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

Omar Fawzi
School of Computer Science
McGill University
Montréal, QC, Canada
ofawzi@cs.mcgill.ca

Patrick Hayden
School of Computer Science
McGill University
Montréal, QC, Canada
patrick@cs.mcgill.ca

Pranab Sen
Tata Institute of Fundamental
Research
Mumbai, India
pgdsen@tcs.tifr.res.in

ABSTRACT

Quantum uncertainty relations are at the heart of many quantum cryptographic protocols performing classically impossible tasks. One operational manifestation of these uncertainty relations is a purely quantum effect referred to as *information locking* [12]. 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 (the message is "locked"). Furthermore, knowing the key, it is possible to recover (or "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. These bases 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 [27] and an extractor construction of Guruswami, Umans and Vadhan [20].

- We apply our metric uncertainty relations to give 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.

Categories and Subject Descriptors

E.4 [**Data**]: Coding and Information Theory; F.1.1 [**Theory of Computation**]: Computation by Abstract Devices—*Models of Computation*

General Terms

Algorithms, Theory

Keywords

quantum information theory, quantum cryptography, quantum uncertainty relation, low-distortion norm embedding, randomness extractor

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 the main reason that some classically impossible cryptographic primitives become possible when quantum communication is allowed. For example, so-called *entropic* uncertainty relations lie at the heart of security proofs in the bounded and noisy quantum storage models [8, 7, 29]. A simple example of an entropic uncertainty relation was given by Maassen and Uffink [11, 31]. 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

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

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 important consequence of entropic uncertainty relations is the effect known as *information locking* [12]. 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 extract from this quantum state by a measurement without knowing K? 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 $\mathbf{I}(X; I) \leq n/2$ [12]. 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 [23] 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, [14] proves 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 and diagonal bases called *mutually unbiased bases* does not work as well for more than two measurements. In fact, it was shown in [4] 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 [23]. Furthermore, standard derandomization techniques are not known to work in this setting. For example, unitary designs [9] define an exponential number of bases. 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 about 2^n (see Appendix of [16]).

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* (see Definition 2.1). Using standard techniques from asymptotic geometric analysis, we prove the existence of strong metric uncertainty relations (Theorem 3.1). This result can be seen as a strengthening of Dvoretzky's theorem [15, 32] 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 [23, 14]. 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 (see Table 1).

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 [27], we obtain explicit bases of $(\mathbb{C}^2)^{\otimes n}$ that verify strong metric uncertainty relations for a number of bases that is polynomial or quasi-polynomial in n (Theorems 4.7 and 4.9). 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 4.3) 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 [20].

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 4.8). Performing these quantum operations can be done using the same technology as implementing the BB84 quantum key distribution protocol [5], 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 4.2 with Lemma 4.1).

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 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 quantum state. This task can be seen as a quantum analogue of the problem of equality testing [1, 30] 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 [25] 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 [3, 2] also used a connection between norm embeddings and quantum information. They use variants of Dvoretzky's theorem to prove the existence of channels that violate additivity of minimum output entropy, as was previously demonstrated by [24, 22].

1.3 Notation

We use the following notation throughout the paper. For a positive integer n, we define $[n] = \{0, \ldots, n-1\}$. Random variables are usually denoted by capital letters $X, K, \ldots$, while p_X denotes the distribution of X, i.e., $\mathbf{P}\{X = x\} = p_X(x)$. $\mathrm{unif}(S)$ 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 $\Delta(p, q) = \frac{1}{2}\sum_{x \in \mathcal{X}} |p(x) - q(x)|$. 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 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 $\mathbf{H}_{\min}(p) = -\log \max_x p(x)$. The weight of a binary vector v (number of ones) is denoted by $\mathbf{w}(v)$ and the Hamming distance between two binary vectors v, v' (number of components that are different) is written as $d_H(v, v')$.

