Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases

Manuel A. Ballester* and Stephanie Wehner†
Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
(Received 27 November 2006; published 21 February 2007)

We prove tight entropic uncertainty relations for a large number of mutually unbiased measurements. In particular, we show that a bound derived from the result by Maassen and Uffink [Phys. Rev. Lett. **60**, 1103 (1988)] for two such measurements can in fact be tight for up to $\sqrt{d}$ measurements in mutually unbiased bases. We then show that using more mutually unbiased bases does not always lead to a better locking effect. We prove that the optimal bound for the accessible information using up to $\sqrt{d}$ specific mutually unbiased bases is $\log d/2$, which is the same as can be achieved by using only two bases. Our result indicates that merely using mutually unbiased bases is not sufficient to achieve a strong locking effect and we need to look for additional properties.

DOI: 10.1103/PhysRevA.75.022319 PACS number(s): 03.67.Dd, 03.65.Ta

I. INTRODUCTION

We investigate two related notions that are of importance in many quantum cryptographic tasks: Entropic uncertainty relations and locking classical information in quantum states.

Entropic uncertainty relations are an alternative way to state Heisenberg's uncertainty principle. They are frequently a more useful characterization, because the "uncertainty" is lower bounded by a quantity that does not depend on the state to be measured [1,2]. Recently, entropic uncertainty relations have gained importance in the context of quantum cryptography in the bounded storage model, where proving the security of such protocols ultimately reduces to bounding such relations [3]. Proving new entropic uncertainty relations could thus give rise to new protocols. Such relations are known for two [4], or $d+1$ [5,6] mutually unbiased measurements (see Sec. II for a definition). Very little, however, is known for any other number of measurements [7].

Here we prove tight entropic uncertainty relations for measurements in a large number of mutually unbiased bases (MUBs) in square dimensions. In particular, we consider any MUBs derived from mutually orthogonal Latin squares [8], and any set of MUBs obtained from the set of unitaries of the form $\{U\otimes U^*\}$, where $\{U\}$ gives a set of MUBs in dimension s when applied to the basis elements of the computational basis. For any s, there are at most $s+1$ such MUBs in a Hilbert space of dimension $d=s^2$. Let $\mathbb{B}$ be the set of MUBs coming from one of these two constructions. We prove that for any subset $\mathbb{T}\subseteq\mathbb{B}$ of size at least 2 of these bases we have

$$\min_{|\phi\rangle}\sum_{\mathcal{B}\in\mathbb{T}}H(\mathcal{B},|\phi\rangle)=\frac{|\mathbb{T}|}{2}\log d,$$

where $H(\mathcal{B},|\phi\rangle)=-\Sigma_{i=1}^{d}|\langle\phi|b_i\rangle|^2\log|\langle\phi|b_i\rangle|^2$ is the Shannon entropy [9] arising from measuring the state $|\phi\rangle$ in the basis $\mathcal{B}=\{|b_1\rangle,\ldots,|b_d\rangle\}$.

Our result furthermore shows that one needs to be careful to think of "maximally incompatible" measurements as being necessarily mutually unbiased. When we take entropic uncertainty relations as our measure of "incompatibility," mutually unbiased measurements are in fact not always the most incompatible when considering more than two observables. In particular, it has been shown [10] that if we choose approximately $(\log d)^4$ bases uniformly at random, then $\min_{|\phi\rangle}(1/|\mathbb{T}|)\Sigma_{\mathcal{B}\in\mathbb{T}}H(\mathcal{B},|\phi\rangle)\geq\log d-3$. This means that there exist $(\log d)^4$ bases for which this sum of entropies is very large, i.e., measurements in such bases are very incompatible. However, we showed that when d is large, there exist $\sqrt{d}$, mutually unbiased bases which are much less incompatible according to this measure. When considering entropic uncertainty relations as a measure of "incompatibility," we must therefore look for different properties for the bases to define incompatible measurements.

Finally, we give an alternative proof that if $\mathbb{B}$ is a set of $d+1$ MUBs we have $\Sigma_{\mathcal{B}\in\mathbb{B}}H(\mathcal{B},|\phi\rangle)\geq(d+1)\log[(d+1)/2]$ [5]. Our proof is based on the fact that such a set forms a 2-design, which may offer new insights.

Locking classical correlations in quantum states is an exciting feature of quantum information [11], intricately related to entropic uncertainty relations. Consider a two-party protocol with one or more rounds of communication. Intuitively, one would expect that in each round the amount of correlation between the two parties cannot increase by much more than the amount of data transmitted. For example, transmitting 2ℓ classical bits or ℓ qubits (and using superdense coding) should not increase the amount of correlation by more than 2ℓ bits, no matter what the initial state of the two party system was. This intuition is accurate when we take the classical mutual information $\mathcal{I}_c$ as our correlation measure, and require all communication to be classical. However, when quantum communication is possible at some point during the protocol, everything changes: There exist two-party mixed quantum states, such that transmitting just a single extra bit of classical communication can result in an arbitrarily large increase in $\mathcal{I}_c$ [11]. The magnitude of this increase thereby only depends on the dimension of the initial mixed state. Since then, similar locking effects have been observed also for other correlation measures [12,13]. Such effects play a role in very different scenarios: They have been used to explain physical phenomena related to black holes [14], but they are also important in cryptographic applications such as quantum key distribution [15] and quantum bit string com-

*Email address: Manuel.Ballester@cwi.nl
†Email address: wehner@cwi.nl

mitment [16,17]. We are thus interested in determining how exactly we can obtain locking effects, and how dramatic they can be.

The correlation measure considered here is the classical mutual information of a bipartite quantum state ρ_{AB}, which is the maximum classical mutual information that can be obtained by local measurements $M_A \otimes M_B$ on the state ρ_{AB} [18]:

$$\mathcal{I}_c(\rho_{AB}) = \max_{M_A \otimes M_B} \mathcal{I}(A:B). \quad (1)$$

The classical mutual information is defined as $\mathcal{I}(A:B) = H(P_A) + H(P_B) - H(P_{AB})$, where H is the Shannon entropy. P_A, P_B, and P_{AB} are the probability distributions corresponding to the individual and joint outcomes of measuring the state ρ_{AB} with $M_A \otimes M_B$. The mutual information between A and B is a measure of the information that B contains about A. This measure of correlation is of particular relevance for quantum bit string commitments [16,17]. Furthermore, the first locking effect was observed for this quantity in the following protocol between two parties: Alice (A) and Bob (B). Let $\mathbb{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ with $\mathcal{B}_t = \{|b_1^t\rangle, \ldots, |b_d^t\rangle\}$ a set of m MUBs in $\mathbb{C}^d$. Alice picks an element $k \in \{1, \ldots, d\}$ and a basis $\mathcal{B}_t \in \mathbb{B}$ uniformly at random. She then sends $|b_k^t\rangle$ to Bob, while keeping t secret. Such a protocol gives rise to the joint state

$$\rho_{AB} = \frac{1}{md} \sum_{k=1}^{d} \sum_{t=1}^{m} (|k\rangle\langle k| \otimes |t\rangle\langle t|)_A \otimes (|b_k^t\rangle\langle b_k^t|)_B.$$

