We then have by the triangle inequality that all $L \in \mathcal{L}$ are $2s\varepsilon$ close to their new representative in $\mathcal{J}$. Clearly $|\mathcal{J}| \le |\mathcal{K}|$ since it was constructed from a subset and if we wish to make an ε-net over $\mathcal{L}(s, \eta)$ we need only rescale the ε from above, giving the result. $\qquad\square$

The Lipschitz constants, expectation value and net size give us all the pieces we need to make the concentration argument. We show that with very high probability, the distinguishability from independence of the joint (potentially unnormalized) distribution of messages and quasi-measurement outcomes is small.

Theorem 4.5 (Concentration of probability for distinguishability from independence)**.** *Given the quantum state $\rho^{MCKEE'} = U^{CKE} \cdot (\sigma^{MCK} \otimes \omega^{EE'})$ where U is a random unitary operator chosen according to the Haar measure, σ is as defined in Equation (1.1), $E' \cong E$, and $\omega^{EE'}$ is a bipartite pure state, the following bound holds*

$$\Pr_U \left\{ \sup_{\mathcal{M} \in \mathcal{L}(s, \eta)} \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right) \right\|_1 > \varepsilon \right\}$$

$$\le \exp\left(2sCE \ln\left(\frac{40\sqrt{CE}}{\varepsilon} \sqrt{\Delta_{M,2}\Delta_{E,2}} \right) - \frac{(CKE)^2}{2^8 \eta^2 \Delta_{M,\infty}\Delta_{E,\infty}} \left(\varepsilon - \frac{4\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \right).$$

In the above, $\Delta_{M,\infty}$, $\Delta_{M,2}$, $\Delta_{E,2}$ and $\Delta_{E,\infty}$ are as defined in Equations (2.2), (2.3), (2.5) and (2.4).

Proof. We apply Theorem 3.4 to $g_{\mathcal{M}}$ and consider only one direction of the divergence from the expected value. The exact statement can be written as

$$\Pr_U \left\{ g_{\mathcal{M}}(U) > \varepsilon \right\} \le \exp\left(-\frac{MCKE^2}{64\eta^2 \Delta_{M,\infty}\Delta_{E,\infty}} \left(\varepsilon - \mathbb{E}_U g_{\mathcal{M}} \right)^2 \right). \qquad (4.22)$$

It is convenient to define

$$f(\mathcal{M}, U) = \left\| \mathcal{M}\left(\rho^{MCE'}\right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'}\right) \right\|_1.$$

Clearly, $g_{\mathcal{M}}$ and h_U are sections of f and we are interested in bounding $\Pr_U \{\sup_{\mathcal{M}} f(\mathcal{M}, U) > \varepsilon\}$. Let

$$\varepsilon' = \frac{s\varepsilon}{2\sqrt{CE\Delta_{M,2}\Delta_{E,2}}},$$

and consider $\mathcal{J}$ an ε'-net over all (s, η)-quasi-measurements $\mathcal{M}$. We found in Lemma 4.3 that if two (s, η)-quasi-measurements were ε' apart with respect to the distance measure $d(\cdot, \cdot)$, then for a fixed unitary U, the values of f for each measurement would not differ by more than ε. Thus we can state that the supremum deviation of f is not more than twice the maximum deviation found on measurements in the net,

$$\Pr_U \left\{ \sup_{\mathcal{M}} f(\mathcal{M}, U) > 2\varepsilon \right\} \leqslant \Pr_U \left\{ \max_{\mathcal{M} \in \mathcal{J}} f(\mathcal{M}, U) > \varepsilon \right\}.$$

A union bound argument now bounds the probability of deviation for the maximum measurement by the probability of deviation for a generic measurement,

$$\Pr_U \left\{ \max_{\mathcal{M} \in \mathcal{J}} f(\mathcal{M}, U) > \varepsilon \right\} \leqslant \sum_{\mathcal{M} \in \mathcal{J}} \Pr_U \left\{ g_{\mathcal{M}}(U) > \varepsilon \right\}.$$

Thankfully, we have an explicit bound for the probability of deviation for an arbitrary measurement and we can make a simplification,

$$
\begin{aligned}
\Pr_U \left\{ \sup_{\mathcal{M}} f(U, \mathcal{M}) > 2\varepsilon \right\} &\leqslant \sum_{\mathcal{M} \in \mathcal{J}} \exp\left(-\frac{MCKE^2}{64\eta^2 \Delta_{M,\infty} \Delta_{E,\infty}} \left(\varepsilon - \mathop{\mathbb{E}}_U f \right)^2 \right) \\
&\leqslant \left(\frac{20\sqrt{CE\Delta_{M,2}\Delta_{E,2}}}{\varepsilon} \right)^{2sCE} \exp\left(-\frac{MCKE^2}{64\eta^2 \Delta_{M,\infty} \Delta_{E,\infty}} \left(\varepsilon - \mathop{\mathbb{E}}_U f \right)^2 \right) \\
&\leqslant \exp\left(2sCE \ln\left(\frac{20\sqrt{CE\Delta_{M,2}\Delta_{E,2}}}{\varepsilon} \right) - \frac{MCKE^2}{64\eta^2 \Delta_{M,\infty} \Delta_{E,\infty}} \left(\varepsilon - \mathop{\mathbb{E}}_U f \right)^2 \right).
\end{aligned}
$$

Substituting in the fact that $CK = M$ yields the desired inequality. $\qquad\square$

5   Locking against projective measurements

In this section we will only consider projective measurements, in other words $(s, \eta) = (CE', 1)$. We will also state all of the subsequent theorems in terms of qubits. For this reason we will identify $C = 2^c$, $K = 2^k$ and $E = E' = 2^e$. This last assumption, namely that E and E' have the same dimension, is crucial for this section because it restricts the size of the set of measurements sufficiently to allow for a straightforward discretization. The restriction will be lifted when we move on to generalized measurements in the next section, however.

