

## Mutually unbiased unitary bases

Jesni Shamsul Shaari,<sup>1</sup> Rinie N. M. Nasir,<sup>1</sup> and Stefano Mancini<sup>2,3</sup>

<sup>1</sup>*Faculty of Science, International Islamic University Malaysia (IIUM), Jalan Sultan Ahmad Shah, Bandar Indera Mahkota, 25200 Kuantan, Pahang, Malaysia*

<sup>2</sup>*School of Science & Technology, University of Camerino, I-62032 Camerino, Italy*

<sup>3</sup>*INFN Sezione di Perugia, I-06123 Perugia, Italy*

(Received 26 March 2016; published 21 November 2016)

We consider the notion of unitary transformations forming bases for subspaces of  $M(d, \mathbb{C})$  such that the square of the Hilbert-Schmidt inner product of matrices from the differing bases is a constant. Moving from the qubit case, we construct the maximal number of such bases for the four- and two-dimensional subspaces while proving the nonexistence of such a construction for the three-dimensional case. Extending this to higher dimensions, we commit to such a construct for the case of qutrits and provide evidence for the existence of such unitaries for prime dimensional quantum systems. Focusing on the qubit case, we show that the average fidelity for estimating any such transformation is equal to the case for estimating a completely unknown unitary from  $SU(2)$ . This is then followed by a quick application for such unitaries in a quantum cryptographic setup.

DOI: [10.1103/PhysRevA.94.052328](https://doi.org/10.1103/PhysRevA.94.052328)

### I. INTRODUCTION

The idea of indistinguishability of quantum states and the inability to clone an arbitrary state has brought with it the acceptance of physical limits on how much one can know of a quantum system. In the context of mutually unbiased bases (MUBs) (for a review on the subject of MUBs, see, e.g., Ref. [1]), considering an unknown quantum state selected from sets of MUBs, a measurement of an observable described by projectors onto states in a basis mutually unbiased with respect to the prepared one produces completely random results. This came to be the key ingredient in the well-known BB84 quantum key distribution (QKD) protocol [2] as well as in most (if not all) prepare and measure QKD schemes where eavesdropping of a transmitted message would statistically induce errors for which, below a certain threshold, legitimate parties may distill a secret key nonetheless.

While the optimal estimation of a quantum state deals with the maximal information extraction of the system's state, the issue of estimating an unknown physical transformation, described by a unitary operator, of a state is another matter. This was studied in Ref. [3] and it is a more challenging task compared to state estimation because it requires not only the use of optimal measurements of the resulting state post transformation but also an optimal state prior to the transformation to begin with. An immediate use of such estimation, namely the alignment of reference frames using quantum spins, was noted in Ref. [4] as being equivalent to estimating unknown rotations of  $SU(2)$ .

This paradigm has also found its way into the field of quantum cryptography where protocols making use of a bidirectional quantum channel and unitary transformations for encoding purposes like those of Refs. [5–7] rely on the inability of an eavesdropper (commonly referred to as Eve) to ascertain the transformations perfectly without inducing errors. However, this inhibition for Eve does not reflect an intrinsic inability with regard to the transformations themselves, rather it is chiefly due to the inability of estimating the encoded states traveling between the legitimate parties (commonly referred to as Alice and Bob). It was in Ref. [8]

that the notion of two-way QKD based on indistinguishable unitaries was first mooted where Alice's transformation for encoding purposes was selected from two orthogonal bases of unitary transformations: one comprising the identity and Pauli matrices, and the other being those unitaries multiplied by a rotation by the angle  $2\pi/3$  about the axis  $(1, 1, 1)/\sqrt{3}$  of  $\mathbb{R}^3$ . In Ref. [9], these bases were referred to as mutually unbiased bases of orthogonal qubit unitaries. A two-way QKD study with nonentangled qubits using “nonorthogonal” unitaries was later reported in Ref. [10], providing for a higher security threshold compared to its conventional predecessors for selected attack strategies.

Such a notion of “nonorthogonal” unitaries is intimately linked to unitary 2-designs [11,12] which are a set of matrices such that the average over them reproduces the average over the entire unitary group. The notion of “mutually unbiased unitary-operator bases” (MUUBs) was put forward in Ref. [11] for unitary operators acting on a  $d$ -dimensional Hilbert space as the set of  $d^2 - 1$  unitary operator bases with the property that each pair is *mutually unbiased*. That is, two sets of operator bases (each of cardinality  $d^2$ ), say  $\mathcal{T}_0$  and  $\mathcal{T}_1$ , are mutually unbiased if

$$|\mathrm{Tr}(T_0^{(i)\dagger} T_1^{(j)})|^2 = 1, \quad \forall T_0^{(i)} \in \mathcal{T}_0, T_1^{(j)} \in \mathcal{T}_1, \quad (1)$$

where  $i, j = 1, \dots, d^2$  and  $\mathrm{Tr}(A^\dagger B)$  is the Hilbert-Schmidt inner product of  $A$  and  $B$ . It was used in the construction of a unitary 2-design, a study done in the context of process tomography of unital quantum channels. Reference [11] also showed that for  $d = 2, 3, 5, 7$ , and  $11$ , a complete set, i.e.,  $d^2 - 1$  MUUB, can be found. The idea of such unbiasedness for a unitary basis is arguably deeper than afforded by the definition of 2-designs, and in our work here, we treat the notion of such unbiased unitary bases in its own right.