Clearly, if Alice told her basis choice t to Bob, he could measure in the right basis and obtain the correct k. Alice and Bob would then share $\log d + \log m$ bits of correlation, which is also their mutual information $\mathcal{I}_c(\sigma_{AB})$, where σ_{AB} is the state obtained from ρ_{AB} after the announcement of t. But, how large is $\mathcal{I}_c(\rho_{AB})$, when Alice does *not* announce t to Bob? It was shown [11] that in dimension $d = 2^n$, using the two MUBs given by the unitaries $\mathbb{I}^{\otimes n}$ and $H^{\otimes n}$ applied to the computational basis, where H is the Hadamard matrix, we have $\mathcal{I}_c(\rho_{AB}) = (1/2)\log d$. This means that the single bit of basis information Alice transmits to Bob "unlocks" $(1/2)\log d$ bits: *Without* this bit, the mutual information is $(1/2)\log d$, but *with* this bit it is $\log d + 1$. It is also known that if Alice and Bob randomly choose a large set of unitaries from the Haar measure to construct $\mathbb{B}$, then $\mathcal{I}_c$ can be brought down to a small constant [10]. However, no explicit constructions with more than two bases are known that give good locking effects. Based on numerical studies for spaces of prime dimension $3 \leqslant d \leqslant 30$, one might hope that adding a third MUB would strengthen the locking effect and give $\mathcal{I}_c(\rho_{AB}) \approx (1/3)\log d$ [11].

Here, however, we show that this intuition fails us. We prove that for three MUBs given by $\mathbb{I}^{\otimes n}$, $H^{\otimes n}$, and $K^{\otimes n}$ where $K = (\mathbb{I} + i\sigma_x)/\sqrt{2}$ and dimension $d = 2^n$ for some even integer n, we have

$$\mathcal{I}_c(\rho_{AB}) = (1/2)\log d, \quad (2)$$

the same locking effect as with two MUBs. We also show that for any subset of the MUBs based on Latin squares and the MUBs in square dimensions based on generalized Pauli matrices [19], we again obtain Eq. (2), i.e., using two or all $\sqrt{d}$ of them makes no difference at all. Finally, we show that for any set of MUBs $\mathbb{B}$ based on generalized Pauli matrices in *any* dimension, $\mathcal{I}_c(\rho_{AB}) = \log d - \min_{|\phi\rangle}(1/|\mathbb{B}|)\Sigma_{\mathcal{B}\in\mathbb{B}} H(\mathcal{B}, |\phi\rangle)$, i.e., it is enough to determine a bound on the entropic uncertainty relation to determine the strength of the locking effect.

Although bounds for general MUBs still elude us, our results show that merely choosing the bases to be mutually unbiased is not sufficient and we must look elsewhere to find bases which provide good locking.

II. PRELIMINARIES

Throughout this paper, we use the shorthand notation $[d] = \{1, \ldots, d\}$. We write

$$H(\mathcal{B}_t, |\phi\rangle) = -\sum_{i=1}^{d} |\langle\phi|b_k^t\rangle|^2 \log |\langle\phi|b_k^t\rangle|^2,$$

for the Shannon entropy [9] arising from measuring the pure state $|\phi\rangle$ in basis $\mathcal{B}_t = \{|b_1^t\rangle, \ldots, |b_d^t\rangle\}$. In general, we will use $|b_k^t\rangle$ with $k \in [d]$ to denote the kth element of a basis $\mathcal{B}_t$ indexed by t. We also briefly refer to the Rényi entropy of order 2 (collision entropy) of measuring $|\phi\rangle$ in basis $\mathcal{B}_t$ given by $H_2(\mathcal{B}_t, |\phi\rangle) = -\log \Sigma_{i=1}^{d} |\langle\phi|b_k^t\rangle|^4$ [20].

A. Mutually unbiased bases

We also need the notion of mutually unbiased bases (MUBs), which were initially introduced in the context of state estimation [21], but appear in many other problems in quantum information. The following definition closely follows the one given in [19].

Definition 1 MUBs. Let $\mathcal{B}_1 = \{|b_1^1\rangle, \ldots, |b_d^1\rangle\}$ and $\mathcal{B}_2 = \{|b_1^2\rangle, \ldots, |b_d^2\rangle\}$ be two orthonormal bases in $\mathbb{C}^d$. They are said to be *mutually unbiased* if $|\langle b_k^1|b_l^2\rangle| = 1/\sqrt{d}$, for every $k, l \in [d]$. A set $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of orthonormal bases in $\mathbb{C}^d$ is called a *set of mutually unbiased bases* if each pair of bases is mutually unbiased.

We use $N(d)$ to denote the maximal number of MUBs in dimension d. In any dimension d, we have that $N(d) \leqslant d+1$ [19]. If $d = p^k$ is a prime power, we have that $N(d) = d+1$ and explicit constructions are known [19,21]. If $d = s^2$ is a square, $N(d) \geqslant \mathrm{MOLS}(s)$, where $\mathrm{MOLS}(s)$ denotes the number of mutually orthogonal $s \times s$ Latin squares [8]. In general, we have $N(nm) \geqslant \min\{N(n), N(m)\}$ for all $n, m \in \mathbb{N}$ [22,23]. It is also known that in any dimension, there exists an explicit construction for three MUBs [24]. Unfortunately, not very much is known for other dimensions. For example, it is still an open problem whether there exists a set of seven MUBs in dimension $d = 6$. We say that a unitary U_t transforms the computational basis into the tth MUB $\mathcal{B}_t = \{|b_1^t\rangle, \ldots, |b_d^t\rangle\}$ if for all $k \in [d]$ we have $|b_k^t\rangle = U_t|k\rangle$. Here we are particularly concerned with two specific constructions of mutually unbiased bases.

