From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking

Omar Fawzi * Patrick Hayden *† Pranab Sen ‡ *

April 8, 2011

Abstract

The existence of quantum uncertainty relations is the essential reason that some classically impossible cryptographic primitives become possible when quantum communication is allowed. One operational manifestation of these uncertainty relations is a purely quantum effect referred to as *information locking* [DHL+04]. A locking scheme can be viewed as a cryptographic protocol in which a uniformly random n-bit message is encoded in a quantum system using a classical key of size much smaller than n. Without the key, no measurement of this quantum state can extract more than a negligible amount of information about the message, in which case the message is said to be "locked". Furthermore, knowing the key, it is possible to recover, that is "unlock", the message.

In this paper, we make the following contributions by exploiting a connection between uncertainty relations and low-distortion embeddings of ℓ_2 into ℓ_1.

- We introduce the notion of *metric uncertainty relations* and connect it to low-distortion embeddings of ℓ_2 into ℓ_1. A metric uncertainty relation also implies an entropic uncertainty relation.
- We prove that random bases satisfy uncertainty relations with a stronger definition and better parameters than previously known. Our proof is also considerably simpler than earlier proofs. We apply this result to show the existence of locking schemes with key size independent of the message length.
- We give *efficient* constructions of bases satisfying metric uncertainty relations. The bases defining these metric uncertainty relations are computable by quantum circuits of almost linear size. This leads to the first explicit construction of a strong information locking scheme. Moreover, we present a locking scheme that can in principle be implemented with current technology. These constructions are obtained by adapting an explicit norm embedding due to Indyk [Ind07] and an extractor construction of Guruswami, Umans and Vadhan [GUV09].
- We apply our metric uncertainty relations to exhibit communication protocols that perform equality testing of n-qubit states. We prove that this task can be performed by a single message protocol using $O(\log(1/\epsilon))$ qubits and n bits of communication, where ϵ is an error parameter. We also give a single message protocol that uses $O(\log^2 n)$ qubits, where the computation of the sender is efficient.

Keywords: uncertainty relations, information locking, low-distortion norm embedding, quantum identification, quantum equality testing, randomness extractors, quantum cryptography.

*School of Computer Science, McGill University, Montréal, Québec, Canada
†Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada
‡School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India

1 Introduction

Uncertainty relations express the fundamental incompatibility of certain measurements in quantum mechanics. Far from just being puzzling constraints on our ability to know the state of a quantum system, uncertainty relations are arguably at the heart of why some classically impossible cryptographic primitives become possible when quantum communication is allowed. For example, so-called *entropic* uncertainty relations introduced in [BBM75, Deu83] are the main ingredients of security proofs in the bounded and noisy quantum storage models [DFSS05, DFR$^+$07, KWW09]. A simple example of an entropic uncertainty relation was given by Maassen and Uffink [MU88]. Let $\mathcal{B}_+$ denote a "rectilinear" or computational basis of $\mathbb{C}^2$ and $\mathcal{B}_\times$ be a "diagonal" or Hadamard basis and let $\mathcal{B}_{+^n}$ and $\mathcal{B}_{\times^n}$ be the corresponding bases obtained on the tensor product space $(\mathbb{C}^2)^{\otimes n}$. Then we have that for *any* quantum state on n qubits described by a unit vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$, the average measurement entropy satisfies

$$\frac{1}{2}\left(\mathbf{H}(p_{\mathcal{B}_{+^n},|\psi\rangle}) + \mathbf{H}(p_{\mathcal{B}_{\times^n},|\psi\rangle})\right) \geq \frac{n}{2} \tag{1}$$

where $p_{\mathcal{B},|\psi\rangle}$ denotes the outcome probability distribution when $|\psi\rangle$ is measured in basis $\mathcal{B}$ and $\mathbf{H}$ denotes the Shannon entropy. Equation (1) expresses the fact that measuring in a random basis $\mathcal{B}_K$ where $K \in_u \{+^n, \times^n\}$ produces an outcome that has some uncertainty irrespective of the state being measured.

A surprising application of entropic uncertainty relations is the effect known as *information locking* [DHL$^+$04] (see also [Leu09]). Suppose Alice holds a uniformly distributed random n-bit string X. She chooses a random basis $K \in_u \{+^n, \times^n\}$ and encodes X in the basis $\mathcal{B}_K$. This random quantum state $\mathcal{E}(X, K)$ is then given to Bob. How much information about X can Bob, who does not know K, extract from this quantum state via a measurement? To better appreciate the quantum case, observe that if X were encoded in a classical state $\mathcal{E}_c(X, K)$, then $\mathcal{E}_c(X, K)$ would "hide" at most one bit about X; more precisely, the mutual information $\mathbf{I}(X; \mathcal{E}_c(X, K)) \geq n - 1$. For the quantum encoding $\mathcal{E}$, one can show that for *any measurement* that Bob applies on $\mathcal{E}(X, K)$ whose outcome is denoted I, we have $\mathbf{I}(X; I) \leq n/2$ [DHL$^+$04]. The $n/2$ missing bits of information about X are said to be *locked* in the quantum state $\mathcal{E}(X, K)$. If Bob had access to K, then X can be easily obtained from $\mathcal{E}(X, K)$: The one-bit key K can be used to *unlock* $n/2$ bits about X.

A natural question is whether it is possible to lock more than $n/2$ bits in this way. In order to achieve this, the key K has to be chosen from a larger set. In terms of uncertainty relations, this means that we need to consider more than two bases to achieve an average measurement entropy larger than $n/2$ (equation (1)). The authors of [HLSW04] show the existence of an encoding that locks $n - 3$ bits about $X \in \{0, 1\}^n$ using a key $K \in \{0, 1\}^{4 \log n}$. They prove this result by showing that *random bases* satisfy entropic uncertainty relations of the form (1) with more than two measurements. Recently, [Dup10, DFHL10] prove that random encodings exhibit a locking behaviour in a stronger sense and that it is possible to lock up to $n - \delta$ bits for any arbitrarily small constant δ while still using a key of $O(\log n)$ bits. In this setting, a locking scheme can be viewed as a cryptographic protocol that uses a key of size $O(\log n)$ to encrypt a random classical n-bit message in a quantum state. Knowing the key, it is possible to recover the message from this quantum state. However, without the key, for any measurement, the distribution of the message X conditioned on the outcome I of the measurement is close to the prior distribution of X in total variation distance.

It should be noted that entropic uncertainty relations of the form of (1) with $t > 2$ measurements are not well understood. A natural generalization of rectilinear $+^n$ and diagonal bases $\times^n$ called *mutually unbiased bases* does not work as well for more than two measurements. In fact, it was shown in [BW07, Amb09] that there are up to $t = 2^{n/2}$ mutually unbiased bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ that only satisfy an average measurement entropy of $n/2$, which is only as good as what can be achieved with two measurements (1). To achieve an average measurement entropy of $(1-\epsilon)n$ for small ϵ while keeping the number of bases subexponential in n, the only known constructions are probabilistic and computationally inefficient [HLSW04]. Furthermore, standard derandomization techniques are not known to work in this setting. For example, unitary designs [DCEL09] define an exponential number of bases. Moreover, using a δ-biased subset of the set of Pauli matrices [AS04, DD10] fails to produce a locking scheme unless the subset has a size of close to 2^n (see Appendix D).

1.1 Our results

In this paper, we study uncertainty relations in the light of a connection with low-distortion embeddings of $(\mathbb{C}^d, \ell_2)$ into $(\mathbb{C}^{d'}, \ell_1)$. The intuition behind this connection is very simple. Consider the measurements defined by a set of orthonormal bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ of $(\mathbb{C}^2)^{\otimes n}$. The bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{t-1}\}$ verify an uncertainty relation if for every n-qubit state $|\psi\rangle$ and "most" bases $\mathcal{B}_k$, the vector representing $|\psi\rangle$ in $\mathcal{B}_k$ is "spread". One way of quantifying the spread of a vector is by its ℓ_1 norm, i.e., the sum of the absolute values of its components. A vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ of unit ℓ_2 norm is well spread if its ℓ_1 norm is close to its maximal value of $\sqrt{2^n}$. For technical reasons, it turns out that the relevant norm for us is not the ℓ_1 norm but rather a closely related norm called $\ell_1(\ell_2)$.

This connection suggests measuring the uncertainty of a distribution by taking a marginal and measuring its closeness to the uniform distribution. This is a stronger requirement than having large Shannon entropy and it leads to the definition of *metric uncertainty relations* (Definition 2.1). Using standard techniques from asymptotic geometric analysis, we prove the existence of strong metric uncertainty relations (Theorem 2.5). This result can be seen as a strengthening of Dvoretzky's theorem [Dvo61, Mil71] for the special case of the $\ell_1(\ell_2)$ norm. In addition to giving a stronger statement with better parameters, our analysis of the uncertainty relations satisfied by random bases is considerably simpler than earlier proofs [HLSW04, DFHL10]. In particular, for large n, we prove the existence of entropic uncertainty relations with average measurement entropy strictly increasing with the number of measurements. This result also leads to better results on the existence of locking schemes (Corollary 3.4). We also show in Theorem 3.7 how to use these locking schemes to build quantum hiding fingerprints as defined by Gavinsky and Ito [GI10].

Moreover, adapting an explicit low-distortion embedding of $(\mathbb{R}^d, \ell_2)$ to $(\mathbb{R}^{d'}, \ell_1)$ with $d' = d^{1+o(1)}$ due to Indyk [Ind07], we obtain explicit bases of $(\mathbb{C}^2)^{\otimes n}$ that verify strong metric uncertainty relations for a number of bases that is polynomial in n. Measuring in these bases can be performed by polynomial size quantum circuits. The main new ingredient that makes our "quantization" of Indyk's construction verify stronger uncertainty relations than do general mutually unbiased bases is the additional use of strong permutation extractors, which are a special kind of randomness extractor. A strong permutation extractor (Definition 2.14) is a small family of permutations of bit strings with the property that for any probability distribution on input bit strings with high min-entropy, applying a typical permutation from the family to the input induces an almost uniform probability distribution on a prefix of the output bits. Our construction of efficiently computable bases satisfying strong metric uncertainty relations involves an alternating application of approximately mutually unbiased bases and strong permutation extractors. Our approximately mutually unbiased bases consist of sets of single-qubit Hadamard gates. Moreover, both the permutations and their inverses have to be efficiently computable for our construction. We build such strong permutation extractors using the results of Guruswami, Umans and Vadhan [GUV09].

We use these uncertainty relations to build an explicit locking scheme whose encoding and decoding operations can be performed by circuits of size almost linear in the length of the message. Moreover, we also obtain a locking scheme where both the encoding and decoding operations consist of a classical computation with polynomial runtime and a quantum computation using only a small number of single-qubit Hadamard gates (Corollary 3.5). Performing these quantum operations can be done using the same technology as implementing the BB84 quantum key distribution protocol [BB84], but as was the case for BB84, our idealized scheme must still be made robust to noise and imperfect devices. It should be noted that this simple scheme requires a ciphertext that is longer than the message. On the way to obtaining this result, we prove a min-entropy uncertainty relation on a sparse set of BB84 states that might be of independent interest (Lemma 2.13 with Lemma 2.12). This locking scheme can be used to obtain string commitment protocols [BCH$^+$08] that are efficient in terms of computation and communication.

We also give an application of our uncertainty relations to a problem called quantum identification. Quantum identification is a communication task for two parties Alice and Bob, where Alice is given a pure quantum state $|\psi\rangle$ and Bob wants to simulate measurements of the form $\{|\varphi\rangle\langle\varphi|, \mathbb{1} - |\varphi\rangle\langle\varphi|\}$ on $|\psi\rangle$ where $|\varphi\rangle$ is a pure quantum state. This task can be seen as a quantum analogue of the problem of equality testing [AD89, KN97] where Alice and Bob hold n-bit strings x and y and Bob wants to determine whether $x = y$ using a one-way classical channel from Alice to Bob. Hayden and Winter [HW10] showed that classical communication alone is useless for quantum identification. However, having access to a negligible amount of quantum communication makes classical communication useful. Their proof is non-explicit. Here, we describe an efficient encoding circuit that also uses less quantum communication: it allows the identification of an n-qubit state by communicating only a single message of $O(\log^2 n)$ qubits and n classical bits.

1.2 Other related work

Aubrun, Szarek and Werner [ASW10b, ASW10a] also used a connection between low-distortion embeddings and quantum information. They show in [ASW10b] that the existence of large subspaces of highly entangled states

	Inf. leakage	Size of key	Size of ciphertext	Efficient ?
[DHL+04]	$n/2$	1	n	yes
[HLSW04]	3	$4\log(n)$	n	no
[DFHL10]	ϵn	$2\log(n/\epsilon^2)+O(1)$	n	no
Corollary 3.4	ϵn	$2\log(1/\epsilon)+O(\log\log(1/\epsilon))$	$n+2\lceil\log(9/\epsilon)\rceil$	no
Corollary 3.4	ϵn	$4\log(1/\epsilon)+O(\log\log(1/\epsilon))$	n	no
Corollary 3.5	ϵn	$O_\delta(\log(n/\epsilon))$	$(4+\delta)\cdot n$, with $\delta>0$	yes
Corollary 3.5	ϵn	$O(\log(n/\epsilon)\log(n))$	n	yes

Table 1: Comparison of different locking schemes. n is the number of bits of the message. The information leakage and the size of the key are measured in bits and the size of the ciphertext in qubits. Efficient locking schemes have encoding and decoding quantum circuits of size polynomial in n. The locking schemes of the first and next to last actually have encoding circuits that are implementable with current technology; they only use classical computations and simple single-qubit transformations. It should be noted that our locking definition is stronger than all the previous definitions. Note that the variable ϵ can depend on n. For example, one can take $\epsilon=\eta/n$ to make the information leakage arbitrarily small. The symbol $O(\cdot)$ refers to constants independent of ϵ and n, but there is a dependence on δ for the next to last row.

follows from Dvoretzky's theorem for the Schatten p-norm[1] for $p>2$. This in turns shows the existence of channels that violate additivity of minimum output p-Rényi entropy as was previously demonstrated by [HW08]. Using a more delicate argument [ASW10a], they are also able to recover Hastings' [Has09] counterexample to the additivity conjecture.

In a cryptographic setting, Damgård, Pedersen and Salvail [DPS04] used ideas related to locking to develop quantum ciphers that have the property that the key used for encryption can be recycled. In [DPS05], they construct a quantum key recycling scheme (see also [OH05]) with near optimal parameters by encoding the message together with its authentication tag using a full set of mutually unbiased bases.

1.3 Notation

We use the following notation throughout the paper. For a positive integer n, we define $[n]=\{0,\dots,n-1\}$. Random variables are usually denoted by capital letters $X,K,\dots$, while p_X denotes the distribution of X, i.e., $\mathbf{P}\{X=x\}=p_X(x)$. The notation $X\sim p$ means that X has distribution p. unif(S) is the uniform distribution on the set S. To measure the distance between probability distributions on a finite set $\mathcal{X}$, we use the total variation distance or trace distance $\Delta(p,q)=\frac{1}{2}\sum_{x\in\mathcal{X}}|p(x)-q(x)|$. We will also write $\Delta(X,Y)$ for $\Delta(p_X,p_Y)$. When $\Delta(X,Y)\le\epsilon$, we say that X is ϵ-close to Y. A useful characterization of the trace distance is $\Delta(p,q)=\max_{X\sim p,Y\sim q}\mathbf{P}\{X=Y\}$ (this equality is known as Doeblin's coupling lemma). Another useful measure of closeness between distributions is the fidelity $F(p,q)=\sum_{x\in\mathcal{X}}\sqrt{p(x)q(x)}$. We have the following relation [FvdG99] between the fidelity and the trace distance

$$1-F(p,q)\le\Delta(p,q)\le\sqrt{1-F(p,q)^2}. \tag{2}$$

The Shannon entropy of a distribution p on $\mathcal{X}$ is defined as $\mathbf{H}(p)=-\sum_{x\in\mathcal{X}}p(x)\log p(x)$ where the $\log$ is taken here and throughout the paper to be base two. We will also write $\mathbf{H}(X)$ for $\mathbf{H}(p_X)$. The mutual information between two random variables X and Y is defined by $\mathbf{I}(X;Y)=\mathbf{H}(X)+\mathbf{H}(Y)-\mathbf{H}(X,Y)$. The min-entropy of a distribution p is defined as $\mathbf{H}_{\min}(p)=-\log\max_x p(x)$. We say that a random variable X is a k-source if $\mathbf{H}_{\min}(X)\ge k$. To refer to the i-th component of a vector $v\in\mathbb{R}^n$, we usually write v_i except when v already has a subscript, in which case we use $v(i)$. The weight of a binary vector v (number of ones) is denoted by $\mathbf{w}(v)$ and the Hamming distance between two binary vector v,v' (number of components that are different) is written as $d_H(v,v')$.

The quantum systems we consider are denoted $A,B,C\dots$ and are identified with their Hilbert spaces. The dimension of a Hilbert space A is denoted by d_A. Every Hilbert space A comes with a preferred orthonormal basis $\{|a\rangle^A\}_{a\in[d_A]}$ that we call the computational basis. The elements of this basis are labeled by integers from 0 to d_A-1. For a Hilbert space of the form $\mathbb{C}^{2^n}$, this canonical basis will also be labeled by strings in $\{0,1\}^n$. $A\simeq B$ means that the Hilbert spaces A and B are isomorphic. For a state $|\psi\rangle\in A$, $p_{|\psi\rangle}$ is the distribution of the outcomes

[1]The Schatten p-norm of a matrix M is defined as the ℓ_p norm of a vector of singular values of M.

of the measurement of $|\psi\rangle$ in the basis $\{|a\rangle\}$. We have $p_{|\psi\rangle}(a) = |\langle a|\psi\rangle|^2$. Similarly, for a mixed state ρ, we define $p_\rho(a) = \mathrm{tr}[|a\rangle\langle a|\rho]$. The tensor product $A \otimes B$ is sometimes denoted simply AB. $\mathcal{S}(A)$ is the set of density operators acting on A. The Hilbert space on which a density operator $\rho \in \mathcal{S}(A)$ acts is denoted by a superscript, as in ρ^A. Partial traces are abbreviated by omitting superscripts so that $\rho^A \stackrel{\text{def}}{=} \mathrm{tr}_B\, \rho^{AB}$. This notation is also used for pure states $|\psi\rangle^A \in A$. The density operator associated with a pure state is abbreviated by omitting the ket and bra $\psi \stackrel{\text{def}}{=} |\psi\rangle\langle\psi|$. The symbol $\mathbb{1}^A$ is reserved for the identity map on A. If U is a unitary acting on A, and $|\psi\rangle$ a state in $A \otimes B$, we sometimes use $U|\psi\rangle$ to denote the state $(U \otimes \mathbb{1}^B)|\psi\rangle$.

The trace distance between density operators acting on A is defined by $\Delta(\rho, \sigma) = \frac{1}{2} \mathrm{tr} \sqrt{(\rho - \sigma)^2}$. The von Neuman entropy of a quantum state ρ^A is defined by $\mathbf{H}(\rho^A) = -\mathrm{tr}\, \rho \log \rho$. It will also be denoted $\mathbf{H}(A)_\rho$. For a bipartite state $\rho^{AB} \in \mathcal{S}(AB)$, the quantum mutual information $\mathbf{I}(A; B)_\rho = \mathbf{H}(A)_\rho + \mathbf{H}(B)_\rho - \mathbf{H}(A, B)_\rho$.

2 Uncertainty relations

Outline of the section In this section, we start by introducing uncertainty relations and setting up some notation (Section 2.1). Then we define metric uncertainty relations in Section 2.2. In Section 2.3, we prove the existence of strong metric uncertainty relations. Explicit constructions are given in Section 2.4.

2.1 Background

Consider a set of orthonormal bases $\mathcal{B} = \{\mathcal{B}_0, \ldots, \mathcal{B}_{t-1}\}$ of the Hilbert space C. Each basis $\mathcal{B}_k = (v_0^k, \ldots, v_{d_C-1}^k)$ defines a measurement on C. The outcomes of these measurements are indexed by $x \in [d_C]$. The outcome distribution $p_{\mathcal{B}_k, |\psi\rangle}$ when the measurement is performed on the state $|\psi\rangle \in C$ is defined by $p_{\mathcal{B}_k,|\psi\rangle}(x) = |\langle v_x^k|\psi\rangle|^2$ for all $x \in [d_C]$. An uncertainty relation for a set of orthonormal bases $\mathcal{B} = \{\mathcal{B}_0, \ldots, \mathcal{B}_{t-1}\}$ expresses the property that for any state $|\psi\rangle \in C$, there are some measurements in $\mathcal{B}$ whose outcomes given state $|\psi\rangle$ have some uncertainty. A common way of quantifying this uncertainty is by using the Shannon entropy. The set of bases $\mathcal{B}$ is said to satisfy an *entropic uncertainty relation* if there exists a positive number h such that for all states $|\psi\rangle \in C$,

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{\mathcal{B}_k,|\psi\rangle}) \geq h.$$

For example, for a qubit space ($\dim C = 2$), consider the two bases $\mathcal{B}_0 = (|0\rangle, |1\rangle)$ and $\mathcal{B}_1 = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$. It was shown in [MU88] that these two bases satisfy the following entropic uncertainty relation: for all states $|\psi\rangle \in C$,

$$\frac{1}{2}\left(\mathbf{H}(p_{\mathcal{B}_0,|\psi\rangle}) + \mathbf{H}(p_{\mathcal{B}_1,|\psi\rangle})\right) \geq \frac{1}{2}.$$

Note that this uncertainty relation cannot be improved: For any bases $\mathcal{B}_0, \mathcal{B}_1$, one can always choose a state $|\psi_0\rangle$ that is aligned with one of the vectors of $\mathcal{B}_0$ so that $\mathbf{H}(p_{\mathcal{B}_0,|\psi_0\rangle}) = 0$, in which case $\frac{1}{2}\left(\mathbf{H}(p_{\mathcal{B}_0,|\psi_0\rangle}) + \mathbf{H}(p_{\mathcal{B}_1,|\psi_0\rangle})\right) \leq \frac{1}{2}$.

It is more convenient here to talk about uncertainty relations for a set of unitary transformations. Let $\{|x\rangle^C\}_x$ be the computational basis of C. We associate to the unitary transformation U the basis $\{U^\dagger|x\rangle\}_x$. On a state $|\psi\rangle$, the outcome distribution is described by

$$p_{U|\psi\rangle}(x) = |\langle x|U|\psi\rangle|^2.$$

As can be seen from this equation, we can equivalently talk about measuring the state $U|\psi\rangle$ in the computational basis. An entropic uncertainty relation for $U_0, \ldots, U_{t-1}$ can be written as

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geq h. \tag{3}$$

Entropic uncertainty relations have been used in proving the security of cryptographic protocols in the bounded and noisy quantum storage models [DFR+07, KWW09]. For more details on entropic uncertainty relations and their applications, see the recent survey [WW10].

2.2 Metric uncertainty relations

Here, instead of using the entropy as a measure of uncertainty, we use closeness to the uniform distribution. In other words, we are interested in sets of unitary transformations $U_0, \ldots, U_{t-1}$ that for all $|\psi\rangle \in C$ satisfy

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi\rangle}, \text{unif}([d_C])\right) \leq \epsilon$$

for some $\epsilon \in (0,1)$. $\Delta(p,q)$ refers to the total variation distance between distributions p and q. This condition is very strong, in fact too strong for our purposes, and we will see that a weaker definition is sufficient to imply entropic uncertainty relations. Let $C = A \otimes B$. (For example, if C consists of n qubits, A might represent the first $n - \log n$ qubits and B the last $\log n$ qubits.) Moreover, let the computational basis for C be of the form $\{|a\rangle^A \otimes |b\rangle^B\}_{a,b}$ where $\{|a\rangle\}$ and $\{|b\rangle\}$ are the computational bases of A and B. Instead of asking for the outcome of the measurement on the computational basis of the whole space to be uniform, we only require that the outcome of a measurement of the A system in its computational basis $\{|a\rangle\}$ be close to uniform. More precisely, we define for $a \in [d_A]$,

$$p^A_{U_k|\psi\rangle}(a) = \sum_{b=0}^{d_B-1} |\langle a|^A \langle b|^B U_k |\psi\rangle|^2.$$

We can then define a metric uncertainty relation. Naturally, the larger the A system, the stronger the uncertainty relation for a fixed B system.

Definition 2.1 (Metric uncertainty relation)**.** *Let A and B be Hilbert spaces. We say that a set $\{U_0, \ldots, U_{t-1}\}$ of unitary transformations on AB satisfies an ϵ-metric uncertainty relation on A if for all states $|\psi\rangle \in AB$,*

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \leq \epsilon. \tag{4}$$

Remark. Observe that this implies that (4) also holds for mixed states: for any $\psi \in \mathcal{S}(A \otimes B)$, $\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k \psi U_k^\dagger}, \text{unif}([d_A])\right) \leq \epsilon$. □

Metric uncertainty relations imply entropic uncertainty relations In the next proposition, we show that a metric uncertainty relation is also an entropic uncertainty relation. It is worth stressing that there are no restrictions on measurements.

Proposition 2.2. *Let $\epsilon \in (0, \frac{1}{2e})$ and $\{U_0, \ldots, U_{t-1}\}$ be a set of unitaries on AB verifying an ϵ-metric uncertainty relation on A:*

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \leq \epsilon.$$

Then

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geq (1-2\epsilon)\log d_A - \eta(\epsilon).$$

where $\eta(\epsilon) = -2\epsilon\ln(2\epsilon)$.

Proof Recall that the distribution $p^A_{U_k|\psi\rangle}$ (see equation (4) for a definition) on $[d_A]$ is a marginal of the distribution $p_{U_k|\psi\rangle}$. Thus $\mathbf{H}(p_{U_k|\psi\rangle}) \geq \mathbf{H}(p^A_{U_k,|\psi\rangle})$. Using Fannes' inequality [Fan73], we have for all k

$$\begin{aligned}\mathbf{H}(p^A_{U_k,|\psi\rangle}) &\geq \log d_A - 2\Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right)\log d_A - \eta(\epsilon) \\ &\geq (1-2\epsilon)\log d_A - \eta(\epsilon).\end{aligned}$$

□

Explicit link to low-distortion embeddings Even though we do not explicitly use the link to low-distortion embeddings, we describe the connection as it might have other applications. In the definition of metric uncertainty relations, the distance between distributions was computed using the trace distance. The connection to low-distortion metric embeddings is clearer when we measure closeness of distributions using fidelity. We have

$$\begin{aligned} F\Big(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\Big) &= \frac{1}{\sqrt{d_A}} \sum_{a=0}^{d_A-1} \sqrt{p^A_{U_k|\psi\rangle}(a)} \\ &= \frac{1}{\sqrt{d_A}} \sum_{a=0}^{d_A-1} \sqrt{\sum_{b=0}^{d_B-1} |\langle a|^A \langle b|^B U_k|\psi\rangle|^2} \\ &= \frac{1}{\sqrt{d_A}} \|U_k|\psi\rangle\|_{\ell_1^A(\ell_2^B)} \end{aligned}$$

where the norm $\ell_1^A(\ell_2^B)$ is defined by

Definition 2.3 ($\ell_1(\ell_2)$ norm)**.** *For a state $|\psi\rangle = \sum_{a,b} \alpha_{a,b} |a\rangle^A |b\rangle^B$,*

$$\big\||\psi\rangle\big\|_{\ell_1^A(\ell_2^B)} = \sum_a \big\|\{\alpha_{a,b}\}_b\big\|_2 = \sum_a \sqrt{\sum_b |\alpha_{a,b}|^2}.$$

We use $\|\cdot\|_{12} \stackrel{def}{=} \|\cdot\|_{\ell_1^A(\ell_2^B)}$ when the systems A and B are clear from the context.

Observe that this definition of norm depends on the choice of the computational basis. The $\ell_1^A(\ell_2^B)$ norm will always be taken with respect to the computational bases.