Our calculations, we will make repeated use of the fact that

$$\log(x + y) \leqslant x + \log(y) \qquad \forall x, y \geqslant 1. \tag{5.1}$$

Corollary 5.1 (Locking for uniform messages with maximal entanglement). *Consider the locking scheme described in Definition 2.4 for a uniform message with maximal entanglement available at the measurement. Choose p and ϵ such that $\varepsilon > 8\sqrt{1/KE}$ and $p > 2^{-2(CE)^2}$. Then the scheme will be an ε-locking locking scheme except with probability p so long as the measurement superoperators are restricted to projective measurements and*

$$k > 9 + 2\log \frac{1}{\varepsilon} + \frac{1}{2} \log(c + e).$$

Proof. Using Theorem 4.5, we ensure that, except with probability p, our state is an ε-locking scheme provided that

$$2(CE)^2 \ln\left(\frac{40\sqrt{CE}}{\varepsilon} \right) - \frac{(CE)^2}{2^8} K^2 (\varepsilon')^2 < \ln p,$$

where we've defined for the time being ε' as $\varepsilon - 4/\sqrt{KE}$. A quick rearrangement of the terms reveals that the inequality will be satisfied if

$$\frac{2^9}{(\varepsilon')^2} \ln\left(\frac{40\sqrt{CE}}{\varepsilon}\left(\frac{1}{p}\right)^{1/2(CE)^2}\right) < K^2. \tag{5.2}$$

From our choice of p we can easily see $(1/p)^{1/2(CE)^2} < 2$ and from our choice of ε we see that $2^9/(\varepsilon')^2 < 2^{13}/\varepsilon^2$. Thus inequality (5.2) is satisfied when

$$\log\left(\frac{2^{13}}{\varepsilon^2}\right) + \log\left(\ln 2 \log\left(\frac{80\sqrt{CE}}{\varepsilon}\right)\right) < 2k.$$

Finally, two applications of Equation (5.1) reveal that the above is satisfied provided,

$$17 + 2\log\frac{1}{\varepsilon} + \log\log\frac{1}{\varepsilon} + \log(c+e) < 2k.$$

Rearranging the terms we see that the above condition is satisfied provided inequality (5.1) is satisfied, and we have completed the proof. $\qquad\square$

Corollary 5.1, and its extension to arbitrary POVM measurements in Corollary 6.4 is a mathematical expression that "generically, information is locked until it can be completely decoded." To arrive at this interpretation, recall from Equation (1.4) that to achieve a decoding error of ϵ, the measurement must be supplied with the entanglement through system E' as well as a system C satisfying $c - n > 2\log(1/\epsilon)$. Of course, this condition could never be met if the constraint $n = c + k$ is assumed, but the constraint was only made for convenience to prove the locking results. Using it to re-express Corollary 5.1, though, we find that the information about the message is ϵ-locked provided $c = n - k < n - 9 - 2\log(1/\epsilon) - 1/2 \cdot \log(c + e)$. Therefore, regardless of the size of the message or the amount of entanglement, the message goes from being ϵ-locked to being decodable with average probability of error at most ϵ with the transfer of $9 + 4\log(1/\epsilon) + 1/2 \cdot \log(c + e)$ qubits.

At this point, we wish to study the dependence of the minimum key size k on the various entropies of the message M and the entanglement E.

Corollary 5.2 (Locking for messages of bounded entropy with imperfect entanglement). *Consider the locking scheme described in Definition 2.4 for a message of bounded entropy with entanglement of a bounded fidelity available at the measurement. Choose ε and p satisfying*

$$\varepsilon > \frac{8\Delta_{E,\infty}}{\sqrt{KE}}, \qquad\qquad p > 2^{-2(CE)^2}.$$

Then the scheme will be an ε-locking locking scheme except with probability p so long as the measurement superoperators are restricted to projective measurements and

$$k' + \frac{1}{2}\left(n - H_{\min}(M)_\sigma\right) + \frac{1}{2}\left(e - H_{\min}(E)_\omega\right) < k, \tag{5.3}$$

where we've defined k' as the lower bound given in Corollary 5.1, i.e.: $k' = 9 + 2\log(1/\varepsilon) + 1/2 \cdot \log(c+e)$.

Proof. From Theorem 4.5, we can ensure ε-locking except with probability p by satisfying

$$2(CE)^2 \ln\left(\frac{40\sqrt{CE}}{\varepsilon}\sqrt{\Delta_{M,2}\Delta_{E,2}}\right) - \frac{(CE)^2}{2^8\Delta_{M,\infty}\Delta_{E,\infty}}K^2(\varepsilon')^2 < \ln p,$$

where we've defined for the time being ε' as $\varepsilon - 4\Delta_{E,\infty}/\sqrt{KE}$. A quick rearrangement of the terms reveals that the inequality can be satisfied if

$$\frac{2^9 \Delta_{M,\infty} \Delta_{E,\infty}}{(\varepsilon')^2} \ln\left(\frac{40\sqrt{CE}}{\varepsilon}\sqrt{\Delta_{E,2}\Delta_{M,2}}\left(\frac{1}{p}\right)^{1/2(CE)^2}\right) < K^2, \tag{5.4}$$

From our choice of p we can easily see $(1/p)^{1/2(CE)^2} < 2$ and from our choice of ε we see that $2^9/(\varepsilon')^2 < 2^{13}/\varepsilon^2$. Thus the inequality in Equation (5.4) is satisfied when

$$13 + 2\log\frac{1}{\varepsilon} + \log(\Delta_{M,\infty}\Delta_{E,\infty}) + \log\left(7 + \log\frac{1}{\varepsilon} + \frac{1}{2}(c+e) + \frac{1}{2}\log(\Delta_{M,2}\Delta_{E,2})\right) < 2k.$$

However, we know that the maximum values of $\Delta_{M,2}$ and $\Delta_{E,2}$ are M and E respectively. Combined with our assumption that $k < c$, we can quickly reduce the above to,

$$18 + 3\log\frac{1}{\varepsilon} + \log(c+e) + \left(n - H_{\min}(M)_\sigma\right) + \left(e - H_{\min}(E)_\omega\right) < 2k.$$

Finally, we can identify k' and give the result as desired. $\qquad\square$

6 Locking against generalized measurements

We will now show that the results of the previous section hold not only for projective measurements, but also for general POVMs, up to very minor changes in the various constants. The main difficulty at this point is that we cannot use Theorem 4.5 directly, since it only gives bounds for (s, η)-quasi-measurements. We must therefore show that a general POVM behaves essentially like an (s, η)-quasi-measurement for the purposes of the theorem. Our strategy will be probabilistic in nature: we will show that doing a general POVM $\mathcal{M}$ is mathematically equivalent to randomly selecting a measurement constructed from possible sequences of s measurement results obtained from $\mathcal{M}$. With overwhelming probability, the sequence chosen will be an (s, η)-quasi-measurement, and Theorem 4.5 will then apply in this case.

We start by proving this last fact, namely that with very high probability, a sequence of s measurement results will be an (s, η)-quasi-measurement, for an appropriately chosen η.