1. Latin squares

First of all, we consider MUBs based on mutually orthogonal Latin squares [8]. Informally, an $s \times s$ Latin square

over the symbol set $[s]=\{1,\ldots,s\}$ is an arrangement of elements of $[s]$ into an $s\times s$ square such that in each row and each column every element occurs exactly once. Let L_{ij} denote the entry in a Latin square in row i and column j. Two Latin squares L and L' are called mutually orthogonal if and only if $\{(L_{i,j},L'_{i,j})|i,j\in[s]\}=\{(u,v)|u,v\in[s]\}$. From any $s\times s$ Latin square we can obtain a basis for $\mathbb{C}^s\otimes\mathbb{C}^s$. First, we construct s of the basis vectors from the entries of the Latin square itself. Let $|v_{1,\ell}\rangle=(1/\sqrt{s})\Sigma_{i,j\in[s]}E^L_{i,j}(\ell)|i,j\rangle$, where E^L is a predicate such that $E^L_{i,j}(\ell)=1$ if and only if $L_{i,j}=\ell$. Note that for each ℓ we have exactly s pairs i,j such that $E_{i,j}(\ell)=1$, because each element of $[s]$ occurs exactly s times in the Latin square. Secondly, from each such vector we obtain $s-1$ additional vectors by adding successive rows of an $s\times s$ (complex) Hadamard matrix $H=(h_{ij})$ as coefficients to obtain the remaining $|v_{t,j}\rangle$ for $t\in[s]$, where $h_{ij}=\omega^{ij}$ with $i,j\in\{0,\ldots,s-1\}$ and $\omega=e^{2\pi i/s}$. Two additional MUBs can then be obtained in the same way from the two non-Latin squares where each element occurs for an entire row or column, respectively. From each mutually orthogonal Latin square and these two extra squares which also satisfy the above orthogonality condition, we obtain one basis. This construction therefore gives MOLS$(s)+2$ many MUBs. It is known that if $s=p^k$ is a prime power itself, we obtain $p^k+1\approx\sqrt{d}$ MUBs from this construction. Note, however, that there do exist many more MUBs in prime power dimensions, namely $d+1$. If s is not a prime power, it is merely known that MOLS$(s)\geqslant s^{1/14.8}$ [8].

As an example, consider the following 3×3 Latin square and the 3×3 Hadamard matrix

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array},\quad H=\begin{pmatrix}1&1&1\\1&\omega&\omega^2\\1&\omega^2&\omega\end{pmatrix},$$

where $\omega=e^{2\pi i/3}$. First, we obtain vectors

$$|v_{1,1}\rangle=(|1,1\rangle+|2,3\rangle+|3,2\rangle)/\sqrt{3},$$

$$|v_{1,2}\rangle=(|1,2\rangle+|2,1\rangle+|3,3\rangle)/\sqrt{3},$$

$$|v_{1,3}\rangle=(|1,3\rangle+|2,2\rangle+|3,1\rangle)/\sqrt{3}.$$

With the help of H we obtain three additional vectors from the ones above. From the vector $|v_{1,1}\rangle$, for example, we obtain

$$|v_{1,1}\rangle=(|1,1\rangle+|2,3\rangle+|3,2\rangle)/\sqrt{3},$$

$$|v_{2,1}\rangle=(|1,1\rangle+\omega|2,3\rangle+\omega^2|3,2\rangle)/\sqrt{3},$$

$$|v_{3,1}\rangle=(|1,1\rangle+\omega^2|2,3\rangle+\omega|3,2\rangle)/\sqrt{3}.$$

This gives us basis $\mathcal{B}=\{|v_{t,\ell}\rangle|t,\ell\in[s]\}$ for $s=3$. The construction of another basis follows in exactly the same way from a mutually orthogonal Latin square. The fact that two such squares L and L' are mutually orthogonal ensures that the resulting bases will be mutually unbiased. Indeed, suppose we are given another such basis, $\mathcal{B}'=\{|u_{t,\ell}\rangle|t,\ell\in[s]\}$ belonging to L'. We then have for any $\ell,\ell'\in[s]$ that $|\langle u_{1,\ell'}|v_{1,\ell}\rangle|^2=|(1/s)\Sigma_{i,j\in[s]}E^{L'}_{i,j}(\ell')E^L_{i,j}(\ell)|^2=1/s^2$, as there exists exactly only one pair $\ell,\ell'\in[s]$ such that $E^{L'}_{i,j}(\ell')E^L_{i,j}(\ell)=1$. Clearly, the same argument holds for the additional vectors derived from the Hadamard matrix.

2. Generalized Pauli matrices

The second construction we consider is based on the generalized Pauli matrices X_d and Z_d [19], defined by their actions on the computational basis $C=\{|1\rangle,\ldots,|d\rangle\}$ as follows:

$$X_d|k\rangle=|k+1\rangle,\quad Z_d|k\rangle=\omega^k|k\rangle,\quad\forall\ |k\rangle\in C,$$

where $\omega=e^{2\pi i/d}$. We say that $(X_d)^{a_1}(Z_d)^{b_1}\otimes\cdots\otimes(X_d)^{a_N}(Z_d)^{b_N}$ for $a_k,b_k\in\{0,\ldots,d-1\}$ and $k\in[N]$ is a *string of Pauli matrices*.

If d is a prime, it is known that the $d+1$ MUBs constructed first by Wootters and Fields [21] can also be obtained as the eigenvectors of the matrices $Z_d,X_d,X_dZ_d,X_dZ_d^2,\ldots,X_dZ_d^{d-1}$ [19]. If $d=p^k$ is a prime power, consider all d^2-1 possible strings of Pauli matrices excluding the identity and group them into sets $C_1,\ldots,C_{d+1}$ such that $|C_i|=d-1$ and $C_i\cup C_j=\{\mathbb{I}\}$ for $i\neq j$ and all elements of C_i commute. Let B_i be the common eigenbasis of all elements of C_i. Then $B_1,\ldots,B_{d+1}$ are MUBs [19]. A similar result for $d=2^k$ has also been shown in [25]. A special case of this construction is the three mutually unbiased bases in dimension $d=2^k$ given by the unitaries $\mathbb{I}^{\otimes k},H^{\otimes k}$, and $K^{\otimes k}$ with $K=(\mathbb{I}+i\sigma_x)/\sqrt{2}$ applied to the computational basis.

B. 2-designs

For the purposes of the present work, *spherical t-designs* (see for example Ref. [26]) can be defined as follows.

Definition 2 (*t-design*). Let $\{|\tau_1\rangle,\ldots,|\tau_m\rangle\}$ be a set of state vectors in $\mathbb{C}^d$. They are said to form a t-design if

$$\frac{1}{m}\sum_{i=1}^{m}[|\tau_i\rangle\langle\tau_i|]^{\otimes t}=\frac{\Pi_+^{(t,d)}}{\mathrm{Tr}\,\Pi_+^{(t,d)}},$$

where $\Pi_+(t,d)$ is a projector onto the completely symmetric subspace of $\mathbb{C}^{d\otimes t}$ and

$$\mathrm{Tr}\,\Pi_+^{(t,d)}=\binom{d+t-1}{d-1}=\frac{(d+t-1)!}{(d-1)!t!},$$

is its dimension.

Any set $\mathbb{B}$ of $d+1$ MUBs forms a spherical 2-design [26,27], i.e., we have for $\mathbb{B}=\{\mathcal{B}_1,\ldots,\mathcal{B}_{d+1}\}$ with $\mathcal{B}_t=\{|b_1^t\rangle,\ldots,|b_d^t\rangle\}$ that

$$\frac{1}{d(d+1)}\sum_{t=1}^{d+1}\sum_{k=1}^{d}[|b_k^t\rangle\langle b_k^t|]^{\otimes2}=2\frac{\Pi_+^{(2,d)}}{d(d+1)}.$$

III. UNCERTAINTY RELATIONS

We now prove tight entropic uncertainty for measurements in MUBs in square dimensions. The main result of [4],

which will be very useful for us, is stated next.