For $\{U_0, \dots, U_{t-1}\}$ to satisfy an uncertainty relation, we want

$$\frac{1}{t} \sum_k \frac{1}{\sqrt{d_A}} \|U_k|\psi\rangle\|_{\ell_1^A(\ell_2^B)} \geq 1 - \epsilon.$$

This expression can be rewritten by introducing a new register K that holds the index k. We get for all $|\psi\rangle$

$$\left\| \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle^C |k\rangle^K \right\|_{\ell_1^{AK}(\ell_2^B)} \geq (1-\epsilon)\sqrt{t \cdot d_A}. \tag{5}$$

Using the Cauchy-Schwarz inequality, we have that for all $|\psi\rangle$,

$$\left\| \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle^C |k\rangle^K \right\|_{\ell_1^{AK}(\ell_2^B)} \leq \sqrt{t \cdot d_A} \left\| \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle^C |k\rangle^K \right\|_2 = \sqrt{t \cdot d_A}. \tag{6}$$

Rewriting (5) and (6) as

$$(1-\epsilon) \leq \frac{1}{\sqrt{t \cdot d_A}} \cdot \frac{\left\| \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle^C |k\rangle^K \right\|_{\ell_1^{AK}(\ell_2^B)}}{\left\| \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle^C |k\rangle^K \right\|_2} \leq 1,$$

we see that the image of C by the linear map $|\psi\rangle \mapsto \frac{1}{\sqrt{t}} \sum_k U_k |\psi\rangle \otimes |k\rangle$ is an almost Euclidean subspace of $(A \otimes K \otimes B, \ell_1^{AK}(\ell_2^B))$. In other words, as the map $|\psi\rangle \mapsto \frac{1}{\sqrt{t}} \sum_k U_k|\psi\rangle \otimes |k\rangle$ is an isometry (in the ℓ_2 sense), it is an embedding of (C, ℓ_2) into $(AKB, \ell_1^{AK}(\ell_2^B))$ with distortion $1/(1-\epsilon)$ [Mat02].

Observe that a general low-distortion embedding of (C, ℓ_2) into $(AKB, \ell_1^{AK}(\ell_2^B))$ does not necessarily give a metric uncertainty relation as it need not be of the form $|\psi\rangle \mapsto \frac{1}{\sqrt{t}} \sum_k U_k|\psi\rangle \otimes |k\rangle$. When $t = 2$, a metric uncertainty relation is related to the notion of Kashin decomposition [Kas77]; see also [Pis89, Sza06].

A remark on the composition of metric uncertainty relations There is a natural way of building an uncertainty relation for a Hilbert space from uncertainty relations on smaller Hilbert spaces. This composition property is also important for the cryptographic applications of metric uncertainty relations presented in the second half of the paper, in which setting it ensures the security of parallel composition of locking-based encryption.

Proposition 2.4. *Consider Hilbert spaces A_1, A_2, B_1, B_2. For $i \in \{0,1\}$, let $\{U^{(i)}_{k_i}\}_{k_i \in [t_i]}$ be a set of unitary transformations of $A_i \otimes B_i$ verifying an ϵ-metric uncertainty relation on A_i. Then, $\{U^{(1)}_{k_1} \otimes U^{(2)}_{k_2}\}_{k_1,k_2 \in [t_1] \times [t_2]}$ verifies a 2ϵ-metric uncertainty relation on $A_1 \otimes A_2$.*

Proof Let $|\psi\rangle \in (A_1 \otimes B_1) \otimes (A_2 \otimes B_2)$ and let p_{k_1,k_2} denote the distribution obtained by measuring $U^{(1)}_{k_1} \otimes U^{(1)}_{k_2} |\psi\rangle$ in the computational basis of $A_1 \otimes A_2$. Our objective is to show that

$$\frac{1}{t_1 t_2} \sum_{k_1 \in [t_1], k_2 \in [t_2]} \Delta(p_{k_1,k_2}, \text{unif}([d_{A_1}] \times [d_{A_2}])) \leq 2\epsilon. \tag{7}$$

We have

$$\begin{aligned}
\Delta(p_{k_1,k_2}, \text{unif}([d_{A_1}] \times [d_{A_2}])) &= \frac{1}{2} \sum_{a_1,a_2} \left| p_{k_1,k_2}(a_1,a_2) - \frac{1}{d_{A_1} d_{A_2}} \right| \\
&\leq \frac{1}{2} \sum_{a_1,a_2} \left| p_{k_1,k_2}(a_1,a_2) - \frac{p_{k_1,k_2}(a_1)}{d_{A_2}} \right| + \frac{1}{2} \sum_{a_1,a_2} \left| \frac{p_{k_1,k_2}(a_1)}{d_{A_2}} - \frac{1}{d_{A_1} d_{A_2}} \right| \\
&= \frac{1}{2} \sum_{a_1} p^{A_1}_{k_1,k_2}(a_1) \sum_{a_2} \left| \frac{p_{k_1,k_2}(a_1,a_2)}{p^{A_1}_{k_1,k_2}(a_1)} - \frac{1}{d_{A_2}} \right| + \frac{1}{2} \sum_{a_1} \left| p^{A_1}_{k_1,k_2}(a_1) - \frac{1}{d_{A_1}} \right|
\end{aligned} \tag{8}$$

where $p^{A_1}_{k_1,k_2}(a_1) \stackrel{\text{def}}{=} \sum_{a_2} p_{k_1,k_2}(a_1,a_2)$ is the outcome distribution of measuring the A_1 system of $U^{(1)}_{k_1} \otimes U^{(2)}_{k_2} |\psi\rangle$. The distribution p_{k_1,k_2} can also be seen as the outcome of measuring the mixed state

$$U^{(1)}_{k_1} \psi^{A_1 B_1} U^{(1)\dagger}_{k_1}$$

in the computational basis $\{|a_1\rangle\}$. Thus, we have for any $k_2 \in [t_2]$,

$$\frac{1}{t_1} \sum_{k_1} \Delta\left(p^{A_1}_{k_1,k_2}, \text{unif}([d_{A_1}])\right) \leq \epsilon.$$

Moreover, for $a_1 \in [d_{A_1}]$, the distribution on $[d_{A_2}]$ defined by $\frac{p_{k_1,k_2}(a_1,a_2)}{p^{A_1}_{k_1,k_2}(a_1)}$ is the outcome distribution of measuring in the computational basis of A_2 the state

$$U^{(2)}_{k_2} \psi^{A_2 B_2}_{k_1,a_1} U^{(2)\dagger}_{k_2}$$

where $\psi^{A_2 B_2}_{k_1,a_1}$ is the density operator describing the state of the system $A_2 B_2$ given that the outcome of the measurement of the A_1 system is a_1. We can now use the fact that $\{U^{(2)}_{k_2}\}$. Taking the average over k_1 and k_2 in equation (8), we get

$$\frac{1}{t_1 t_2} \sum_{k_1,k_2} \Delta(p_{k_1,k_2}, \text{unif}([d_{A_1}] \times [d_{A_2}])) \leq 2\epsilon.$$

□

This observation is in the same spirit as [IS10, Proposition 1], and can in fact be used to build large almost Euclidean subspaces of $\ell_1^A(\ell_2^B)$.

2.3 Metric uncertainty relations: existence

In this section, we prove the existence of families of unitary transformations satisfying strong uncertainty relations. The proof proceeds by showing that choosing random unitaries according to the Haar measure defines a metric uncertainty relation with positive probability. The techniques used are quite standard and date back to Milman's proof of Dvoretzky's theorem [Mil71, FLM77]. In fact, using the connection to embeddings of ℓ_2 into $\ell_1(\ell_2)$ presented in the previous section, this existential theorem can be viewed as a strengthening of Dvoretzky's theorem for the $\ell_1(\ell_2)$ norm [MS86]. Explicit constructions of uncertainty relations are presented in the next section.

In order to use metric uncertainty relations to build quantum hiding fingerprints, we require an additional property for $\{U_0, \dots, U_{t-1}\}$. A set of unitary transformations $\{U_0, \dots, U_{t-1}\}$ of $\mathbb{C}^d$ are said to γ-approximately mutually unbiased bases (γ-MUBs) if for all elements $|x\rangle$ and $|y\rangle$ of the computational basis and all $k \neq k'$, we have

$$|\langle x|U_k^\dagger U_{k'}|y\rangle| \leq \frac{1}{d^{\gamma/2}}. \tag{9}$$

1-MUBs correspond to the usual notion of mutually unbiased bases.

Theorem 2.5 (Existence of metric uncertainty relations). *Let $c = 9\pi^2$ and $\epsilon \in (0,1)$. Let A and B be Hilbert spaces with $\dim B \geq 9/\epsilon^2$ and $d \stackrel{def}{=} \dim A \otimes B \geq \frac{9c \cdot 16^2 \pi}{\epsilon^2}$. Then, for all $t > \frac{4 \cdot 18c \cdot \ln(9/\epsilon)}{\epsilon^2}$, there exists a set $\{U_0, \dots, U_{t-1}\}$ of unitary transformations of AB satisfying an ϵ-metric uncertainty relation on A: for all states $|\psi\rangle \in AB$,*

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \leq \epsilon.$$

Moreover, for d such that $4td^2 \exp\left(-d^{1-\gamma}\right) < 1/2$, the unitaries $\{U_0, \dots, U_{t-1}\}$ can be chosen to also form γ-MUBs.

Remark. The proof proceeds by choosing a set of unitary transformations at random. See (12) and (13) for a precise bound on the probability that such a set does not form a metric uncertainty relation or a 0.9-MUB. □

Proof The basic idea is to evaluate the expected value of $\Delta\left(p^A_{U|\psi\rangle}, \text{unif}([d_A])\right)$ for a fixed state when U is a random unitary chosen according to the Haar measure. Then, we use a concentration argument to show that with high probability, this distance is close to its expected value. After this step, we show that the additional averaging $\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right)$ of t independent copies results in additional concentration at a rate that depends on t. We conclude by showing the existence of a family of unitaries that makes this expression small for all states $|\psi\rangle$ using a union bound over a δ-net. The four main ingredients of the proof are precisely stated here but only proved in Appendix A.

We start by computing the expected value of the fidelity $\mathbf{E}\left\{F\left(p^A_{U|\psi\rangle}, \text{unif}([d_A])\right)\right\}$, which can be seen as an $\ell_1(\ell_2)$ norm.

Lemma 2.6 (Expected value of $\ell_1^A(\ell_2^B)$ over the sphere). *Let $|\varphi\rangle^{AB}$ be a Haar-distributed random pure state on AB. Then,*

$$\mathbf{E}\left\{F\left(p^A_{|\varphi\rangle}, \textit{unif}([d_A])\right)\right\} \geq \sqrt{1 - \frac{1}{d_B}}.$$

We then use the inequality $\Delta(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2}$ to get

$$\mathbf{E}\left\{\Delta\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)\right\} \leq \mathbf{E}\left\{\sqrt{1 - F\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)^2}\right\}.$$

By the concavity of the function $x \mapsto \sqrt{1-x^2}$ on the interval $[0,1]$,

$$\begin{aligned}
\mathbf{E}\left\{\Delta\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)\right\} &\leq \sqrt{1 - \mathbf{E}\left\{F\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)\right\}^2} \\
&\leq \sqrt{1 - \left(1 - \frac{1}{d_B}\right)} \\
&\leq \epsilon/3.
\end{aligned}$$

The last inequality comes from the hypothesis of the theorem that $d_B \geq 9/\epsilon^2$. In other words, for any fixed $|\psi\rangle$, the average over U of the trace distance between $p^A_{U|\psi\rangle}$ and the uniform distribution is at most $\epsilon/3$. The next step is to show that this trace distance is close to its expected value with high probability. For this, we use a version of Lévy's lemma presented in [MS86].

Lemma 2.7 (Lévy's lemma). *Let $f : \mathbb{C}^d \to \mathbb{R}$ and $\eta > 0$ be such that for all pure states $|\varphi_1\rangle, |\varphi_2\rangle$ in $\mathbb{C}^d$,*

$$|f(|\varphi_1\rangle) - f(|\varphi_2\rangle)| \leq \eta \| |\varphi_1\rangle - |\varphi_2\rangle \|_2.$$

Let $|\varphi\rangle$ be a random pure state in dimension d. Then for all $0 \leq \delta \leq \eta$,

$$\mathbf{P}\left\{|f(|\varphi\rangle) - \mathbf{E}\left\{f(\varphi)\right\}| \geq \delta\right\} \leq 4\exp\left(-\frac{\delta^2 d}{c\eta^2}\right)$$

where c is a constant. We can take $c = 9\pi^2$.

We apply this concentration result to $f : |\varphi\rangle^{AB} \mapsto \Delta\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)$. We start by finding an upper bound on the Lipshitz constant η. For any pure states $|\varphi_1\rangle^{AB}$ and $|\varphi_2\rangle^{AB}$

$$\begin{aligned}
|f(|\varphi_1\rangle) - f(|\varphi_2\rangle)| &\leq \Delta\left(p^A_{\varphi_1}, p^A_{\varphi_2}\right) \\
&\leq \frac{1}{2}\sum_{a,b}\left||\langle a|^A\langle b|^B|\varphi_1\rangle|^2 - \sum_b |\langle a|^A\langle b|^B|\varphi_2\rangle|^2\right| \\
&= \Delta\left(p_{|\varphi_1\rangle}, p_{|\varphi_2\rangle}\right) \\
&\leq \sqrt{1 - F\left(p_{|\varphi_1\rangle}, p_{|\varphi_2\rangle}\right)^2} \\
&\leq \sqrt{2\left(1 - F\left(p_{|\varphi_1\rangle}, p_{|\varphi_2\rangle}\right)\right)} \\
&= \sqrt{2 - 2\sum_{a,b}|\langle a|\langle b||\varphi_1\rangle| \cdot |\langle a|\langle b||\varphi_2\rangle|} \\
&= \sqrt{\sum_{a,b}\left||\langle a|\langle b||\varphi_1\rangle| - |\langle a|\langle b||\varphi_2\rangle|\right|^2} \\
&\leq \||\varphi_1\rangle - |\varphi_2\rangle\|_2.
\end{aligned} \tag{10}$$

The first two inequalities follow from the triangle inequality. The third inequality is an application of (2). The fourth inequality follows from the fact that $1 - x^2 \leq 2(1-x)$ for all $x \in [0,1]$. The last inequality follows again from the triangle inequality. Thus, applying Lemma 2.7, we get for all $0 \leq \delta \leq 1$,

$$\mathbf{P}\left\{\left|\Delta\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right) - \mu\right| \geq \delta\right\} \leq 4\exp\left(-\frac{\delta^2 d}{c}\right)$$

where $\mu = \mathbf{E}\left\{\Delta\left(p^A_{|\varphi\rangle}, \text{unif}([d_A])\right)\right\}$. The following lemma bounds the tails of the average of independent copies of a random variable.

Lemma 2.8 (Concentration of the average)**.** *Let $a, b \geq 1$, $\delta \in (0,1)$ and t a positive integer. Suppose X is a random variable with 0 mean satisfying the tail bounds*

$$\mathbf{P}\left\{X \geq \delta\right\} \leq ae^{-b\delta^2} \quad \text{and} \quad \mathbf{P}\left\{X \leq -\delta\right\} \leq ae^{-b\delta^2}.$$

Let $X_1, \ldots X_t$ be independent copies of X. Then if $\delta^2 b \geq 16a^2\pi$,

$$\mathbf{P}\left\{\left|\frac{1}{t}\sum_{k=1}^{t} X_k\right| \geq \delta\right\} \leq \exp\left(-\frac{\delta^2 bt}{2}\right).$$

Taking $\delta = \epsilon/3$ and using Lemma 2.8 (which we can apply because we have $(\epsilon/3)^2 \cdot \frac{d}{c} \geq 16 \cdot 4^2 \cdot \pi$), we get

$$\mathbf{P}\left\{\left|\frac{1}{t}\sum_{k=0}^{t-1}\Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) - \mu\right| \geq \epsilon/3\right\} \leq \exp\left(-\frac{1}{2}\frac{(\epsilon/3)^2 td}{c}\right).$$

Using this together with Lemma 2.6, we have

$$\mathbf{P}\left\{\frac{1}{t}\sum_{k=0}^{t-1}\Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) \geq 2\epsilon/3\right\} \leq \exp\left(-\frac{\epsilon^2 td}{18c}\right). \tag{11}$$

We would like to have the event described in (11) hold for all $|\psi\rangle \in AB$. For this, we construct a finite set $\mathcal{N}$ of states (a δ-net) for which we can ensure that $\frac{1}{t}\sum_{k=0}^{t-1}\Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) < 2\epsilon/3$ for all $|\psi\rangle \in \mathcal{N}$ holds with high probability.

Lemma 2.9 (δ-net)**.** *Let $\delta \in (0,1)$. There exists a set $\mathcal{N}$ of pure states in $\mathbb{C}^d$ with $|\mathcal{N}| \leq (3/\delta)^{2d}$ such that for every pure state $|\psi\rangle \in \mathbb{C}^d$ (i.e., $\||\psi\rangle\|_2 = 1$), there exists $|\tilde{\psi}\rangle \in \mathcal{N}$ such that*

$$\||\psi\rangle - |\tilde{\psi}\rangle\|_2 \leq \delta.$$

Let $\mathcal{N}$ be the $\epsilon/3$-net obtained by applying this lemma to the space AB with $\delta = \epsilon/3$. We have

$$\begin{aligned}\mathbf{P}\left\{\exists|\psi\rangle \in \mathcal{N} : \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) \geq 2\epsilon/3\right\} &\leq |\mathcal{N}| \cdot \exp\left(-\frac{\epsilon^2 td}{18c}\right) \\ &\leq \exp\left(-d\left(\frac{\epsilon^2 t}{18c} - 2\ln(9/\epsilon)\right)\right).\end{aligned}$$

Now for an arbitrary state $|\psi\rangle \in AB$, we know that there exists $|\tilde{\psi}\rangle \in \mathcal{N}$ such that $\||\psi\rangle - |\tilde{\psi}\rangle\|_2 \leq \epsilon/3$. As a consequence, for any unitary transformation U,

$$\begin{aligned}\Delta\left(p^A_{U|\psi\rangle}, \text{unif}([d_A])\right) &\leq \Delta\left(p^A_{U|\tilde{\psi}\rangle}, \text{unif}([d_A])\right) + \Delta\left(p^A_{U|\tilde{\psi}\rangle}, p^A_{U|\psi\rangle}\right) \\ &\leq \Delta\left(p^A_{U|\tilde{\psi}\rangle}, \text{unif}([d_A])\right) + \|U|\tilde{\psi}\rangle - U|\psi\rangle\|_2 \\ &\leq \Delta\left(p^A_{U|\tilde{\psi}\rangle}, \text{unif}([d_A])\right) + \epsilon/3.\end{aligned}$$

In the first inequality, we used the triangle inequality and the second inequality can be derived as in (10). Thus,

$$\mathbf{P}\left\{\exists|\psi\rangle \in AB : \frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi\rangle}, \text{unif}([d_A])\right) \geq \epsilon\right\} \leq \exp\left(-d\left(\frac{\epsilon^2 t}{18c} - 2\ln(9/\epsilon)\right)\right). \tag{12}$$

If $t > \frac{4\cdot 18c\cdot\ln(9/\epsilon)}{\epsilon^2}$, this bound is strictly smaller than $1/2$ and the result follows.

To prove that we can suppose that $\{U_0, \ldots, U_{t-1}\}$ define γ-MUBs, consider the function $f : |\varphi\rangle \mapsto \langle\psi|\varphi\rangle$ for some fixed vector $|\psi\rangle$. Then, if $|\varphi\rangle$ is a random pure state, we have $\mathbf{E}\left\{f(|\varphi\rangle)\right\} = 0$. Moreover, using Levy's Lemma with $\delta = d^{-\gamma/2}$

$$\mathbf{P}\left\{|\langle\psi|\varphi\rangle| \geq d^{-\gamma/2}\right\} \leq 4\exp\left(-\frac{d^{1-\gamma}}{c}\right).$$

Thus,

$$\mathbf{P}\left\{\exists k \neq k', x, y \in [d], |\langle x|U_k^\dagger U_{k'}|y\rangle| \geq d^{-\gamma}\right\} \leq 4td^2\exp\left(-\frac{d^{1-\gamma}}{c}\right) \tag{13}$$

which completes the proof. □

Corollary 2.10 (Existence of entropic uncertainty relations)**.** *Let C be a Hilbert space of dimension $d > 2$. There exists a constant $c' \geq 1$ such that for any integer $t > 2$ such that $\frac{9\cdot 16^2 t}{5\cdot 18\log t} \leq d$, there exists a set $\{U_0, \ldots, U_{t-1}\}$ of unitary transformations of C satisfying the following entropic uncertainty relation: for any state $|\psi\rangle$,*

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geq \left(1 - \sqrt{\frac{c'\log t}{t}}\right)\log d - \log\left(\frac{18t}{c'\log t}\right) - \eta\left(\sqrt{\frac{c'\log t}{t}}\right)$$

where $\eta(\epsilon) = -2\epsilon\ln(2\epsilon)$ for all $\epsilon > 0$. In particular, in the limit $d \to \infty$, we obtain the existence of a sequence of sets of t bases satisfying

$$\lim_{d\to\infty} \frac{\frac{1}{t}\sum_{k=0}^{t-1}\mathbf{H}(p_{U_k|\psi\rangle})}{\log d} \geq 1 - \sqrt{\frac{c'\log t}{t}}.$$

Remark. Recall that the bases (or measurements) that constitute the uncertainty relation are defined as the images of the computational basis by $U_k^\dagger$. Note that for any set of unitaries $\{U_0, \ldots, U_{t-1}\}$, we have

$$\frac{1}{t}\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \leq \left(1 - \frac{1}{t}\right)\log d.$$

It is an open question whether there exists uncertainty relations matching this bound, even asymptotically as $d \to \infty$ [WW10]. Wehner and Winter [WW10] ask whether there even exists a growing function f such that

$$\lim_{d\to\infty} \frac{1}{t} \frac{\sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle})}{\log d} \geq 1 - \frac{1}{f(t)}.$$

The corollary answers this question in the affirmative with $f(t) = \sqrt{\frac{t}{c' \log t}}$. □

Proof Define $c' = 5 \cdot 18c$ where c comes from Lévy's Lemma 2.7, $\epsilon = \sqrt{\frac{c' \log t}{t}}$ and decompose $C = A \otimes B$ with $d_B = \lceil 9/\epsilon^2 \rceil$. As $d \geq \frac{9c \cdot 16^2}{\epsilon^2}$ and

$$\frac{4 \cdot 18c \log(9/\epsilon)}{\epsilon^2} = 4 \cdot 18c \log\left(\sqrt{\frac{t}{c' \log t}}\right) \cdot \frac{t}{5 \cdot 18c \log t} \leq t,$$

we get a family $U_0, \ldots, U_{t-1}$ of unitary transformations that satisfies

$$\frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) \leq \epsilon.$$

By Proposition 2.2, these unitary transformations also satisfy an entropic uncertainty relation:

$$\begin{aligned}\frac{1}{t} \sum_{k=0}^{t-1} \mathbf{H}(p^A_{U_k|\psi\rangle}) &\geq (1-\epsilon) \log\left(\frac{d}{\lceil 9/\epsilon^2 \rceil}\right) - \eta(\epsilon) \\ &\geq (1-\epsilon) \log d - \log(18/\epsilon^2) - \eta(\epsilon).\end{aligned}$$

□

2.4 Metric uncertainty relations: explicit construction

In this section, we are interested in obtaining families $\{U_0, \ldots, U_{t-1}\}$ of unitaries verifying metric uncertainty relations where $U_0, \ldots, U_{t-1}$ are explicit and efficiently computable using a quantum computer. For this section, we consider for simplicity a Hilbert space composed of qubits, i.e., of dimension $d = 2^n$ for some integer n. This Hilbert space is of the form $A \otimes B$ where A describes the states of the first $\log d_A$ qubits and B the last $\log d_B$ qubits. Note that we assume that both d_A and d_B are powers of two.

We construct a set of unitaries by adapting an explicit low-distortion embedding of $(\mathbb{R}^d, \ell_2)$ into $(\mathbb{R}^{d'}, \ell_1)$ with $d' = d^{1+o(1)}$ by Indyk [Ind07]. Indyk's construction has two main ingredients: a set of mutually unbiased bases and an extractor. Our construction uses the same paradigm while requiring additional properties on both the mutually unbiased bases and the extractor.

In order to obtain a locking scheme that only needs simple quantum operations, we construct sets of *approximately* mutually unbiased bases from a restricted set of unitaries that can be implemented with single-qubit Hadamard gates. Moreover, we impose three additional properties on the extractor: we need our extractor to be strong, to define a permutation and to be efficiently invertible. We want the extractor to be strong because we are constructing metric uncertainty relations as opposed to a norm embedding. The property of being a permutation extractor is needed to ensure that the induced transformation on $(\mathbb{C}^2)^{\otimes n}$ preserves the ℓ_2 norm. We also require the efficient invertibility condition to be able to build an efficient quantum circuit for the permutation. See Definition 2.14 for a precise formulation.

The intuition behind Indyk's idea is as follows. Let $V_0, \ldots, V_{r-1}$ be unitaries defining (approximately) mutually unbiased bases and let $\{P_y\}_{y \in S}$ be a permutation extractor (these terms are defined later in equation (14) and Definition 2.14). The role of the mutually unbiased bases is to guarantee that for all states $|\psi\rangle$ and for most values of $j \in [r]$, most of the mass of the state $V_j|\psi\rangle$ is "well spread" in the computational basis. This spread is measured in terms of the min-entropy of the distribution $p_{V_j|\psi\rangle}$. Then, the extractor $\{P_y\}_y$ will ensure that on average over $y \in S$, the masses $\sum_b |\langle a|\langle b|P_y V_j|\psi\rangle|^2$ are almost equal for all $a \in [d_A]$. More precisely, the distribution $p^A_{P_y V_j|\psi\rangle}$ is close to uniform.

We start by recalling the definition of mutually unbiased bases. A set of unitary transformations $V_0, \ldots, V_{r-1}$ is said to define *γ-approximately mutually unbiased bases* (or γ-MUBs) if for $i \neq j$ and any elements $|x\rangle$ and $|y\rangle$ of the computational basis, we have

$$|\langle x|V_i^\dagger V_j|y\rangle| = \frac{1}{d^{\gamma/2}}. \tag{14}$$

As shown in the following lemma, there is a construction of mutually unbiased bases that can be efficiently implemented [WF89]. The proof of the lemma is deferred to Appendix B.

Lemma 2.11 (Quantum circuits for MUBs). *Let n be a positive integer and $d = 2^n$. For any integer $r \leq d+1$, there exists a family $V_0, \ldots, V_{r-1}$ of unitary transformations of $\mathbb{C}^d$ that define mutually unbiased bases. Moreover, there is a randomized classical algorithm with runtime $O(n^2 \operatorname{polylog} n)$ that takes as input $j \in [r]$ and outputs a binary vector $\alpha_j \in \{0,1\}^{2n-1}$, and a quantum circuit of size $O(n \operatorname{polylog} n)$ and depth $O(\log n)$ that when given as input the vector α_j (classical input) and a quantum state $|\psi\rangle \in \mathbb{C}^d$ outputs $V_j|\psi\rangle$.*

Remark. The randomization in the algorithm is used to find an irreducible polynomial of degree n over $\mathbb{F}_2[X]$. It could be replaced by a deterministic algorithm that runs in time $O(n^4 \operatorname{polylog} n)$. Observe that if n is odd and $r \leq (d+1)/2$, it is possible to choose the unitary transformations to be real (see [HSP06]). □

It is also possible to obtain approximately mutually unbiased bases that use smaller circuits. In fact, the following lemma shows that we can construct large sets of approximately mutually unbiased bases defined by unitaries in the restricted set

$$\mathcal{H} = \{H^v \stackrel{\text{def}}{=} H^{v_1} \otimes \cdots \otimes H^{v_n}, v \in \{0,1\}^n\},$$

where H is the Hadamard transform on $\mathbb{C}^2$ defined by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

In our construction of metric uncertainty relations (Theorem 2.16), we could use the 1-MUBs of Lemma 2.11 or the $(1/2 - \delta)$-MUBs of Lemma 2.12. As the construction of approximate MUBs is simpler and can be implemented with simpler circuits, we use Lemma 2.12 when the choice of γ-MUBs is not specified.