Lemma 6.1. *Let $\mathcal{M}^{CE' \to X}$ be any complete measurement superoperator, with $\mathcal{M}(\pi) = \sum_i \alpha_i |i\rangle\langle\chi_i|\pi|\chi_i\rangle\langle i|$, and consider the operator-valued random variable Y which takes the value $|\chi_i\rangle\langle\chi_i|$ with probability $\alpha_i\langle\chi_i|\pi|\chi_i\rangle = \alpha_i/CE'$. Then, s i.i.d. copies of Y will fail to be an (s, η)-quasi-measurement with probability at most $2CE'e^{-s(\eta-1)^2/CE'2\ln 2}$.*

Proof. Y fulfills all the conditions for the operator Chernoff bound (Lemma A.2) to apply, with $\mathbb{E}Y = \pi^{CE'}$. This yields

$$\Pr\left\{\frac{1}{s}\sum_{j=1}^s Y_j \nleq \eta\pi\right\} \leqslant 2CE'e^{-s(\eta-1)^2/CE'2\ln 2},$$

and the probability on the left is an upper bound on the probability that the s-tuple $Y_1, \ldots, Y_s$ is not an (s, η)-quasi-measurement. $\qquad\square$

We now use this to show that best general POVM cannot do much better than the best (s, η)-quasi-measurement:

Lemma 6.2. *It is true that*

$$\sup_{\mathcal{M}} \left\|\mathcal{M}\left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'}\right)\right\|_1$$

$$\leqslant \max_{\mathcal{M}' \in \mathcal{L}(s,\eta)} \left\|\mathcal{M}'\left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'}\right)\right\|_1 + 4(CE')^2 e^{-s(\eta-1)^2/(CE'(2\ln 2))}, \tag{6.1}$$

where the supremum on the left-hand side is taken over all measurement superoperators.

Proof. Let $\mathcal{M}^{CE' \to X}$ be any complete measurement superoperator of the form $\mathcal{M}(\sigma) = \sum_i \alpha_i |i\rangle\langle\chi_i|\sigma|\chi_i\rangle\langle i|$, and define Y to be the operator-valued random variable which takes value χ_i with probability α_i/CE'. Let Q be the event that $Y_1, \ldots, Y_n$ is an (s, η)-quasi-measurement, where the Y_i are i.i.d. with the same distribution as Y.

$$\left\| \mathcal{M}\left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right\|_1$$
$$= \sum_i \alpha_i \left\| \mathrm{Tr}_{CE'} \left[\chi_i \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right] \right\|_1$$
$$= CE' \mathbb{E}_Y \left\| \mathrm{Tr}_{CE'} \left[Y \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right] \right\|_1$$
$$= \frac{CE'}{s} \mathbb{E}_{Y_1, \ldots, Y_s} \sum_i^s \left\| \mathrm{Tr}_{CE'} \left[Y_i \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right] \right\|_1.$$

At this point we separate the expression into two terms, one for the event Q and another for its complement.

$$\left\| \mathcal{M}\left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right\|_1$$
$$= \frac{CE'}{s} \Pr\{Q\} \mathbb{E} \left[\sum_{i=1}^s \left\| \mathrm{Tr}_{CE'} \left[Y_i \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right] \right\|_1 \,\middle|\, Q \right]$$
$$+ \frac{CE'}{s} \Pr\{\bar{Q}\} \mathbb{E} \left[\sum_{i=1}^s \left\| \mathrm{Tr}_{CE'} \left[Y_i \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right] \right\|_1 \,\middle|\, \bar{Q} \right]$$
$$\leqslant \max_{\mathcal{M}' \in \mathcal{L}(s,\eta)} \left\| \mathcal{M}' \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right\|_1 \Pr\{Q\} + 2CE' \Pr\{\bar{Q}\}$$
$$\leqslant \max_{\mathcal{M}' \in \mathcal{L}(s,\eta)} \left\| \mathcal{M}' \left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right\|_1 + 4(CE')^2 e^{-s(\eta-1)^2/CE' 2 \ln 2}.$$

In the above, the sum of trace distances given Q was interpreted as executing an (s, η)-quasi-measurement described by $Y_1, \ldots, Y_s$, and the same sum given $\bar{Q}$ was simply bounded by 2η (there are s terms in the sum, each of which cannot exceed 2). In the last step, we have bounded $\Pr\{\bar{Q}\}$ using Lemma 6.1 and made use of the fact that we can assume without loss of generality that $|E| = |E'|$.

Finally, a non-complete measurement superoperator can always be decomposed into a complete one by splitting the POVM elements of rank greater than 1; this process always increases the trace distance. $\qquad\square$

What we have achieved with the above statement is to show that the decoupling distance for a general measurement superoperator is very close to the decoupling distance of an (s, η)-quasi-measurement. All that is now left to do is to use Theorem 4.5 to bound the supremum over (s, η)-quasi-measurements, and we get the main theorem of this section:

Theorem 6.3 (Locking theorem for general measurements)**.** *Given the quantum state $\rho^{MCKEE'} = U^{CKE} \cdot (\sigma^{MCK} \otimes \omega^{EE'})$ where U is a random unitary operator chosen according to the Haar measure, σ is as defined in Equation (1.1) and $\omega^{EE'}$ a bipartite pure state, then*

$$\Pr_U \left\{ \sup_{\mathcal{M}} \left\| \mathcal{M}\left(\rho^{MCE'} \right) - \mathcal{M}\left(\rho^M \otimes \rho^{CE'} \right) \right\|_1 > \varepsilon \right\}$$
$$\leqslant \exp\left(9(CE)^2 \ln(CE) \ln\left(\frac{40\sqrt{CE}}{\varepsilon} \sqrt{\Delta_{M,2}\Delta_{E,2}} \right) - \frac{(CKE)^2}{2^{10}\Delta_{M,\infty}\Delta_{E,\infty}} \left(\varepsilon - \frac{8\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \right).$$

In the above, $\Delta_{M,\infty}$, $\Delta_{M,2}$, $\Delta_{E,2}$ and $\Delta_{E,\infty}$ are as defined in Equations (2.2), (2.3), (2.5) and (2.4).

Proof. We may assume without loss of generality that $|E'| \leq |E|$. If not, let E'' be the range of $\rho^{E'} = \omega^{E'}$. Because ω is pure, $|E''| = \mathrm{rank}\,\omega^{E'} \leq |E|$. Let V be the isometric embedding $E'' \hookrightarrow E'$ and $\rho^{MCE''}$ the

20

projection of ρ to MCE''. Then for any POVM measurement superoperator $\mathcal{M}^{CE' \to X}$,

$$\mathcal{M}(\rho^{MCE'}) = \mathcal{M}(V\rho^{MCE''}V^\dagger)$$

so measuring $\mathcal{M}$ or $M \circ (V \cdot V^\dagger)$ will yield exactly the same measurement statistics. But the latter is a POVM on CE'' and E'' satisfies the desired dimension bound.