Theorem 1 (Maassen and Uffink). Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two orthonormal bases in a Hilbert space of dimension d. Then for all pure states $|\psi\rangle$

$$\frac{1}{2}[H(\mathcal{B}_1,|\psi\rangle)+H(\mathcal{B}_2,|\psi\rangle)] \geqslant -\log c(\mathcal{B}_1,\mathcal{B}_2), \tag{3}$$

where $c(\mathcal{B}_1,\mathcal{B}_2)=\max\{|\langle b_1|b_2\rangle|:|b_1\rangle\in\mathcal{B}_1,|b_2\rangle\in\mathcal{B}_2\}$.

The case when $\mathcal{B}_1$ and $\mathcal{B}_2$ are MUBs is of special interest for us. More generally, when one has a set of MUBs a trivial application of Eq. (3) leads to the following corollary also noted in [7].

Corollary 1. Let $\mathbb{B}=\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$, be a set of MUBs in a Hilbert space of dimension d. Then

$$\frac{1}{m}\sum_{t=1}^{m} H(\mathcal{B}_t,|\psi\rangle) \geqslant \frac{\log d}{2}. \tag{4}$$

Proof. Using Eq. (3), one gets that for any pair of MUBs $\mathcal{B}_t$ and $\mathcal{B}_{t'}$ with $t\neq t'$

$$\frac{1}{2}[H(\mathcal{B}_t,\psi)+H(\mathcal{B}_{t'},\psi)] \geqslant \frac{\log d}{2}. \tag{5}$$

Adding up the resulting equation for all pairs $t\neq t'$ we get the desired result (4). ■

Here, we now show that this bound can in fact be tight for a large set of MUBs.

A. MUBs in square dimensions

Corollary 1 gives a lower bound on the average of the entropies of a set of MUBs. The obvious question is whether that bound is tight. We show that the bound is indeed tight when we consider product MUBs in a Hilbert space of square dimension.

Theorem 2. Let $\mathbb{B}=\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ with $m\geqslant 2$ be a set of MUBs in a Hilbert space $\mathcal{H}$ of dimension s. Let U_t be the unitary operator that transforms the computational basis to $\mathcal{B}_t$. Then $\mathbb{V}=\{\mathcal{V}_1,\ldots,\mathcal{V}_m\}$, where

$$\mathcal{V}_t=\{U_t|k\rangle\otimes U_t^*|l\rangle:k,l\in[s]\},$$

is a set of MUBs in $\mathcal{H}\otimes\mathcal{H}$, and it holds that

$$\min_{|\psi\rangle}\frac{1}{m}\sum_{t=1}^{m} H(\mathcal{V}_t,|\psi\rangle)=\frac{\log d}{2}, \tag{6}$$

where $d=\dim(\mathcal{H}\otimes\mathcal{H})=s^2$.

Proof. It is easy to check that $\mathbb{V}$ is indeed a set of MUBs. Our proof works by constructing a state $|\psi\rangle$ that achieves the bound in corollary 1. It is easy to see that the maximally entangled state

$$|\psi\rangle=\frac{1}{\sqrt{s}}\sum_{k=1}^{s}|kk\rangle,$$

satisfies $U\otimes U^*|\psi\rangle=|\psi\rangle$ for any $U\in U(d)$. Indeed,

$$\langle\psi|U\otimes U^*|\psi\rangle=\frac{1}{s}\sum_{k,l=1}^{s}\langle k|U|l\rangle\langle k|U^*|l\rangle=\frac{1}{s}\sum_{k,l=1}^{s}\langle k|U|l\rangle\langle l|U^\dagger|k\rangle$$

$$=\frac{1}{s}\,\mathrm{Tr}UU^\dagger=1.$$

Therefore, for any $t\in[m]$ we have that

$$H(\mathcal{V}_t,|\psi\rangle)=-\sum_{kl}|\langle kl|U_t\otimes U_t^*|\psi\rangle|^2\log|\langle kl|U_t\otimes U_t^*|\psi\rangle|^2=$$

$$-\sum_{kl}|\langle kl|\psi\rangle|^2\log|\langle kl|\psi\rangle|^2=\log s=\frac{\log d}{2}.$$

Taking the average of the previous equation we get the desired result. ■

B. MUBs based on Latin squares

We now consider mutually unbiased bases based on Latin squares [8] as described in Sec. II. Our proof again follows by providing a state that achieves the bound in corollary 1, which turns out to have a very simple form.

Lemma 1. Let $\mathbb{B}=\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ with $m\geqslant 2$ be any set of MUBs in a Hilbert space of dimension $d=s^2$ constructed on the basis of Latin squares. Then

$$\min_{|\psi\rangle}\frac{1}{m}\sum_{\mathcal{B}\in\mathbb{B}}H(\mathcal{B},|\psi\rangle)=\frac{\log d}{2}.$$

Proof. Consider the state $|\psi\rangle=|1,1\rangle$ and fix a basis $\mathcal{B}_t=\{|v_{i,j}^t\rangle|\,i,j\in[s]\}\in\mathbb{B}$ coming from a Latin square. It is easy to see that there exists exactly one $j\in[s]$ such that $\langle v_{1,j}^t|1,1\rangle=1/\sqrt{s}$. Namely this will be the $j\in[s]$ at position (1,1) in the Latin square. Fix this j. For any other $\ell\in[s]$, $\ell\neq j$, we have $\langle v_{1,\ell}^t|1,1\rangle=0$. But this means that there exist exactly s vectors in $\mathcal{B}$ such that $|\langle v_{i,j}^t|1,1\rangle|^2=1/s$, namely exactly the s vectors derived from $|v_{1,j}^t\rangle$ via the Hadamard matrix. The same argument holds for any such basis $\mathcal{B}\in\mathbb{T}$. We get

$$\sum_{\mathcal{B}\in\mathbb{B}}H(\mathcal{B},|1,1\rangle)=\sum_{\mathcal{B}\in\mathbb{B}}\sum_{i,j\in[s]}|\langle v_{i,j}^t|1,1\rangle|^2\log|\langle v_{i,j}^t|1,1\rangle|^2$$

$$=|\mathbb{T}|s\frac{1}{s}\log\frac{1}{s}=|\mathbb{T}|\frac{\log d}{2}.$$

The result then follows directly from corollary 1. ■

C. Using a full set of MUBs

We now provide an alternative proof of an entropic uncertainty relation for a full set of mutually unbiased bases. This has previously been proved in [5]. Nevertheless, because our proof is so simple using existing results about 2-designs we include it here for completeness, in the hope that if may offer additional insight.