Lemma 2.12 (Approximate MUBs in $\mathcal{H}$). *Let n' be a positive integer and $n = 2^{n'}$.*

1. *For any integer $r \leq n$, there exists a family $V_0, \ldots, V_{r-1} \in \mathcal{H}$ that define $1/2$-MUBs.*
2. *For any $\delta \in (0, 1/2)$, there exists a constant $c > 0$ independent of n such that for any $r \leq 2^{cn}$ there exists a family $V_0, \ldots, V_{r-1}$ of unitary transformations in $\mathcal{H}$ that define $(1/2 - \delta)$-MUBs.*

Moreover, in both cases, given an index $j \in [r]$, there is a polynomial time (classical) algorithm that computes the vector $v \in \{0,1\}^n$ that defines the unitary $V_j = H^v$.

Proof Observe that for any $v \in \{0,1\}^n$ and any $y \in \{0,1\}^n$, we have

$$H^v\left(|y_1\rangle \otimes \cdots \otimes |y_n\rangle\right) = H^{v_1}|y_1\rangle \otimes \cdots \otimes H^{v_n}|y_n\rangle = \sum_{\substack{y'_i \in \{0,1\} \text{ for } v_i = 1 \\ y'_i = y_i \text{ for } v_i = 0}} \frac{(-1)^{v \cdot y'}}{\sqrt{2}^{\mathbf{w}(v)}} |y'_1 \ldots y'_n\rangle.$$

Thus,

$$|\langle x|H^v H^{v'}|y\rangle| = |\langle x|H^{v+v'}|y\rangle| \leq \frac{1}{2^{d_H(v,v')/2}}. \tag{15}$$

Using this observation, we see that a binary code $C \subseteq \{0,1\}^n$ with minimum distance γn defines a set of γ-MUBs in $\mathcal{H}$. It is now sufficient to find binary codes with minimum distance as large as possible. For the first construction, we use the Hadamard code that has minimum distance $n/2$. The Hadamard codewords are indexed by $x \in \{0,1\}^{n'}$; the codeword corresponding to x is the vector $v \in \{0,1\}^n$ whose coordinates are $v_z = x \cdot z$ for all $z \in \{0,1\}^{n'}$. This code has the largest possible minimum distance for a non-trivial binary code but its shortcoming is that the number of codewords is only n. For our applications, it is sometimes desirable to have r larger than n (this is useful to allow the error parameter ϵ of our metric uncertainty relation to be smaller than $n^{-1/2}$).

For the second construction, we use families of linear codes with minimum distance $(1/2-\delta)n$ with a number of codewords that is exponential in n. For this, we can use Reed-Solomon codes concatenated with linear codes on $\{0,1\}^{\Theta(n')}$ that match the performance of random linear codes; see for example Appendix E in [Gol08]. For a simpler construction, note that we can also get $2^{\Omega(\sqrt{n})}$ codewords by using a Reed-Solomon code concatenated with a Hadamard code. □

The next lemma shows that for any state $|\psi\rangle$, for most values of j, the distribution $p_{V_j|\psi\rangle}$ is close to a distribution with large min-entropy provided $\{V_j\}$ define γ-MUBs. This result might be of independent interest. In fact, the authors of [DFR+07] prove a lower bound close to $n/2$ on the min-entropy of a measurement in the computational basis of the state $U|\psi\rangle$ where U is chosen uniformly from the full set of the 2^n unitaries of $\mathcal{H}$. They leave as an open question the existence of small subsets of $\mathcal{H}$ that satisfy the same uncertainty relation. When used with the γ-MUBs of Lemma 2.12, the following lemma partially answers this question by exhibiting such sets of size polynomial in n but with a min-entropy lower bound close to $n/4$ instead. This can be used to reduce the amount of randomness needed for many protocols in the bounded and noisy quantum storage models.

Lemma 2.13. *Let $n \geq 1, d = 2^n$ and $\epsilon \in (0,1)$ and consider a set of $r = \left\lceil \frac{2}{\epsilon^2} \right\rceil$ unitary transformations $V_0, \ldots, V_{r-1}$ of $\mathbb{C}^d$ defining γ-MUBs. For all $|\psi\rangle \in \mathbb{C}^d$,*

$$\left| \left\{ j \in [r] : \exists \text{ distribution } q_j, \Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leq \epsilon \text{ and } \mathbf{H}_{\min}(q_j) \geq \frac{\gamma n}{2} - \log(8/\epsilon^2) \right\} \right| \geq (1-\epsilon) r.$$

Proof This proof proceeds along the lines of [Ind07, Lemma 4.2]. Similar results can also be found in the sparse approximation literature; see [Tro04, Proposition 4.3] and references therein.

Consider the $rd \times d$ matrix V obtained by concatenating the rows of the matrices $V_0, \ldots, V_{r-1}$. For $S \subseteq [rd]$, V_S denotes the submatrix of V obtained by selecting the rows in S. The coordinates of the vector $V|\psi\rangle \in \mathbb{C}^{rd}$ are indexed by $z \in [rd]$ and denoted by $(V|\psi\rangle)_z$.

Claim. We have for any set $S \subseteq [rd]$ of size at most $d^{\gamma/2}$ and any unit vector $|\psi\rangle$,

$$\|(V|\psi\rangle)_S\|_2^2 \leq 1 + \frac{|S|}{d^{\gamma/2}}. \tag{16}$$

To prove the claim, we want an upper bound on the operator 2-norm of the matrix (V_S), which is the square root of the largest eigenvalue of $G = V_S^\dagger V_S$. As two distinct rows of V have an inner product bounded by $\frac{1}{d^{\gamma/2}}$, the non-diagonal entries of G are bounded by $\frac{1}{d^{\gamma/2}}$. Moreover, the diagonal entries of G are all 1. By the Gershgorin circle theorem, all the eigenvalues of G lie in the disc centered at 1 of radius $\frac{|S|-1}{d^{\gamma/2}}$. We conclude that (16) holds.

Now pick S to be the set of indices of the d^γ largest entries of the vector $\{|(V|\psi\rangle)_z|^2\}_{z\in[rd]}$. Using the previous claim, we have $\|(V|\psi\rangle)_S\|_2^2 \leq 2$. Moreover, since S contains the $d^{\gamma/2}$ largest entries of $\{|(V|\psi\rangle)_z|^2\}_z$, we have that for all $z \notin S$, $|(V|\psi\rangle)_z|^2 d^{\gamma/2} \leq \|V|\psi\rangle\|_2^2 = \sum_{j=0}^{r-1} \|V_j|\psi\rangle\|_2^2 = r$. Thus, for all $z \notin S$, $|(V|\psi\rangle)_z|^2 \leq \frac{r}{d^{\gamma/2}}$.

We now build the distributions q_j. For every $j \in [r]$, define

$$w_j = \sum_{z \in S \cap \{jr, \ldots, (j+1)r-1\}} |(V|\psi\rangle)_z|^2,$$

which is the total weight in S of $V_j|\psi\rangle$. Defining $T_\epsilon = \{j : w_j > \epsilon\}$, we have $|T_\epsilon|\epsilon \leq \|(V|\psi\rangle)_S\|_2^2 \leq 2$. Thus,

$$|T_\epsilon| \leq 2/\epsilon \leq \epsilon r.$$

We define the distribution q_j for $j \in [r]$ by

$$q_j(x) = \begin{cases} |\langle x|V_j|\psi\rangle|^2 + \frac{w_j}{d} & \text{if } jd + x \notin S \\ \frac{w_j}{d} & \text{if } jd + x \in S. \end{cases}$$

Since

$$\sum_x q_j(x) = w_j + \sum_{x \in [d] : jd + x \notin S} |\langle x|V_j|\psi\rangle|^2 = \sum_{x\in[d]} |\langle x|V_j|\psi\rangle|^2 = 1,$$

q_j is a probability distribution. Moreover, we have that for $j \notin T_\epsilon$

$$\Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leq \frac{1}{2}\left(\sum_{x : jd+x \notin S} \frac{w_j}{d} + \sum_{x : jd+x \in S} \left(\frac{w_j}{d} + |\langle x|V_j|\psi\rangle|^2 \right) \right) = w_j \leq \epsilon.$$

The distribution q_j also has the nice property that for all $x \in [d]$, $q_j(x) \leq \frac{r}{d^{\gamma/2}} + \frac{1}{d} \leq \frac{2r}{d^{\gamma/2}}$. In other words, $\mathbf{H}_{\min}(q_j) \geq \frac{\gamma n}{2} - \log(8/\epsilon^2)$. □

We now move to the second building block in Indyk's construction: randomness extractors. Randomness extractors are functions that extract uniform random bits from weak sources of randomness.

Definition 2.14 (Strong permutation extractor)**.** *Let n and $m \leq n$ be positive integers, $\ell \in [0, n]$ and $\epsilon \in (0, 1)$. A family of permutations $\{P_y\}_{y \in S}$ of $\{0,1\}^n$ where each permutation P_y is described by two functions $P_y^E : \{0,1\}^n \to \{0,1\}^m$ (the first m output bits of P_y) and $P_y^R : \{0,1\}^n \to \{0,1\}^{n-m}$ (the last $n - m$ output bits of P_y) is said to be an explicit $(n, \ell) \to_\epsilon m$ strong permutation extractor if:*

- *For any random variable X on $\{0,1\}^n$ such that $\mathbf{H}_{\min}(X) \geq \ell$, and an independent seed U_S uniformly distributed over S, we have*
$$\Delta\left(p_{\left(U_S, P^E_{U_S}(X)\right)}, \textit{unif}(S \times \{0,1\}^m)\right) \leq \epsilon,$$
which is equivalent to
$$\frac{1}{|S|} \sum_{y \in S} \Delta\left(p_{P_y^E(X)}, \textit{unif}(\{0,1\}^m)\right) \leq \epsilon. \tag{17}$$
- *For all $y \in S$, both the function P_y and its inverse P_y^{-1} are computable in time polynomial in n.*

Remark. A similar definition of permutation extractors was used in [RVW00] in order to avoid some entropy loss in an extractor construction. Here, the reason we use permutation extractors is different; it is because we want the induced transformation P_y on $\mathbb{C}^{2^n}$ to preserve the ℓ_2 norm. □

We can adapt an extractor construction of [GUV09] to obtain a permutation extractor with the following parameters. The details of the construction are presented in Appendix C.

Theorem 2.15 (Explicit strong permutation extractors)**.** *For all (constant) $\delta \in (0, 1)$, all positive integers n, all $k \in [c \log(n/\epsilon), n]$ (c is a constant independent of n and ϵ), and all $\epsilon \in (0, 1/2)$, there is an explicit $(n, k) \to_\epsilon (1-\delta)k$ strong permutation extractor $\{P_y\}_{y \in S}$ with $\log|S| \leq O(\log(n/\epsilon))$. Moreover, the functions $(x, y) \mapsto P_y(x)$ and $(x, y) \mapsto P_y^{-1}(x)$ can be computed by circuits of size $O(n \operatorname{polylog}(n/\epsilon))$.*

A permutation P on $\{0,1\}^n$ defines a unitary transformation on $(\mathbb{C}^2)^{\otimes n}$ that we also call P. The permutation extractor $\{P_y\}$ will be seen as a family of unitary transformations over n qubits. Moreover, just as we decomposed the space $\{0,1\}^n$ into the first m bits and the last $n - m$ bits, we decompose the space $(\mathbb{C}^2)^{\otimes n}$ into $A \otimes B$, where A represents the first m qubits and B represents the last $n - m$ qubits. The properties of $\{P_y^E\}$ will then be reflected in the system A.

Combining Theorem 2.15 and Lemma 2.11, we obtain a set of unitaries satisfying a metric uncertainty relation.

Theorem 2.16 (Explicit uncertainty relations: key optimized)**.** *Let $\delta > 0$ be a constant, n be a positive integer, $\epsilon \in (2^{-c'n}, 1)$ (c' is a constant independent of n). Then, there exist $t \leq \left(\frac{n}{\epsilon}\right)^c$ (for some constant c independent of n and ϵ) unitary transformations $U_0, \ldots, U_{t-1}$ acting on n qubits such that: if A represents the first $(1-\delta)n/4 - O(\log(1/\epsilon))$ qubits and B represents the remaining qubits, then for all $|\psi\rangle \in AB$,*
$$\frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \leq \epsilon.$$
Moreover, the mapping that takes the index $k \in [t]$ and a state $|\psi\rangle$ as inputs and outputs the state $U_k|\psi\rangle$ can be performed by a classical computation with polynomial runtime and a quantum circuit that consists of single-qubit Hadamard gates on a subset of the qubits followed by a permutation in the computational basis. This permutation can be computed by (classical or quantum) circuits of size $O(n \operatorname{polylog}(n/\epsilon))$.

Remark. Observe that in terms of the dimension d of the Hilbert space, the number of unitaries t is polylogarithmic. □

Proof Let $\epsilon' = \epsilon/6$. Lemma 2.11 gives $r = \lceil 2/\epsilon'^2 \rceil \leq 2^n$ unitary transformations $V_0, \ldots, V_{r-1}$ that define mutually unbiased bases. Moreover, all theses unitaries can be computed by circuits of size $O(n \operatorname{polylog} n)$. Theorem 2.15 with $\ell = n/2 - \log(8/\epsilon'^2)$ and error ϵ' gives $|S| \leq 2^{c \log(n/\epsilon')}$ permutations $\{P_y\}_{y \in S}$ of $\{0,1\}^n$ that are computable by classical circuits of size $O(n \operatorname{polylog}(n/\epsilon))$. We now argue that this classical circuit can be used to build a quantum circuit of size $O(n \operatorname{polylog} n)$ that computes the unitaries P_y.

Given classical circuits that compute P and P^{-1}, we can construct reversible circuits C_P and $C_{P^{-1}}$ for P and P^{-1}. The circuit C_P when given input $(x, 0)$ outputs the state $(x, P(x))$, so that it keeps the input x. Such a circuit can readily be transformed into a quantum circuit that acts on the computational basis states as the classical circuit. We also call these circuits C_P and $C_{P^{-1}}$. Observe that we want to compute the unitary P, so we have to erase the input x. For this, we can then combine the circuits C_P and $C_{P^{-1}}$ as described in Figure 1. Note that the size of this quantum circuit is the same as the size of the original classical circuit up to some multiplicative constant. Thus, this quantum circuit has size $O(n \operatorname{polylog} n)$.

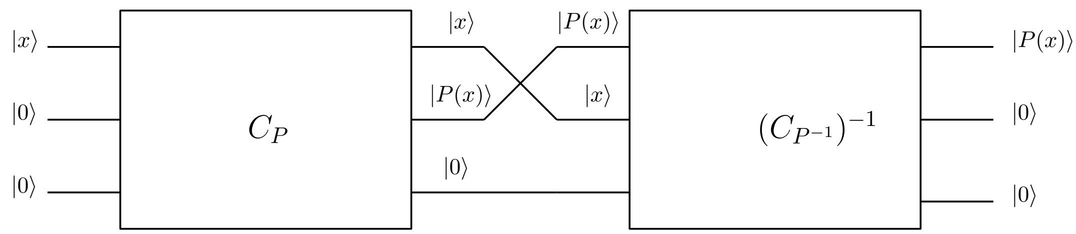

Figure 1: Quantum circuit to compute the permutation P using quantum circuits C_P for P and $C_{P^{-1}}$ for P^{-1}. $(C_{P^{-1}})^{-1}$ is simply the circuit $C_{P^{-1}}$ taken backwards. The bottom register is an ancilla register.

The unitaries $\{U_0, \dots, U_{t-1}\}$ are obtained by taking all the possible products $P_y V_j$ for $j \in [r], y \in S$. Note that $t = r|S|$. We now show that the set $\{U_0, \dots, U_{t-1}\}$ verifies the uncertainty relation property. Using Lemma 2.13, for any state $|\psi\rangle$, the set

$$T_{|\psi\rangle} \stackrel{\text{def}}{=} \left| \left\{ j : \exists \text{ distribution } q_j, \Delta\left(p_{V_j|\psi\rangle}, q_j\right) \le \epsilon' \text{ and } \forall x \in [d], q_j(x) \le \frac{2r}{\sqrt{d}} \right\} \right|$$

has size at least $(1-\epsilon')r$. Moreover, for all $a \in [d_A]$, $p^A_{P_y V_i|\psi\rangle}(a) = \sum_b |\langle a|^A \langle b|^b P_y V_i |\psi\rangle|^2 = \mathbf{P}\left\{P_y^E(X) = a\right\}$ where X has distribution $p_{V_i|\psi\rangle}$. By definition, for $i \in T_{|\psi\rangle}$, we have $\Delta\left(p_{V_i|\psi\rangle}, q_i\right) \le \epsilon'$ with $\mathbf{H}_{\min}(q_i) \ge n/2 - \log(8/\epsilon'^2)$. Using the fact that $\{P_y^E\}$ is a strong extractor (see (17)) for min-entropy $n/2 - \log(8/\epsilon'^2)$, it follows that

$$\frac{1}{|S|} \sum_{y \in S} \Delta\left(p^A_{P_y V_i|\psi\rangle}, \text{unif}([d_A])\right) \le 2\epsilon'$$

for all $i \in T_{|\psi\rangle}$. As $|T_{|\psi\rangle}| \ge (1-\epsilon')r$, we obtain

$$\frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \text{unif}([d_A])\right) \le 3\epsilon' = \epsilon/2.$$

To conclude, we show that t can be taken to be a power of two at the cost of multiplying the error by at most two. In fact, let p be the smallest integer verifying $t \le 2^p$, so that $2^p \le 2t$. By repeating $2^p - t$ unitaries, it is easily seen that we obtain an ϵ-metric uncertainty relation with $2p$ unitaries from an $\epsilon/2$-metric uncertainty relation with t unitaries. □

Note that the B system we obtain is quite large and to get strong uncertainty relations, we want the system B to be as small as possible. For this it is possible to repeat the construction of the previous theorem on the B system. The next theorem gives a construction where the A system is composed of $n - O(\log\log n) - O(\log(1/\epsilon))$ qubits. Of course, this is at the expense of increasing the number of unitaries in the uncertainty relation.

Theorem 2.17 (Explicit uncertainty relation: message length optimized)**.** *Let n be a positive integer and $\epsilon \in (2^{-c'n}, 1)$ (c' is a constant independent of n). Then, there exist $t \le \left(\frac{n}{\epsilon}\right)^{c \log n}$ (for some constant c independent of n and ϵ) unitary transformations $U_0, \dots, U_{t-1}$ acting on n qubits that are all computable by quantum circuits of size $O(n \operatorname{polylog}(n/\epsilon))$ such that: if A represents the first $n - O(\log\log n) - O(\log(1/\epsilon))$ qubits and B represents the remaining qubits, then for all $|\psi\rangle \in AB$,*

$$\frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \le \epsilon. \tag{18}$$

Moreover, the mapping that takes the index $k \in [t]$ and a state $|\psi\rangle$ as inputs and outputs the state $U_k|\psi\rangle$ can be performed by a classical precomputation with polynomial runtime and a quantum circuit of size $O(n \operatorname{polylog}(n/\epsilon))$. The number of unitaries t can be taken to be a power of two.

Proof Using the construction of Theorem 2.16, we obtain a system A over which we have some uncertainty relation and a system B that we do not control. In order to decrease the dimension of the system B, we can apply the same construction to that system. The system B then gets decomposed into A_2B_2, and we know that the distribution of the measurement outcomes of system A_2 in the computational basis is close to uniform. As a result, we obtain an uncertainty relation on the system AA_2 (see Figure 2).

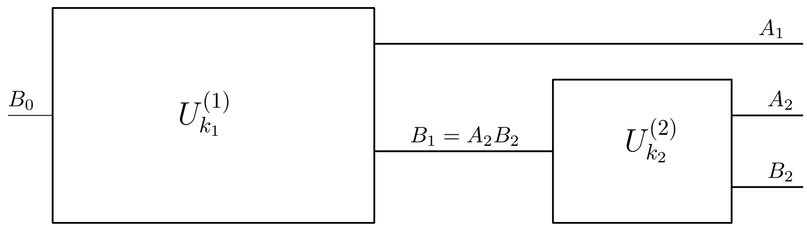

Figure 2: Composition of the construction of Theorem 2.16: In order to reduce the dimension of the B system, we can re-apply the uncertainty relation to the B system.

More precisely, we start by demonstrating a simple property about the composition of metric uncertainty relations. Note that this composition is different from the one described in (7), but the proof is quite similar.

Claim. Suppose the set $\{U_0^{(1)}, \dots, U_{t_1-1}^{(1)}\}$ of unitaries on A_1B_1 satisfies a (t_1, ϵ_1)-metric uncertainty relation on system A_1 and the $\{U_0^{(2)}, \dots, U_{t_2-1}^{(2)}\}$ of unitaries on $B_1 = A_2B_2$ satisfies a (t_2, ϵ_2)-metric uncertainty relation on A_2. Then the set of unitaries $\left\{(\mathbb{1}^{A_1} \otimes U_{k_2}^{(2)}) \cdot U_{k_1}^{(1)}\right\}_{k_1,k_2 \in [t_1]\times[t_2]}$ satisfies a $(t_1t_2, \epsilon_1 + \epsilon_2)$-metric uncertainty relation on A_1A_2: for all $|\psi\rangle \in A_1A_2B_2$,

$$\frac{1}{t_1t_2} \sum_{k_1,k_2 \in [t_1]\times[t_2]} \Delta\left(p_{U_{k_2}^{(2)}U_{k_1}^{(1)}|\psi\rangle}, \operatorname{unif}([d_{A_1}d_{A_2}])\right) \leq \epsilon_1 + \epsilon_2.$$

For a fixed value of $k_1 \in [t_1]$ and $a_1 \in [d_{A_1}]$, we can apply the second uncertainty relation to the state $\frac{\langle a_1|^{A_1}U_{k_1}|\psi\rangle}{\|\langle a_1|^{A_1}U_{k_1}|\psi\rangle\|_2} = \frac{1}{\sqrt{p^{A_1}_{U_{k_1}|\psi\rangle}(a_1)}} \sum_{b_1} \left(\langle a_1|\langle b_1|U_{k_1}|\psi\rangle\right)|b_1\rangle \in B_1 = A_2B_2$. As $\{|b_1\rangle\}_{b_1} = \{|a_2\rangle|b_2\rangle\}_{a_2,b_2}$, we have

$$\frac{1}{t_2}\sum_{k_2}\sum_{a_2}\left|\frac{1}{p^{A_1}_{U_{k_1}|\psi\rangle}(a_1)}\sum_{b_2}|\langle a_1|^{A_1}\langle a_2|^{A_2}\langle b_2|^{B_2}(\mathbb{1}^{A_1}\otimes U_{k_2})U_{k_1}|\psi\rangle|^2 - \frac{1}{d_{A_2}}\right| \leq \epsilon_2.$$

We can then calculate, in the same vein as (8)

$$\begin{aligned}
&\frac{1}{t_1t_2}\sum_{k_1,k_2}\sum_{a_1,a_2}\left|\sum_{b_2}|\langle a_1|^{A_1}\langle a_2|^{A_2}\langle b_2|^{B_2}(\mathbb{1}^{A_1}\otimes U_{k_2})U_{k_1}|\psi\rangle|^2 - \frac{1}{d_{A_1}d_{A_2}}\right| \\
&\leq \frac{1}{t_1t_2}\sum_{k_1,k_2}\sum_{a_1}\left|\sum_{b_2}|\langle a_1|^{A_1}\langle a_2|^{A_2}\langle b_2|^{B_2}(\mathbb{1}^{A_1}\otimes U_{k_2})U_{k_1}|\psi\rangle|^2 - \frac{p^{A_1}_{U_{k_1}|\psi\rangle}(a_1)}{d_{A_2}}\right| + \frac{1}{t_1}\sum_{k_1}\sum_{a_1,a_2}\left|\frac{p^{A_1}_{U_{k_1}|\psi\rangle}(a_1)}{d_{A_2}} - \frac{1}{d_{A_1}d_{A_2}}\right| \\
&\leq \frac{1}{t_1}\sum_{k_1}\sum_{a_1} p^{A_1}_{U_{k_1}|\psi\rangle}(a_1)\epsilon_2 + \epsilon_1 \\
&\leq \epsilon_2 + \epsilon_1.
\end{aligned}$$

This completes the proof of the claim.

To obtain the claimed dimensions, we compose the construction of Theorem 2.16 h times with an error parameter $\epsilon' = \epsilon/h$ and $\delta = 1/8$. Starting with a space of n qubits, the dimension of the B system (after one step) can be bounded by

$$\frac{7}{8}n - O(\log(1/\epsilon')) \leq \log d_B \leq \frac{7}{8}n$$

So after h steps, we have

$$(7/8)^h n - O(\log(1/\epsilon')) \cdot 8(1 - (7/8)^h) \leq \log d_{B_h} \leq (7/8)^h n.$$

Thus,

$$(7/8)^h n - O(\log(1/\epsilon')) \leq \log d_{B_h} \leq (7/8)^h n.$$

Note that h cannot be arbitrarily large: in order to apply the construction of Theorem 2.16 on a system of m qubits with error ϵ', we should have $\epsilon' \geq 2^{-c'm}$. In other words, if

$$\log d_{B_h} \geq \frac{1}{c'} \log(h/\epsilon), \tag{19}$$

then we can apply the construction h times. Let c'' be a constant to be chosen later and $h = \left\lfloor \frac{1}{\log(8/7)} (\log n - \log(c \log\log n + c\log(1/\epsilon))) \right\rfloor$. This choice of h satisfies (19). In fact,

$$\begin{aligned}\log d_{B_h} &\geq c \log\log n + c\log(1/\epsilon) - O(\log(h/\epsilon)) \\ &\geq \frac{1}{c'} \log(h/\epsilon)\end{aligned}$$

if c is chosen large enough. Moreover, we get

$$\log d_{B_h} = 2^{-\log n} \cdot 2^{\log O(\log\log n + \log(1/\epsilon))} \cdot n = O(\log\log n + \log(1/\epsilon))$$

as stated in the theorem.

Each unitary of the obtained uncertainty relation is a product of h unitaries. The overall number of unitaries is product of the number of unitaries for each of the h steps. As a result, we have $t \leq \left(\frac{n}{\epsilon}\right)^{c \log n}$ for some constant c. t can be taken to be a power of two as the number of unitaries at each step can be taken to be power of two.

As for the running time, each unitary of the uncertainty relation is a product of $O(\log n)$ unitaries from Theorem 2.16. Hence, each unitary can be computed by a quantum circuit of size $O(n \operatorname{polylog} n)$. □

It is of course possible to obtain a trade-off between the key size and the dimension of the B system by choosing the number of times the construction of Theorem 2.16 is applied. In the next corollary, we show how to obtain an explicit entropic uncertainty relation whose average entropy is $(1-\epsilon)n$.