The state of a quantum system is described by a unit vector $|\psi\rangle$ in a Hilbert space. The quantum systems we consider are denoted $A, B, C \ldots$ and are identified with their corresponding 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 $d_A - 1$ and also by strings in $\{0, 1\}^n$ for n-qubit spaces. For a state $|\psi\rangle \in A$, $p_{|\psi\rangle}$ is the distribution of the outcomes of the measurement of $|\psi\rangle$ in the computational basis $\{|a\rangle\}$. We have

$$p_{|\psi\rangle}(a) = |\langle a|\psi\rangle|^2. \tag{2}$$

The tensor product $A \otimes B$ is sometimes denoted AB. $\mathcal{S}(A)$ is the set of density operators acting on A.

2. METRIC UNCERTAINTY RELATIONS AND INFORMATION LOCKING

2.1 Metric uncertainty relations

The most common way of quantifying uncertainty of measurement outcomes is the entropy. As described in the introduction, a set of measurements defined by bases $\{\mathcal{B}_0, \ldots, \mathcal{B}_{t-1}\}$ of $\mathbb{C}^d$ verifies an entropic uncertainty relation if for all states $|\psi\rangle \in \mathbb{C}^d$, the average measurement entropy obeys

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

for some positive h. It is more convenient here to talk about uncertainty relations for the set of unitary transformations $\{U_k\}$ that transform the bases $\{\mathcal{B}_k\}$ to the fixed computational basis $\{|x\rangle\}$. By definition, we then have $p_{U_k|\psi\rangle} = p_{\mathcal{B}_k, |\psi\rangle}$ (see equation (2)). Entropic uncertainty relations have been used in proving the security of cryptographic protocols in the bounded and noisy quantum storage models [7, 29]. For more details on entropic uncertainty relations and their applications, see the recent survey [37].

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 $|\psi\rangle \in \mathbb{C}^d$, satisfy $\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi\rangle}, \mathrm{unif}([d])\right) \leq \epsilon$ for some $\epsilon \in (0, 1)$. This condition is too strong and we will see that a weaker definition is enough to give entropic uncertainty relations. Let $\mathbb{C}^d = A \otimes B$ (for example, if $d = 2^n$, A might represent the first $n - \log n$ qubits and B the last $\log n$ qubits) and let the computational basis for $\mathbb{C}^d$ 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 in the computational basis of the whole space to be uniform, we only require the outcome of a measurement of the A system in its computational basis $\{|a\rangle\}$ to be close to uniform. Naturally, the larger the A system, the stronger the uncertainty relation is for a fixed size for the B system. We define for $a \in [d_A]$,

$$p^A_{U_k|\psi\rangle}(a) = \sum_{b=0}^{d_B-1} |\langle a|^A \langle b|^B U_k|\psi\rangle|^2. \tag{4}$$

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 $|\psi\rangle \in AB$,*

$$\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p^A_{U_k|\psi\rangle}, \mathit{unif}([d_A])\right) \leq \epsilon. \tag{5}$$

Remark. Using Fannes' inequality, one can show that $\{U_0, \ldots, U_{t-1}\}$ defines an uncertainty relation with average measurement entropy of $(1 - \epsilon) \log d_A - \eta(\epsilon)$ where η is independent of the dimensions. Hence, all our results on metric uncertainty relations imply entropic uncertainty relations. $\square$

We briefly mention the connection to low-distortion embeddings. A metric uncertainty relation directly defines an embedding of ℓ_2 into $\ell_1(\ell_2)$. In fact, the linear map $|\psi\rangle \mapsto \frac{1}{\sqrt{t}}\sum_k U_k|\psi\rangle \otimes |k\rangle$ is an embedding of (AB, ℓ_2) into $(AKB, \ell_1^{AK}(\ell_2^B))$ with distortion $(1-\epsilon)^{-1}$, where the $\ell_1^A(\ell_2^B)$ norm of a vector $|\psi\rangle = \sum_{a,b} \alpha_{a,b}|a\rangle|b\rangle$ in AB is defined by $\||\psi\rangle\|_{12} = \sum_a \sqrt{\sum_b |\alpha_{a,b}|^2}$. Observe that a general low-distortion embedding of (AB, 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 $|\psi\rangle \mapsto \frac{1}{\sqrt{t}}\sum_k U_k|\psi\rangle \otimes |k\rangle$.