Lemma 2. Let $\mathbb{B}$ be a set of $d+1$ MUBs in a Hilbert space of dimension d. Then

$$\frac{1}{d+1}\sum_{\mathcal{B}\in\mathbb{B}}H_2(\mathcal{B},|\psi\rangle)\geqslant\log\left(\frac{d+1}{2}\right).$$

Proof. Let $\mathcal{B}_t=\{|b_1^t\rangle,\ldots,|b_d^t\rangle\}$ and $\mathbb{B}=\{\mathcal{B}_1,\ldots,\mathcal{B}_{d+1}\}$. We can then write

$$\frac{1}{d+1}\sum_{\mathcal{B}\in\mathbb{B}} H_2(\mathcal{B},|\psi\rangle) = -\frac{1}{d+1}\sum_{t=1}^{d+1}\log\sum_{k=1}^{d}|\langle b_k^t|\psi\rangle|^4$$
$$\geqslant \log\left(\frac{1}{d+1}\sum_{t=1}^{d+1}\sum_{k=1}^{d}|\langle b_k^t|\psi\rangle|^4\right)$$
$$= \log\left(\frac{d+1}{2}\right),$$

where the first inequality follows from the concavity of the log, and the final inequality follows directly from the fact that a full set of MUBs forms a 2-design and ([27], theorem 1). ■

We then obtain the original result by Sanchez-Ruiz [5] by noting that $H(\cdot)\geqslant H_2(\cdot)$.

Corollary 2. Let $\mathbb{B}$ be a set of $d+1$ MUBs in a Hilbert space of dimension d. Then

$$\frac{1}{d+1}\sum_{\mathcal{B}\in\mathbb{B}} H(\mathcal{B},|\psi\rangle)\geqslant\log\left(\frac{d+1}{2}\right).$$

IV. LOCKING

We now turn our attention to locking. We first explain the connection between locking and entropic uncertainty relations. In particular, we show that for MUBs based on generalized Pauli matrices, we only need to look at such uncertainty relations to determine the exact strength of the locking effect. We then consider how good MUBs based on Latin squares are for locking.

In order to determine how large the locking effect is for some set of mutually unbiased bases $\mathbb{B}$, and the state

$$\rho_{AB}=\sum_{t=1}^{|\mathbb{B}|}\sum_{k=1}^{d} p_{t,k}(|k\rangle\langle k|\otimes|t\rangle\langle t|)_A\otimes(|b_k^t\rangle\langle b_k^t|)_B, \tag{7}$$

we must find an optimal bound for $\mathcal{I}_c(\rho_{AB})$. Here, $\{p_{t,k}\}$ is a probability distribution over $\mathbb{B}\times[d]$. That is, we must find a positive operator valued measure (POVM) $M_A\otimes M_B$ that maximizes Eq. (1). It has been shown in [11] that we can restrict ourselves to taking M_A to be the local measurement determined by the projectors $\{|k\rangle\langle k|\otimes|t\rangle\langle t|\}$. It is also known that we can limit ourselves to take the measurement M_B consisting of rank one elements $\{\alpha_i|\Phi_i\rangle\langle\Phi_i|\}$ only [28], where $\alpha_i\geqslant 0$ and $|\Phi_i\rangle$ is normalized. Maximizing over M_B then corresponds to maximizing Bob's accessible information [[29], Eq. (9.75)] for the ensemble $\mathcal{E}=\{p_{k,t},|b_k^t\rangle\langle b_k^t|\}$

$$\mathcal{I}_{\mathrm{acc}}(\mathcal{E})=\max_M\left(-\sum_{k,t}p_{k,t}\log p_{k,t}\right.$$
$$\left.+\sum_i\sum_{k,t}p_{k,t}\alpha_i\langle\Phi_i|\rho_{k,t}|\Phi_i\rangle\log\frac{p_{k,t}\langle\Phi_i|\rho_{k,t}|\Phi_i\rangle}{\langle\Phi_i|\mu|\Phi_i\rangle}\right), \tag{8}$$

where $\mu=\Sigma_{k,t}p_{k,t}\rho_{k,t}$ and $\rho_{k,t}=|b_k^t\rangle\langle b_k^t|$. Therefore, we have $\mathcal{I}_c(\rho_{AB})=\mathcal{I}_{\mathrm{acc}}(\mathcal{E})$. We are now ready to prove our locking results.

A. An example

We first consider a very simple example with only three MUBs that provides the intuition behind the remainder of our paper. The three MUBs we consider now are generated by the unitaries $\mathbb{I}$, H, and $K=(\mathbb{I}+i\sigma_x)/\sqrt{2}$ when applied to the computational basis. For this small example, we also investigate the role of the prior over the bases and the encoded basis elements. It turns out that this does not affect the strength of the locking effect positively. Actually, it is possible to show the same for encodings in many other bases. However, we do not consider this case in full generality as to not obscure our main line of argument.

Lemma 3. Let $U_0=\mathbb{I}^{\otimes n}$, $U_1=H^{\otimes n}$, and $U_2=K^{\otimes n}$, where $k\in\{0,1\}^n$ and n is an even integer. Let $\{p_t\}$ with $t\in[2]$ be a probability distribution over the set $\mathcal{S}=\{U_1,U_2,U_3\}$. Suppose that $p_1,p_2,p_3\leqslant 1/2$ and let $p_{t,k}=p_t(1/d)$. Consider the ensemble $\mathcal{E}=\{p_t(1/d),U_t|k\rangle\langle k|U_t^\dagger\}$; then

$$\mathcal{I}_{\mathrm{acc}}(\mathcal{E})=\frac{n}{2}.$$

If, on the other hand, there exists a $t\in[2]$ such that $p_t>1/2$, then $\mathcal{I}_{\mathrm{acc}}(\mathcal{E})>n/2$.

Proof. We first give an explicit measurement strategy and then prove a matching upper bound on $\mathcal{I}_{\mathrm{acc}}$. Consider the Bell basis vectors $|\Gamma_{00}\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$, $|\Gamma_{01}\rangle=(|00\rangle-|11\rangle)/\sqrt{2}$, $|\Gamma_{10}\rangle=(|01\rangle+|10\rangle)/\sqrt{2}$, and $|\Gamma_{11}\rangle=(|01\rangle-|10\rangle)/\sqrt{2}$. Note that we can write for the computational basis

$$|00\rangle=\frac{1}{\sqrt{2}}(|\Gamma_{00}\rangle+|\Gamma_{01}\rangle),$$

$$|01\rangle=\frac{1}{\sqrt{2}}(|\Gamma_{10}\rangle+|\Gamma_{11}\rangle),$$

$$|10\rangle=\frac{1}{\sqrt{2}}(|\Gamma_{10}\rangle-|\Gamma_{11}\rangle),$$

$$|11\rangle=\frac{1}{\sqrt{2}}(|\Gamma_{00}\rangle-|\Gamma_{01}\rangle).$$

The crucial fact to note is that if we fix some k_1k_2, then there exist exactly two Bell basis vectors $|\Gamma_{i_1i_2}\rangle$ such that $|\langle\Gamma_{i_1i_2}|k_1k_2\rangle|^2=1/2$. For the remaining two basis vectors the inner product with $|k_1k_2\rangle$ will be zero. A simple calculation shows that we can express the two qubit basis states of the other two mutually unbiased bases analogously: For each two qubit basis state there are exactly two Bell basis vectors such that the inner product is zero and for the other two the inner product squared is 1/2.