Corollary 2.18 (Explicit entropic uncertainty relations). *Let $n \geq 100$ be an integer, and $\epsilon \in (10n^{-1/2}, 1/(2e))$. Then, there exists $t \leq \left(\frac{n}{\epsilon}\right)^{c\log(1/\epsilon)}$ (for some constant c independent of n and ϵ) unitary transformations $U_0, \ldots, U_{t-1}$ acting on n qubits that are all computable by quantum circuits of size $O(n \operatorname{polylog} n)$ verifying an entropic uncertainty relation: for all pure states $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$,*

$$\frac{1}{t} \sum_{k=0}^{t-1} \mathbf{H}(p_{U_k|\psi\rangle}) \geq (1 - 3\epsilon)n - \eta(\epsilon) \tag{20}$$

where $\eta(\epsilon) = -2\epsilon \ln(2\epsilon)$. Moreover, the mapping that takes the index $k \in [t]$ and a state $|\psi\rangle$ as inputs and outputs the state $U_k|\psi\rangle$ can be performed by a classical randomized precomputation with expected runtime $O(n^2 \operatorname{polylog} n)$ and a quantum circuit of size $O(n \operatorname{polylog} n)$. The number of unitaries t can be taken to be a power of two.

Proof The proof is basically the same as the proof of Theorem 2.17, except that we repeat the construction $h = \lceil \log(1/\epsilon)/\log(8/7) \rceil$ times. We thus have

$$\log d_{B_h} \leq (7/8)^h n \leq \epsilon n.$$

We obtain a set of $t \leq \left(\frac{n}{\epsilon}\right)^{c\log(1/\epsilon)}$ unitary transformations. Applying Proposition 2.2, we get

$$\begin{aligned}\frac{1}{t}\sum_{i=0}^{t-1}\mathbf{H}(p_{U_k|\psi\rangle}) &\geq (1-2\epsilon)(1-\epsilon)n - \eta(\epsilon)\\ &\geq (1-3\epsilon)n - \eta(\epsilon).\end{aligned}$$

□

3 Locking classical information in quantum states

Outline of the section We apply the results on metric uncertainty relations of the previous section to obtain locking schemes. After an introductory section on locking classical correlations (Section 3.1), we show how to obtain a locking scheme using a metric uncertainty relation in Section 3.2. Using the constructions of the previous section, this leads to locking schemes presented in Corollaries 3.4 and 3.5. In Section 3.3, we show how to construct quantum hiding fingerprints by locking a classical fingerprint. In Section 3.4, we observe that these locking schemes can be used to construct efficient string commitment protocols. Section 3.5 discusses the link to locking entanglement of formation.

3.1 Background

Locking of classical correlations was first described in [DHL+04] as a violation of the incremental proportionality of the maximal classical mutual information that can be obtained by local measurement on a bipartite state. More precisely, for a bipartite state ω^{AB}, the maximum classical mutual information $\mathbf{I}_c$ is defined by

$$\mathbf{I}_c(A;B)_\omega = \max_{\{M_i^A\},\{M_i^B\}} \mathbf{I}(I_A;I_B),$$

where $\{M_i^A\}$ and $\{M_i^B\}$ are measurements on A and B, and I_A, I_B are the (random) outcomes of these measurements on the state ω^{AB}. Incremental proportionality is the intuitive property that ℓ bits of communication between two parties can increase their mutual information by at most ℓ bits. The authors of [DHL+04] considered the states

$$\omega^{XKC} = \frac{1}{2d}\sum_{k=0}^{1}\sum_{x=0}^{d-1}|x\rangle\langle x|^X \otimes |k\rangle\langle k|^K \otimes (U_k|x\rangle\langle x|U_k^\dagger)^C \quad (21)$$

for $k \in \{0,1\}$ where $U_0 = \mathbb{1}$ and U_1 is the Hadamard transform. It was shown in [DHL+04] that the classical mutual information $\mathbf{I}_c(XK;C)_\omega = \frac{1}{2}\log d$. However, if the holder of the C system also knows the value of k, then we can represent the global state by the following density operator

$$\omega^{XKCK'} = \frac{1}{2d}\sum_{k=0}^{1}\sum_{x=0}^{d-1}|x\rangle\langle x|^X \otimes |k\rangle\langle k|^K \otimes (U_k|x\rangle\langle x|U_k^\dagger)^C \otimes |k\rangle\langle k|^{K'}.$$

It is easy to see that $\mathbf{I}_c(XK;CK')_\omega = 1 + \log d$. This means that with only one bit of communication (represented by the register K'), the classical mutual information between systems XK and C jumped from $\frac{1}{2}\log d$ to $1+\log d$. In other words, it is possible to unlock $\frac{1}{2}\log d$ bits of information (about X) from the quantum system C using a single bit.

The authors of [HLSW04] proved an even stronger locking result. They generalize the state in equation (21) to

$$\omega^{XKC} = \frac{1}{td}\sum_{x=0}^{d-1}\sum_{k=0}^{t-1}|x\rangle\langle x|^X \otimes |k\rangle\langle k|^K \otimes (U_k|x\rangle\langle x|U_k^\dagger)^C \otimes |k\rangle\langle k|^{K'} \quad (22)$$

where U_k are chosen independently at random according to the Haar measure. They show that for any $\epsilon > 0$, by taking $t = (\log d)^3$ and if d is large enough,

$$\mathbf{I}_c(X;C)_\omega \leq \epsilon\log d \qquad \text{and} \qquad \mathbf{I}_c(XK;CK')_\omega = \log d + \log t$$

with high probability. Note that the size of the key measured in bits is only $\log t = O(\log\log d)$ and it should be compared to the $(1-\epsilon)\log d$ bits of unlocked (classical) information. It should be noted that their argument is probabilistic, and it does not say how to construct the unitary transformations U_k. It is worth stressing that standard derandomization techniques are not known to work in this setting. For example, unitary t-designs use far too many bits of randomness [DCEL09]. Moreover, using a δ-biased subset of the set of Pauli matrices fails to produce a locking scheme unless the subset has a size of the order of the dimension d [AS04, DD10] (see Appendix D).

Here, we view locking as a cryptographic task in which a message is encoded into a quantum state using a key whose size is much smaller than the message. Having access to the key, one can decode the message. However, an eavesdropper who does not have access to the key and has complete uncertainty about the message can extract almost no classical information about the message. We should stress here that this is not a composable cryptographic task, namely because an eavesdropper could choose to store quantum information about the message instead of measuring. In fact, as shown in [KRBM07], using the communicated message X as a key for a one-time pad encryption might not be secure; see also [DFHL10]. It is however strictly stronger that the notion of entropic security [RW02, DS05, DD10] (see Appendix D for an example of an entropically secure encryption scheme that is not ϵ-locking).

Definition 3.1 (ϵ-locking scheme). *Let n be a positive integer, $\ell \in [0,n]$ and $\epsilon \in [0,1]$. An encoding $\mathcal{E} : [2^n] \times [t] \to \mathcal{S}(C)$ is said to be (ℓ,ϵ)-*locking *for the quantum system C if:*

- *For all $x \neq x' \in [2^n]$ and all $k \in [t]$, $\Delta(\mathcal{E}(x,k), \mathcal{E}(x',k)) = 1$.*
- *Let X (the message) be a random variable on $[2^n]$ with min-entropy $\mathbf{H}_{\min}(X) \geq \ell$, and K (the key) be an independent uniform random variable on $[t]$. For any measurement $\{M_i\}$ on C and any outcome i,*

$$\Delta\left(p_{X|[I=i]}, p_X\right) \leq \epsilon. \tag{23}$$

where I is the outcome of measurement $\{M_i\}$ on the (random) quantum state $\mathcal{E}(X,K)$.

When the min-entropy bound ℓ is not specified, it should be understood that $\ell = n$ meaning that X is uniformly distributed on $[2^n]$. The state $\mathcal{E}(x,k)$ for $x \in [2^n]$ and $k \in [t]$ is referred to as the ciphertext.

Remark. The relevant parameters of a locking scheme are: the number of bits n of the (classical) message, the dimension d of the (quantum) ciphertext, the number t of possible values of the key and the error ϵ. Strictly speaking, a classical one-time pad encryption, for which $t = 2^n$, is $(0,0)$-locking according to this definition. However, here we seek locking schemes for which t is much smaller than 2^n, say t polynomial in n. This cannot be achieved using a classical encryption scheme.

Observe that one can simply guess the key and apply the corresponding decoding. This observation shows that the error of an ϵ-locking scheme satisfies $\epsilon \geq \frac{1}{t} - \frac{1}{2^n}$ [DHL$^+$04]. □

Note that we used the statistical distance between $p_{X|[I=i]}$ and p_X instead of the mutual information between X and I to measure the information gained about X from a measurement. Using the trace distance is a stronger requirement as demonstrated by the following proposition.

Proposition 3.2. *Let $\epsilon \in [0, \frac{1}{2e}]$ and $\mathcal{E} : [2^n] \times [t] \to \mathcal{S}(C)$ be an ϵ-locking scheme. Define the state*

$$\omega^{XKCK'} = \frac{1}{td} \sum_{k=0}^{t-1} \sum_{x=0}^{2^n-1} |x\rangle\langle x|^X \otimes |k\rangle\langle k|^K \otimes \mathcal{E}(x,k)^C \otimes |k\rangle\langle k|^{K'}.$$

Then,

$$\mathbf{I}_c(X;C)_\omega \leq 2\epsilon n + \eta(\epsilon) \qquad \text{and} \qquad \mathbf{I}_c(XK;CK')_\omega = n + \log t$$

where $\eta(\epsilon) = -2\epsilon\ln(2\epsilon)$ with $\eta(0) = 0$.

Proof First, we can suppose that the measurement performed on the system X is in the basis $(|x\rangle^X)_{x,k}$. In fact, the outcome distribution of any measurement on the X system can be simulated classically using the values of the random variables X.

Now let I be the outcome of a measurement performed on the C system. Using Fannes' inequality, we have for any i

$$\begin{aligned}\mathbf{H}(X) - \mathbf{H}(X|I=i) &\leq 2\Delta\left(p_X, p_{X|[I=i]}\right) - \eta\left(\Delta\left(p_X, p_{X|[I=i]}\right)\right) \\ &\leq 2\epsilon n + \eta(\epsilon)\end{aligned}$$

using the face that $\mathcal{E}$ defines an ϵ-locking scheme. Thus,

$$\begin{aligned}\mathbf{I}(X;I) &= \mathbf{H}(X) - \sum_i \mathbf{P}\{I=i\}\,\mathbf{H}(X|I=i)\\ &\leq 2\epsilon n + \eta(\epsilon).\end{aligned}$$

As this holds for any measurement, we get $\mathbf{I}_c(X;C)_\omega \leq 2\epsilon n + \eta(\epsilon)$. □

The trace distance was also used in [Dup10, DFHL10] to define a locking scheme. To measure the leakage of information about X caused by a measurement, they used the probably more natural trace distance between the joint distribution of $p_{(X,I)}$ and the product distribution $p_X \times p_I$. Note that our definition is stronger, in that for all outcomes of the measurement i, $\Delta\left(p_{X|[I=i]}, p_X\right) \leq \epsilon$ whereas the definition of [DFHL10] says that this only holds on average over i. To the best of our knowledge, even the existence of such a strong locking scheme with small key was unknown.

For a survey on locking classical correlations, see [Leu09].

3.2 Locking using a metric uncertainty relation

The following theorem shows that a locking scheme can easily be constructed using a metric uncertainty relation.

Theorem 3.3. *Let $\epsilon \in (0,1)$ and $\{U_0, \dots, U_{t-1}\}$ be a set of unitary transformations of $A \otimes B$ that satisfies an ϵ-metric uncertainty relation on A, i.e., for all states $|\psi\rangle \in AB$,*

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \textit{unif}([d_A])\right) \leq \epsilon.$$

Assume $d_A = 2^n$. Then, the mapping $\mathcal{E} : [2^n] \times [t] \to \mathcal{S}(AB)$ defined by

$$\mathcal{E}(x,k) = \frac{1}{d_B}\sum_{b=0}^{d_B-1} U_k^\dagger \left(|x\rangle\langle x|^A \otimes |b\rangle\langle b|^B\right) U_k.$$

is ϵ-locking. Moreover, for all $\ell \in [0,n]$ such that $2^{\ell-n} > \epsilon$, it is $(\ell, \frac{2\epsilon}{2^{\ell-n}-\epsilon})$-locking.

Remark. The state that the encoder inputs in the B system is simply private randomness. The encoder chooses a uniformly random $b \in [d_B]$ and sends the quantum state $U_k^\dagger|x\rangle^A|b\rangle^B$. Note that b does not need to be part of the key (i.e., shared with the receiver). This makes the dimension $d = d_A d_B$ of the ciphertext larger than the number of possible messages 2^n. If one insists on having a ciphertext of the same size as the message, it suffices to consider b as part of the message and apply a one-time pad encryption to b. The number of possible values taken by the key increases to $t \cdot d_B$. □

Proof First, it is clear that different messages are distinguishable. In fact, for $x \neq x'$ and any k,

$$\Delta(\mathcal{E}(x,k), \mathcal{E}(x',k)) = \frac{1}{2}\operatorname{tr}\left[\sqrt{|x\rangle\langle x|^A \otimes \frac{\mathbb{1}^B}{\dim B} - |x'\rangle\langle x'|^A \otimes \frac{\mathbb{1}^B}{\dim B}}\right] = 1.$$

We now prove the locking property. Let X be the random variable representing the message. Assume that X is uniformly distributed over some set $S \subseteq [d_A]$ of size $|S| \geq 2^\ell$. Let K be a uniformly random key in $[t]$ that is independent of X. Consider a POVM $\{M_i\}$ on the system AB. Without loss of generality, we can suppose that the POVM elements M_i have rank 1. Otherwise, by writing M_i in its eigenbasis, we could decompose outcome i into more outcomes that can only reveal more information. So we can write the elements as weighted rank one projectors: $M_i = \xi_i|e_i\rangle\langle e_i|$ where $\xi_i > 0$. Our objective is to show that the outcome I of this measurement on the state $\mathcal{E}(X,K)$ is almost independent of X. More precisely, for a fixed measurement outcome $I = i$, we want to compare the conditional distribution $p_{X|[I=i]}$ with p_X. The trace distance between these distributions can be written as

$$\frac{1}{2}\sum_{x=0}^{d_A-1}\left|\mathbf{P}\{X=x|I=i\} - \mathbf{P}\{X=x\}\right|. \tag{24}$$

Towards this objective, we start by computing the distribution of the measurement outcome I, given the value of the message $X = x$ (note that the receiver does not know the key):

$$\begin{aligned}
\mathbf{P}\{I = i | X = x\} &= \frac{\xi_i}{t d_B} \sum_{k=0}^{t-1} \sum_{b=0}^{d_B-1} \operatorname{tr}\left[U_k |e_i\rangle\langle e_i| U_k^\dagger \cdot |x\rangle\langle x|^A \otimes |b\rangle\langle b|^B\right] \\
&= \frac{\xi_i}{t d_B} \sum_{k=0}^{t-1} \sum_{b=0}^{d_B-1} \langle x|^A \langle b|^B U_k |e_i\rangle\langle e_i| U_k^\dagger |x\rangle^A |b\rangle^B \\
&= \frac{\xi_i}{t d_B} \sum_{k=0}^{t-1} \sum_{b=0}^{d_B-1} \left|\langle x|^A \langle b|^B U_k |e_i\rangle\right|^2 \\
&= \frac{\xi_i}{d_B} \frac{1}{t} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(x).
\end{aligned}$$

Since X is uniformly distributed over S, we have that for all $x \in S$

$$\begin{aligned}
\mathbf{P}\{X = x | I = i\} &= \frac{\mathbf{P}\{X = x\}\mathbf{P}\{I = i | X = x\}}{\sum_{x' \in S} \mathbf{P}\{X = x'\}\mathbf{P}\{I = i | X = x'\}} \\
&= \frac{(1/t) \cdot \sum_k p^A_{U_k|e_i\rangle}(x)}{(1/t) \cdot \sum_{x' \in S} \sum_k p^A_{U_k|e_i\rangle}(x')}.
\end{aligned} \tag{25}$$

Observe that in the case where X is uniformly distributed over $[2^n]$ ($S = [2^n]$), it is simple to obtain directly that

$$\Delta\left(p_{X|[I=i]}, p_X\right) = \frac{1}{2} \sum_{x=0}^{d_A-1} \left| \frac{1}{t} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(x) - \frac{1}{2^n} \right| \leq \epsilon$$

using the fact that $\{U_k\}$ satisfies a metric uncertainty relation on A. Now let S be any set of size at least 2^ℓ, let $\alpha = \frac{1}{t} \sum_{x' \in S} \sum_k p^A_{U_k|e_i\rangle}(x')$. We then bound

$$\begin{aligned}
\frac{1}{2} \sum_{x=0}^{d_A-1} \left|\mathbf{P}\{X = x | I = i\} - \mathbf{P}\{X = x\}\right| &= \frac{1}{2} \sum_{x \in S} \left| \frac{(1/t) \cdot \sum_k p^A_{U_k|e_i\rangle}(x)}{\alpha} - \frac{1}{|S|} \right| \\
&= \frac{1}{2\alpha} \cdot \sum_{x \in S} \left| \frac{1}{t} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(x) - \frac{\alpha}{|S|} \right| \\
&\leq \frac{1}{2\alpha} \cdot \frac{1}{t} \sum_k \left(\sum_{x \in S} \left| p^A_{U_k|e_i\rangle}(x) - \frac{1}{2^n} \right| + \left| \frac{1}{2^n} - \frac{\alpha}{|S|} \right| \right).
\end{aligned}$$

We now use the fact that $\{U_k\}$ satisfies a metric uncertainty relation on A: we get

$$\frac{1}{t} \sum_k \frac{1}{2} \sum_{x \in S} \left| p^A_{U_k|e_i\rangle}(x) - \frac{1}{2^n} \right| \leq \frac{1}{t} \sum_k \frac{1}{2} \sum_{x \in [d_A]} \left| p^A_{U_k|e_i\rangle}(x) - \frac{1}{2^n} \right| \leq \epsilon$$

and

$$\frac{1}{2} \left| \frac{|S|}{2^n} - \alpha \right| = \frac{1}{2} \left| \frac{|S|}{2^n} - \frac{1}{t} \sum_{x' \in S} \sum_{k=0}^{t-1} p^A_{U_k|e_i\rangle}(x') \right| \leq \epsilon. \tag{26}$$

As a result, we have

$$\Delta\left(p_{X|[I=i]}, p_X\right) \leq \frac{2\epsilon}{\alpha}.$$

Using (26), we have $\alpha \geq |S| 2^{-n} - \epsilon \geq 2^{\ell - n} - \epsilon$. If $\epsilon < 2^{\ell - n}$, we get

$$\Delta\left(p_{X|[I=i]}, p_X\right) \leq \frac{2\epsilon}{2^{\ell - n} - \epsilon}.$$

In the general case when X has min-entropy ℓ, the distribution of X can be seen as a mixture of uniform distributions over sets of size at least 2^ℓ. So there exist independent random variables $J \in \mathbb{N}$ and $\{X_j\}$ uniformly distributed on sets of size at least 2^ℓ such that $X = X_J$. One can then write

$$\frac{1}{2}\sum_x |\mathbf{P}\{X = x|I = i\} - \mathbf{P}\{X = x\}| = \frac{1}{2}\sum_{x,j} |\mathbf{P}\{J = j\}(\mathbf{P}\{X_j = x|I = i, J = j\} - \mathbf{P}\{X_j = x|J = j\})|$$
$$\leq \frac{2\epsilon}{2^{\ell-n} - \epsilon}.$$

□

Using Theorem 3.3 together with the existence of metric uncertainty relations (Theorem 2.5), we show the existence of ϵ-locking schemes whose key size depends only on ϵ and not on the size of the encoded message. This result was not previously known.

Corollary 3.4 (Existence of locking schemes)**.** *Let $c = 9\pi^2$, $n \geq 8 + \log c$ and $\epsilon \in (0, 1)$. Then there exists an ϵ-locking scheme encoding an n-bit message using a key of at most $2\log(1/\epsilon) + O(\log\log(1/\epsilon))$ bits into at most $n + 2\log(18/\epsilon)$ qubits.*

Remark. Observe that in terms of number of bits, the size of the key is only a factor of two larger (up to smaller order terms) than the lower bound of $\log(1/(\epsilon + 2^{-n}))$ bits that can be obtained by guessing the key. In fact, consider the strategy of performing the decoding operation corresponding to the key value 0. In this case, we have $\mathbf{P}\{X = i|I = i\} \geq \mathbf{P}\{K = 0\} = 1/t$. Thus, $\Delta(p_{X|I=i}, p_X) \geq 1/t - 2^{-n}$.

Recall that we can increase the size of the message to be equal to the number of qubits of the ciphertext. The key size becomes at most $4\log(1/\epsilon) + O(\log(\log(1/\epsilon))$. □

Proof Use the construction of Theorem 2.5 with $d_A = 2^n$ and $d_B = 2^q$ such that $2^{q-1} < 9/\epsilon^2 \leq 2^q$ and $d = d_A d_B$. Take $t = 2^p$ to be the power of two with $2^{p-1} \leq \frac{4 \cdot 18 c \log(9/\epsilon)}{\epsilon^2} < 2^p$. □

The following corollary gives explicit locking schemes. We mention the constructions based on Theorems 2.16 and 2.17. Of course, one could obtain a tradeoff between the key size and the dimension of the quantum system.

Corollary 3.5 (Explicit locking schemes)**.** *Let $\delta > 0$ be a constant, n be a positive integer, $\epsilon \in (2^{-c'n}, 1)$ (c' is a constant independent of n).*

- *Then, there exists an efficient ϵ-locking scheme encoding an n-bit message in a quantum state of $n' \leq (4+\delta)n + O(\log(1/\epsilon))$ qubits using a key of size $O(\log(n/\epsilon))$ bits. In fact, both the encoding and decoding operations are computable using a classical computation with polynomial running time and a quantum circuit with only Hadamard gates and preparations and measurements in the computational basis.*
- *There also exists an efficient ϵ-locking scheme $\mathcal{E}'$ encoding an n-bit message in a quantum state of n qubits using a key of size $O(\log(n/\epsilon) \cdot \log n)$ bits. $\mathcal{E}'$ is computable by a classical algorithm with expected runtime $O(n^2 \operatorname{polylog} n)$ and a quantum circuit of size $O(n \operatorname{polylog}(n/\epsilon))$.*

Proof For the first result, we observe that the construction of Theorem 3.3 encodes the message in the computational basis. Recall that the untaries U_k of Theorem 2.16 are of the form $U_k = P_k V_k$ where P_k is a permutation of the computational basis. Hence, it is possible to *classically* compute the element of the computational basis $P_k^\dagger |x\rangle|b\rangle$. One can then prepare the state $P_k^\dagger |x\rangle|b\rangle$ and apply the unitary $V_k^\dagger$ to obtain the ciphertext. The decoding is performed in a similar way. One first applies the unitary V_k, measures in the computational basis and then applies the permutation P_k to the n-bit string corresponding to the outcome.

For the second construction, we apply Theorem 2.17 with $n' = n + c'\lceil\log\log n + \log(1/\epsilon)\rceil$ for some large enough constant c'. We can then use a one-time pad encryption on the input to the B system. This increases the size of the key by only $c'\lceil\log\log n + \log(1/\epsilon)\rceil$ bits. □

As mentioned earlier (see equation (21)), explicit states that exhibit locking behaviour have been presented in [DHL+04]. However, this is the first explicit construction of states ω that achieves the following strong locking behaviour: for any $\delta > 0$, for n large enough, the state ω^{XCK} verifies $\mathbf{I}_c(X; C)_\omega \leq \delta$ and $\mathbf{I}_c(X; CK)_\omega = n + \log d_K$ where K is a classical $O(\log(n/\delta))$-bit system. This is a direct consequence of Corollary 3.5 taking $\epsilon = \delta/(20n)$, and Proposition 3.2. We should also mention that the authors of [KRBM07] explicitly construct a state exhibiting some weak locking behaviour.

3.3 Quantum hiding fingerprints

In this section, we show that the locking scheme of Corollary 3.4 can be used to build mixed state quantum hiding fingerprints as defined by Gavinsky and Ito [GI10]. A quantum fingerprint [BCWdW01] encodes an n-bit string into a quantum state ρ_x of $n' \ll n$ qubits such that given $y \in \{0,1\}^n$ and the fingerprint ρ_x, it is possible to decide with small error probability whether $x = y$. The additional hiding property ensures that measuring ρ_x leaks very little information about x. Gavinsky and Ito [GI10] used the accessible information[2] as a measure of the hiding property. Here, we strengthen this definition by imposing a bound on the total variation distance instead (see Proposition 2.2).

Definition 3.6 (Quantum hiding fingerprint)**.** *Let n be a positive integer, $\delta, \epsilon \in (0,1)$ and C be a Hilbert space. An encoding $f : \{0,1\}^n \to \mathcal{S}(C)$ together with a set with a set of measurements $\{M^y, \mathbb{1} - M^y\}$ for each $y \in \{0,1\}^n$ is a (δ, ϵ)-hiding fingerprint if*

1. *(Fingerprint property) For all $x \in \{0,1\}^n$, $\mathrm{tr}\,[M^x f(x)] = 1$ and for $y \neq x$, $\mathrm{tr}\,[M^y f(x)] \leq \delta$.*
2. *(Hiding property) Let X be uniformly distributed. Then, for any POVM $\{N_i\}$ on the system C whose outcome on $f(X)$ is denoted I, we have for all possible outcomes i,*

$$\Delta\left(p_{X|[I=i]}, p_X\right) \leq \epsilon.$$

We usually want the Hilbert space C to be composed of $O(\log n)$ qubits. Gavinsky and Ito [GI10] proved that for any constant c, there exists efficient quantum hiding fingerprinting schemes for which the dimension of the quantum system C is $O(\log n)$ and both the error probability δ and the accessible information are bounded by $1/n^c$. Here, we prove that the same result can be obtained by locking a classical fingerprint. The general structure of our quantum hiding fingerprint for parameters n, δ and ϵ is as follows:

1. Choose a random prime $p \in \mathcal{P}_{n,\epsilon,\delta}$ uniformly from the set $\mathcal{P}_{n,\epsilon,\delta}$.
2. Set $t = \lceil c \log(1/\epsilon)\epsilon^{-2} \rceil$, $d_A = p$ and $d_B = \lceil c'/\epsilon^2 \rceil$ and generate t random unitaries $U_0^p, \dots, U_{t-1}^p$ acting on $A \otimes B$.
3. The fingerprint consists of the random prime p and the state $(U_k^p)^\dagger |x \bmod p\rangle^A |b\rangle^B$ where $k \in [t]$ and $b \in [d_B]$ are chosen uniformly and independently. The density operator representing this state is denoted $f(x) \stackrel{\text{def}}{=} \frac{1}{td_B} \sum_{k,b} (U_k^p)^\dagger |x \bmod p\rangle\langle x \bmod p|^A |b\rangle\langle b|^B U_k^p$.

Observe that even though this protocol is randomized because the unitaries are chosen at random, it is possible to implement it with polynomial resources in n as the size of the message to be locked is $O(\log n)$ bits. In fact, one can approximately sample a random unitary in dimension $2^{O(\log n)}$ using a polynomial number of public random bits. The mixed state protocol of [GI10] achieves roughly the same parameters. Their construction is also randomized but it uses random codes instead of random unitaries. For this reason, the protocol of [GI10] would probably be more efficient in practice.

Theorem 3.7. *There exists constants c, c' and c'', such that for all positive integer n, $\delta, \epsilon \in (0, 1/4)$ if we define $\mathcal{P}_{n,\delta,\epsilon}$ to be the set of primes in the interval $[l, u]$ where*

$$l = \left(\frac{c''}{\delta} \cdot \frac{\log^2(1/\epsilon)}{\epsilon^8}\right)^{1/0.9} + 10n \quad \textit{and} \quad u = l + (2n/\delta)^2$$

and provided $u \leq 2^{n-2}$, the scheme described above is a (δ, ϵ)-hiding fingerprint with probability $1 - 2^{-\Omega(n)}$ over the choice of random unitaries.

The proof of this result involves two parts. First, we need to show that the fingerprint of a uniformly distributed $X \in \{0,1\}^n$ does not give away much information about X. This follows easily from Theorem 2.5 and Theorem 3.3. We also need to show that for every $y \in \{0,1\}^n$, there is a measurement that Bob can apply to the fingerprint to determine with high confidence whether it corresponds to a fingerprint of y or not. In order to prove this, we use the following proposition on the Gram-Schmidt orthonormalisation of a set of almost orthogonal vectors.