Substituting the results of Lemma 6.2 into those of Theorem 4.5, we get the following:

$$\Pr_U \left\{ \sup_{\mathcal{M}} \left\| \mathcal{M}\left(\rho^{MCE'} - \rho^M \otimes \rho^{CE'} \right) \right\|_1 \geqslant \varepsilon \right\} \leqslant \exp\left(2sCE \ln\left(\frac{40\sqrt{CE}}{\varepsilon} \sqrt{\Delta_{M,2}\Delta_{E,2}} \right) \right.$$
$$\left. - \frac{(CKE)^2}{2^8 \eta^2 \Delta_{M,\infty}\Delta_{E,\infty}} \left(\varepsilon - 4(CE)^2 e^{-s(\eta-1)^2/(CE(2\ln 2))} - \frac{4\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \right). \quad (6.2)$$

We now choose $\eta = 2$ and $s = (6\ln 2)CE \ln CE$ and note that this immediately implies

$$2(CE)^2 e^{-s(\eta-1)^2/CE2\ln 2} = \frac{2}{CE}.$$

We absorb this factor into our "offset" for the ε factor,

$$\left(\varepsilon - 4(CE)^2 e^{-s(\eta-1)^2/CE2\ln 2} - \frac{4\Delta_{E,\infty}}{\sqrt{KE}} \right)^2 \geqslant \left(\varepsilon - \frac{8\Delta_{E,\infty}}{\sqrt{KE}} \right)^2.$$

Substituting the choices for s and η into Equation 6.2 reveals the desired result. $\qquad \square$

We now wish to express, in qubits, a lower bound for the key size for a given probability p and a given ε. The relevant variables are $M = 2^n$, $C = 2^c$, $K = 2^k$, and $E = 2^e$. Unlike in the previous section, it is unnecessary to make any assumptions about the dimension of E'.

Corollary 6.4 (Locking against POVMs for a uniform message with maximal entanglement)**.** *Consider the locking scheme described in Definition 2.4 for a uniform message and maximal entanglement available at the measurement. Choose p and ϵ such that $\varepsilon > 16\sqrt{1/KE}$ and $p > 2^{-9(CE)^2}$. Then the scheme will be an ε-locking locking scheme except with probability p so long as*

$$11 + 2\log\frac{1}{\varepsilon} + \log(c+e) < k.$$

Proof. From Theorem 6.3 we can ensure ε-locking except with probability p given

$$9\ln(CE)\ln\left(\frac{40\sqrt{CE}}{\varepsilon} \right) + \frac{1}{9(CE')^2} \ln\frac{1}{p} < \frac{K^2(\varepsilon')^2}{2^{10}},$$

where we've defined for the time being ε' as $\varepsilon - 8/\sqrt{KE}$. We now make use of our lower bound for p as well as the assumption that $\ln(CE) \geqslant 1$ to show that the above can satisfied provided

$$9\ln(CE)\ln\left(\frac{80\sqrt{CE}}{\varepsilon} \right) < \frac{K^2(\varepsilon')^2}{2^{10}}.$$

Solving the above equation for k and applying the condition on ε reveals that the bound can be satisfied by the statement in the lemma. $\qquad \square$

Corollary 6.5 (Locking against POVMs for messages of bounded entropy with imperfect entanglement)**.**
Consider the locking scheme described in Definition 2.4 for a uniform message and maximal entanglement available at the measurement. Choose p and ϵ such that

$$\varepsilon > \frac{16\Delta_{E,\infty}}{\sqrt{KE}}, \qquad\qquad p > 2^{-9(CE)^2}.$$

Then the scheme will be an ε-locking locking scheme except with probability p so long as

$$k' + \frac{1}{2}\Big(n - H_{\min}(M)_\sigma\Big) + \frac{1}{2}\Big(e - H_{\min}(E)_\omega\Big) < k, \tag{6.3}$$

where we've defined k' as the lower bound given in Corollary 6.4, i.e.: $k' = 11 + 2\log(1/\varepsilon) + \log(c+e)$.

Proof. From Theorem 4.5, we can ensure ε-locking with probability p by satisfying, From Theorem 6.3 we can ensure ε-locking with probability p given

$$9\ln(CE)\ln\left(\frac{40\sqrt{CE}\sqrt{\Delta_{M,2}\Delta_{E,2}}}{\varepsilon}\right) + \frac{1}{9(CE')^2}\ln\frac{1}{p} < \frac{K^2(\varepsilon')^2}{2^{10}\Delta_{M,\infty}\Delta_{E,\infty}},$$

where we've defined for the time being ε' as $\varepsilon - 8/\sqrt{KE}$. We now make use of our lower bound for p as well as the assumption that $\ln(CE) \geqslant 1$ to show that the above can satisfied provided

$$9\ln(CE)\ln\left(\frac{80\sqrt{CE}\sqrt{\Delta_{M,2}\Delta_{E,2}}}{\varepsilon}\right) < \frac{K^2(\varepsilon')^2}{2^{10}\Delta_{M,\infty}\Delta_{E,\infty}}.$$

Next, we use our definition for ε' and our bound for ε and we solve for k to find that the bound is satisfied provided

$$21 + 3\log\frac{1}{\varepsilon} + 2\log(c+e) + \log(\Delta_{M,\infty}\Delta_{E,\infty}) < 2k.$$

Finally, we can identify k' and give the result as desired. $\qquad\square$

The lower bound requirement on ε in Corollary 6.5 limits the corollary's range of applicability to situations in which $H_{\min}(E)_\omega$ is not too small. Specifically, the requirement can be rewritten in light of (6.3) as

$$2\log(c+e) + (n - H_{\min}(M)_\sigma) + 3H_{\min}(E)_\omega > e + \text{const.}$$

So, at least when the message is uniform, the requirement is roughly that $H_{\min}(E)_\sigma > e/3$. We suspect that this requirement can be eliminated but leave it as an open problem to find a way to do so.

7 Locking versus decodability

The previous sections have shown that, under certain conditions, no classical information is recoverable by the receiver. Here we aim to show that, in many regimes, these results are essentially optimal. We do this by showing that if we make the key only very slightly smaller, then with overwhelming probability, the classical message will be decodable with a negligible error probability. In fact we prove even more: in this regime where the information is decodable, the decoder can even decode a *purification* of the classical message. In other words, in this generic scenario where U is chosen with no preferred basis, either all *classical* information is locked away, or we can decode *quantum* information. This is formalized in the next theorem.

In order to study decodability, we must discard the identifications made in Figure 2 to study locking and return to the original scenario described by Figure 1. Whereas k was previously the number of qubits in

system K, there is no system K in Figure 2. Instead, we define $k = n - c$, which is consistent with its earlier definition. Now, however, it might be the case that k is negative since decoding could require the cyphertext to be longer than the message.

The following theorem generalizes the discussion of Section 1.1 to nonuniform messages and imperfect entanglement.