We now take the measurement given by $\{|\Gamma_i\rangle\langle\Gamma_i|\}$ with $|\Gamma_i\rangle=|\Gamma_{i_1i_2}\rangle\otimes\ldots\otimes|\Gamma_{i_{n-1}i_n}\rangle$ for the binary expansion of $i=i_1,i_2,\ldots,i_n$. Fix a $k=k_1,k_2,\ldots,k_n$. By the above argument,

there exist exactly $2^{n/2}$ strings $i \in \{0,1\}^n$ such that $|\langle \Gamma_i|k\rangle|^2 = 1/(2^{n/2})$. Putting everything together, Eq. (8) now gives us for any prior distribution $\{p_{t,k}\}$ that

$$-\sum_i \langle \Gamma_i|\mu|\Gamma_i\rangle \log\langle \Gamma_i|\mu|\Gamma_i\rangle - \frac{n}{2} \leqslant \mathcal{I}_{\mathrm{acc}}(\mathcal{E}). \tag{9}$$

For our particular distribution we have $\mu = \mathbb{I}/d$ and thus

$$\frac{n}{2} \leqslant \mathcal{I}_{\mathrm{acc}}(\mathcal{E}).$$

We now prove a matching upper bound that shows that our measurement is optimal. For our distribution, we can rewrite Eq. (8) for the POVM given by $\{\alpha_i|\Phi_i\rangle\langle\Phi_i|\}$ to

$$\begin{aligned}\mathcal{I}_{\mathrm{acc}}(\mathcal{E}) &= \max_M \Bigg(\log d \\ &\quad + \sum_i \frac{\alpha_i}{d} \sum_{k,t} p_t |\langle \Phi_i|U_t|k\rangle|^2 \log |\langle \Phi_i|U_t|k\rangle|^2 \Bigg) \\ &= \max_M \left(\log d - \sum_i \frac{\alpha_i}{d} \sum_t p_t H(\mathcal{B}_t, |\Phi_i\rangle) \right).\end{aligned}$$

It follows from corollary 1 that $\forall i \in \{0,1\}^n$ and $p_1, p_2, p_3 \leqslant 1/2$,

$$\begin{aligned}&(1/2 - p_1)[H(\mathcal{B}_2, |\Phi_i\rangle) + H(\mathcal{B}_3, |\Phi_i\rangle)] + (1/2 - p_2)[H(\mathcal{B}_1, |\Phi_i\rangle) \\ &\quad + H(\mathcal{B}_3, |\Phi_i\rangle)] + (1/2 - p_3)[H(\mathcal{B}_1, |\Phi_i\rangle) + H(\mathcal{B}_2, |\Phi_i\rangle)] \\ &\geqslant n/2.\end{aligned}$$

Reordering the terms we now get $\Sigma_{t=1}^3 p_t H(\mathcal{B}_t, |\Phi_i\rangle) \geqslant n/2$. Putting things together and using the fact that $\Sigma_i \alpha_i = d$, we obtain

$$\mathcal{I}_{\mathrm{acc}}(\mathcal{E}) \leqslant \frac{n}{2},$$

from which the result follows.

If, on the other hand, there exists a $t \in [2]$ such that $p_t > 1/2$, then by measuring in the basis $\mathcal{B}_t$ we obtain $\mathcal{I}_{\mathrm{acc}}(\mathcal{E}) \geqslant p_t n > n/2$. ■

Above, we have only considered a nonuniform prior over the set of bases. In [30] it is observed that when we want to guess the XOR of a string of length 2 encoded in one (unknown to us) of these three bases, the uniform prior on the strings is not the one that gives the smallest probability of success. This might lead one to think that a similar phenomenon could be observed in the present setting, i.e., that one might obtain better locking with three basis for a nonuniform prior on the strings. In what follows, however, we show that this is not the case.

Let $p_t = \Sigma_k p_{k,t}$ be the marginal distribution on the basis, then the difference in Bob's knowledge between receiving only the quantum state and receiving the quantum state *and* the basis information is given by

$$\Delta(p_{k,t}) = H(p_{k,t}) - \mathcal{I}_{\mathrm{acc}}(\mathcal{E}) - H(p_t),$$

substracting the basis information itself. Consider the post-measurement state $\nu = \Sigma_i \langle \Gamma_i|\mu|\Gamma_i\rangle |\Gamma_i\rangle\langle\Gamma_i|$. Using Eq. (9) we obtain

$$\Delta(p_{k,t}) \leqslant H(p_{k,t}) - S(\nu) + n/2 - H(p_t), \tag{10}$$

where S is the von Neuman entropy. Considering the state

$$\rho_{12} = \sum_{k=1}^{d} \sum_{t=1}^{3} p_{k,t} (|t\rangle\langle t|)_1 \otimes (U_t|k\rangle\langle k|U_t^\dagger)_2,$$

we have that

$$\begin{aligned}S(\rho_{12}) = H(p_{k,t}) &\leqslant S(\rho_1) + S(\rho_2) = H(p_t) + S(\mu) \leqslant H(p_t) \\ &\quad + S(\nu).\end{aligned}$$

Using Eq. (10) and the previous equation we get

$$\Delta(p_{k,t}) \leqslant n/2,$$

for any prior distribution. This bound is saturated by the uniform prior and therefore we conclude that the uniform prior results in the largest gap possible.

B. MUBs from generalized Pauli matrices

We first consider MUBs based on the generalized Pauli matrices X_d and Z_d as described in Sec. II. We consider a uniform prior over the elements of each basis and the set of bases. Choosing a nonuniform prior does not lead to a better locking effect.