2.2 Information locking

We view information 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. We propose a definition of a locking scheme that is stronger than all previous definitions [12, 23, 14].

DEFINITION 2.2 (ϵ-LOCKING SCHEME). *Let n be a positive integer and $\epsilon \in [0, 1]$. An encoding $\mathcal{E} : [2^n] \times [t] \to \mathcal{S}(C)$ is said to be ϵ-locking for the quantum system C if:*

	Inf. leakage	Size of key	Size of ciphertext	Efficient ?
[12]	$n/2$	1	n	yes
[23]	3	$4\log(n)$	n	no
[14]	ϵn	$2\log(n/\epsilon^2) + O(\log\log(1/\epsilon))$	n	no
Corollary 3.2	ϵn	$2\log(1/\epsilon) + O(\log\log(1/\epsilon))$	$n + 2\lceil\log(9/\epsilon)\rceil$	no
Corollary 3.2	ϵn	$4\log(1/\epsilon) + O(\log\log(1/\epsilon))$	n	no
Corollary 4.8	ϵn	$O_\delta(\log(n/\epsilon))$	$(4+\delta)\cdot n$, with $\delta > 0$	yes
Corollary 4.10	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 is measured in bits and gives a bound on the mutual information between the message and the outcome of a measurement applied on the ciphertext. The size of the key is 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 row 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.

- *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 be a uniformly distributed random variable on $[2^n]$ and K be an independent uniform random variable on $[t]$. For any measurement $\{M_i\}$ on C and any outcome i,*

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

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

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-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 encoding. $\square$

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

THEOREM 2.3. *Let $\epsilon \in (0,1)$ and $\{U_0, \ldots, U_{t-1}\}$ be a set of unitary transformations of AB that satisfies an ϵ-metric uncertainty relation on A, where $d_A = 2^n$. 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.

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 $t \cdot d_B$. $\square$

PROOF. First, it is clear that for any value of the key, the ciphertexts for different messages $x \neq x'$ are distinguishable. We now prove the locking property. Let X be the uniformly distributed random variable representing the message. Let K be a uniformly random key in $[t]$ that is independent of X. Consider a POVM $\{M_i\}_i$ on the system AB. Without loss of generality, we can suppose that the POVM elements M_i have rank 1. So we can write the elements as weighted rank one projectors: $M_i = \xi_i |e_i\rangle\langle e_i|$ where $\xi_i > 0$. To evaluate the trace distance between $p_{X|[I=i]}$ and p_X, we start by computing the distribution of the measurement outcome I, given the value of the message $X = x$:

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

Recall that $p_{|\psi\rangle}^A$ is defined in (4). Since X is uniformly distributed, $\mathbf{P}\{I = i\} = \xi_i/(d_B \cdot 2^n)$. Then, for all $x \in [d_A]$, $\mathbf{P}\{X = x | I = i\} = \frac{1}{t} \cdot \sum_{k=0}^{t-1} p_{U_k|e_i\rangle}^A(x)$. Thus, $\Delta\left(p_{X|[I=i]}, p_X\right) \leq \epsilon$ using the fact that $\{U_k\}$ satisfies a metric uncertainty relation on A. $\square$

3. METRIC UNCERTAINTY RELATIONS: EXISTENCE

In this section, we prove the existence of families of unitary transformations satisfying strong metric 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 we use date back to Milman's proof of Dvoretzky's theorem [32, 17]. In fact, using the connection to embeddings of ℓ_2 into $\ell_1(\ell_2)$ described in Section 2, Theorem 3.1 can be viewed as a strengthening of Dvoretzky's theorem for the $\ell_1(\ell_2)$ norm [33].