Theorem 7.1. *If U is chosen according to the Haar measure, then the information in the scheme described in Figure 1 is such that there exists a decoding CPTP map $\mathcal{D}^{CE' \to N}$ such that*

$$\left\| \mathcal{D} \left(\operatorname{Tr}_D \left[U^{NE \to CD} \left(\sigma^{RMN} \otimes \omega^{E'E} \right) (U^{NE \to CD})^\dagger \right] \right) - \sigma^{RMN} \right\|_1 \leqslant \varepsilon$$

asymptotically almost surely, where σ^{RMN} is a purification of σ^{MN}, as long as

$$k \leqslant \frac{1}{2} \left(n - H_{\max}(M)_\sigma \right) - \frac{1}{2} \left(e - H_2(E)_\omega \right) - 2 \log(1/\varepsilon) - 4$$

Proof. Using Theorem 3.7 from [Dup09], we get that

$$\mathbb{E}_U \left\| \operatorname{Tr}_C \left[U^{NE \to CD} \left(\sigma^{RMN} \otimes \omega^E \right) (U^{NE \to CD})^\dagger \right] - \sigma^{RM} \otimes \rho^D \right\|_1 \leqslant 2^{\frac{1}{2} H_{\max}(M)_\sigma - \frac{1}{2} H_2(E)_\omega} \sqrt{\frac{D}{C}}.$$

It can also be shown that the value of this trace distance will asymptotically almost surely not exceed twice this bound. Under this condition, we have that:

$$\left\| \operatorname{Tr}_C \left[U^{NE \to CD} \left(\sigma^{RMN} \otimes \omega^E \right) (U^{NE \to CD})^\dagger \right] - \sigma^{RM} \otimes \rho^D \right\|_1 \leqslant 2 \times 2^{\frac{1}{2} H_{\max}(M)_\sigma - \frac{1}{2} H_2(E)_\omega} \sqrt{\frac{D}{C}}.$$

Uhlmann's Theorem then implies the existence of a partial isometry $V^{CE' \to NG}$ and of a purification of ρ^D on system G that we call θ^{DG} such that

$$\left\| VU \left(\sigma^{RMN} \otimes \omega^{E'E} \right) U^\dagger V^\dagger - \sigma^{RMN} \otimes \theta^{DG} \right\|_1 \leqslant 4 \left(2^{H_{\max}(M)_\sigma - H_2(E)_\omega} \frac{D}{C} \right)^{1/4}.$$

Defining $\mathcal{D}^{CE' \to N}$ as $\mathcal{D}(\xi) = \operatorname{Tr}_G \left[V \xi V^\dagger \right]$ and tracing out system D, we get that

$$\left\| \mathcal{D} \left(\operatorname{Tr}_D \left[U^{NE \to CD} \left(\sigma^{RMN} \otimes \omega^{E'E} \right) (U^{NE \to CD})^\dagger \right] \right) - \sigma^{RMN} \right\|_1 \leqslant 4 \left(2^{H_{\max}(M)_\sigma - H_2(E)_\omega} \frac{D}{C} \right)^{1/4}.$$

Now, to satisfy the theorem statement, we need to ensure that

$$4 \left(2^{H_{\max}(M)_\sigma - H_2(E)_\omega} \frac{D}{C} \right)^{1/4} \leqslant \varepsilon.$$

Taking logarithms on both sides and using the fact that $\log D = k + e$, we get that

$$2 + \frac{1}{4} \left[H_{\max}(M)_\sigma - H_2(E)_\omega + e + k - c \right] \leqslant \log \varepsilon.$$

Substituting in the fact that $c = n - k$, we arrive at the statement of the theorem. □

8 Implications for the security of quantum protocols against quantum adversaries

When designing quantum cryptographic protocols, it is often necessary to show that a quantum adversary ("Eve") is left with only a negligible amount of information on some secret string. An initial attempt at formalizing this idea is to say that, at the end of the protocol, regardless of what measurement Eve makes on her quantum system, the mutual information between her measurement result and the secret string is at most ε (in other words, her accessible information about the message is at most ε). This was often taken as the security definition for quantum key distribution, usually implicitly by simply not considering that the adversary might keep quantum data at the end of the protocol [LC99, SP00, NC00, GL03, LCA05] (see also discussion in [BOHL+05, RK05, KRBM07]). In [KRBM07], it is shown that this definition of security is inadequate, precisely because of possible locking effects. Indeed, this security definition does not exclude the possibility that Eve, upon gaining partial knowledge of S after the end of the protocol, could then gain more by making a measurement on her quantum register that depends on the partial information that she has learned. In [KRBM07], the authors exhibit an admittedly contrived quantum key distribution protocol which generates a secret n-bit key such that, if Eve learns the first $n - 1$ bits, she can then learn the remaining bit by measuring her own quantum register.

The locking scheme presented above allows us to demonstrate a much more spectacular failure of this security definition. We will show that there exists a quantum key distribution protocol that ensures that an adversary has negligible accessible information about the final key, but with which an adversary can recover the entire key upon learning only a very small fraction of it.

8.1 Description of the protocol

We will derive this faulty protocol by starting with a protocol that is truly secure, and then making Alice send a locked version of the secret string directly to Eve. We will be able to prove that regardless of what measurement Eve makes on her state, she will learn essentially no information on the string, but of course, she only needs to learn a tiny amount of information to unlock what Alice sent her. More precisely, let P be a quantum key distribution protocol such that, at the end of its execution, Alice and Bob share an n-bit string, and Eve has a quantum state representing everything that she has managed to learn about the string. We will also assume that P is a truly secure protocol: the string together with Eve's quantum state can be represented as a quantum state σ^{SE} such that $\|\sigma^{SE} - \pi^S \otimes \sigma^E\|_1 \leqslant \varepsilon$, where S is a quantum register holding the secret string, and E is Eve's quantum register. Now, we will define the protocol P' to be the following quantum key distribution protocol: Alice and Bob first run P to generate a string s of length n, and then Alice splits s into two parts: the first part s_k is of size $O(\log n)$, and the second part s_c contains the rest of the key. Alice then uses the classical key s_k to create a quantum state in register C that contains a locked version of s_c and sends the system C to Eve.

How secure is P'? It is clearly very insecure, since, if Eve ever ends up learning s_k (via a known plaintext attack, for instance), she can then completely recover s_c. However, the next theorem shows that, right after the execution of P', Eve cannot make any measurement that will reveal information about the key. In particular, P' satisfies the requirement that Eve's accessible information on the key be very low.

Theorem 8.1. *Let P and P' be quantum key distribution protocols as defined as above, and let ρ^{CES} be the state at the end of the execution of P': S contains the n-bit string s, E is Eve's quantum register after the execution of P, and C contains the locked version of s_c that Alice sent to Eve. Then, for any measurement superoperator $\mathcal{M}^{CE \to X}$, there exists a state ξ^X such that*

$$\left\| \mathcal{M}(\rho^{CES}) - \xi^X \otimes \pi^S \right\|_1 \leqslant 2\varepsilon.$$

This also entails that

$$I_{\mathrm{acc}}(S; CE) \leqslant 8\varepsilon n + 2\eta(1 - 2\varepsilon) + 2\eta(2\varepsilon)$$

via the Alicki-Fannes inequality (see Lemma 2.1).