[2]The accessible information about X in a quantum system C refers to the maximum over all measurements of the system C of $\mathbf{I}(X; I)$ where I is the outcome of that measurement.

Proposition 3.8. *Let $v'_1, \ldots, v'_r$ be a sequence of unit length vectors in a Hilbert space. Let $0 < \delta \leq \frac{1}{16r}$. For any $i \neq j$, suppose $|\langle v'_i | v'_j \rangle| \leq \delta$. Let $v_1, \ldots, v_r$ be the corresponding sequence of vectors got by Gram-Schmidt orthonormalising $v'_1, \ldots, v'_r$. Then for any i, $\|v_i - v'_i\|_2 \leq \delta\sqrt{32(i-1)}$.*

Proof Since $|\langle v'_i | v'_j \rangle| < \delta < 1/r$ for any $i \neq j$, the vectors $v'_1, \ldots, v'_r$ are linearly independent. Define Π_0 to be the zero linear operator. For $i \geq 1$, define Π_i to be the orthogonal projection onto the subspace spanned by the vectors $v'_1, \ldots, v'_i$. Observe that for any i, $v'_1, \ldots, v'_i$ and $v_1, \ldots, v_i$ span the same space, and $v_{i+1} = \frac{v'_{i+1} - \Pi_i(v'_{i+1})}{\|v'_{i+1} - \Pi_i(v'_{i+1})\|_2}$. We shall prove by induction on i that $\|\Pi_i(v'_k)\|_2 \leq 4\delta\sqrt{i}$ for all i and all $k > i$. This will prove the desired statement since

$$\begin{aligned} \|v_i - v'_i\|_2^2 &= \|\Pi_{i-1}(v'_i)\|_2^2 + \left(1 - \|v'_i - \Pi_{i-1}(v'_i)\|_2\right)^2 \\ &= \|\Pi_{i-1}(v'_i)\|_2^2 + \left(1 - \sqrt{1 - \|\Pi_{i-1}(v'_i)\|_2^2}\right)^2 \\ &= 2 - 2\sqrt{1 - \|\Pi_{i-1}(v'_i)\|_2^2} \;\leq\; 2 - 2\sqrt{1 - 16\delta^2(i-1)} \\ &\leq 32\delta^2(i-1). \end{aligned}$$

The base case of $i = 1$ is trivial. Assume that the induction hypothesis holds for a particular i. Let $1 \leq j \leq i+1$ and $k > i+1$. Observe that $v'_j = \Pi_{j-1}(v'_j) + \sqrt{1 - \|\Pi_{j-1}(v'_j)\|_2^2}\, v_j$. We have

$$\begin{aligned} |\langle v'_k | v'_j \rangle| &= \left| \langle v'_k | \Pi_{j-1}(v'_j) \rangle + \sqrt{1 - \|\Pi_{j-1}(v'_j)\|_2^2}\, \langle v'_k | v_j \rangle \right| \\ &= \left| \langle \Pi_{j-1}(v'_k) | \Pi_{j-1}(v'_j) \rangle + \sqrt{1 - \|\Pi_{j-1}(v'_j)\|_2^2}\, \langle v'_k | v_j \rangle \right| \\ &\geq \sqrt{1 - \|\Pi_{j-1}(v'_j)\|_2^2}\, |\langle v'_k | v_j \rangle| - \|\Pi_{j-1}(v'_k)\|_2\, \|\Pi_{j-1}(v'_j)\|_2, \end{aligned}$$

which implies that

$$\begin{aligned} |\langle v'_k | v_j \rangle| &\leq \frac{|\langle v'_k | v'_j \rangle| + \|\Pi_{j-1}(v'_k)\|_2\, \|\Pi_{j-1}(v'_j)\|_2}{\sqrt{1 - \|\Pi_{j-1}(v'_j)\|_2^2}} \\ &\leq \frac{\delta + 16\delta^2(j-1)}{\sqrt{1 - 16\delta^2(j-1)}} \;\leq\; \frac{\delta + \delta}{\sqrt{1 - \delta}} \\ &\leq 4\delta. \end{aligned}$$

Thus, $\|\Pi_{i+1}(v'_k)\|_2^2 = \sum_{j=1}^{i+1} |\langle v'_k | v_j \rangle|^2 \leq 16\delta^2(i+1)$, which gives $\|\Pi_{i+1}(v'_k)\|_2 \leq 4\delta\sqrt{i+1}$ completing the induction. □

Using this result we can prove the following lemma.

Lemma 3.9. *Let $\{U_0, \ldots, U_{t-1}\}$ be a set of unitary transformations on AB that define γ-MUBs and $d^{-\gamma/2} \leq 1/(16td_B)$ where $d \stackrel{def}{=} d_A d_B$. Define for $y \in [d_A]$ the subspace $F_y = span\{U_k^\dagger |y\rangle|b\rangle, k \in [t], b \in [d_B]\}$. Then for any $x \in [d_A]$, $y \neq x$, $k_0 \in [t]$ and $b_0 \in [d_B]$,*

$$\mathrm{tr}\left[\Pi_{F_y} U_{k_0}^\dagger |x\rangle|b_0\rangle\right] \leq 2\sqrt{32}(td_B)^2 d^{-\gamma}.$$

where Π_F is the projector on the subspace F.

Proof Consider the set of vector $\{U_k^\dagger|y\rangle|b\rangle\}_{k\in[t],b\in[d_B]}$. We have for all $(k,b) \neq (k',b')$,

$$|\langle y|\langle b'|U_{k'} U_k^\dagger|y\rangle|b\rangle| \leq d^{-\gamma/2}.$$

Picking any fixed ordering on $[t] \times [d_B]$, define $\{|e_{k,b}(y)\rangle\}_{k,b}$ to be the set of vectors obtained by Gram-Schmidt orthonormalising $\{U_k^\dagger|y\rangle|b\rangle\}_{k\in[t],b\in[d_B]}$. Using Proposition 3.8, we have $\||e_{k,b}(y)\rangle - U_k^\dagger|y\rangle|b\rangle\|_2 \leq d^{-\gamma/2}\sqrt{32td_B}$.

Thus,

$$\begin{aligned}
\operatorname{tr}\left[\Pi_{F_y} U_{k_0}^\dagger |x\rangle|b_0\rangle\right] &= \sum_{k,b} |\langle e_{k,b}(y)|U_{k_0}^\dagger|x\rangle|b_0\rangle|^2 \\
&\leq \sum_{k,b} \left| |\langle y|\langle b'|U_{k'}U_{k_0}^\dagger|x\rangle|b_0\rangle| + \| |e_{k,b}(y)\rangle - U_k^\dagger|y\rangle|b\rangle\|_2 \right|^2 \\
&\leq td_B \cdot d^{-\gamma}\left(\sqrt{32td_B}+1\right)^2 \\
&\leq 2\sqrt{32}(td_B)^2 d^{-\gamma}.
\end{aligned}$$

□

Proof of Theorem 3.7 We start by proving the hiding property. For any fixed p, the random variable $Z \stackrel{\text{def}}{=} X \bmod p$ is almost uniformly distributed on $[p]$. In fact, we have for any $z \in [p]$, $\mathbf{P}\{Z=z\} \leq \frac{2^n/p+1}{2^n}$. In other words, $\mathbf{H}_{\min}(Z) \geq \log p - \log(1+p2^{-n})$. Thus, using Theorem 2.5 and Theorem 3.3, we have that except with probability exponentially small in n (on the choice of the random unitary), the fingerprinting scheme satisfies for any measurement outcome i

$$\Delta\left(p_{Z|[I=i]}, p_Z\right) \leq \frac{2\epsilon}{\frac{1}{1+p2^{-n}} - \epsilon} \leq 4\epsilon$$

where I denotes the outcome of a measurement on the state $f(X)$. Recall that we are interested in the information leakage about X not Z. For this, we note that the random variables X, Z, I form a Markov chain. Thus,

$$\begin{aligned}
\Delta\left(p_{X|[I=i]}, p_X\right) &= \sum_{x\in\{0,1\}^n}\left|\sum_{z\in[p]} \mathbf{P}\{Z=z|I=i\}\,\mathbf{P}\{X=x|I=i,Z=z\} - \mathbf{P}\{Z=z\}\,\mathbf{P}\{X=x|Z=z\}\right| \\
&= \sum_{x\in\{0,1\}^n}\left|\sum_{z\in[p]} \mathbf{P}\{Z=z|I=i\}\,\mathbf{P}\{X=x|Z=z\} - \mathbf{P}\{Z=z\}\,\mathbf{P}\{X=x|Z=z\}\right| \\
&\leq \sum_{z\in[p]} |\mathbf{P}\{Z=z|I=i\} - \mathbf{P}\{Z=z\}| \sum_{x\in\{0,1\}^n} \mathbf{P}\{X=x|Z=z\} \\
&= \Delta\left(p_{Z|[I=i]}, p_Z\right) \leq 4\epsilon.
\end{aligned}$$

This proves the hiding property.

We then analyse the fingerprint property. Let $x, y \in [2^n]$ and p be the random prime of the fingerprint. We define the measurements by $M^y = \Pi_{F_y}$ for all $y \in \{0,1\}^n$ where Π_{F_y} is the projector onto the subspace $F_y = \text{span}\{U_k^{p\dagger}|y \bmod p\rangle|b\rangle, k\in[t], b\in[d_B]\}$. If $x=y$, then $f(x)$ is a mixture of states in $\text{span}\{U_k^{p\dagger}|y \bmod p\rangle|b\rangle, k\in[t], b\in[d_B]\}$. Thus $\operatorname{tr}[M^y f(x)] = 1$.

We now suppose that $x \neq y$. First, we have $\mathbf{P}\{x \bmod p = y \bmod p\} = \mathbf{P}\{x-y \bmod p = 0\} \leq \delta/2$ as the number of distinct prime divisors of $x-y$ is at most n and the number of primes in $[l,u]$ is at least $2n/\delta$ for n large enough. Then, whenever $x \bmod p \neq y \bmod p$, Lemma 3.9 gives

$$\begin{aligned}
\operatorname{tr}\left[\Pi_{F_y} f(x)\right] &\leq 2\sqrt{32}(td_B)^2(d_Ad_B)^{-0.9} \\
&\leq 2\sqrt{32}\cdot 4c^2c'^2\frac{\log^2(1/\epsilon)}{\epsilon^8}\cdot\frac{\delta\epsilon^8}{c''\log^2(1/\epsilon)} \\
&\leq \delta/2
\end{aligned}$$

for c'' large enough with probability $1-2^{-\Omega(d_Ad_B)} = 1-2^{-\Omega(n)}$ over the choice of the random unitaries (using Theorem 2.5). Finally, we get $\operatorname{tr}\left[\Pi_{F_y} f(x)\right] \leq \delta$ with probability $1-2^{-\Omega(n)}$. □

3.4 String commitment

In this section, we show how to use a locking scheme to obtain a weak form of bit commitment [BCH+06]. Bit commitment is an important two-party cryptographic primitive defined as follows. Consider two mutually distrustful parties Alice and Bob who are only allowed to communicate over some channel. The objective is to be able to achieve the following: Alice secretly chooses a bit x and communicates with Bob to convince him that she fixed her choice, without revealing the actual bit x. This is the commit stage. At the reveal stage, Alice reveals the secret x and enables Bob to open the commitment. Bob can then check whether Alice was honest.

Using classical or quantum communication, unconditionally secure bit commitment is known to be impossible [May97, LC97]. However, commitment protocols with weaker security guarantees do exist [SR01, DFSS05, BCH$^+$06, BCH$^+$08]. Here, we consider the string commitment scenario studied in [BCH$^+$08, Section III]. In a string commitment protocol, Alice commits to an n-bit string. Alice's ability to cheat is quantified by the number of strings she can reveal successfully. The ability of Bob to cheat is quantified by the information he can obtain about the string to be committed. One can formalize these notions in many ways. We use a security criterion that is similar to the one of [BCH$^+$08] except that we use the statistical distance between the outcome distribution and the uniform distribution, instead of the accessible information. Our definition is slightly stronger by virtue of Proposition 3.2. For a detailed study of string commitment in a more general setting, see [BCH$^+$08].

Definition 3.10. *An (n, α, β)-*quantum bit string commitment *is a quantum communication protocol between Alice (the committer) and Bob (the receiver) which has two phases. When both players are honest the protocol takes the following form.*

- *(Commit phase) Alice chooses a string $X \in \{0,1\}^n$ uniformly. Alice and Bob communicate, after which Bob holds a state ρ_X.*
- *(Reveal phase) Alice and Bob communicate and Bob learns X.*

The parameters α and β are security parameters.

- *If Alice is honest, then for any measurement performed by Bob on her state ρ_X, we have $\Delta\left(p_X, p_{X|[I=i]}\right) \leq \frac{\beta}{n}$ where I is the outcome of the measurement.*
- *If Bob is honest, then for all commitments of Alice: $\sum_{x\in\{0,1\}^n} p_x \leq 2^\alpha$, where p_x is the probability that Alice successfully reveals x.*

Following the strategy of [BCH$^+$08], the following protocol for string commitment can be defined using a locking scheme $\mathcal{E}$.

- Commit phase: Alice has the string $X \in \{0,1\}^n$ and chooses a key $K \in [t]$ uniformly at random. She sends the state $\mathcal{E}(X, K)$ to Bob.
- Reveal phase: Alice announces both the string X and the key K. Using the key, Bob decodes some value X'. He accepts if $X = X'$.

A protocol is said to be efficient if both the communication (in terms of the number of qubits exchanged) is polynomial in n and the computations performed by Alice and Bob can be done in polynomial time on a quantum computer. The protocol presented in [BCH$^+$08] is not efficient in terms of computation and is efficient in terms of communication only if the cost of communicating a (random) unitary in dimension 2^n is disregarded. Using the efficient locking scheme of Corollary 3.5, we get

Corollary 3.11. *Let n be a positive integer and $\beta \in (n2^{-cn}, n)$ (c is a constant independent of n). There exists an efficient $(n, c\log(n^2/\beta), \beta)$-quantum bit string commitment protocol for some constant c independent of n and β.*

Proof We use the first construction of Corollary 3.5 with $\epsilon = \beta/n$. If Bob is honest, the security analysis is exactly the same as [BCH$^+$08]. If Alice is honest, the security follows directly from the definition of the locking scheme. □

3.5 Locking entanglement of formation

The entanglement of formation is a measure of the entanglement in a bipartite quantum state that attempts to quantify the number of singlets required to produce the state in question using only local operations and classical communication [BDSW96]. For a bipartite state ρ^{XY}, the entanglement of formation is defined as

$$\mathbf{E}_f(X;Y)_\rho = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i \mathbf{S}(X)_{\psi_i}. \tag{27}$$

where the minimization is taken over all possible ways to write $\rho^{XY} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with $\sum_i p_i = 1$. Entanglement of formation is related to the following quantity:

$$\mathbf{I}^{\leftarrow}(X;Y')_\rho = \max_{\{M_i\}} \mathbf{I}(X;I)$$

where the maximization is taken over all measurements $\{M_i\}$ performed on the system Y' and I is the outcome of this measurement. Koashi and Winter [KW04] showed that for a pure state $|\rho\rangle^{XYY'}$, a simple identity holds:

$$\mathbf{E}_f(X;Y)_\rho + \mathbf{I}^{\leftarrow}(X;Y')_\rho = \mathbf{S}(X)_\rho. \tag{28}$$

Let $\{U_0, \dots, U_{t-1}\}$ be a set of unitary transformations of $A \otimes B \simeq C$ and define

$$|\rho\rangle^{ABCA'K} = \frac{1}{d_A d_B} \sum_{k\in[t], a\in[d_A], b\in[d_B]} |a\rangle^A |b\rangle^B \left(U_k^\dagger |a\rangle \otimes |b\rangle\right)^C |a\rangle^{A'} |k\rangle^K.$$

If $\{U_0, \dots, U_{t-1}\}$ satisfies an ϵ-metric uncertainty relation, then we get a locking effect using Theorem 3.3 and Proposition 3.2. In fact, we have $\mathbf{I}^{\leftarrow}(A;C)_\rho \le 2\epsilon \log d_A + \eta(\epsilon)$ and $\mathbf{I}^{\leftarrow}(A;CK) = \log d_A$. Thus, using (28), we get

$$\mathbf{E}_f(A;A'BK)_\rho = \mathbf{S}(A)_\rho - \mathbf{I}^{\leftarrow}(A;C)_\rho \ge (1-2\epsilon)\log d_A - \eta(\epsilon)$$

and discarding the system K of dimension t we obtain a separable state

$$\mathbf{E}_f(A;A'B)_\rho = 0.$$

Explicit states exhibiting weak locking behaviour of the entanglement of formation have been presented in [HHHO05]. Strong but non-explicit instances of locking the entanglement of formation were derived in [HLW06]. Here, using Theorem 2.16, we obtain explicit examples of strong locking behaviour.

4 Quantum identification codes

Consider the following quantum analogue of the equality testing communication problem. Alice is given an n-qubit state $|\psi\rangle \in C$ and Bob is given $|\varphi\rangle \in C$. Namely, Bob wants to output 1 with probability in the interval $[|\langle\psi|\varphi\rangle|^2 - \epsilon, |\langle\psi|\varphi\rangle|^2 + \epsilon]$ and 0 with probability in the interval $[1 - |\langle\psi|\varphi\rangle|^2 - \epsilon, 1 - |\langle\psi|\varphi\rangle|^2 + \epsilon]$. This task is referred to as quantum identification [Win04]. Note that communication only goes from Alice to Bob. There are many possible variations to this problem. One of the interesting models is when Alice receives the quantum state $|\psi\rangle$ and Bob gets a classical description of $|\varphi\rangle$. An ϵ-quantum-ID code is defined by an encoder, which is a quantum operation that maps Alice's quantum state $|\psi\rangle$ to another quantum state which is transmitted to Bob, and a family of decoding POVMs $\{D_\varphi, \mathbb{1} - D_\varphi\}$ for all $|\varphi\rangle$ that Bob performs on the state he receives from Alice.

Definition 4.1 (Quantum identification [Win04])**.** *Let $\mathcal{H}_1, \mathcal{H}_2, C$ be Hilbert spaces and $\epsilon \in (0,1)$. An* ϵ-quantum-ID code *for the space C using the channel $\mathcal{N} : \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ consists of an encoding map $\mathcal{E} : \mathcal{S}(C) \to \mathcal{S}(\mathcal{H}_1)$ and a set of POVMs $\{D_\varphi, \mathbb{1} - D_\varphi\}$ acting on $\mathcal{S}(\mathcal{H}_2)$, one for each pure state $|\varphi\rangle$ such that*

$$\forall |\psi\rangle, |\varphi\rangle \in C, \qquad \left| \mathrm{tr}\left[D_\varphi \mathcal{N}(\mathcal{E}(\psi))\right] - |\langle\varphi|\psi\rangle|^2 \right| \le \epsilon.$$

Here we consider channels $\mathcal{N}$ transmitting noiseless qubits and noiseless classical bits. We also say that ϵ-quantum identification of n-qubit states can be performed using ℓ bits and m qubits when there exists an ϵ-quantum-ID code for the space $C = (\mathbb{C}^2)^{\otimes n}$ using the channel $\mathcal{N} = \overline{\mathrm{id}}_2^{\otimes \ell} \otimes \mathrm{id}_2^{\otimes m}$, where $\overline{\mathrm{id}}_2$ and id_2 are the noiseless bit and qubit channels. Hayden and Winter [HW10] showed that classical communication alone cannot be used for quantum identification. However, a small amount of quantum communication makes classical communication useful. Using our metric uncertainty relations, we prove better bounds on the number of qubits of communication and give an efficient encoder for this problem.

Our protocol is based on a duality between quantum identification and geometry preservation demonstrated in [HW10, Theorem 7]. In our particular setting, the direction we use of this duality states that if $V : C \to A \otimes B$ defines a low-distortion embedding of (C, ℓ_2) into $(AB, \ell_1^A(\ell_2^B))$, then the maps $\Gamma_a : C \to B$ for $a \in [d_A]$ defined by $|\psi\rangle \mapsto \sum_{b \in d_B} (\langle a|\langle b|V|\psi\rangle)|b\rangle$ approximately preserve inner products on average. The following lemma gives a precise statement. We give an elementary proof for completeness.

Lemma 4.2. *Let $V : C \to A \otimes B$ be an isometry, i.e., for all $|\psi\rangle \in C$, $\|V|\psi\rangle\|_2 = \||\psi\rangle\|_2$. For any vector $|\psi\rangle \in C$, we define the vectors $|\psi_a\rangle \in B$ by $V|\psi\rangle = \sum_{a\in[d_A]} |a\rangle|\psi_a\rangle$. Assume that V satisfies the following property:*

$$\forall |\psi\rangle \in C \qquad \sum_{a\in[d_A]} \left| \||\psi_a\rangle\|_2^2 - \frac{\||\psi\rangle\|_2^2}{d_A} \right| \leq \epsilon \||\psi\rangle\|_2^2. \tag{29}$$

Then we have for all unit vectors $|\psi\rangle, |\varphi\rangle \in C$ with $V|\psi\rangle = \sum_{a\in[d_A]} |a\rangle|\psi_a\rangle$ and $V|\varphi\rangle = \sum_{a\in[d_A]} |a\rangle|\varphi_a\rangle$

$$\frac{1}{d_A} \sum_{a\in[d_A]} \left| \frac{|\langle\psi_a|\varphi_a\rangle|^2}{\||\psi_a\rangle\|_2 \||\varphi_a\rangle\|_2} - |\langle\psi|\varphi\rangle|^2 \right| \leq 12\epsilon + 4\sqrt{\epsilon}. \tag{30}$$

Proof Let $|\psi\rangle$ and $|\varphi\rangle$ be unit vectors in C. We use the triangle inequality to get

$$\begin{aligned} &\frac{1}{d_A} \sum_{a\in[d_A]} \left| \frac{|\langle\psi_a|\varphi_a\rangle|^2}{\||\psi_a\rangle\|_2 \||\varphi_a\rangle\|_2} - |\langle\psi|\varphi\rangle|^2 \right| \\ &\quad \leq \sum_{a\in[d_A]} \left| \frac{|\langle\psi|\varphi\rangle|^2}{d_A} - |\langle\psi_a|\varphi_a\rangle|^2 \right| + \sum_{a\in[d_A]} \left| |\langle\psi_a|\varphi_a\rangle|^2 - \frac{|\langle\psi_a|\varphi_a\rangle|^2}{d_A \||\psi_a\rangle\|_2 \||\varphi_a\rangle\|_2} \right|. \end{aligned} \tag{31}$$

We start by dealing with the first term in (31). Observe that

$$\begin{aligned} \left| |\langle\psi_a|\varphi_a\rangle|^2 - \frac{|\langle\psi|\varphi\rangle|^2}{d_A} \right| &\leq \left| (\mathbf{Re}\langle\psi_a|\varphi_a\rangle)^2 - \frac{(\mathbf{Re}\langle\psi|\varphi\rangle)^2}{d_A} \right| + \left| (\mathbf{Im}\langle\psi_a|\varphi_a\rangle)^2 - \frac{(\mathbf{Im}\langle\psi|\varphi\rangle)^2}{d_A} \right| \\ &\leq 2 \left| \mathbf{Re}\langle\psi_a|\varphi_a\rangle - \frac{\mathbf{Re}\langle\psi|\varphi\rangle}{d_A} \right| + 2 \left| \mathbf{Im}\langle\psi_a|\varphi_a\rangle - \frac{\mathbf{Im}\langle\psi|\varphi\rangle}{d_A} \right|. \end{aligned} \tag{32}$$

In the last inequality, we used the fact that $(x-y)^2 \leq 2|x-y|$ whenever $|x+y| \leq 2$. To bound these terms, we apply the assumption about V (equation (29)) to the vector $|\psi\rangle - |\varphi\rangle$:

$$\sum_{a\in[d_A]} \left| \||\psi_a\rangle - |\varphi_a\rangle\|_2^2 - \frac{\||\psi\rangle - |\varphi\rangle\|_2^2}{d_A} \right| \leq \epsilon \||\psi\rangle - |\varphi\rangle\|_2^2 \leq 4\epsilon.$$

By expanding $\||\psi_a\rangle - |\varphi_a\rangle\|_2^2$ and $\||\psi\rangle - |\varphi\rangle\|_2^2$, we obtain using the triangle inequality

$$\begin{aligned} \sum_{a\in[d_A]} \left| 2\mathbf{Re}\langle\psi_a|\varphi_a\rangle - \frac{2\mathbf{Re}\langle\psi|\varphi\rangle}{d_A} \right| &\leq 4\epsilon + \sum_{a\in[d_A]} \left| \||\psi_a\rangle\|_2^2 - \frac{\||\psi\rangle\|_2^2}{d_A} \right| + \left| \||\varphi_a\rangle\|_2^2 - \frac{\||\varphi\rangle\|_2^2}{d_A} \right| \\ &\leq 6\epsilon. \end{aligned}$$

In the last inequality, we used equation (29) for $|\psi\rangle$ and $|\varphi\rangle$. The same argument can be applied to $i|\psi\rangle$ and $|\varphi\rangle$ to get

$$2 \sum_{a\in[d_A]} \left| \mathbf{Im}\langle\psi_a|\varphi_a\rangle - \frac{\mathbf{Im}\langle\psi|\varphi\rangle}{d_A} \right| \leq 6\epsilon$$

Thus, substituting in equation (32) we obtain

$$\left| |\langle\psi_a|\varphi_a\rangle|^2 - \frac{|\langle\psi|\varphi\rangle|^2}{d_A} \right| \leq 12\epsilon.$$

We now consider the second term in (31). We have using the Cauchy-Schwarz inequality

$$\begin{aligned}\sum_{a\in[d_A]}\left||\langle\psi_a|\varphi_a\rangle|^2-\frac{|\langle\psi_a|\varphi_a\rangle|^2}{d_A\||\psi_a\rangle\|_2\||\varphi_a\rangle\|_2}\right| &\le \sum_{a\in[d_A]}\left|\||\psi_a\rangle\|_2\||\varphi_a\rangle\|_2-\frac{1}{d_A}\right|\\ &\le \sum_{a\in[d_A]}\||\psi_a\rangle\|_2\left|\||\varphi_a\rangle\|_2-\frac{1}{\sqrt{d_A}}\right|+\sum_{a\in[d_A]}\left|\frac{\||\psi_a\rangle\|_2}{\sqrt{d_A}}-\frac{1}{d_A}\right|\\ &\le \sqrt{\sum_{a\in[d_A]}\||\psi_a\rangle\|_2^2}\sqrt{\sum_{a\in[d_A]}\left|\||\varphi_a\rangle\|_2-\frac{1}{\sqrt{d_A}}\right|^2}+\sqrt{\sum_{a\in[d_A]}\left|\||\psi_a\rangle\|_2-\frac{1}{\sqrt{d_A}}\right|^2}\\ &\le \sqrt{2\sum_{a\in[d_A]}\left|\||\varphi_a\rangle\|_2^2-\frac{1}{d_A}\right|}+\sqrt{2\sum_{a\in[d_A]}\left|\||\psi_a\rangle\|_2^2-\frac{1}{d_A}\right|}\\ &\le 4\sqrt{\epsilon}.\end{aligned}$$

For the third inequality, we used once again the Cauchy-Schwarz inequality and for the fourth inequality, we used the fact that $\sum_{a\in[d_A]}\||\psi_a\rangle\|_2^2=\|V|\psi\rangle\|_2^2=1$. Plugging this bound in equation (31), we obtain the desired result. □

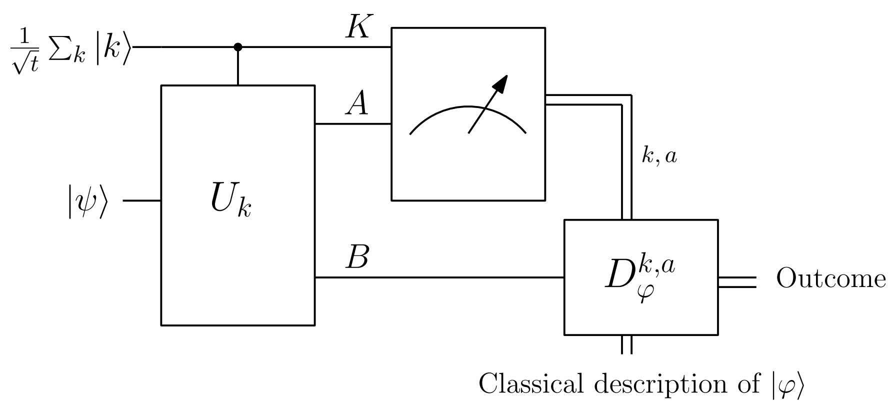

Figure 3: The system K is prepared in a uniform superposition state $\frac{1}{\sqrt{t}}\sum_k|k\rangle$. Then, controlled by system K, the unitary U_k is applied to $C=A\otimes B$. The KA system is then measured in its computational basis. The outcome k,a of this measurement is sent through the classical channel. The system B is sent using the noiseless quantum channel. The receiver constructs a POVM $D_\varphi^{k,a}$ based on a classical description of his state $|\varphi\rangle$ and the classical communication k,a he receives.