THEOREM 3.1 (EXISTENCE OF UNCERTAINTY RELATIONS). *Let $\epsilon \in (0,1)$. Let A and B be Hilbert spaces with $d_B \geq 9/\epsilon^2$ and $d_{AB} \geq \frac{9^2 \cdot 16^2 \pi^3}{\epsilon^2}$. Then, for all $t > \frac{2 \cdot 9^2 \cdot \pi^2 \cdot \ln(9/\epsilon)}{\epsilon^2}$, there exists a set $\{U_0, \ldots, U_{t-1}\}$ of unitary transformations of AB satisfying an*

ϵ-metric uncertainty relation on A: for all states $|\psi\rangle \in AB$,

$$\frac{1}{t} \sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi}^A, unif([d_A])\right) \le \epsilon.$$

PROOF. The basic idea is to evaluate the expected value of $\Delta\left(p_{U|\psi}^A, \mathrm{unif}([d_A])\right)$ for a fixed state when U is a random unitary chosen according to the Haar measure. Then, we use a concentration argument (Lévy's lemma) to show that with high probability, this distance is close to its expected value. After this step, we show that the additional averaging $\frac{1}{t}\sum_{k=0}^{t-1} \Delta\left(p_{U_k|\psi}^A, \mathrm{unif}([d_A])\right)$ 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. $\square$

The previous theorem together with Theorem 2.3 proves the existence of ϵ-locking schemes whose key size depends only on ϵ and not on the size of the encoded message.

COROLLARY 3.2 (EXISTENCE OF LOCKING SCHEMES). *Let n be a positive integer 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 $n + 2\log(1/\epsilon) + O(1)$ 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 $\mathbf{P}\{X = i | I = i\} \ge \mathbf{P}\{K = 0\} = 1/t$. Thus, $\Delta\left(p_{X|I=i}, p_X\right) \ge 1/t - 2^{-n}$. $\square$

4. METRIC UNCERTAINTY RELATIONS: EXPLICIT CONSTRUCTION

In this section, we are interested in obtaining families of unitaries $\{U_0, \ldots, U_{t-1}\}$ verifying metric uncertainty relations where $U_0, \ldots, U_{t-1}$ are 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 [27]. 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 (see equation (6) below for a definition) 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 4.3 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. The role of the MUBs 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 $p_{V_j|\psi}$. 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 $p_{P_y V_j|\psi}^A$ is close to uniform.

Mutually unbiased bases.

We start by presenting the construction of γ-MUBs. A set of unitary transformations $\{U_0, \ldots, U_{t-1}\}$ of $\mathbb{C}^d$ is said to define γ-approximately mutually unbiased bases (γ-MUBs) if for all elements $|x\rangle$ and $|y\rangle$ of the computational basis and all $k \ne k'$, we have

$$|\langle x|U_k^\dagger U_{k'}|y\rangle| \le \frac{1}{d^{\gamma/2}}. \tag{6}$$

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

We want to construct a set of γ-MUBs consisting of n-qubit unitaries from the set $\mathcal{H} = \{H^v = H^{v_1} \otimes \cdots \otimes H^{v_n}, v \in \{0,1\}^n\}$, where H is the Hadamard transform on $\mathbb{C}^2$ defined by

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

LEMMA 4.1 (APPROXIMATE MUBS IN $\mathcal{H}$). *Let n' be a positive integer and $n = 2^{n'}$.*

1. *For any integer $r \le n$, 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 $c > 0$ independent of n such that for any $r \le 2^{cn}$ 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,

$$|\langle x|H^v H^{v'}|y\rangle| = |\langle x|H^{v+v'}|y\rangle| \le \frac{1}{2^{d_H(v,v')/2}}. \tag{7}$$

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 $\{0,1\}^{n'}$ that match the performance of random linear codes; see for example Appendix E in [19]. 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. $\square$

Observe that using 1-MUBs is possible (for example, the construction of [39]), but the effect on the final parameters of the construction is minimal. 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 [7] 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 4.1, 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 4.2. *Let $n \geq 1$ and $\epsilon \in (0,1)$ and consider a set of $r = \lceil \frac{2}{\epsilon^2} \rceil$ unitary transformations $V_0, \ldots, V_{r-1}$ of $(\mathbb{C}^2)^{\otimes n}$ defining γ-MUBs. For all $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$,*

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

We give a proof along the lines of the proof of [27, Lemma 4.2]. Similar results can also be found in the sparse approximation literature; see [36, Proposition 4.3] and references therein.