Proof. From the definition of P, we have that

$$\left\| \rho^{ES} - \pi^S \otimes \rho^E \right\|_1 \leqslant \varepsilon. \tag{8.1}$$

Now, let $\mathcal{C}^{S \to CS}$ be a superoperator that takes a classical string in S, splits it into s_k and s_c, creates a locked version of s_c with s_k as the key into the quantum system C, and leaves the classical string in S unchanged; this is simply the operation that Alice performs when preparing C for Eve. The above inequality, combined with the monotonicity of the trace distance under CPTP maps yields

$$\left\| \rho^{CES} - \mathcal{C}(\pi^S) \otimes \rho^E \right\|_1 \leqslant \varepsilon \tag{8.2}$$

and hence, for any measurement superoperator $\mathcal{M}^{CE \to X}$,

$$\left\| \mathcal{M}(\rho^{CES}) - \mathcal{M}(\mathcal{C}(\pi^S) \otimes \rho^E) \right\|_1 \leqslant \varepsilon \tag{8.3}$$

Consider now the expression $\mathcal{M}^{CE \to X}(\mathcal{C}(\pi^S) \otimes \rho^E)$: it can be viewed as a measurement on the C system of $\mathcal{C}^{S \to CS}(\pi^S)$ alone that is implemented by creating the state ρ^E and then measuring $\mathcal{M}^{CE \to X}$. Furthermore, note that, by the definition of an ε-locking scheme, we have that, for every measurement superoperator $\mathcal{N}^{C \to X}$,

$$\left\| \mathcal{N}(\mathcal{C}(\pi^S)) - \mathcal{N}(\mathrm{Tr}_S[\mathcal{C}(\pi^S)]) \otimes \pi^S \right\|_1 \leqslant \varepsilon. \tag{8.4}$$

Applying this to $\mathcal{M}^{CE \to X}(\mathcal{C}(\pi^S) \otimes \rho^E)$, we get that

$$\left\| \mathcal{M}(\mathcal{C}(\pi^S) \otimes \rho^E) - \mathcal{M}(\mathrm{Tr}_S[\mathcal{C}(\pi^S)] \otimes \rho^E) \otimes \pi^S \right\|_1 \leqslant \varepsilon. \tag{8.5}$$

We now use the triangle inequality on Equations (8.3) and (8.5) to obtain

$$\left\| \mathcal{M}(\rho^{CES}) - \mathcal{M}(\mathrm{Tr}_S[\mathcal{C}(\pi^S)] \otimes \rho^E) \otimes \pi^S \right\|_1 \leqslant 2\varepsilon \tag{8.6}$$

which yields the theorem with $\xi^X := \mathcal{M}(\mathrm{Tr}_S[\mathcal{C}(\pi^S)] \otimes \rho^E)$. $\qquad\square$

Hence, we have shown that requiring that Eve's accessible information on the generated key be low is not an adequate definition of security for quantum key distribution. We have exhibited a protocol P' which guarantees low accessible information and yet is clearly insecure due to locking effects.

9 Discussion

It is natural in physics to measure the "correlation" between two quantum physical systems using the correlation between the outcomes of measurements on those two systems. Two-point correlation functions are but the most ubiquitous examples. The results in this article demonstrate that this practice can sometimes be very misleading. The ϵ-locking quantum states exhibited in this article would reveal no correlations using any type of measurement, but enlarging one of the two systems by a small number of qubits would expose near-perfect correlation between the two systems. This is an important and counterintuitive property of information in quantum mechanical systems: measurements can be distressingly bad ways to detect correlation.

The extensive literature on quantum discord is essentially devoted to exploring the relationship between accessible, or classical, and quantum mutual information [OZ01, HV01, BKZ06]. Since the discord is defined as the gap between the quantum and classical mutual informations, locking can be viewed as the extreme case where classical mutual information doesn't detect any of the very abundant quantum mutual information. Previous work had demonstrated that transmitting a constant number of physical qubits can cause the classical mutual information to increase from a fixed small constant to an arbitrarily large value.

In this article, we have strengthened the definition of locking, replacing the mutual information by the trace distance to a product distribution. Moreover, we have shown that the locking effect still exists even when the trace distance (or the classical mutual information) is made arbitrarily small. In light of these results, claims that the discord is a robust measure of quantum correlation [WSFB09] should treated with skepticism. While discord is certainly a signature of quantumness, its susceptibility to locking means that it is in this important respect not robust.

Previous studies of information locking had also always focused on the example of sending classical information in one of a small number of different bases unknown to the receiver. The intuition was that a receiver ignorant of the basis could not do much better than guessing the basis and then measuring. Most of the time, he would guess incorrectly and his measurement would then destroy the information. Moving away from that paradigm, in this article we consider classical information encoded using a single generic unitary transformation mixing the input information with half of an entangled state shared with the receiver. The "key" then becomes a quantum system. While the original paradigm can be recovered by eliminating the entanglement and encrypting the key quantum system with a private quantum channel, the setting considered here is strictly more general.

Indeed, we find that, for an n-bit uniform message and maximal entanglement, the information is generically ϵ-locked until the receiver is within $O(\log n/\epsilon)$ qubits of being able to completely decode the message. Our definition of locking is stronger than those previously studied and our results imply, for the first time, that the classical mutual information can be made arbitrarily small. Our method of proof in the case of projective measurements was a fairly standard discretization argument but the extension to POVM measurements required a new strategy exploiting the operator Chernoff bound. In contrast to previous studies of locking, we do not require the message to be uniformly distributed, working instead with a min-entropy bound on the distribution of messages. In that case, we found that the key size was at most the gap between the max- and min-entropies of the message, modulo the logarithmic terms that dominate in the uniform situation.

For information theorists, this may appear reminiscent of a strong converse to a channel capacity problem. Roughly, a strong converse theorem states that any attempt to transmit above the channel capacity will result in the decoding error probability approaching one. In our setting, the analog of the strong converse would be a matching lower bound to Equation (1.5) of the form

$$1 - \epsilon < \frac{1}{M} \sum_m \sum_{m' \neq m} p(m'|m) \tag{9.1}$$

whenever $C < M$, indicating the the probability of incorrectly decoding the message is at least $1 - \epsilon$. What we prove here is much stronger. Equation (9.1) doesn't rule out the possibility of being able to pin the message down to some relatively small set. More generally, it doesn't imply a small mutual information between the message and the measurement outcome. Information locking does imply these stronger statements.