Theorem 4.3 (Quantum identification using classical communication)**.** *Let n be a positive integer and $\epsilon\in(2^{-c'n},1)$ (c' is a constant independent of n). Then for some $m=O(\log(1/\epsilon))$, ϵ-quantum identification of n-qubit states can be performed using a single message of n bits and m qubits.*

Moreover, for some $m=O(\log(n/\epsilon)\cdot\log(n))$, ϵ-quantum identification of n-qubit states can be performed using a single message of n bits and m qubits with an encoding quantum circuit of polynomial size.

Proof Let $\{U_0,\ldots,U_{t-1}\}$ be a set of unitaries on n qubits verifying an ϵ'- metric uncertainty relation with $\epsilon'=2(\epsilon/32)^2$ We start by preparing the uniform superposition $\frac{1}{\sqrt{t}}\sum_{k=0}^{t-1}|k\rangle^K$ and apply the unitary U_k on system C controlled by the register K. We get the state $\frac{1}{\sqrt{t}}\sum_k|k\rangle^K(U_k|\psi\rangle)^{AB}=\sum_{k,a}|k\rangle^K|a\rangle^A|\psi_{k,a}\rangle^B$ for some not normalized vectors $|\psi_{k,a}\rangle\in B$. Alice then measures the system KA in the computational basis obtaining an outcome k,a and sends k,a and $|\psi_{k,a}\rangle$ to Bob. Observe that $\sum_{k,a}\||\psi_{k,a}\rangle\|_2^2=1$ and $\||\psi_{k,a}\rangle\|_2^2=\frac{1}{t}\cdot p^A_{U_k|\psi\rangle}(a)$ so that the metric uncertainty relation property can be written as

$$\frac{1}{2}\sum_{k,a}\left|\||\psi_{k,a}\rangle\|_2^2-\frac{1}{td_A}\right|\le\epsilon'. \tag{33}$$

This shows that the isometry $|\psi\rangle \mapsto \frac{1}{\sqrt{t}}\sum_k |k\rangle^K (U_k|\psi\rangle)^{AB}$ satisfies the condition (29) of Lemma 4.2.

The decoding POVMs for received classical information k, a and state $|\varphi\rangle$ are defined by $D_\varphi^{k,a} = |\hat{\varphi}_{k,a}\rangle\langle\hat{\varphi}_{k,a}|$ where $\frac{1}{\sqrt{t}}\sum_k |k\rangle^K (U_k|\varphi\rangle)^{AB} = \sum_{k,a} |k\rangle^K |a\rangle^A |\varphi_{k,a}\rangle^B$ and $|\hat{\varphi}_{k,a}\rangle = |\varphi_{k,a}\rangle / \||\varphi_{k,a}\|_2^2$. Hence, when performing the POVM $\{D_\varphi^{k,a}, \mathbb{1} - D_\varphi^{k,a}\}$ on the state $|\hat{\psi}_{k,a}\rangle \stackrel{\text{def}}{=} |\psi_{k,a}\rangle / \||\psi_{k,a}\rangle\|_2^2$. The protocol is illustrated in Figure 3.

We now analyse the probability that Bob outputs 1. Recall that outcome 1 corresponds to the projector $|\varphi\rangle\langle\varphi|$. The probability that the protocol in Figure 3 outputs 1 is

$$\sum_{k,a} \||\psi_{k,a}\rangle\|_2^2 \cdot \operatorname{tr}\left[D_\varphi^{k,a} |\hat{\psi}_{k,a}\rangle\langle\hat{\psi}_{k,a}|\right] = \sum_{k,a} \||\psi_{k,a}\rangle\|_2^2 |\langle\hat{\psi}_{k,a}|\hat{\varphi}_{k,a}\rangle|^2.$$

Applying Lemma 4.2, we get

$$\frac{1}{td_A}\sum_{k,a} \left| |\langle\hat{\psi}_{k,a}|\hat{\varphi}_{k,a}\rangle|^2 - |\langle\psi|\varphi\rangle|^2 \right| \leq 16\sqrt{2\epsilon'} = \epsilon/2 \tag{34}$$

Using the triangle inequality, equations (34) and (33), we obtain

$$\begin{aligned}\sum_{k,a} \||\psi_{k,a}\rangle\|_2^2 \left| |\langle\hat{\psi}_{k,a}|\hat{\varphi}_{k,a}\rangle|^2 - |\langle\psi|\varphi\rangle|^2 \right| &\leq \sum_{k,a} \frac{1}{td_A} \left| |\langle\hat{\psi}_{k,a}|\hat{\varphi}_{k,a}\rangle|^2 - |\langle\psi|\varphi\rangle|^2 \right| + \sum_{k,a} \left| \||\psi_{k,a}\rangle\|_2^2 - \frac{1}{td_A} \right| \cdot 2 \\ &\leq \epsilon/2 + 4\epsilon' \leq \epsilon.\end{aligned}$$

Thus, the probability of obtaining outcome 1 is in the interval $[|\langle\psi|\varphi\rangle|^2 - \epsilon, |\langle\psi|\varphi\rangle|^2 + \epsilon]$. Note that we actually proved something stronger: by a simple application of Markov's inequality, we get that *for most* values of $(k, a) \in [t] \times [d_A]$, the measurement $\{D_\varphi^{k,a}, \mathbb{1} - D_\varphi^{k,a}\}$ as defined above approximately simulates the measurement $\{|\varphi\rangle\langle\varphi|, \mathbb{1} - |\varphi\rangle\langle\varphi|\}$.

We conclude by using the metric uncertainty relations of Theorems 2.5 and 2.17. For the explicit construction, we still need to argue that the encoding can be computed by a quantum circuit of size $O(n^2 \operatorname{polylog}(n/\epsilon))$ and depth $O(n \operatorname{polylog}(n/\epsilon))$ using classical precomputation. To obtain this running time, we actually use the 1-MUBs of Lemma 2.11 in the construction of Theorem 2.17. The only thing we need to precompute is an irreducible polynomial of degree n over $\mathbb{F}_2[X]$. Then, using the same argument as in the proof of Lemma 2.11, we can compute the unitary operation that takes as input the state $|j\rangle \otimes |\psi\rangle$ and outputs the state $|j\rangle \otimes V_j|\psi\rangle$ using a circuit of size $O(n^2 \operatorname{polylog} n)$ and depth $O(n \operatorname{polylog} n)$. Since the permutation extractor we use can be implemented by a quantum circuit of size $O(n \operatorname{polylog}(n/\epsilon))$, the unitary transformation $|k\rangle \otimes |\psi\rangle \mapsto |k\rangle \otimes U_k|\psi\rangle$ can be computed by a quantum circuit of size $O(n^2 \operatorname{polylog}(n/\epsilon))$ and depth $O(n \operatorname{polylog}(n/\epsilon))$. □

This result can be thought of as an analogue of the well-known fact that the public-coin randomized communication complexity of equality is $O(\log(1/\epsilon))$ for an error probability ϵ. Quantum communication replaces classical communication and classical communication replaces public random bits. Classical communication can be thought of as an extra resource because on its own it is useless for quantum identification [HW10, Theorem 11].

5 Conclusion

We have seen how the problem of finding uncertainty relations is closely related to the problem of finding large almost Euclidean subspaces of $\ell_1(\ell_2)$. Even though we did not use any norm embedding result directly, many of the ideas presented here come from the proofs and constructions in the study of the geometry of normed spaces. In particular, we obtained an explicit family of bases that satisfy a strong metric uncertainty relation by adapting a construction of Indyk [Ind07]. Moreover, using standard techniques from asymptotic geometric analysis, we were able to prove a strong result on the uncertainty relations defined by random unitaries [HLSW04].

We used these uncertainty relations to exhibit strong locking effects. In particular, we obtained the first explicit construction of a method for encrypting a random n-bit string in an n-qubit state using a classical key of size polylogarithmic in n. Moreover, our non-explicit results give better key sizes than previous constructions while simultaneously meeting a stronger locking definition. In particular, we showed that an arbitrarily long message can be encrypted with a constant-sized key. Our results on locking are summarized in Table 1. We should emphasize that, even though we presented information locking from a cryptographic point of view, it is not a composable primitive because an eavesdropper could choose to store quantum information about the message instead of measuring. For this reason, a locking scheme has to be used with great care when composed with other cryptographic primitives.

As a cryptographic task, one could compare a locking scheme to an entropically secure encryption scheme [RW02, DS05]. These two schemes achieve the same task of encrypting a high entropy message using a small key. The security definition of a locking scheme is strictly stronger. In fact, for a classical eavesdropper (i.e., an eavesdropper that can only measure) an ϵ-locking scheme is secure in a strong sense. This additional security guarantee comes at the cost of upgrading classical communication to quantum communication. With respect to quantum entropically secure encryption [Des09, DD10], the security condition of a locking scheme is also more stringent. However, a quantum entropically secure scheme allows the encryption of quantum states.

Nonetheless, we note that an ϵ-locking scheme hides the message in a stronger sense if the adversary is limited to a small quantum memory. In fact, using the same technique as [HMR$^+$10, Corollary 2] based on [RRS09], if the adversary is allowed to store m qubits, then the joint state of the message and the knowledge of the adversary is $(c2^{m/2}\epsilon)$-close to a product state for some universal constant c. For example, if $m = O(\log n)$, then a key of logarithmic size can still be used. This is especially interesting for the scheme presented in Corollary 3.5, for which the sender and the receiver do not use any quantum memory. One could then use such a scheme for key distribution in the bounded quantum storage model, where the adversary is only allowed to have a quantum memory of logarithmic size in n and an arbitrarily large classical memory. Note that even though this is a strong assumption compared to the unconditional security of BB84 [BB84], one advantage of such a protocol for key distribution is that it only uses one-way communication between the two parties. In fact, the BB84 quantum key distribution protocol needs interaction between the two parties.

We also used uncertainty relations to construct quantum identification codes. We proved that it is possible to identify a quantum state of n qubits by communicating n classical bits and $O(\log(1/\epsilon))$ quantum bits. We also presented an efficient encoder for this problem that uses $O(\log^2(n/\epsilon))$ qubits of communication instead. The main weakness of this result is that the decoder uses a classical description of the state $|\varphi\rangle$ that is in general exponential in the number of qubits of $|\varphi\rangle$. But as shown in [Win04], if Bob was to receive a copy of the quantum state $|\varphi\rangle$, the task of quantum identification becomes the same as the task of transmission.

Acknowledgments

OF would like to thank Luc Devroye for many discussions on concentration inequalities and in particular about Lemma 2.8. We would also like to thank Tsuyoshi Ito, Marius Junge, Gideon Schechtman, Stanislaw Szarek and Andreas Winter for helpful conversations, as well as the Mittag-Leffler Institute for its hospitality. This research was supported by the Canada Research Chairs program, the Perimeter Institute, CIFAR, FQRNT's INTRIQ, MITACS, NSERC, ONR through grant N000140811249 and QuantumWorks.

Appendices

A Existence of metric uncertainty relations

In this section, we prove the lemmas used in Theorem 2.5.

Lemma 2.6 (Average value of $\ell_1^A(\ell_2^B)$ on the sphere)**.** *Let $|\varphi\rangle^{AB}$ be a random pure state on AB. Then,*

$$\sqrt{d_A}\mathbf{E}\left\{F\left(p^A_{|\varphi\rangle}, \textit{unif}([d_A])\right)\right\} = \mathbf{E}\left\{\||\varphi\rangle^{AB}\|_{\ell_1^A(\ell_2^B)}\right\} = \frac{\Gamma(d_B+\frac{1}{2})}{\Gamma(d_B)}\frac{\Gamma(d_A d_B)}{\Gamma(d_A d_B + \frac{1}{2})} \geq \sqrt{1-\frac{1}{d_B}}\sqrt{d_A}.$$

where Γ is the Gamma function $\Gamma(z) = \int_0^\infty u^{z-1}e^{-u}du$ for $z \geq 0$.

Proof The presentation uses methods described in [Bal97].

Observe that the random variable $\||\varphi\rangle^{AB}\|_{12}$ is distributed as the $\ell_1^{d_A}(\ell_2^{2d_B})$ norm of a Haar-distributed *real* random vector on $\mathbb{S}^{2d_A d_B - 1}$. We define for integers n and m the norm $\ell_1^n(\ell_2^m)$ of a real $n+m$-dimensional vector

$\{v_{i,j}\}_{i\in[n],j\in[m]}$ as for the complex case (Definition 2.3)

$$\|v\|_{\ell_1^n(\ell_2^m)} = \sum_i \sqrt{\sum_j |v_{i,j}|^2}.$$

Note that we only specify the dimension of the systems as the systems themselves are not relevant here. In the rest of the proof, we use $\|\cdot\|_{12}$ as a shorthand for $\|\cdot\|_{\ell_1^{d_A}(\ell^{2d_B})}$. Our objective is to evaluate the expected value $\mathbf{E}\{\|\Theta\|_{12}\}$ where Θ has the Haar distribution on the real sphere $\mathbb{S}^{s-1}$ and $s = 2d$ with $d = d_A d_B$. For this, we start by relating the $\mathbf{E}\{\|Z\|_{12}\}$ and $\mathbf{E}\{\|\Theta\|_{12}\}$ where Z has a standard Gaussian distribution on $\mathbb{R}^s$. By changing to polar coordinates, we get

$$\begin{aligned}
\mathbf{E}\{\|Z\|_{12}\} &= \int_{\mathbb{R}^s} \|x\|_{12} \frac{e^{-\frac{1}{2}\sum_{i=1}^s x_i^2}}{(2\pi)^{s/2}} dx \\
&= \int_0^\infty \int_{\mathbb{S}^{s-1}} \|r\theta\|_{12} \frac{e^{-r^2/2}}{(2\pi)^{s/2}} \cdot \frac{s\pi^{s/2} d\sigma(\theta)}{\Gamma(\frac{s}{2}+1)} r^{s-1} dr
\end{aligned}$$

where σ is the normalized Haar measure on $\mathbb{S}^{s-1}$. The term $\frac{s\pi^{s/2}}{\Gamma(\frac{s}{2}+1)}$ is the surface area of the sphere in dimension $s-1$. Using the equality $\Gamma(z+1) = z\Gamma(z)$, we have $\frac{s\pi^{s/2}}{\Gamma(\frac{s}{2}+1)} = \frac{2\pi^{s/2}}{\Gamma(\frac{s}{2})}$. Thus,

$$\begin{aligned}
\mathbf{E}\{\|Z\|_{12}\} &= \frac{2\pi^{s/2}}{(2\pi)^{s/2}\Gamma(\frac{s}{2})} \int_0^\infty r^s e^{-r^2/2} dr \cdot \int_{\mathbb{S}^{s-1}} \|\theta\|_{12} d\sigma(\theta) \\
&= \frac{1}{2^{s/2-1}\Gamma(\frac{s}{2})} \int_0^\infty r^s e^{-r^2/2} dr \cdot \int_{\mathbb{S}^{s-1}} \|\theta\|_{12} d\sigma(\theta)
\end{aligned}$$

We then perform a change of variable $u = r^2/2$:

$$\begin{aligned}
\mathbf{E}\{\|Z\|_{12}\} &= \frac{1}{2^{s/2-1}\Gamma(\frac{s}{2})} \int_0^\infty (2u)^{(s-1)/2} e^{-u} du \cdot \int_{\mathbb{S}^{s-1}} \|\theta\|_{12} d\sigma(\theta) \\
&= \frac{2^{(s-1)/2}\Gamma(\frac{s-1}{2}+1)}{2^{s/2-1}\Gamma(\frac{s}{2})} \cdot \int_{\mathbb{S}^{s-1}} \|\theta\|_{12} d\sigma(\theta) \\
&= \frac{\sqrt{2}\Gamma(\frac{s+1}{2})}{\Gamma(\frac{s}{2})} \cdot \mathbf{E}\{\|\Theta\|_{12}\}. \qquad (35)
\end{aligned}$$

Now, we compute

$$\begin{aligned}
\mathbf{E}\{\|Z\|_{12}\} &= \int_{\mathbb{R}^s} \|x\|_{12} \frac{e^{-\frac{1}{2}\|x\|_2^2}}{(2\pi)^{s/2}} dx \\
&= \sum_{i=0}^{d_A-1} \int_{\mathbb{R}^s} \|x_i\|_2 \frac{e^{-\frac{1}{2}\|x\|_2^2}}{(2\pi)^{s/2}} dx
\end{aligned}$$

where we decomposed $x = (x_0, \ldots, x_{d_A-1})$ where $x_i \in \mathbb{R}^{2d_B}$. As all the terms of the sum are equal

$$\begin{aligned}
\mathbf{E}\{\|Z\|_{12}\} &= d_A \int_{\mathbb{R}^{2d_B}} \|x_0\|_2 \frac{e^{-\frac{1}{2}\|x_0\|_2^2}}{(2\pi)^{d_B}} dx_0 \left(\int_{\mathbb{R}^{2d_B}} \frac{e^{-\frac{1}{2}\|x_1\|_2^2}}{(2\pi)^{d_B}} dx_1 \right)^{d_A-1} \\
&= d_A \frac{\sqrt{2}\Gamma(\frac{2d_B+1}{2})}{\Gamma(d_B)} \int_{\mathbb{S}^{2d_B-1}} \|\theta\|_2 d\sigma(\theta) \\
&= d_A \frac{\sqrt{2}\Gamma(\frac{2d_B+1}{2})}{\Gamma(d_B)}.
\end{aligned}$$

To get the second equality, we use the same argument as for (35). We conclude using equation (35)

$$\begin{aligned}
\mathbf{E}\left\{\||\varphi\rangle\|_{\ell_1^A(\ell_2^B)}\right\} &= \mathbf{E}\{\|\Theta\|_{12}\} \\
&= d_A \frac{\Gamma(d_B + \frac{1}{2})}{\Gamma(d_B)} \cdot \frac{\Gamma(d_A d_B)}{\Gamma(d_A d_B + \frac{1}{2})}.
\end{aligned}$$

We now prove the inequality in the statement of the lemma. We use the following two facts about the Γ function: $\log \Gamma$ is convex and for all $z > 0$, $\Gamma(z+1) = z\Gamma(z)$. The first property can be seen by using Hölder's inequality for example and the second using integration by parts. Using these properties, we have

$$\begin{aligned}\log \Gamma\left(x+\frac{1}{2}\right) &\leq \frac{1}{2}\log\Gamma(x) + \frac{1}{2}\log\Gamma(x+1) \\ &= \frac{1}{2}\log\left(x\Gamma(x)^2\right) \\ &= \log\left(\sqrt{x}\Gamma(x)\right).\end{aligned}$$

Thus, $\frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)} \leq \sqrt{x}$. Similarly, we have $\frac{\Gamma(x)}{\Gamma(x-\frac{1}{2})} \leq \sqrt{x-\frac{1}{2}}$ which implies that $\frac{\Gamma(x+\frac{1}{2})}{\Gamma(x)} \geq \sqrt{x-\frac{1}{2}}$ when writing $\Gamma(x+1/2) = (x-1/2)\Gamma(x-1/2)$.

We conclude that

$$\begin{aligned}\mathbf{E}\left\{\||\varphi\rangle\|_{\ell_1^A(\ell_2^B)}\right\} &\geq d_A \cdot \sqrt{d_B - \frac{1}{2}}\frac{1}{\sqrt{d_A d_B}} \\ &= \sqrt{d_A}\cdot\sqrt{1-\frac{1}{2d_B}}.\end{aligned}$$

□

Lemma 2.7 (Levy's lemma)**.** *Let $f : \mathbb{C}^d \to \mathbb{R}$ and $\eta > 0$ be such that for all pure states $|\varphi_1\rangle, |\varphi_2\rangle$ in $\mathbb{C}^d$,*

$$|f(|\varphi_1\rangle) - f(|\varphi_2\rangle)| \leq \eta \||\varphi_1\rangle - |\varphi_2\rangle\|_2.$$

Let $|\varphi\rangle$ be a random pure state in dimension d. Then for all $0 \leq \delta \leq \eta$,

$$\mathbf{P}\left\{|f(|\varphi\rangle) - \mathbf{E}\left\{f(\varphi)\right\}| \geq \delta\right\} \leq 4\exp\left(-\frac{\delta^2 d}{c\eta^2}\right)$$

where c is a constant. We can take $c = 9\pi^2$.

Proof We can instead study the concentration of a Lipschitz function on the real sphere $\mathbb{S}^{2d-1}$. Note that the induced function (that we also call f) is still α-Lipschitz. Concentration on $\mathbb{S}^{2d-1}$ can be proved in a simple way using concentration of the standard Gaussian distribution. This proof is due to Maurey and Pisier and can be found in Appendix V of [MS86]. Specifically, using Corollary V.2 in [MS86], we get

$$\begin{aligned}\mathbf{P}\left\{|f(Z) - \mathbf{E}\left\{f(Z)\right\}| \geq t\right\} &\leq 2\exp\left(-\frac{\delta^2(2d)}{18\pi^2\eta^2}\right) + 2\exp\left(-\frac{2d}{2\pi^2}\right) \\ &\leq 4\exp\left(-\frac{\delta^2 d}{9\pi^2\eta^2}\right).\end{aligned}$$

In the notation of the proof of Corollary V.2 [MS86], we have set $\delta = 1/2$. This can be done because using the same arguments as in the proof of Lemma 2.6, we can show that the expected ℓ_2 norm of the standard Gaussian distribution in dimension n at least $\sqrt{2}\sqrt{n-\frac{1}{2}} > \sqrt{n}$ for $n \geq 2$.

We used this version of Levy's lemma because it has an elementary proof and it gives directly the concentration about the expected value. Different versions involving the median of f and giving better constants can be found in Corollary 2.3 of [MS86] or Proposition 1.3 in [Led01] for example. □

Lemma 2.9 (δ-net)**.** *Let $\delta \in (0,1)$. There exists a set $\mathcal{N}$ of pure states in $\mathbb{C}^d$ with $|\mathcal{N}| \leq (3/\delta)^{2d}$ such that for every pure state $|\psi\rangle \in \mathbb{C}^d$ (i.e., $\||\psi\rangle\|_2 = 1$), there exists $|\tilde{\psi}\rangle \in \mathcal{N}$ such that*

$$\||\psi\rangle - |\tilde{\psi}\rangle\|_2 \leq \delta.$$

Proof A proof can be found in [HLSW04] as Lemma II.4. □

Lemma 2.8 (Concentration of the average). *Let $a, b \geq 1$, $\delta \in (0,1)$ and t a positive integer. Suppose X is a random variable with 0 mean satisfying the tail bounds*

$$\mathbf{P}\left\{X \geq \delta\right\} \leq a e^{-b\delta^2} \quad \text{and} \quad \mathbf{P}\left\{X \leq -\delta\right\} \leq a e^{-b\delta^2}.$$

Let $X_1, \dots X_t$ be independent copies of X. Then if $\delta^2 b \geq 16a^2\pi$,

$$\mathbf{P}\left\{\left|\frac{1}{t}\sum_{k=1}^{t} X_k\right| \geq \delta\right\} \leq \exp\left(-\frac{\delta^2 bt}{2}\right).$$

Proof For any $\lambda > 0$, using Markov's inequality

$$\begin{aligned}
\mathbf{P}\left\{\sum_{k=1}^{t} X_k \geq t\delta\right\} &= \mathbf{P}\left\{\exp\left(\lambda\sum_{k=1}^{t} X_k\right) \geq \exp\left(\lambda t\delta\right)\right\} \\
&\leq \mathbf{E}\left\{\exp\left(\lambda\sum_{k=1}^{t} X_k\right)\right\} e^{-\lambda t\delta} \\
&= \mathbf{E}\left\{e^{\lambda X}\right\}^t e^{-\lambda t\delta}.
\end{aligned}$$

We now bound the moment generating function $\mathbf{E}\left\{e^{\lambda X}\right\}$ of X using the tail bounds.

$$\begin{aligned}
\mathbf{E}\left\{e^{\lambda X}\right\} &= \int_0^\infty \mathbf{P}\left\{e^{\lambda X} \geq u\right\} du \\
&= \int_0^\infty \mathbf{P}\left\{X \geq \frac{\ln u}{\lambda}\right\} du \\
&= \int_0^1 \mathbf{P}\left\{X \geq \frac{\ln u}{\lambda}\right\} du + \int_1^\infty \mathbf{P}\left\{X \geq \frac{\ln u}{\lambda}\right\} du \\
&\leq 1 + \int_1^\infty a\exp\left(-\frac{b\ln^2 u}{\lambda^2}\right) du \\
&= 1 + a\int_0^\infty \exp\left(-\frac{bz^2}{\lambda^2}\right) e^z dz
\end{aligned}$$

by making the change of variable $z = \log u$.

$$\begin{aligned}
\mathbf{E}\left\{e^{\lambda X}\right\} &\leq 1 + a\int_0^\infty \exp\left(-\frac{b}{\lambda^2}\left(z - \frac{\lambda^2}{2b}\right)^2 + \frac{\lambda^2}{4b}\right) dz \\
&\leq 1 + a\exp\left(\frac{\lambda^2}{4b}\right)\int_{-\infty}^\infty \exp\left(-\frac{b}{\lambda^2}\left(z - \frac{\lambda^2}{2b}\right)^2\right) dz \\
&= 1 + a\exp\left(\frac{\lambda^2}{4b}\right)\frac{\lambda}{\sqrt{2b}}\int_{-\infty}^\infty \exp\left(-\frac{u^2}{2}\right) du \\
&= 1 + a\frac{\sqrt{2\pi}\lambda}{\sqrt{2b}} \cdot \exp\left(\frac{\lambda^2}{4b}\right) \\
&\leq 2\max\left(1, a\frac{\sqrt{\pi}\lambda}{\sqrt{b}} \cdot \exp\left(\frac{\lambda^2}{4b}\right)\right).
\end{aligned}$$

We choose $\lambda = 2\delta b$ (this is not the optimal choice but it makes expressions simpler),

$$\begin{aligned}
\mathbf{P}\left\{\sum_{k=1}^{t} X_k \geq t\delta\right\} &\leq \max\left(2^t, \left(2a\frac{\sqrt{\pi}\lambda}{\sqrt{b}}\right)^t \cdot \exp\left(\frac{\lambda^2 t}{4b}\right)\right)\exp\left(-\lambda t\delta\right) \\
&= \max\left(\exp\left(-2\delta^2 bt + t\ln 2\right), \exp\left(\delta^2 bt - 2\delta^2 bt + t\ln(4a\sqrt{\pi}\delta\sqrt{b})\right)\right) \\
&= \max\left\{\exp\left(\left(-2\delta^2 b + \ln 2\right)t\right), \exp\left(\left(-\delta^2 b + \ln(4a\sqrt{\pi}\delta\sqrt{b})\right)t\right)\right\}.
\end{aligned}$$

Claim. For all $c \geq 1$ and $x \geq c$

$$\frac{1}{2}\ln(cx) - x \leq -\frac{x}{2}.$$

The function $x \mapsto \frac{x}{2} - \frac{1}{2}\ln(cx)$ is increasing for $x \geq 1$. It suffices to show that it is nonnegative for $x = c$. To see that, we differentiate the function $y \mapsto y - \ln(y^2)$ to prove that for all $y \geq 1$, we have $y - \ln(y^2) \geq 0$. This proves the claim.