PROOF. Let $d = 2^n$. 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 $|\psi\rangle$,

$$\|(V|\psi\rangle)_S\|_2^2 \leq 1 + \frac{|S|}{d^{\gamma/2}}. \tag{8}$$

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 $G = V_S V_S^\dagger$. 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 (8) holds.

Now pick S to be the set of indices of the $d^{\gamma/2}$ 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

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

One can easily verify that for $j \notin T_\epsilon$, $\Delta\left(p_{V_j|\psi\rangle}, q_j\right) \leq \epsilon$. The distribution q_j for $j \notin T_\epsilon$ 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, $\mathbf{H}_{\min}(q_j) \geq \frac{\gamma n}{2} - \log(8/\epsilon^2)$. $\square$

Permutation extractors.

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

DEFINITION 4.3 (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 $\mathbf{H}_{\min}(X) \geq \ell$, we have*

$$\frac{1}{|S|} \sum_{y \in S} \Delta\left(p_{P_y^E(X)}, \text{unif}(\{0,1\}^m)\right) \leq \epsilon. \tag{9}$$

- *For all $y \in S$, both the function P_y and its inverse P_y^{-1} are computable in time polynomial in n.*

We can adapt an extractor construction of [20] to obtain a permutation extractor with the following parameters.

THEOREM 4.4 (EXPLICIT PERMUTATION EXTRACTORS). *For all (constant) $\delta \in (0,1)$, there exists $c > 0$, such that for all positive integers n, all $\epsilon \in (0, 1/2)$, and all $k \in [c \log(n/\epsilon), n]$, 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 $O(n \operatorname{polylog}(n/\epsilon))$.*

The main construction of Guruswami, Umans and Vadhan [20] 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. Here, we describe how to turn the Reed-Solomon condenser into a permutation condenser. For a complete description of the resulting permutation extractor, we refer the reader to the full version [16].

DEFINITION 4.5 (PERMUTATION 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.*

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 $P^C : (x,y) \mapsto P_y^C(x)$ where $P_y^C(x)$ 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 [20].

THEOREM 4.6. *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 [20], for any integer h, C' is a

$$\left(nt, \log\left(\frac{q^\ell - 1}{\epsilon_0}\right)\right) \to_{2\epsilon_0} \left(\ell t + t, \log\left(\frac{Ah^\ell - 1}{2\epsilon_0}\right)\right) \quad (10)$$

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

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

Plugging these values in equation (10), we get that C' is a

$$(nt, (\ell+1)t) \to_{2\epsilon_0} (\ell t + t, (1-\alpha)\ell t + t - 3)) \quad (11)$$

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 $S \stackrel{\text{def}}{=} \mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ instead of being uniform on the whole field $\mathbb{F}_q$. Note that this increases the error of the extractor 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: for any distributions p and q, there exist joint random variables X and Y, $X \sim p$ and $Y \sim q$ such that $\Delta(p, q) = \mathbf{P}\{X = Y\}$.

Equation (11) 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 $y \in S$,

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

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

$$(nt, (\ell+1)t) \to_\epsilon (\ell t, (1-\alpha)\ell t - 4)) \quad (12)$$

strong condenser.

To define our permutation condenser, we set the first $n' = \ell t$ bits $RS_y^C(x)$ of $RS_y(x)$ to be $RS_y^C(x) = C(x, y)$. We then define the remaining bits by $RS_y^R(f) = [f(\zeta^\ell y), \dots, f(\zeta^{n-1}y)]$. 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.