Lemma 4. Let $\mathbb{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ be any set of MUBs constructed on the basis of generalized Pauli matrices in a Hilbert space of prime power dimension $d = p^N$. Consider the ensemble $\mathcal{E} = \{1/(dm), |b_k^t\rangle\langle b_k^t|\}$. Then

$$I_{\mathrm{acc}}(\mathcal{E}) = \log d - \frac{1}{m} \min_{|\psi\rangle} \sum_{\mathcal{B}_t \in \mathbb{B}} H(\mathcal{B}_t, |\psi\rangle).$$

Proof. We can rewrite Eq. (8) for the POVM given by $\{\alpha_i|\Phi_i\rangle\langle\Phi_i|\}$ to

$$\begin{aligned}\mathcal{I}_{\mathrm{acc}}(\mathcal{E}) &= \max_M \left(\log d + \sum_i \frac{\alpha_i}{dm} \sum_{k,t} |\langle \Phi_i|b_k^t\rangle|^2 \log |\langle \Phi_i|b_k^t\rangle|^2 \right) \\ &= \max_M \left(\log d - \sum_i \frac{\alpha_i}{d} \sum_t p_t H(\mathcal{B}_t, |\Phi_i\rangle) \right).\end{aligned}$$

For convenience, we split up the index i into $i = ab$ with $a = a_1, \ldots, a_N$ and $b = b_1, \ldots, b_N$, where $a_\ell, b_\ell \in \{0, \ldots, p-1\}$ in the following.

We first show that applying generalized Pauli matrices to the basis vectors of a MUB merely permutes those vectors.

Claim 1. Let $\mathcal{B}_t = \{|b_1^t\rangle, \ldots, |b_d^t\rangle\}$ be a basis based on generalized Pauli matrices (Sec. II) with $d = p^N$. Then $\forall\ a, b \in \{0, \ldots, p-1\}^N$, $\forall\ k \in [d]$ we have that $\exists\ k' \in [d]$, such that $|b_{k'}^t\rangle = X_d^{a_1} Z_d^{b_1} \otimes \ldots \otimes X_d^{a_N} Z_d^{b_N} |b_k^t\rangle$.

Proof. Let Σ_p^i for $i \in \{0,1,2,3\}$ denote the generalized Pauli matrices $\Sigma_p^0 = \mathbb{I}_p$, $\Sigma_p^1 = X_p$, $\Sigma_p^3 = Z_p$, and $\Sigma_p^2 = X_p Z_p$. Note that $X_p^u Z_p^v = \omega^{uv} Z_p^v X_p^u$, where $\omega = e^{2\pi i/p}$. Furthermore, define

$\Sigma_p^{i,(x)} = \mathbb{I}^{\otimes(x-1)} \otimes \Sigma_p^i \otimes \mathbb{I}^{N-x}$ to be the Pauli operator Σ_p^i applied to the xth qupit. Recall from Sec. II that the basis $\mathcal{B}_t$ is the unique simultaneous eigenbasis of the set of operators in C_t, i.e., for all $k \in [d]$ and $f, g \in [N]$, $|b_k^t\rangle \in \mathcal{B}_t$ and $c_{f,g}^t \in C_t$, we have $c_{f,g}^t |b_k^t\rangle = \lambda_{k,f,g}^t |b_k^t\rangle$ for some value $\lambda_{k,f,g}^t$. Note that any vector $|v\rangle$ that satisfies this equation is proportional to a vector in $\mathcal{B}_t$. To prove that any application of one of the generalized Pauli matrices merely permutes the vectors in $\mathcal{B}_t$ is therefore equivalent to proving that $\Sigma_p^{i,(x)} |b_k^t\rangle$ are eigenvectors of $c_{f,g}^t$ for any $f, g \in [k]$ and $i \in \{1,3\}$. This can be seen as follows: Note that $c_{f,g}^t = \otimes_{n=1}^N (\Sigma_p^{1,(n)})^{f_N} (\Sigma_p^{3,(n)})^{g_N}$ for $f = (f_1, \ldots, f_N)$ and $g = (g_1, \ldots, g_N)$ with $f_N, g_N \in \{0, \ldots, p-1\}$ [19]. A calculation then shows that

$$c_{f,g}^t \Sigma_p^{i,(x)} |b_k^t\rangle = \tau_{f_x, g_x, i} \lambda_{k,f,g}^t \Sigma_p^{i,(x)} |b_k^t\rangle,$$

where $\tau_{f_x,g_x,i} = \omega^{g_x}$ for $i=1$ and $\tau_{f_x,g_x,i} = \omega^{-f_x}$ for $i=3$. Thus $\Sigma_p^{i,(x)} |b_k^t\rangle$ is an eigenvector of $c_{f,g}^t$ for all t, f, g, and i, which proves our claim. ■

Suppose we are given $|\psi\rangle$ that minimizes $\Sigma_{\mathcal{B}_t \in \mathbb{T}} H(\mathcal{B}_t, |\psi\rangle)$. We can then construct a full POVM with d^2 elements by taking $\{(1/d) |\Phi_{ab}\rangle\langle\Phi_{ab}|\}$ with $|\Phi_{ab}\rangle = (X_d^{a^1} Z_d^{b^1} \otimes \ldots \otimes X_d^{a^N} Z_d^{b^N})^\dagger |\psi\rangle$. However, it follows from our claim above that $\forall\ a, b, k, \exists\ k'$ such that $|\langle\Phi_{ab}|b_k^t\rangle|^2 = |\langle\psi|b_{k'}^t\rangle|^2$, and thus $H(\mathcal{B}_t, |\psi\rangle) = H(\mathcal{B}, |\Phi_{ab}\rangle)$ from which the result follows. ■

Determining the strength of the locking effects for such MUBs is thus equivalent to proving bounds on entropic uncertainty relations. We thus obtain as a corollary of theorem 2 and lemma 4 that, for dimensions which are the square of a prime power $d = p^{2N}$, using any product MUBs based on generalized Pauli matrices does not give us any better locking than just using 2 MUBs.

Corollary 3. Let $\mathbb{S} = \{\mathcal{S}_1, \ldots, \mathcal{S}_m\}$ with $m \geq 2$ be any set of MUBs constructed on the basis of generalized Pauli matrices in a Hilbert space of prime (power) dimension $s = p^N$. Define U_t as the unitary that transforms the computational basis into the tth MUB, i.e., $\mathcal{S}_t = \{U_t|1\rangle, \ldots, U_t|s\rangle\}$. Let $\mathbb{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ be the set of product MUBs with $\mathcal{B}_t = \{U_t \otimes U_t^* |1\rangle, \ldots, U_t \otimes U_t^* |d\rangle\}$ in dimension $d = s^2$. Consider the ensemble $\mathcal{E} = \{1/(dm), |b_k^t\rangle\langle b_k^t|\}$. Then

$$I_{\mathrm{acc}}(\mathcal{E}) = \frac{\log d}{2}.$$

Proof. The claim follows from theorem 2 and the proof of lemma 4 by constructing a similar measurement formed from vectors $|\hat{\Phi}_{\hat{a}\hat{b}}\rangle = K_{a^1 b^1} \otimes K_{a^2 b^2}^* |\psi\rangle$ with $\hat{a} = a^1 a^2$ and $\hat{b} = b^1 b^2$, where a^1, a^2 and b^1, b^2 are defined like a and b in the proof of lemma 4 and $K_{ab} = (X_d^{a^1} Z_d^{b^1} \otimes \ldots \otimes X_d^{a^N} Z_d^{b^N})^\dagger$ from above. ■

The simple example we considered above is in fact a special case of corollary 3. It shows that if the vector that minimizes the sum of entropies has certain symmetries, such as for example the Bell states, the resulting POVM can even be much simpler.