As such, information locking has a natural cryptographic interpretation even if we haven't emphasized it in this article. The special case of our scenario mentioned above, with no entanglement and a quantum key encrypted using a private quantum channel, leads to a method for encrypting classical messages using a secret key of size independent of the length of the message. Similarly, information locking schemes can be used to construct string commitment protocols with surprisingly good parameters [BCH+06, BCH+08]. These cryptographic applications are emphasized in the companion article [FHS10].

To the extent that random unitary transformations provide good models of black hole evaporation, our results might also have implications for that process. Oppenheim and Smolin had previously suggested that information locking could rescue the long-lived remnant hypothesis [SO06]. In essence, their idea was that a remnant with a small number of states could lock all the information of a large black hole, thereby evading the inconsistencies with low energy physics that arise from having large numbers of remnant species [ACN87, CW87]. Their proposal, however, relied on previously studied locking states

that treated the encoded message and the key very differently. Consequently, the proposal required that the black hole keep hold of the key until the very last moments of its evaporation, implying some ad hoc dynamical distinction between encoded message and key in the evaporation process. Our results imply that *if* the dynamics are well-modeled by a Haar random unitary transformation, then any small portion of the output system can be used as the key. No ad hoc distinction is necessary.

Ironically, the information locking effect is also perfectly compatible with the rapid release of information from a black hole predicted in [HP07], assuming a unitary evaporation process. That article observed that if a black hole is already highly entangled with Hawking radiation from an earlier time, then messages would be released from the black hole in the Hawking radiation once the black hole dynamics had sufficiently "scrambled" the message with internal black hole degrees of freedom. By virtue of the fact that we treat generic unitary transformations acting on a message and half of an entangled state, our results apply to the setting of that paper and the followup [SS08]. Specifically, our results imply that in the case of a larger message, *no* information about the message could be obtained from the Hawking radiation until moments before it could *all* be obtained. The conclusion depends, of course, on whether the random unitary transformation is a good model of the evaporation process. While the generic unitary transformations considered here would take exponential time to implement on a quantum computer, the follow-up article [FHS10] shows, at least, that locking can be achieved with a quantum circuit of depth only slightly superlinear in the number of qubits in the system. Other attempts to apply random unitary transformations to the black hole information problem, such as [Llo06, BSZ09], will be affected similarly by information locking.

To summarize, this article defined information locking more stringently than previously and nonetheless found that this stronger form of locking is generic: if information is encoded using a random unitary transformation, then it will either be decodable or locked. Almost no middle ground occurs. This observation has implications for cryptography and, potentially, for black hole physics.

Acknowledgments

References

[ACN87]   Y. Aharonov, A. Casher, and S. Nussinov. The unitarity puzzle and Planck mass stable particles. *Physics Letters B*, 191:51–55, 1987.

[ADHW09]   Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information's family tree. *Proceedings of the Royal Society A*, (465):2537–2563, 2009. quant-ph/0606225.

[AF04]   Robert Alicki and Mark Fannes. Continuity of quantum mutual information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, 2004. quant-ph/0312081.

[AGZ09]   Greg W. Anderson, Alice Guionnet, and Ofer Zeitouni. *An Introduction to Random Matrices*. Cambridge University Press, 2009. http://www.wisdom.weizmann.ac.il/ zeitouni/cupbook.pdf.

[AW02]   Rudolf Ahlswede and Andreas Winter. Strong converse for identification via quantum channels. *IEEE Transactions on Information Theory*, 48(3):569–579, 2002. quant-ph/0012127.

[BCH⁺06]   Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Security of quantum bit string commitment depends on the information measure. *Physical Review Letters*, 97:250501, 2006. arXiv:quant-ph/0609237.

[BCH⁺08]   Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility, and cheat-sensitivity of quantum bit string commitment. *Physical Review A*, 78:022316, 2008. arXiv:quant-ph/0504078.

[Bha96]   Rajendra Bhatia. *Matrix Analysis*. Springer-Verlag, 1996.

[BKZ06]   Robin Blume-Kohout and Wojciech H. Zurek. Quantum Darwinism: Entanglement, branches, and the emergence of classicality of redundantly stored quantum information. *Physical Review A*, 73:062310, 2006.

[BOHL⁺05] Michael Ben-Or, Michał Horodecki, Debbie Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. *Second Theory of Cryptography Conference, TCC 2005*, 3378:386–406, 2005. quant-ph/0409078.

[BSZ09]   Samuel L. Braunstein, Hans-Jürgen Sommers, and Karol Zyczkowski. Entangled black holes as ciphers of hidden information. arXiv:0907.0739, 2009.

[CW87]   R. D. Carlitz and R. S. Willey. Lifetime of a black hole. *Physical Review D*, 36:2336–2341, 1987.

[DHL⁺04]   David P. DiVincenzo, Michał Horodecki, Debbie W. Leung, John A. Smolin, and Barbara M. Terhal. Locking classical correlation in quantum state. *Phys. Rev. Lett.*, (92, 067902), 2004. quant-ph/0303088.

[Dup09]   Frédéric Dupuis. *The decoupling approach to quantum information theory*. PhD thesis, Université de Montréal, 2009. arXiv:1004.1641.

[FHS10]   Omar Fawzi, Patrick Hayden, and Pranab Sen. From low-distortion embeddings to metric uncertainty relations and information locking. to appear, 2010.

[Fuc96]   Christopher A. Fuchs. *Distinguishability and accessible information in quantum theory*. PhD thesis, University of New Mexico, 1996. quant-ph/0601020.

[GL03]   Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003. quant-ph/0105121.

[HLSW04]   Patrick Hayden, Debbie Leung, Peter Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Comm. Math. Phys.*, 250(2):371–391, 2004. quant-ph/0307104.

[HP07]   Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 07(09):120, 2007.

[HV01]   Leah Henderson and Vlatko Vedral. Classical, quantum and total correlations. *Journal of physics A: mathematical and general*, 34(35):6899, 2001.

[KRBM07]   Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Locking of accessible information and implications for the security of quantum cryptography. *Phys. Rev. Lett.*, 98(140502), 2007. quant-ph/0512021.

[LC99]   Hoi-Kwong Lo and Hoi-Fung Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999. quant-ph/9803006.

[LCA05]   Hoi-Kwong Lo, Hoi-Fung Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security. *Journal of Cryptology*, 18(133), 2005. quant-ph/0011056.

[Llo06]   Seth Lloyd. Almost certain escape from black holes in final state projection models. *Physical Review Letters*, 96:061302, 2006.

[NC00]   Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[OZ01]   Harold Ollivier and Wojciech H. Zurek. Quantum discord: a measure of the quantumness of correlations. *Physical Review Letters*, 88:017901, 2001.