It only remains to show that RS_y and RS_y^{-1} can be efficiently computed. This follows from the fact that RS_y is simply the evaluation of a polynomial on elements of a field $\mathbb{F}_q$ in which computations can be performed efficiently. $\square$

In addition to the lossless condenser based on Parvaresh-Vardy codes, the extractor construction of [20, Theorem 5.10] uses a simple extractor based on two-universal hash functions [26], which is easily seen to be strong and invertible. Hence, using Theorem 4.6 in the recursive extractor construction of [20, Theorem 5.10], we obtain the strong permutation extractor of Theorem 4.4

The permutation extractor $\{P_y\}$ will be seen as a family of unitary transformations over n qubits. In fact, a permutation P on $\{0,1\}^n$ naturally defines a unitary transformation on $(\mathbb{C}^2)^{\otimes n}$ that we also call P. 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.

The construction.
Combining the γ-MUBs of Lemma 4.1 with the permutation extractor of Theorem 4.4 via Lemma 4.2, we obtain a set of unitaries of the form $P_y V_j$ for $j \in [r]$ and $y \in S$ satisfying a metric uncertainty relation. We just mention that the reason we wanted the permutations defining the extractors to be efficiently invertible is to be able to build quantum circuits that compute the permutation P_y acting on $(\mathbb{C}^2)^{\otimes n}$.

THEOREM 4.7 (EXPLICIT UNCERTAINTY RELATIONS I). *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 $t \leq \left(\frac{n}{\epsilon}\right)^c$ (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 $|\psi\rangle \in AB$,*

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

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 $O(n \operatorname{polylog}(n/\epsilon))$.

We use these uncertainty relations to build locking schemes as described in Theorem 2.3. Observe that such a locking scheme encodes x into a quantum state of the form $V^\dagger P^\dagger |x\rangle \otimes |b\rangle$ where P is a permutation of the computational basis elements and V is a tensor product of single-qubit unitaries. Therefore the state $V^\dagger P^\dagger |x\rangle \otimes |b\rangle$ can be prepared only using classical computations and single-qubit gates. The resulting efficient locking scheme can be used to obtain efficient string commitment protocols [6].

COROLLARY 4.8 (EFFICIENT LOCKING SCHEME I). *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.

Note that in Theorem 4.7, the B system we obtain is quite large. To strengthen the uncertainty relations, we can repeat the construction of the Theorem 4.7 on the B system.

THEOREM 4.9 (EXPLICIT UNCERTAINTY RELATION II). *Let n be a positive integer and $\epsilon \in (2^{-c'n}, 1)$ (c' is a constant independent of n). Then, there exists $t \leq \left(\frac{n}{\epsilon}\right)^{c\log n}$ (for some constant c independent of n and ϵ) unitary transformations $U_0, \ldots, U_{t-1}$ acting on the n-qubit system AB that satisfy an ϵ-metric uncertainty relation on A where A represents the first $n - O(\log\log n) - O(\log(1/\epsilon))$ qubits. All the unitaries U_k can be implemented by quantum circuits of size $O(n \operatorname{polylog}(n/\epsilon))$.*

COROLLARY 4.10 (EFFICIENT LOCKING SCHEME II). *Let 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 into an n-qubit system using a key of size $O(\log(n)\log(n/\epsilon))$ bits.*

5. QUANTUM IDENTIFICATION

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 [38]. 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. Hayden and Winter [25] 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. This protocol is illustrated in Figure 1.

THEOREM 5.1 (QUANTUM IDENTIFICATION). *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 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 can be performed using a single message of n bits and m qubits with an encoding quantum circuit of polynomial size.
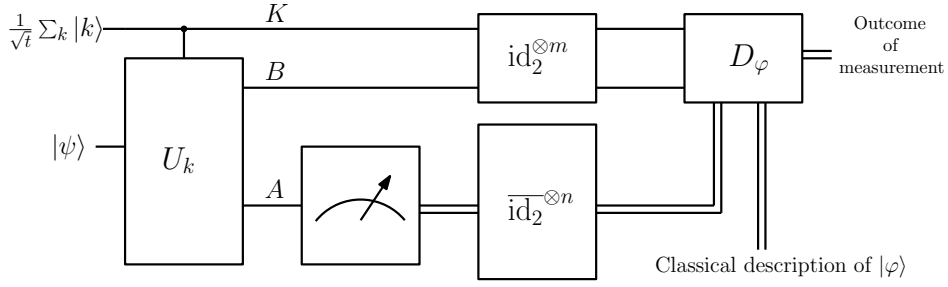
PROOF. We use the following result.