C. MUBs from Latin squares

At first glance, one might think that maybe the product MUBs based on generalized Paulis are not well suited for locking just because of their product form. Perhaps MUBs with entangled basis vectors do not exhibit this problem. To this end, we examine how well MUBs based on Latin squares can lock classical information in a quantum state. All such MUBs are highly entangled, with the exception of the two extra MUBs based on non-Latin squares. Surprisingly, it turns out, however, that *any* set of at least two MUBs based on Latin squares does equally well at locking as using just two such MUBs. Thus such MUBs perform equally "badly," i.e., we cannot improve the strength of the locking effect by using more MUBs of this type.

Lemma 5. Let $\mathbb{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ with $m \geq 2$ be any set of MUBs in a Hilbert space of dimension $d = s^2$ constructed on the basis of Latin squares. Consider the ensemble $\mathcal{E} = \{1/(dm), |b_k^t\rangle\langle b_k^t|\}$. Then

$$\mathcal{I}_{\mathrm{acc}}(\mathcal{E}) = \frac{\log d}{2}.$$

Proof. Note that we can again rewrite $\mathcal{I}_{\mathrm{acc}}(\mathcal{E})$ as in the proof of lemma 4. Consider the simple measurement in the computational basis $\{|i,j\rangle\langle i,j| \, | \, i,j \in [s]\}$. The result then follows by the same argument as in lemma 1. ■

V. CONCLUSION AND OPEN QUESTIONS

We have shown tight bounds on entropic uncertainty relations and locking for specific sets of mutually unbiased bases. Surprisingly, it turns out that using a more mutually unbiased basis does not always lead to a better locking effect. It is interesting to consider what may make these bases so special. The example of three MUBs considered in lemma 3 may provide a clue. These three bases are given by the common eigenbases of $\{\sigma_x \otimes \sigma_x, \sigma_x \otimes \mathbb{I}, \mathbb{I} \otimes \sigma_x\}$, $\{\sigma_z \otimes \sigma_z, \sigma_z \otimes \mathbb{I}, \mathbb{I} \otimes \sigma_z\}$, and $\{\sigma_y \otimes \sigma_y, \sigma_y \otimes \mathbb{I}, \mathbb{I} \otimes \sigma_y\}$, respectively [19]. However, $\sigma_x \otimes \sigma_x$, $\sigma_z \otimes \sigma_z$, and $\sigma_y \otimes \sigma_y$ commute and thus also share a common eigenbasis, namely the Bell basis. This is exactly the basis we will use as our measurement. For all MUBs based on generalized Pauli matrices, the MUBs in prime power dimensions are given as the common eigenbasis of similar sets consisting of strings of Pauli matrices. It would be interesting to determine the strength of the locking effect on the basis of the commutation relations of elements of different sets. Perhaps it is possible to obtain good locking from a subset of such MUBs where none of the elements from different sets commute.

It is also worth noting that the numerics of [11] indicate that at least in dimension p using more than three bases does indeed lead to a stronger locking effect. It would be interesting to know whether the strength of the locking effect depends not only on the number of bases, but also on the dimension of the system in question.

Whereas general bounds still elude us, we have shown that merely choosing mutually unbiased bases is not sufficient to obtain good locking effects or high lower bounds for entropic uncertainty relations. We thus have to look for different properties.

ACKNOWLEDGMENTS

We would like to thank Harry Buhrman, Hartwig Bosse, Matthias Christandl, Richard Cleve, Debbie Leung, Serge Massar, David Poulin, and Ben Toner for discussions. We would especially like to thank Andris Ambainis and Andreas Winter for many helpful comments and interesting discussions. We would also like to thank Debbie Leung, John Smolin, and Barbara Terhal for providing us with explicit details on the numerical studies conducted in [11]. Thanks also to Matthias Christandl and Serge Massar for discussions on errors in string commitment protocols, to which end claim 1 was proved in the first place. Thanks also to Matthias Christandl and Ronald de Wolf for helpful comments on an earlier version of this paper. We are supported by an NWO vici grant 2004-2009 and by the EU project QAP (IST 015848).

[1] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[2] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[3] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, e-print quant-ph/0612014.
[4] H. Maassen and J. Uffink, Phys. Rev. Lett.we **60**, 1103 (1988).
[5] J. Sanchez-Ruiz, Phys. Lett. A **173**, 233 (1993).
[6] J. Sanchez-Ruiz, Phys. Lett. A **201**, 125 (1995).
[7] A. Azarchs, e-print quant-ph/0412083.
[8] P. Wocjan and T. Beth, Quantum Inf. Comput. **5**, 93 (2005).
[9] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[10] P. Hayden, D. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[11] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[12] M. Christandl and A. Winter, IEEE Trans. Inf. Theory **51**, 3159 (2005).
[13] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 200501 (2005).
[14] J. Smolin and J. Oppenheim, Phys. Rev. Lett. **96**, 081302 (2006).
[15] R. Koenig, R. Renner, A. Bariska, and U. Maurer, e-print quant-ph/0512021.
[16] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, e-print quant-ph/0504078.
[17] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Phys. Rev. Lett. **97**, 250501 (2006).
[18] B. Terhal, M. Horodecki, D. W. Leung, and D. P. DiVincenzo, J. Math. Phys. **43**, 4286 (2002).
[19] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[20] C. Cachin, in *Proceedings of EUROCRYPT'97*, Lecture Notes in Computer Science Vol. 1233 (Springer, Berlin, 1997), pp. 193–208.
[21] W. Wootters and B. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[22] G. Zauner, Ph.D. thesis, Universität Wien, 1999.
[23] A. Klappenecker and M. Rötteler, in *Finite Fields and Applications: 7th International Conference Fq7*, Lecture Notes in Computer Science Vol. 2948 (Springer, Berlin, 2004), pp. 137–144, e-print quant-ph/0309120.
[24] M. Grassl, in Proceedings ERATO Conference on Quantum Information Science, Tokyo, 2004, pp. 60–61, e-print quant-ph/0406175, .
[25] J. Lawrence, C. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).
[26] J. Renes, R. Blume-Kohout, A. Scott, and C. Caves, J. Math. Phys. **45**, 2171 (2004).
[27] A. Klappenecker and M. Rötteler, in Proceedings of the International Symposium on Information Theory, e-print quant-ph/0502031, pp. 1740–1744.
[28] E. B. Davies, IEEE Trans. Inf. Theory **24**, 596 (1978).
[29] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Academic Publishers, Dordrecht, 1993).
[30] M. Ballester, S. Wehner, and A. Winter, e-print quant-ph/0608014.