Using this inequality, we have for $\delta^2 b \geq 16a^2\pi$,

$$-\delta^2 b + \ln(4a\sqrt{\pi}\delta\sqrt{b}) \leq -\frac{\delta^2 b}{2} \quad \text{and} \quad -2\delta^2 b + \ln 2 \leq -\frac{\delta^2 b}{2}.$$

Finally,

$$\mathbf{P}\left\{\sum_{k=1}^{t} X_k \geq t\delta\right\} \leq \exp\left(-\frac{\delta^2 bt}{2}\right).$$

□

B Proof of Lemma 2.11

We define $V_0 = \mathbb{1}$, and the remaining unitaries are indexed by binary vectors $u \in \{0,1\}^n$, for example the binary representations of integers from 0 to $r-2$. The construction is based on operations in the finite field $\mathbb{F}_{2^n}$. The field $\mathbb{F}_{2^n}$ can be seen as an n-dimensional vector space over $\mathbb{F}_2$. Choose $\theta \in \mathbb{F}_{2^n}$ such that $1, \theta, \dots, \theta^{n-1}$ forms a basis of $\mathbb{F}_{2^n}$. For any $x, y \in [n]$, $\theta^x \cdot \theta^y \in \mathbb{F}_{2^n}$ can be decomposed in our chosen basis as $\theta^x \cdot \theta^y = \sum_{\ell=0}^{n-1} m_\ell(x,y)\theta^\ell$ for some $m_\ell(x,y) \in \mathbb{F}_2$. We can thus define the matrices $M_0, M_1, \dots, M_{n-1}$ from the multiplication table

$$\begin{pmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & \theta & \dots & \theta^{n-1} \end{pmatrix} = M_0 + M_1\theta + \dots + M_{n-1}\theta^{n-1}.$$

where $M_\ell = (m_\ell(x,y))_{x,y\in[n]}$. For a given $u \in \{0,1\}^n$, we define the matrix

$$N_u = \sum_{\ell=0}^{n-1} u_\ell M_\ell.$$

Notice that as $\theta^x \cdot \theta^y = \theta^{x+y}$, the entry $N_u(x,y)$ of N_u only depends on $x+y$, i.e., $N_u(x,y) = N_u(x',y')$ if $x+y = x'+y'$. So we can represent this matrix by a vector $\alpha_u(x+y) = N_u(x,y)$ of length $2n-1$. We then define a quadratic form on $\mathbb{Z}_4$ by: for $v \in \{0,1\}^n$,

$$T_u(v) = v^T N_u v \mod 4.$$

Note that the operations $v^T N_u v$ are not performed in $\mathbb{F}_2$ but rather in $\mathbb{Z}$. Using the vector α_u, we can write

$$T_u(v) = \sum_{x,y\in[n]} v_x N_u(x,y) v_y \mod 4 = \sum_{z=0}^{2n-2}\left(\sum_{x=0}^{z} v_x v_{z-x}\right)\alpha_u(z) \mod 4$$

if we define $v_x = 0$ for $x \geq n$. We then define the diagonal matrix $D_u = \text{diag}\left(i^{T_u(v)}\right)_{v\in\mathbb{F}_2^n}$. Finally, we define for $1 \leq j \leq r-1$,

$$V_j = D_{\text{bin}(j-1)} H^{\otimes n}$$

where $\text{bin}(j) \in \{0,1\}^n$ is the binary representation of length n of the integer j.

The fact that these unitaries define mutually unbiased bases was proved in [WF89]. We now analyse how fast these unitary transformations can be implemented. Note that we want a circuit that takes as input a state $|\psi\rangle$ together with the index j of the unitary transformation and that outputs $V_j|\psi\rangle$.

Given the index j as input, we show it is possible to compute $u = \text{bin}(j-1)$ and compute the vector $\alpha_j \stackrel{\text{def}}{=} \alpha_u$ in time $O(n^2 \operatorname{polylog} n)$. In fact, we start by computing a representation of the field $\mathbb{F}_{2^n}$ by finding an irreducible polynomial Q of degree n in $\mathbb{F}_2[X]$, so that $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/Q$. This can be done in expected time $O(n^2 \operatorname{polylog} n)$ (Corollary 14.43 in the book [vzGG99]). There also exists a deterministic algorithm for finding a irreducible polynomial in time $O(n^4 \operatorname{polylog} n)$ [Sho90]. We then take $\theta = X$. Computing the polynomial $X^x \cdot X^y = X^{x+y} \mod Q$ can be done in time $O(n \operatorname{polylog} n)$ using the fast Euclidean algorithm (see Corollary 11.8 in [vzGG99]). As $x + y \in [0, 2n-2]$, we can explicitly represent all the polynomials X^z for $0 \leq z \leq 2n-2$ in time $O(n^2 \operatorname{polylog} n)$. It is then simple to compute the vector α_u using the vector u in time $O(n^2)$.

To build the quantum circuit, we first observe that applying a Hadamard transform only takes n single-qubit Hadamard gates. Then, to design a circuit performing the unitary transformation $D_{\text{bin}(j-1)}$, we start by building a classical circuit that computes

$$T_u(v) = \sum_{z=0}^{2n-2} \left(\sum_{x=0}^{z} v_x v_{z-x} \right) \alpha_u(z) \mod 4$$

on inputs v and α_u. Observing that $\sum_{x=0}^{z} v_x v_{z-x}$ is the coefficient of Y^z in the polynomial $\left(\sum_{x=0}^{n-1} v_x Y^x\right)^2$, we can use fast polynomial multiplication to compute $T_u(v)$ in time $O(n \operatorname{polylog} n)$ (Corollary 8.27 in [vzGG99]). Moreover, computing the inner product of two vectors can easily be implemented by a circuit of depth $O(\log n)$. Thus, $T_u(v)$ can be computed by a circuit of size $O(n \operatorname{polylog} n)$ and depth $O(\log n)$. This circuit can be transformed into a reversible circuit with the same size and depth (up to some multiplicative constant) that takes as input (v, α_j, g) where $v \in \{0,1\}^n$, $\alpha_j \in \{0,1\}^{2n-1}$ and $g \in \mathbb{Z}_4$, and outputs $(v, \alpha_j, g + T_u(v) \mod 4)$.

This reversible classical circuit can be readily transformed into a quantum circuit that computes the unitary transformation defined by $W : |v\rangle|g\rangle \mapsto |v\rangle|g+T_u(v) \mod 4\rangle$. Recall that we want to implement the transformation $D_u : |v\rangle \mapsto i^{T_u(v)}|v\rangle$ efficiently. This is simple to obtain using the quantum circuit for W. In fact, if we use a catalyst state $|\phi\rangle = |0\rangle - i|1\rangle - |2\rangle + i|3\rangle$, we have

$$W|v\rangle|\phi\rangle = i^{T_u(v)}|v\rangle|\phi\rangle = D_{\text{bin}(j-1)}|v\rangle|\phi\rangle.$$

Finally, $D_{\text{bin}(j-1)} H^{\otimes n}$ can be implemented by a quantum circuit of size $O(n \operatorname{polylog} n)$ and depth $O(\log n)$.

C Permutation extractors

In order to prove the existence of strong permutation extractors with good parameters, we use the construction of Guruswami, Umans and Vadhan [GUV09] which is inspired by list decoding. Their main construction is a lossless condenser based on Parvaresh-Vardy codes. Using this condenser, they build an explicit extractor with good parameters. However, this lossless condenser based on Parvaresh-Vardy codes does not seem to be easily extended into a permutation condenser. The same paper also presents a lossy condenser based on Reed-Solomon codes, which can indeed be transformed into a permutation condenser. This permutation condenser can then be used in the extractor construction instead of the lossless condenser giving a strong permutation extractor. In this section, we describe this construction. For completeness, we reproduce most of the proof here, except the results that are used exactly as stated in [GUV09].

It is also worth mentioning that to obtain metric uncertainty relations, we want strong extractors. Even though the extractors in [GUV09] are not directly described as strong, they are essentially strong. In this section, we describe all the condensers and extractors as strong.

Definition C.1 (Condenser)**.** *A function $C : \{0,1\}^n \times S \to \{0,1\}^{n'}$ is an $(n,k) \to_\epsilon (n',k')$* condenser *if for every X with min-entropy at least k, $C(X, U_S)$ is ϵ-close to a distribution with min-entropy k' when U_S is uniformly distributed on S. A condenser C is* strong *if $(U_S, C(X, U_S))$ is ϵ-close to (U_S, Z) for some random variable Z such that for all $y \in S$, $Z|_{U_S=y}$ has min-entropy at least k.*

A condenser is explicit *if it is computable in polynomial time in n.*

Remark. The set S is usually of the form $\{0,1\}^d$ for some integer d. Here, it is convenient to take sets S not of this form to obtain permutation extractors. Note also that an extractor is an $(n,k) \to_\epsilon (m,m)$ condenser. □

Definition C.2 (Permutation condenser)**.** *A family $\{P_y\}_{y \in S}$ of permutations of $\{0,1\}^n$ is an $(n,k) \to_\epsilon (n',k')$* strong permutation condenser *if the function $P^C : (x,y) \mapsto P^C_y(x)$ where $P^C_y(x)$ refers to the first n' bits of $P_y(x)$ is an $(n,k) \to_\epsilon (n',k')$ strong condenser.*

A strong permutation condenser is explicit *if for all $y \in S$, both P_y and P_y^{-1} are computable in polynomial time.*

The following theorem describes the condenser that will be used as a building block in the extractor construction. It is an analogue of Theorem 7.2 in [GUV09].

Theorem C.3. *For all positive integers n and $\ell \leq n$, as well as $\alpha, \epsilon \in (0, 1/2)$, there exists an explicit family of permutations $\{RS_y\}_{y \in S}$ of $\mathbb{F}_{2^t}^n$ that is an*

$$(nt, (\ell+1)t) \to_\epsilon (\ell t, (1-\alpha)\ell t - 4)$$

strong permutation condenser with $t = \lceil 1/\alpha \cdot \log(24n^2/\epsilon) \rceil$ and $\log |S| \leq t$. Moreover, the functions $(x, y) \mapsto RS_y(x)$ and $(x, y) \mapsto RS_y^{-1}(x)$ can be computed by a circuit of size $O(n \operatorname{polylog}(n/\epsilon))$.

Remark. Note that the input space of the condenser is $\{0,1\}^{nt}$ instead of $\{0,1\}^n$. But one can see such a condenser as a permutation condenser (P'_y) on the smaller space $\{0,1\}^n$ defined by $P'_y(x) = P_y(x0^t)$ for all $x \in \{0,1\}^n$ where $x0^t$ is obtained by appending t zeros to x. □

Proof Set $q = 2^t$ and $\epsilon_0 = \epsilon/6$. Consider the function $C' : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^{\ell+1}$ defined by

$$C'(f, y) = [y, f(y), f(\zeta y), \dots, f(\zeta^{\ell-1} y)]$$

where $\mathbb{F}_q^n$ is interpreted as the set of polynomials over $\mathbb{F}_q$ of degree at most $n-1$ and ζ is a generator of the multiplicative group $\mathbb{F}_q^*$. First, we compute the input and output sizes in terms of bits. The inputs can be described using $\log |\mathbb{F}_q^n| = n \log q = nt$ bits, the seed using $\log |\mathbb{F}_q| = t$ bits and the output using $\log |\mathbb{F}_q^{\ell+1}| = (\ell+1)t$. Using Theorem 7.1 in [GUV09], for any integer h, C' is a

$$\left(nt, \log\left(\frac{q^\ell - 1}{\epsilon_0}\right)\right) \to_{2\epsilon_0} \left(\ell t + t, \log\left(\frac{Ah^\ell - 1}{2\epsilon_0}\right)\right) \tag{36}$$

condenser where $A \stackrel{\text{def}}{=} \epsilon_0 q - (n-1)(h-1)\ell$. We now choose $h = \lceil q^{1-\alpha} \rceil$. As $q \geq (4n^2/\epsilon_0)^{1/\alpha}$, we have $A \geq \epsilon_0 q - n^2 h \geq \epsilon_0 q - \epsilon_0 q^\alpha/4 \cdot (q^{1-\alpha} + 1) \geq \epsilon_0 q/2$. Thus, we can compute the bounds we obtain on the condenser C':

$$\log\left(\frac{q^\ell - 1}{\epsilon_0}\right) = \ell t + \log(1/\epsilon_0) \leq (\ell+1)t$$

and

$$\begin{aligned} \log\left(\frac{Ah^\ell - 1}{2\epsilon_0}\right) &= \log\left(\frac{Ah^\ell}{2\epsilon_0}\right) + \log\left(1 - \frac{1}{Ah^\ell}\right) \\ &\geq \log(q/4) + \ell \log h - 1 \\ &\geq t + (1-\alpha)\ell t - 3. \end{aligned}$$

Plugging these values in equation (36), we get that C' is a

$$(nt, (\ell+1)t) \to_{2\epsilon_0} (\ell t + t, (1-\alpha)\ell t + t - 3)) \tag{37}$$

condenser.

Observe that the seed y is part of the output of the condenser. As we want to construct a strong condenser, we do not consider the seed as part of the output of the condenser. For this, we define $C : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q^\ell$ by $C(f, y) = [f(y), \dots, f(\zeta^{\ell-1} y)]$. Moreover, as will be clear later when we try to build a permutation condenser, we take the seed to be uniform on $S \stackrel{\text{def}}{=} \mathbb{F}_q^*$ instead of being uniform on the whole field $\mathbb{F}_q$. Note that this increases the error of the condenser by at most $2^{-t} \leq \epsilon_0$ (because one can choose $U_{\mathbb{F}_q^*} = U_{\mathbb{F}_q}$ with probability $1 - 2^{-t}$). Here and in the rest of this proof, we will be using Doeblin's coupling lemma.

Equation (37) then implies that if X has min-entropy at least $(\ell+1)t$ and U_S is uniform on S, then the distribution of $(U_S, C(X, U_S))$ is $3\epsilon_0$-close to a distribution with min-entropy at least $(1-\alpha)\ell t + t - 3$. Let $Y \in S$ and $Z \in \{0,1\}^{(\ell+1)t}$ be random variables such that $\mathbf{H}_{\min}(Y, Z) \geq (1-\alpha)\ell t + t - 3$ and $(U_S, C(X, U_S)) = (Y, Z)$ with probability at least $1 - 3\epsilon_0$. If Y was uniformly distributed on S, then it would follow directly that for all $y \in S$, $\mathbf{H}_{\min}(Z | Y = y) \geq (1-\alpha)\ell t$. However, Y is not necessarily uniformly distributed. We define a new random variable Z' by

$$Z' = \begin{cases} Z & \text{if } Y = U_S \\ U' & \text{if } Y \neq U_S \end{cases}$$

where U' is uniformly distributed on $\{0,1\}^{(\ell+1)t}$ and independent of all the other random variables. We have for any $z \in \{0,1\}^{(\ell+1)t}$ and $y \in S$,

$$\begin{aligned}\mathbf{P}\{Z' = z | U_S = y\} &= \frac{1}{\mathbf{P}\{U_S = y\}} \left(\mathbf{P}\{Z' = z, Y = y, Y = U_S\} + \mathbf{P}\{Z' = z, U_S = y, Y \neq U_s\}\right) \\ &\leq \frac{1}{\mathbf{P}\{U_S = y\}} \left(2^{-(1-\alpha)\ell t - t + 3} + 2^{-(\ell+1)t} \cdot \frac{1}{|S|}\right) \\ &\leq 2 \cdot 2^{-(1-\alpha)\ell t + 3}.\end{aligned}$$

Moreover, we have $(U_S, C(X, U_S)) = (U_S, Z')$ with probability at least $1 - 6\epsilon_0$.

We conclude that C is a

$$(nt, (\ell+1)t) \to_\epsilon (\ell t, (1-\alpha)\ell t - 4)) \tag{38}$$

strong condenser.

To define our permutation condenser, we set the first $n' = \ell t$ bits $RS^C_y(x)$ of $RS_y(x)$ to be $RS^C_y(x) = C(x, y)$. We then define the remaining bits by defining $RS^R_y(f) = [f(\zeta^\ell y), \dots, f(\zeta^{n-1} y)]$. As $q \geq n - 1$ and ζ is a generator of $\mathbb{F}_q^*$, the elements $y, \zeta y, \dots, \zeta^{n-1} y$ are distinct provided $y \neq 0$. So for $y \neq 0$, $(RS^C, RS^R)_y(f)$ is the evaluation of the polynomial f of degree at most $n-1$ in n distinct points. Thus, $f \mapsto P_y(f)$ is a bijection in $\mathbb{F}_q^n$ for all $y \neq 0$. This is why the value 0 for the seed was excluded earlier.

Concerning the computation of the functions RS^C_y and RS^R_y, they only require the evaluation of a polynomial on elements of the finite field $\mathbb{F}_q$. Computations in the finite field $\mathbb{F}_q$ can be performed efficiently by finding an irreducible polynomial of degree $\log q$ over $\mathbb{F}_2$ and doing computations modulo this polynomial. In fact, finding an irreducible polynomial of degree $\log q$ over $\mathbb{F}_2$ can be done in time polynomial in $\log q$ (see for example [Sho90] for a deterministic algorithm and Corollary 14.43 in the book [vzGG99] for a simpler randomized algorithm). Since addition, multiplication and finding the greatest common divisor of polynomials in $\mathbb{F}_2[X]$ can be done using a number of operations in $\mathbb{F}_2$ that is polynomial in the degrees, we conclude that computations in $\mathbb{F}_q$ can be implemented in time $O(\text{polylog}(n/\epsilon))$. Moreover, one can efficiently find a generator ζ of the group $\mathbb{F}_q^*$. For example, Theorem 1.1 in [Sho92] shows the existence of a deterministic algorithm having a runtime $O(\text{poly}(\log(q))) = O(\text{polylog}(n/\epsilon))$.

To evaluate RS_y at a polynomial f, we compute the field elements $y, \zeta y, \dots, \zeta^{n-1} y$, and then evaluate the polynomial f on these points. Using a fast multipoint evaluation, this step can be done in $O(n \,\text{polylog}\, n)$ number of operations in $\mathbb{F}_q$ (see Corollary 10.8 in [vzGG99]). Moreover, given a list $[f(y), \dots, f(\zeta^{n-1} y)]$ for $y \neq 0$, we can find f by fast interpolation in $\mathbb{F}_q[X]$ (see Corollary 10.12 in [vzGG99]). As a result RS_y^{-1} can also be computed in $O(n \,\text{polylog}\, n)$ operations in $\mathbb{F}_q$. □

This condenser will be composed with other extractors, the following lemma shows how to compose condensers.

Lemma C.4 (Composition of strong permutation condensers). *Let $(P_{1,y_1})_{y_1 \in S_1}$ be an $(n,k) \to_\epsilon (n',k')$ strong permutation condenser and $(P_{2,y_2})_{y_2 \in S_2}$ be an $(n',k') \to_\epsilon (n'',k'')$ strong permutation condenser. Then $(P_y)_{y=(y_1,y_2) \in S_1 \times S_2} = (P^C_y, P^R_y)$ where $P^C_{y_1 y_2} = P^C_{2,y_2} \circ P^C_{1,y_1}$ and $P^R_{y_1 y_2} = (P^R_{2,y_2} \circ P^C_{1,y_1}) \cdot P^R_{1,y_1}$ is an $(n,k) \to_{2\epsilon} (n'',k'')$ strong permutation extractor.*

Proof P_y is clearly a permutation of $\{0,1\}^n$. We only need to check that P^C is a strong condenser. By definition, if $\mathbf{H}_{\min}(X) \geq k$, $(U_{S_1}, P^C_{1,U_{S_1}}(X))$ is ϵ-close to (U_{S_1}, Z) where $Z|_{U_{S_1}=y_1}$ has min-entropy at least k'. Now putting Z into the condenser P^C_2, we get that for any y_1, $(U_{S_2}, P^C_{2,U_{S_2}}(Z_{U_{S_1}})$ is ϵ-close to (U_{S_2}, Z_2) where $Z_2|_{U_{S_2}=y_2}$ has min-entropy at least k'' for any $y_2 \in S_2$. Thus, $Z_2|_{U_{S_1} U_{S_2} = y_1 y_2}$ has min-entropy at least k''. Moreover, by the triangle inequality, we have $\Delta\Big((U_{S_1}, U_{S_2}, P^C_{U_{S_1} U_{S_2}}(X)), (U_{S_1}, U_{S_2}, Z_2)\Big) \leq 2\epsilon$. □

Next, we present one of the standard extractors that are used as a building block in many constructions.

Lemma C.5 ("Leftover Hash Lemma" extractor [ILL89]). *For all positive integers n and $k \leq n$, and $\epsilon > 0$, there exists an explicit family $(P_y)_{y \in S}$ of permutations of $\{0,1\}^n$ that is an $(n,k) \to_\epsilon m$ strong permutation extractor with $\log|S| = \log(2^n - 1)$ and $m \geq k - 2\log(2/\epsilon)$.*

Proof We view $\{0,1\}^n$ as the finite field $\mathbb{F}_{2^n}$ and the set $S = \mathbb{F}^*_{2^n}$. We then define the permutation $P_y(x) = x \cdot y$ where the product $x \cdot y$ is taken in the field $\mathbb{F}_{2^n}$. The family of functions P_y is pairwise independent. Applying the

Leftover Hash Lemma [ILL89], we get that if Y uniform on $\mathbb{F}_{2^n}$, the distribution of the first $\lceil k - 2\log(1/\epsilon)\rceil$ bits of $P_Y(X)$ together with Y is ϵ-close to uniform. Now if U_S is only uniform in $\mathbb{F}^*_{2^n}$, $(U_S, P_{U_S}(X))$ is $\epsilon + 2^{-n}$-close to the uniform distribution. The result follows from the fact that we can suppose $\epsilon \geq 2^{-n}$ (otherwise, $k - 2\log(1/\epsilon) \leq 0$ and the theorem is true). □

The problem with this extractor is that it uses a seed that is as long as the input. Next, we introduce the notion of a block source.

Definition C.6 (Block source). *$X = (X_1, X_2, \dots, X_s)$ is a $(k_1, k_2, \dots, k_s)$ block source if for every $i \in \{1, \dots, s\}$ and $x_1, \dots, x_{i-1}$, $X|_{X_1 = x_1, \dots, X_{i-1} = x_{i-1}}$ is a k_i-source. When $k_1 = \dots = k_s = k$, we call X a $s \times k$ source.*

A block source has more structure than a general source. However, for a source of large min-entropy k (or equivalently with small entropy deficiency $\Delta = n - k$), one does not lose too much entropy by viewing a general source as a block source where each block has entropy deficiency roughly Δ. See Corollary 5.9 in [GUV09] for a precise statement.

Lemma C.7 (Lemma 5.4 in [GUV09]). *Let s be a (constant) positive integer. For all positive integers n and $\ell \leq n$ and all $\epsilon > 0$, setting $t = \lceil 8s\log(24n^2 \cdot (4s+1)/\epsilon)\rceil$, there is an explicit family $\{L_y\}_{y \in S}$ of permutations of $\{0,1\}^n$ that is an*

$$(n, 2\ell t) \rightarrow_\epsilon \ell t$$

strong permutation extractor with $\log|S| \leq 2\ell t/s + t$.

Proof As the extractor is composed of many building blocks, each generating some error, we define $\epsilon_0 = \epsilon/(4s+1)$ where ϵ is the target error of the final extractor. The idea is to first apply the condenser RS of Theorem C.3 with $\alpha = \frac{1}{8s}$ to obtain a string $X' = C(X, U_{\mathbb{F}^*_{2^t}})$ of length $n' = (2\ell - 1)t$ which is ϵ_0-close to a k'-source where

$$k' = \left(1 - \frac{1}{8s}\right)(2\ell - 1)t - 4$$

The entropy deficiency Δ of this k'-source can be bounded by $\Delta = n' - k' \leq \frac{(2\ell-1)t}{8s} + 4$. Then, we partition $X' = (X'_1, \dots, X'_{2s})$ (arbitrarily) into $2s$ blocks of size $n'' = \lfloor n'/2s \rfloor$ or $n'' + 1$. Using Corollary 5.9 of [GUV09], $(X'_1, \dots, X'_{2s})$ is $2s\epsilon_0$-close to some $2s \times k''$-source where $k'' = (n'' - \Delta - \log(1/\epsilon_0))$.

We have $\Delta \leq \ell t/(4s) + 3 \leq \ell t/(3s)$ for n large enough. Thus,

$$k'' \geq \frac{2\ell t}{2s} - \frac{\ell t}{3s} - \log(1/\epsilon_0) = \frac{2}{3s}\ell t - \log(1/\epsilon_0).$$

We can then apply the extractor Lemma C.5 to all the $2s$ blocks using the same seed of size $n'' + 1$. Note that we can reuse the same seed because we have a strong extractor and the seed is independent of all the blocks. This extractor extracts almost all the min-entropy of the sources. More precisely, if we input to this extractor a $2s \times k''$-source, the output distribution is $2s\epsilon_0$-close to m uniform bits where

$$m \geq 2s \cdot (k'' - 2\log(2/\epsilon_0)) \geq \frac{4}{3}\ell t - 6s\log(2/\epsilon_0) \geq \ell t.$$

Overall, the output of this extractor is $\epsilon_0 + 2s\epsilon_0 + 2s\epsilon_0 = \epsilon$-close to the uniform distribution on m bits.

It only remains to show that the extractor we just described is strong and can be extended to a permutation. This follows from Lemma C.4 and the fact the condensers (coming from Theorem C.3 and Lemma C.5) are strong permutation condensers. □

Remark. As pointed out in [GUV09], a stronger version of this lemma (i.e., with larger output) can be proved by using the condenser of Theorem C.3 and the high min-entropy extractor in [GW97] with a Ramanujan expander (for example, the expander of [LPS88]). This construction can also give a strong permutation extractor. However, using this extractor would slightly complicate the exposition and does not really influence the final extractor construction presented in Theorem 2.15. □

The following lemma basically says that the entropy is conserved by a permutation extractor. It is an adapted version of Lemma 26 in [RRV99].