THEOREM 5.2 (THEOREM 7 IN [25]). *Let $\epsilon > 0$ and $V^{C \to ABKE}$ be an isometry satisfying*

$$\forall |\psi\rangle \in C, \qquad \Delta\left(\operatorname{tr}_{ABK}\left(V\psi V^\dagger\right), \frac{\mathbb{1}}{\dim E}\right) \leq \epsilon.$$

Then, there exists a family of POVMs $\{D_\varphi, \mathbb{1} - D_\varphi\}$ for $|\varphi\rangle \in C$ such that together with the encoding map $\mathcal{E}(\cdot) = \operatorname{tr}_E\left(V \cdot V^\dagger\right)$, they define an η-quantum-ID code for the noiseless quantum channel with $\eta = 6\epsilon^{1/4}$.

Figure 1: 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 $A \otimes B$. The A system is then measured in the computational basis. The outcome of this measurement is sent through the classical channel $\overline{\mathrm{id}}_2$. The systems B and K are sent using the quantum channel id_2. The receiver constructs a POVM $\{D_\varphi, I - D_\varphi\}$ based on a classical description of his state $|\varphi\rangle$ and the classical communication he receives.

Let $\{U_0, \ldots, U_{t-1}\}$ be a set of unitaries on n qubits given by Theorem 4.9 verifying an ϵ'- metric uncertainty relation with $\epsilon' = (\epsilon/6)^4$. 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 $\frac{1}{\sqrt{t}} \sum_k |k\rangle^K (U_k|\psi\rangle)^{AB}$. The next step is to measure the system A in the computational basis. To apply Theorem 5.2, we purify this operation by introducing a new ancilla system E initialized to $|0\rangle$ having the same dimension as A. We replace the measurement on A by a coherent copy (controlled-NOT gates) of the computational basis of A into the ancilla E. We obtain the state

$$|\rho\rangle^{KABE} = \frac{1}{\sqrt{t}} \sum_{k,a,b} |k\rangle^K \left(\langle a|^A \langle b|^B U_k|\psi\rangle \right) |a\rangle^A |b\rangle^B |a\rangle^E.$$

We now verify that the reduced state on E is close to maximally mixed for all states $|\psi\rangle$.

$$\rho^E = \frac{1}{t} \sum_{k,a,b} \left| \langle a|^A \langle b|^B U_k|\psi\rangle \right|^2 |a\rangle\langle a|^E = \frac{1}{t} \sum_{k,a} p^A_{U_k|\psi\rangle}(a)|a\rangle\langle a|^E. \tag{13}$$

As a result,

$$\Delta\left(\rho^E, \frac{\mathbb{1}}{\dim E} \right) = \Delta\left(\frac{1}{t} \sum_k p_{U_k|\psi\rangle}, \mathrm{unif}([d_A]) \right)$$
$$\leq \frac{1}{t} \sum_k \Delta\left(p_{U_k|\psi\rangle}, \mathrm{unif}([d_A]) \right)$$
$$\leq \epsilon'.$$

Using Theorem 5.2, the encoder described in Figure 1 and some set of POVM's $\{D_\varphi, \mathbb{1} - D_\varphi\}$ form an η-quantum-ID code for the noiseless qubit channel with $\eta = 6\epsilon'^{1/4} = \epsilon$. We conclude by observing that sending the outcome of the measurement can be done using a classical channel. The number of uses of the noiseless bit channel is $\log \dim A \leq \log \dim C = n$. The number of uses of the noiseless qubit channel is $m = \log \dim B + \log \dim K \leq c \log(n/\epsilon) \cdot \log(n)$ for some constant c.