[Ren05]   Renato Renner. *Security of quantum key distribution*. PhD thesis, ETH Zurich, 2005. quant-ph/0512258.

[RK05]   Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. *Second Theory of Cryptography Conference, TCC 2005*, 3378:407–425, 2005. quant-ph/0403133.

[SO06]   John Smolin and Jonathan Oppenheim. Locking information in black holes. *Physical Review Letters*, 96(8):081302–+, 2006.

[SP00]   Peter Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85, 2000. quant-ph/0003004.

[SS08]   Y. Sekino and L. Susskind. Fast scramblers. *Journal of High Energy Physics*, 10:65–+, 2008. arxiv:0808.2096.

[WSFB09]   T. Werlang, S. Souza, F. F. Fanchini, and C. J. Villas Boas. Robustness of quantum discord to sudden death. *Physical Review A*, 80:024103, 2009.

A Miscellany

Definition A.1 (Lipschitz constant)**.** *Let $f : \mathfrak{X} \to \mathfrak{Y}$ be a function from the metric space $(\mathfrak{X}, d_{\mathfrak{X}})$ to the metric space $(\mathfrak{Y}, d_{\mathfrak{Y}})$. Then, the Lipschitz constant of f is defined as*

$$\sup_{x_1, x_2 \in \mathfrak{X}} \frac{d_{\mathfrak{Y}}(f(x_1), f(x_2))}{d_{\mathfrak{X}}(x_1, x_2)}.$$

If the above quantity is not bounded, the constant is not defined.

Lemma A.1 (Lemma IV.3 in [ADHW09])**.** *For any matrix $X^{A\overline{A}R}$ and for $\mathrm{d}U$ the Haar measure over unitaries, we have the following property:*

$$\int_U \left(U_A \otimes U_{\overline{A}} \otimes \mathbb{I}^R\right) X^{A\overline{A}R} \left(U_A^\dagger \otimes U_{\overline{A}}^\dagger \otimes \mathbb{I}^R\right) \mathrm{d}U = \alpha_+ (X) \otimes \Pi_+^A + \alpha_- (X) \otimes \Pi_-^A$$

where

$$\alpha_\pm (X) = \frac{\mathrm{Tr}_{A\overline{A}}\left[X(\Pi_\pm^A \otimes \mathbb{I}^R)\right]}{\mathrm{rank}\left(\Pi_\pm^A\right)} \qquad \Pi_\pm^A = \frac{1}{2}\left(\mathbb{I}^{A\overline{A}} \pm F_{\overline{A}}^A\right) \qquad \mathrm{rank}\left(\Pi_\pm^A\right) = \frac{|A|(|A| \pm 1)}{2}.$$

Lemma A.2 (Operator Chernoff bound [AW02])**.** *Let $X_1, \ldots, X_M$ be i.i.d. random variables taking values in the operators $\mathrm{Pos}(\mathsf{A})$, with $0 \leqslant X_j \leqslant \mathbb{I}$, with $A = \mathbb{E}X_j \geqslant \alpha\mathbb{I}$, and let $0 < \eta \leqslant 1/2$. Then*

$$\Pr\left\{\frac{1}{M}\sum_{j=1}^M X_j \nleqslant (1+\eta)A\right\} \leqslant 2|A|\exp\left(-M\frac{\alpha\eta^2}{2\ln 2}\right). \tag{A.1}$$

Lemma A.3 (Trace distance versus Euclidean norm for pure states (See, e.g. [NC00].))**.** *Consider any two quantum states $|\varphi\rangle, |\tilde{\varphi}\rangle$ with density associated operators $\varphi, \tilde{\varphi}$ respectively. We can relate the 1-norm distance between the operators to the 2-norm distance of the states as follows,*

$$\|\varphi - \tilde{\varphi}\|_1 \leq 2\,\||\varphi\rangle - |\tilde{\varphi}\rangle\|_2.$$

Lemma A.4 (A bound for the 1-norm in terms of conditional entropy [Ren05, Dup09])**.** *Let $\rho \in \mathrm{L}(A)$ be any Hermitian operator and let $\gamma \in \mathrm{Pos}(A)$ be a positive definite operator. Then,*

$$\|\rho\|_1 \leqslant \sqrt{\mathrm{Tr}\,[\gamma]\,\mathrm{Tr}\left[\left(\gamma^{-1/4}\rho\gamma^{-1/4}\right)^2\right]}.$$

Proof.

$$
\begin{aligned}
\|\rho\|_1 &= \max_{U \in \mathcal{U}(A)} |\mathrm{Tr}\,[U\rho]| \\
&= \max_{U \in \mathcal{U}(A)} \left|\mathrm{Tr}\left[\left(\gamma^{1/4}U\gamma^{1/4}\right)\left(\gamma^{-1/4}\,\rho\,\gamma^{-1/4}\right)\right]\right| \\
&\leqslant \max_{U \in \mathcal{U}(A)} \sqrt{\mathrm{Tr}\left[\left(\gamma^{1/4}U\gamma^{1/4}\right)\left(\gamma^{1/4}U^\dagger\gamma^{1/4}\right)\right]\mathrm{Tr}\left[\gamma^{-1/4}\,\rho\,\gamma^{-1/2}\,\rho^\dagger\,\gamma^{-1/4}\right]} \\
&= \sqrt{\max_{U \in \mathcal{U}(A)} \mathrm{Tr}\left[\gamma^{1/2}U\gamma^{1/2}U^\dagger\right]\mathrm{Tr}\left[\gamma^{-1/4}\,\rho\,\gamma^{-1/2}\,\rho^\dagger\,\gamma^{-1/4}\right]} \\
&= \sqrt{\mathrm{Tr}\,[\gamma]\,\mathrm{Tr}\left[\gamma^{-1/4}\,\rho\,\gamma^{-1/2}\,\rho^\dagger\,\gamma^{-1/4}\right]},
\end{aligned}
$$

where the first equality is an application of Lemma I.6 in [Dup09] and the inequality results from an application of Cauchy-Schwarz, and the maximizations are over all unitaries on A. The last equality follows from

$$
\begin{aligned}
\max_{U \in \mathcal{U}(A)} \mathrm{Tr} \left[\gamma^{1/2} U \gamma^{1/2} U^\dagger \right] &\leqslant \max_{U \in \mathcal{U}(A)} \sqrt{\mathrm{Tr} \left[\gamma \right] \mathrm{Tr} \left[U \gamma^{1/2} U^\dagger U \gamma^{1/2} U^\dagger \right]} \\
&= \mathrm{Tr} \left[\gamma \right] \\
&\leqslant \max_{U \in \mathcal{U}(A)} \mathrm{Tr} \left[\gamma^{1/2} U \gamma^{1/2} U^\dagger \right].
\end{aligned}
$$

$\square$