Lemma C.8. *Let $\{P_y\}_{y\in S}$ be a $(n,k) \to_\epsilon m$ strong permutation extractor. Let X be a k-source, then $(U_S, P^E_{U_S}(X), P^R_{U_S}(X))$ is 2ϵ-close to $(U_{S\times\{0,1\}^m}, W)$ where $U_{S\times\{0,1\}^m}$ is uniform on $S\times\{0,1\}^m$ and for all $y\in S, z\in\{0,1\}^m$*

$$\mathbf{H}_{\min}(W|U_{S\times\{0,1\}^m} = (y,z)) \geq k - m - 1.$$

Proof As $\{P^E_y\}$ is a strong extractor, there exists a random variable $U_{S\times\{0,1\}^m}$ uniformly distributed on $S\times\{0,1\}^n$ such that $\mathbf{P}\left\{(U_S, P^E_{U_S}(X)) \neq U_{S\times\{0,1\}^m}\right\} \leq \epsilon$. Define $\Gamma = \{(y,z)\in S\times\{0,1\}^m : \mathbf{P}\left\{P^E_y(X) = z\right\} < \frac{1}{2}\cdot 2^{-m}\}$. We have for every $(y,z)\notin\Gamma$ and $x\in\{0,1\}^{n-m}$,

$$\begin{aligned}\mathbf{P}\left\{P^R_y(X) = x | P^E_y(X) = z\right\} &\leq \frac{\mathbf{P}\left\{P^R_y(X) = x, P^E_y(X) = z\right\}}{2^{-m-1}}\\ &\leq 2^{m+1}\mathbf{P}\left\{X = P^{-1}_y(x,z)\right\}\\ &\leq 2^{-(k-m-1)}.\end{aligned}$$

We then show that $\mathbf{P}\left\{(U_S, P^E_{U_S}) \in \Gamma\right\} \leq \epsilon$. Using the fact that $\{P^E_y\}$ is a strong extractor, we have

$$\left|\mathbf{P}\left\{U_S, U_{\{0,1\}^m} \in \Gamma\right\} - \mathbf{P}\left\{(U_S, P^E_{U_S}) \in \Gamma\right\}\right| \leq \epsilon.$$

But recall that, by definition of Γ, $\mathbf{P}\left\{(U_S, P^E_{U_S}) \in \Gamma\right\} < \frac{1}{2}\mathbf{P}\left\{U_S, U_{\{0,1\}^m} \in \Gamma\right\}$, so we get

$$\mathbf{P}\left\{(U_S, P^E_{U_S}) \in \Gamma\right\} \leq \epsilon.$$

Finally we define

$$W = \begin{cases} P^R_{U_S}(X) & \text{if } (U_S, P^E_{U_S}(X)) \notin \Gamma \\ U' & \text{if } (U_S, P^E_{U_S}(X)) \in \Gamma \end{cases}$$

where U' is uniform on $\{0,1\}^{n-m}$ and independent of all other random variables. We conclude by observing that with probability at least $1-2\epsilon$, we have $(U_S, P^E_{U_S}(X)) = U_{S\times\{0,1\}^m}$ and $P^R_{U_S}(X) = W$. □

We then combine these results to obtain the desired extractor. The proof of the following theorem closely follows Theorem 5.10 in [GUV09] but using the lossy condenser presented in Theorem C.3 and making small modifications to obtain a permutation extractor.

Theorem C.9. *For all integers $n \geq 1$, all $\epsilon \in (0, 1/2)$, and all $k \in \left[200\left\lceil 200\log(24n^2/\epsilon)\right\rceil, n\right]$ there is an explicit $(n,k) \to_\epsilon \lfloor k/4 \rfloor$ strong permutation extractor $\{P_y\}_{y\in S}$ with $\log|S| \leq 200\left\lceil 200\log(24n^2/\epsilon)\right\rceil$. Moreover, the function $(x,y)\mapsto P_y(x)$ can be computed by circuit of size $O(n\,\mathrm{polylog}(n/\epsilon))$.*

Proof If $n \leq 2\cdot 10^6$, we can use the extractor of Lemma C.7 with $s = 200$ and $\ell \geq 1$ such that $2\ell t \leq k \leq 2(\ell+1)t$. This gives an extractor whose seed has size $\frac{k}{200} \leq 10^4 \leq 200\left\lceil 200\log(24n^2/\epsilon)\right\rceil$ and that extracts $\ell t \geq \frac{1}{4}\cdot 2(\ell+1)t \geq \frac{k}{4}$ bits, so the statement still holds true. In the rest of the proof, we assume $n > 2\cdot 10^6$.

The idea of the construction is to build for an integer $i \geq 0$ an explicit $(n, 2^i\cdot 8d) \to_\epsilon 2^{i-1}\cdot 8d$ using d bits of seed by induction on i. Fix $t(\epsilon) = \left\lceil 200\log(24n^2/\epsilon)\right\rceil$ and $d(\epsilon) = 200t(\epsilon)$. The induction hypothesis for an integer $i \geq 0$ is as follows: For all integers $i' \leq i$ and n and $\epsilon > 0$, there is an explicit

$$(n, 2^{i'}\cdot 8d(\epsilon)) \to_\epsilon 2^{i'-1}\cdot 8d(\epsilon)$$

strong permutation extractor with seed size $d(\epsilon)$. This extractor is called $\{P^{(i)}_y\}_{y\in S_i}$.

For both $i = 0$ and $i = 1$ we can use the extractor of Lemma C.7 with $s = 20$. For $i \in \{0,1\}$, we obtain an $(n, 2^i\cdot 8d(\epsilon/(4s+1))) \to_\epsilon 2^{i-1}8d$ strong permutation extractor with Let $\epsilon_0 = \frac{\epsilon}{4s+1}$. For $i \in \{0,1\}$, this gives an extractor with seed $\frac{2^i\cdot 8d(\epsilon/81)}{20} + t \leq \frac{16}{20}d(\epsilon) + \frac{16}{20}200\left\lceil 200\log(81)\right\rceil \leq d(\epsilon)$.

We now show for $i \geq -1$ how to build the extractor $\{P^{(i)}_y\}$ using the extractors $\{P^{(i')}_y\}$ for $i' < i$. Using the induction hypothesis, we construct the following extractor, which will be applied four times to extract the necessary random bits to prove the induction step. The choice of the form of the min-entropy values will become clear later. Set $\epsilon_0 = \epsilon/20$.

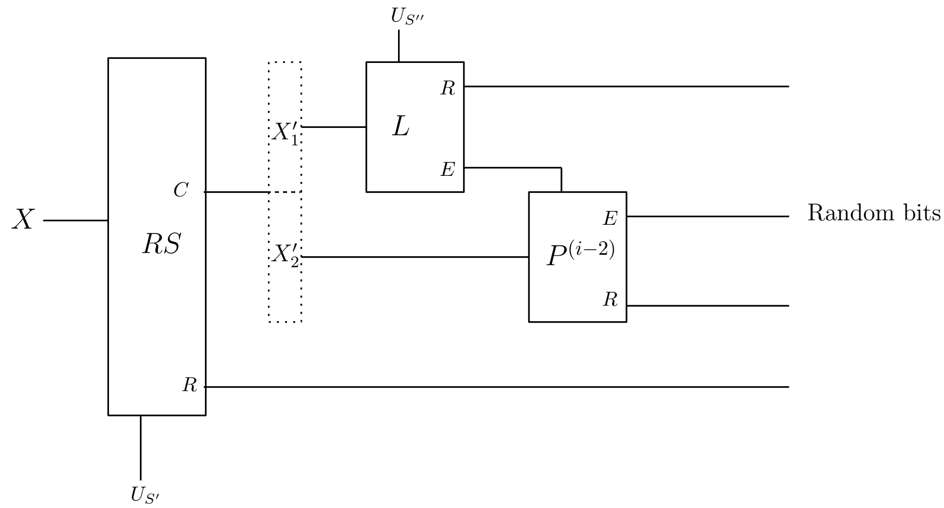

Figure 4: The extractor Q is obtained by first applying the condenser of Theorem C.3 and decomposing the output into two parts. The Leftover Hash Lemma extractor (Lemma C.7) is applied to the first half and its output is used as a seed for the extractor $\{P_y^{(i-2)}\}$ coming from the induction hypothesis.

Claim. There exists an

$$(n, 2^i \cdot 4.5d(\epsilon_0)) \rightarrow_{5\epsilon_0} 2^i \cdot d(\epsilon_0)$$

strong permutation extractor $\{Q_y\}_{y \in T}$ with seed size $\log|T| \leq \frac{d(\epsilon_0)}{8}$.

To prove the claim, we start by applying the condenser of Theorem C.3 with $\alpha = 1/200$ and $\epsilon = \epsilon_0$ (so we use a seed of size $t(\epsilon_0)$). The output X' of size at most $2^i \cdot 4.5d(\epsilon_0)$ is then ϵ_0-close to having min-entropy is at least $(1-\alpha)2^i \cdot 4.5d(\epsilon_0) - t(\epsilon_0)$. The entropy deficiency of this distribution is $\alpha 2^i \cdot 4.5d(\epsilon_0) + \frac{d(\epsilon_0)}{200} \leq \frac{2^i \cdot 4.5d(\epsilon_0)}{100}$. We then divide X' into two equal blocks $X' = (X'_1, X'_2)$, and we know that it is $2\epsilon_0$ close to being a $2 \times k'$-source for

$$k' = \frac{2^i \cdot 4.5d(\epsilon_0)}{2} - \frac{2^i \cdot 4.5d(\epsilon_0)}{100} - \log(1/\epsilon_0) \geq \left(\frac{49}{100} \cdot 2^i \cdot 4.5 - \frac{1}{200}\right) d(\epsilon_0)$$

as $\log(1/\epsilon_0) \leq t(\epsilon_0) = \frac{d(\epsilon_0)}{200}$. For the extractors we will apply next to this source, we should note that $k' \geq 2d(\epsilon_0)$ and that $2^i \cdot 4d(\epsilon_0) \leq k' < 2^i \cdot 8d(\epsilon_0)$.

We now apply the extractor of Lemma C.7 to X'_1 (viewed as a $2d(\epsilon_0)$-source) using a seed of size $\frac{2d(\epsilon_0)}{20}$ and obtaining X'' that is ϵ_0 close to uniform on $d(\epsilon_0)$ bits. We then use the extractor $\{P_y^{(i-2)}\}$ obtained by induction for $i-2$ to the X'_2 (of size $2^i \cdot 4.5d(\epsilon_0) \leq n$) with seed X'' (of size $d(\epsilon_0)$): it is an $(n, 2^{i-2} \cdot 8d(\epsilon_0)) \rightarrow_{\epsilon_0} 2^i \cdot d(\epsilon_0)$ permutation extractor.

The construction is illustrated in Figure 4. Note that the number of bits of the seed is $\log|T| \leq t(\epsilon_0) + \frac{2d(\epsilon_0)}{20} \leq \frac{d(\epsilon_0)}{8}$. This concludes the proof of the claim.

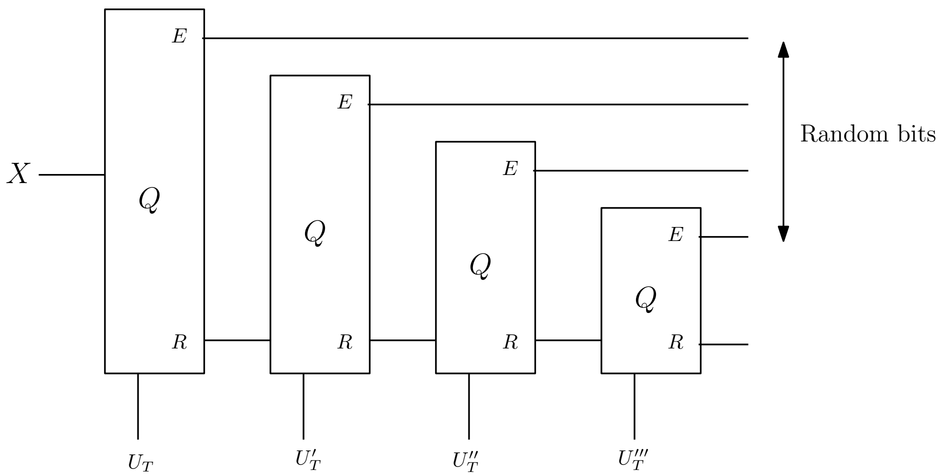

Figure 5: The permutation extractor $\{Q_y\}$ described in the claim is applied four times with independent seeds in order to extract $2^{i-1} \cdot 8d(\epsilon)$ random bits.

The source X we begin with is a $2^i \cdot 8d(\epsilon)$-source. But we have $2^i \cdot 8d(\epsilon) \geq 2^i \cdot 8d(\epsilon_0) - 2^i \cdot 8 \cdot 200^2 \log 20 \geq 2^i \cdot 4.5d(\epsilon_0)$ so that we can apply the permutation extractor $(Q_y)_{y \in T}$ of the claim. We obtain $Q^E_{U_T}(X)$ which is ϵ_0-close to $2^i \cdot d(\epsilon_0)$ random bits. As Q^E is part of a permutation extractor, the remaining entropy is not lost: it is in $Q^R_{U_T}(X)$. More precisely, applying Lemma C.8, we get $Q^R_{U_T}(X)$ is ϵ_0-close to a source of min-entropy at least $2^i \cdot 8d(\epsilon) - 2^i \cdot d(\epsilon_0) - 1$. As $2^i \cdot 8d(\epsilon) - 2^i \cdot d(\epsilon_0) - 1 \geq 2^i \cdot 4.5d(\epsilon_0)$, we can apply the extractor $(Q)_{y \in T}$ of the claim to this source. Note that the input size has decreased but as mentioned earlier this only makes it easier to extract random bits as one can always encode in part of the input space. To apply Q, we use a fresh new seed that outputs a bit string that is close to uniform on $2^{i-3} \cdot 8d(\epsilon_0)$ bits and the remaining entropy can be found in the R register. We apply this procedure four times in total as shown in Figure 5. Note that the reason we can apply it four times is that at the last application $2^i \cdot 8d(\epsilon) - 3 \cdot 2^{i-3} \cdot 8d(\epsilon_0) - 3 \geq 2^i \cdot 4.5d(\epsilon_0)$. As the extractor $(Q_y)_{y \in T}$ has error at most $5\epsilon_0$, the total error is bounded by $20\epsilon_0 = \epsilon$.

We thus obtain an

$$(n, 2^i \cdot 8d(\epsilon)) \to_\epsilon 4 \cdot 2^{i-3} \cdot 8d(\epsilon_0)$$

strong permutation extractor with seed set $S = T^4$ so that $\log |S| \leq 4 \cdot \frac{d(\epsilon_0)}{8} \leq d(\epsilon)$.

□

By a repeated application of the previous theorem, we can extract a larger fraction of the min-entropy.

Theorem 2.15. *For all (constant) $\delta \in (0,1)$, there exists $c > 0$, such that for all positive integers n, all $k \in [c \log(n/\epsilon), n]$, and all $\epsilon \in (0, 1/2)$, there is an explicit $(n,k) \to_\epsilon (1-\delta)k$ strong permutation extractor $\{P_y\}_{y \in S}$ with $\log |S| = O(\log(n/\epsilon))$. Moreover, the functions $(x,y) \mapsto P_y(x)$ and $(x,y) \mapsto P_y^{-1}(x)$ can be computed by circuits of size $O(n \operatorname{polylog}(n/\epsilon))$.*

Proof We start by applying the extractor of Theorem C.9. We extract part of the min-entropy of the source and the remaining min-entropy is in the R system (Lemma C.8). This min-enrtopy can be extracted using once again the extractor of Theorem C.9. After $O(\log(1/\delta))$ applications of the extractor, we obtain the desired result. □

D Impossibility of locking using Pauli operators

The objective of this section is to give an example of a construction that is not a locking scheme to illustrate what is needed to obtain a locking scheme. The 2×2 Pauli matrices are the four matrices $\{\mathbb{1}, \sigma_x, \sigma_z, \sigma_x \sigma_z\}$ where

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For bit strings $u, v \in \{0,1\}^n$, we define the unitary operation $\sigma_x^u \sigma_z^v$ on $\left(\mathbb{C}^2\right)^{\otimes n}$ by

$$\sigma_x^u \sigma_z^v = \sigma_x^{u_1} \sigma_z^{v_1} \otimes \cdots \otimes \sigma_x^{u_n} \sigma_z^{v_n}.$$

It was shown in [AMTdW00] that one can encrypt an n-qubits state $|\psi\rangle$ perfectly using a key (U, V) of $2n$ bits. To encrypt $|\psi\rangle$, one simply applies $\sigma_x^U \sigma_z^V$ to $|\psi\rangle$. This can be thought of as a quantum version of one-time pad encryption. Of course, this encryption scheme also defines a $(0,0)$-locking scheme, but the size of the key is $2n$ bits. Recall that we want to use the assumption that the message is random to reduce the key size to something like $O(\text{polylog}(n))$ bits.

Ambainis and Smith [AS04] showed that to achieve approximate encryption, it is sufficient to choose the key uniformly at random from a subset $S \subseteq \{0,1\}^{2n}$ of size only $O(n^2 2^n)$. Such pseudorandom subsets are called δ-biased sets and have also been used to construct entropically secure encryption schemes [DS05, DD10]. For example, [DD10] showed that it is possible to encrypt a uniformly random state by applying $\sigma_x^U \sigma_z^V$ where (U, V) is chosen uniformly from a set $S \subset \{0,1\}^n$ of size $O(n^2)$ (see [DS05, DD10] for a precise definition of entropic security). Such a scheme can seem like a good candidate for a locking scheme. The following proposition shows that this encyption scheme is far from being ϵ-locking. Note that this also shows that the notion of entropic security defined in [Des09, DD10] is weaker than the definition of locking.

Proposition D.1. *Consider an ϵ-locking scheme $\mathcal{E}$ of the form $\mathcal{E}(x, k = (u,v)) = \sigma_x^u \sigma_y^v |x\rangle$ where the message $x \in \{0,1\}^n$ and the key $u, v \in \{0,1\}^n$ (see Definition 3.1). Suppose the key K is chosen uniformly from a set $S \subseteq \{0,1\}^{2n}$. Then $|S| \geq (1-\epsilon)2^n$.*

Proof Let X be the message (recall X is uniform on $\{0,1\}^n$) and (U, V) be the key. The key is uniformly distributed on S. We show that a measurement in the computational basis gives a lot of information about X . Let I be the outcome of measuring $\mathcal{E}(X, K)$ in the computational basis. We have for $x, i \in \{0,1\}^n$,

$$\begin{aligned}
\mathbf{P}\{X = x | I = i\} &= \mathbf{P}\{I = i | X = x\} \\
&= \frac{1}{|S|} \sum_{(u,v) \in S} \left|\langle i | \sigma_x^u \sigma_z^v | x \rangle\right|^2 .
\end{aligned}$$

Observing that the term $\left|\langle i | \sigma_x^u \sigma_z^v | x \rangle\right|^2 \in \{0,1\}$, we have that for any fixed i, there are at most $|S|$ different values of x for which $\mathbf{P}\{X = x | I = i\} > 0$. Thus, defining $T = \{x \in \{0,1\}^n : \mathbf{P}\{X = x | I = i\} = 0\}$, we have

$$\Delta\left(p_{X|[I=i]}, p_X\right) \geq \mathbf{P}\{X \in T\} - \mathbf{P}\{X \in T | I = i\} = \frac{|T|}{2^n} = 1 - \frac{|S|}{2^n}.$$

By the definition of a locking scheme, we should have

$$\Delta\left(p_{X|[I=i]}, p_X\right) \leq \epsilon$$

which concludes the proof. □

References

[AD89] R. Ahlswede and G. Dueck. Identification via channels. *IEEE Transactions on Information Theory*, 35(1):15 –29, Jan 1989.

[Amb09] A. Ambainis. Limits on entropic uncertainty relations for 3 and more MUBs. 2009, arXiv:0909.3720.

[AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science, 2000*, pages 547–553, 2000.

[AS04] A. Ambainis and A. Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In *Proceedings of RANDOM*, pages 249–260. Springer, 2004, arXiv:quant-ph/0404075.

[ASW10a] G. Aubrun, S. Szarek, and E. Werner. Hastings additivity counterexample via Dvoretzkys theorem. 2010, arXiv:1003.4925.

[ASW10b] G. Aubrun, S. Szarek, and E. Werner. Nonadditivity of Rényi entropy and Dvoretzky's theorem. *Journal of Mathematical Physics*, 51(2):022102, 2010, arXiv:0910.1189.

[Bal97] K. Ball. An elementary introduction to modern convex geometry. *Flavors of geometry*, 31:1–58, 1997.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[BBM75] I. Bialynicki-Birula and J. Mycielski. Uncertainty relations for information entropy in wave mechanics. *Communications in Mathematical Physics*, 44(2):129–132, 1975.

[BCH+06] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner. Security of quantum bit string commitment depends on the information measure. *Physical Review Letters*, 97(25):250501, 2006.

[BCH+08] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Physical Review A*, 78(2):22316, 2008, arXiv:quant-ph/0504078.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[BDSW96] C. H. Bennett, D. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, Nov 1996, arXiv:quant-ph/9604024.

[BW07] M. A. Ballester and S. Wehner. Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases. *Physical Review A*, 75(2):022319, Feb 2007, arXiv:quant-ph/0606244.

[DCEL09] C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Physical Review A*, 80(1):12304, 2009, arXiv:quant-ph/0606161.

[DD10] S. P. Desrosiers and F. Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*, 56(7):3455 –3464, Jul 2010, arXiv:0707.0691.

[Des09] S. P. Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8:331–345, 2009.

[Deu83] D. Deutsch. Uncertainty in quantum measurements. *Physical Review Letters*, 50(9):631–633, Feb 1983.

[DFHL10] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung. Locking classical information. 2010, arXiv:1011.1612.

[DFR+07] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in cryptology – CRYPTO '07*, Lecture Notes in Computer Science, pages 360–378. Springer-Verlag, 2007, arXiv:quant-ph/0612014.

[DFSS05] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 449–458. IEEE, 2005, arXiv:quant-ph/0508222.

[DHL+04] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. Locking classical correlations in quantum states. *Physical Review Letters*, 92(6):67902, 2004, arXiv:quant-ph/0303088.

[DPS04] I. Damgård, T. B. Pedersen, and L. Salvail. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. In *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science, pages 91–108. Springer, 2004, arXiv:quant-ph/0407066.

[DPS05] I. Damgård, T. B. Pedersen, and L. Salvail. A quantum cipher with near optimal key-recycling. In *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 494–510. Springer Berlin / Heidelberg, 2005.

[DS05] Y. Dodis and A. Smith. Entropic security and the encryption of high entropy messages. *Theory of Cryptography*, pages 556–577, 2005.

[Dup10] F. Dupuis. *A decoupling approach to quantum information theory*. PhD thesis, Université de Montreal, 2010, arXiv:1004.1641.

[Dvo61] A. Dvoretzky. Some results on convex bodies and Banach spaces. In *Proc. Internat. Sympos. Linear Spaces*, pages 123–160. Jerusalem Academic Press, 1961.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Communications in Mathematical Physics*, 31(4):291–294, 1973.

[FLM77] T. Figiel, J. Lindenstrauss, and V. D. Milman. The dimension of almost spherical sections of convex bodies. *Acta Mathematica*, 139(1):53–94, 1977.

[FvdG99] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999, arXiv:quant-ph/9712042.

[GI10] D. Gavinsky and T. Ito. Quantum Fingerprints that Keep Secrets. 2010, arXiv:1010.5342.

[Gol08] O. Goldreich. *Computational complexity: a conceptual perspective*. Cambridge University Press, 2008.

[GUV09] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):1–34, 2009.

[GW97] O. Goldreich and A. Wigderson. Tiny families of functions with random properties: A quality-size trade-off for hashing. *Random Structures and Algorithms*, 11(4):315–343, 1997.

[Has09] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, 2009.

[HHHO05] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Locking entanglement with a single qubit. *Physical Review Letters*, 94(20):200501, May 2005, arXiv:quant-ph/0404096.

[HLSW04] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004, arXiv:quant-ph/0307104.

[HLW06] P. Hayden, D. W. Leung, and A. Winter. Aspects of generic entanglement. *Communications in Mathematical Physics*, 265(1):95–117, 2006, arXiv:quant-ph/0407049.

[HMR$^+$10] S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen. Limitations of quantum coset states for graph isomorphism. *Journal of the ACM*, 57(6), Oct 2010.

[HSP06] R. W. Heath, T. Strohmer, and A. J. Paulraj. On quasi-orthogonal signatures for CDMA systems. *IEEE Transactions on Information Theory*, 52(3):1217–1226, 2006.

[HW08] P. Hayden and A. Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$. *Communications in Mathematical Physics*, 284(1):263–280, 2008, arXiv:0807.4753.

[HW10] P. Hayden and A. Winter. The fidelity alternative and quantum measurement simulation. 2010, arXiv:1003.4994.

[ILL89] R. Impagliazzo, L. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21th annual ACM Symposium on Theory of computing*, pages 12–24. ACM, 1989.

[Ind07] P. Indyk. Uncertainty principles, extractors, and explicit embeddings of L2 into L1. In *Proceedings of the 39th annual ACM Symposium on Theory of Computing*, pages 615–620. ACM, 2007.

[IS10] P. Indyk and S. Szarek. A simple construction of almost-Euclidean subspaces of via tensor products. 2010, arXiv:1001.0041.

[Kas77] B. Kashin. Sections of some finite dimensional sets and classes of smooth functions. *Izv. Acad. Nauk SSSR*, 41:334–351, 1977.

[KN97] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, Cambridge, 1997.

[KRBM07] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, Apr 2007, arXiv:quant-ph/0512021.

[KW04] M. Koashi and A. Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69(2):022309, Feb 2004, arXiv:quant-ph/0310037.

[KWW09] R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. 2009, arXiv:0906.1030.

[LC97] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997, arXiv:quant-ph/9603004.

[Led01] M. Ledoux. *The concentration of measure phenomenon*. American Mathematical Society, 2001.

[Leu09] D. Leung. A survey on locking of bipartite correlations. In *Journal of Physics: Conference Series*, volume 143, page 012008. Institute of Physics Publishing, 2009.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Mat02] J. Matoušek. *Lectures on discrete geometry*. Springer Verlag, 2002.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997, arXiv:quant-ph/9605044.

[Mil71] V. D. Milman. New proof of the theorem of A. Dvoretzky on intersections of convex bodies. *Functional Analysis and Its Applications*, 5:288–295, 1971.

[MS86] V. D. Milman and G. Schechtman. *Asymptotic theory of finite dimensional normed spaces*, volume 1200 of *Lecture Notes in Mathematics*. Springer-Verlag, 1986.

[MU88] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12):1103–1106, Mar 1988.

[OH05] J. Oppenheim and M. Horodecki. How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information. *Physical Review A*, 72(4):042309, Oct 2005, arXiv:quant-ph/0306161.

[Pis89] G. Pisier. *The volume of convex bodies and Banach space geometry*. Cambridge University Press, 1989.

[RRS09] J. Radhakrishnan, M. Rötteler, and P. Sen. Random Measurement Bases, Quantum State Distinction and Applications to the Hidden Subgroup Problem. *Algorithmica*, 55(3):490–516, 2009.

[RRV99] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. In *Proceedings of the thirty-first annual ACM Symposium on Theory of Computing*, pages 149–158. ACM, 1999.

[RVW00] O. Reingold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings. 41st Annual Symposium on Foundations of Computer Science, 2000*, pages 3 –13, 2000.

[RW02] A. Russell and H. Wang. How to fool an unbounded adversary with a short key. In *Advances in Cryptology—EUROCRYPT 2002*, pages 133–148. Springer, 2002.

[Sha48] C. Shannon. A mathematical theory of communications. *Bell System Technical Journal*, 27:379–423, 1948.

[Sho90] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990.

[Sho92] V. Shoup. Searching for primitive roots in finite fields. *Mathematics of Computation*, 58(197):pp. 369–380, 1992.

[SP00] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2):441–444, Jul 2000, arXiv:quant-ph/0003004.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65(1):12310, 2001, arXiv:quant-ph/0106019.

[Sza06] S. Szarek. Convexity, complexity, and high dimensions. In *International Congress of Mathematicians*, volume 2, pages 1599–1621, 2006.

[Tro04] J. Tropp. *Topics in Sparse Approximation*. PhD thesis, University of Texas at Austin, 2004.

[vzGG99] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, 1999.

[WF89] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989.

[Win04] A. Winter. Quantum and classical message identification via quantum channels. *In O. Hirota, editor,* Festschrift "A. S. Holevo 60", *pages 171–188. Rinton Press, 2004. Reprinted in Quantum Inf. Comput. 4(6&7):563-578*, 2004, arXiv:quant-ph/0401060.

[WW10] S. Wehner and A. Winter. Entropic uncertainty relations—a survey. *New Journal of Physics*, 12:025009, 2010, arXiv:0907.3704.