The fact that the encoding can be computed by a quantum circuit of polynomial size follows from Lemma 4.1 and Theorem 4.4. $\square$

This result can be thought of as a quantum analogue of the well-known fact that the public-coin randomized communication complexity of the classical equality function is $O(\log(1/\epsilon))$ for an error probability ϵ [30]. 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 [25, Theorem 11].

6. CONCLUSION

We have seen how the problem of finding uncertainty relations is closely related to the problem of finding large almost Euclidean subspaces of $(\mathbb{C}^d, \ell_1(\ell_2))$. Using techniques from the study of the geometry of normed spaces, we were able to obtain explicit families of bases satisfying strong metric uncertainty relations and to improve previous analyses of the uncertainty relations satisfied by random bases.

We used these uncertainty relations to exhibit strong locking effects. 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. In fact, as shown in [28], using the communicated message X as a key for a one-time pad encryption might not be secure. On the other hand, a locking scheme achieves a higher security standard than entropically-secure schemes [35, 13, 10]. 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 [21, Corollary 2] based on [34], if the adversary is allowed to store m qubits, then the joint state of the message and the knowledge of the adversary is $(c2^m\epsilon)$-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. Thus, the locking scheme in Corollary 4.8 can be used as a quantum key distribution protocol with no interaction between the parties that is secure in the bounded quantum storage model where the quantum memory of the adversary is limited to $O(\log n)$ qubits. We also show in the full version [16] how a locking scheme can be used to build quantum hiding fingerprints [18] and string commitment protocols [6].

7. REFERENCES

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

[2] G. Aubrun, S. Szarek, and E. Werner. Hastings' additivity counterexample via Dvoretzky's theorem. 2010, arXiv:1003.4925.

[3] G. Aubrun, S. Szarek, and E. Werner. Nonadditivity of Rényi entropy and Dvoretzky's theorem. *J. Math. Phys.* 51(2):022102, 2010, arXiv:0910.1189.

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

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[6] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner. Security of quantum bit string commitment depends on the information measure. *Phys. Rev. Lett.* 97(25):250501, 2006.

[7] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. *Advances in Cryptology – CRYPTO*, pp. 360–378, 2007, arXiv:quant-ph/0612014.

[8] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. *Proc. IEEE FOCS*, pp. 449–458, 2005, arXiv:quant-ph/0508222.

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

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

[11] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.* 50(9):631–633, Feb 1983.

[12] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. Locking classical correlations in quantum states. *Phys. Rev. Lett.* 92(6):67902, 2004, arXiv:quant-ph/0303088.

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

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

[15] A. Dvoretzky. Some results on convex bodies and Banach spaces. *Proc. Internat. Sympos. Linear Spaces*, pp. 123-160, 1961.

[16] O. Fawzi, P. Hayden, and P. Sen. From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking. 2010, arXiv:1010.3007.

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

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

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

[20] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM* 56(4), 2009.

[21] S. Hallgren, C. Moore, M. Rötteler, A. Russell, and P. Sen. Limitations of quantum coset states for graph isomorphism. *J. ACM* 57(6), 2010.

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

[23] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing quantum states: Constructions and applications. *Comm. Math. Phys.* 250(2):371–391, 2004, arXiv:quant-ph/0307104.

[24] P. Hayden and A. Winter. Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$. *Comm. Math. Phys.* 284(1):263–280, 2008, arXiv:0807.4753.

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

[26] R. Impagliazzo, L. Levin, and M. Luby. Pseudo-random generation from one-way functions. *Proc. ACM STOC*, pp. 12–24, 1989.

[27] P. Indyk. Uncertainty principles, extractors, and explicit embeddings of L2 into L1. *Proc. ACM STOC*, pp. 615–620, 2007.

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

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

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

[31] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.* 60(12):1103–1106, Mar 1988.

[32] 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.

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

[34] 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.

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

[36] J. Tropp. *Topics in Sparse Approximation*. Ph.D. thesis, University of Texas at Austin, 2004.

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

[38] A. Winter. Quantum and classical message identification via quantum channels. *Quantum Inf. Comput.* 4(6&7):563–578, 2004, arXiv:quant-ph/0401060.

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