Motivated by the equiprobable transition between states in one basis to another in the case of MUBs, we consider an analogous idea of equiprobable guesses of unitaries towards a generalized notion of unbiased unitary operator bases (though we retain the abbreviation, MUUB) and provide a systematic study of their properties. The generalization here is made in

the sense of neither restricting the value of the Hilbert-Schmidt norm of Eq. (1) to unity nor the cardinality of the operator basis. We proceed in Sec. II with the characterization on the maximal number of MUUBs on a two-dimensional Hilbert space,  $\mathcal{H}_2$ , namely, a qubit. We then show how this is immediately connected to maximally entangled states forming MUUBs (Sec. III), explicitly so for the relevant subspaces of the Hilbert space  $\mathcal{H}_2 \otimes \mathcal{H}_2$ . We then provide in the subsequent section an explicit construction for the case of MUUBs on a three-dimensional Hilbert space and follow up with a simple proof of the existence of MUUBs on prime numbered dimensional quantum systems. Focusing on the MUUBs for  $\mathcal{H}_2$ , we calculate the fidelities in distinguishing between the unitaries. We show how this is equal to the discrimination of the maximally entangled states from the varying MUBs as well as the estimation of a completely unknown unitary from  $SU(2)$  (Sec. IV). Before concluding, we discuss the use of MUUBs in a QKD setup.

## II. MUUB FOR QUBITS

MUB refers to orthonormal bases of a Hilbert space such that the transition from any one state in one basis to any state in the other basis is equiprobable [1]. In other words, if one is asked to guess an unknown state,  $|u\rangle$ , prepared in one basis of say a  $d$ -dimensional Hilbert space,  $\mathcal{H}_d$ , and we let the states  $|r\rangle$  and  $|s\rangle$  be “guesses” (resulting from a measurement) from a mutually unbiased basis, then

$$|\langle u|r\rangle|^2 = |\langle u|s\rangle|^2 = 1/d. \quad (2)$$

In estimating an unknown unitary,  $U \in SU(d)$ , with a guess,  $U_r$ , Ref. [3] considers how closely  $U_r$  resembles  $U$  by determining the behavior of the unitaries, averaged over all states  $|\alpha\rangle \in \mathcal{H}_d$  given by

$$\left| \int \langle \alpha | U_r^\dagger U | \alpha \rangle d\alpha \right|^2 = \frac{1}{d^2} |\text{Tr}(U U_r^\dagger)|^2. \quad (3)$$

Thus, beginning with a unitary,  $U$ , and letting  $U_r$  and  $U_s$  be guesses for  $U$ , we could say that the guesses are equiprobable if  $|\text{Tr}(U U_r^\dagger)|^2 = |\text{Tr}(U U_s^\dagger)|^2$ .

*Definition 1.* Consider two distinct orthogonal bases,  $\mathcal{A}_0$  and  $\mathcal{A}_1$ , composed of unitary transformations for some subspace of the vector space  $M(d, \mathbb{C})$ .  $\mathcal{A}_0$  and  $\mathcal{A}_1$  are sets of MUUBs provided

$$|\text{Tr}(A_0^{(i)\dagger} A_1^{(j)})|^2 = C, \quad \forall A_0^{(i)} \in \mathcal{A}_0, A_1^{(j)} \in \mathcal{A}_1, \quad (4)$$

for  $i, j, = 1, \dots, n$  and some constant  $C \neq 0$ .

With the number  $n$  as the cardinality of the basis sets which reflect the dimensionality of the subspace, in the following subsections, we limit ourselves to unitaries acting on states in  $\mathcal{H}_2$ , i.e.,  $d = 2$ , and provide explicit constructions of MUUBs for  $n = 4$  and 2. Furthermore we note that no MUUBs exist for  $n = 3$ . This is simply due to the fact that any subspace spanned by three orthogonal  $2 \times 2$  matrices necessitates the uniqueness of such a basis.

We should like to note that, differently from Ref. [11], the definition given above is motivated by the idea of equiprobable guesses of a unitary and is more general in the sense that the definition in Ref. [11] requires the Hilbert-Schmidt inner

product of the matrices to equal 1, restricted to the subspace of dimension  $d^2$ ; ours is a constant  $C$  without specifying the dimensionality of the subspace. We see later, at least through the explicit construction of MUUBs acting on  $\mathcal{H}_2$ , how our definition reduces to that in Ref. [11] in the case of  $n = 4$  while the value of  $C$  is different in the case of  $n = 2$ . We further note that our constructions for MUUBs are straightforwardly derived from our definition and could possibly provide for simpler insights to higher dimensions.

### A. MUUBs for $n = 4$

We first need to ensure that our construction here will provide for a result which holds in general. To this end, we define the equivalence between bases for possibly distinct subspaces.

*Definition 2.* Consider two distinct orthogonal bases,  $\mathcal{X} = \{X_1, X_2, \dots, X_n\}$  and  $\mathcal{Y} = \{Y_1, Y_2, \dots, Y_n\}$ , for some  $n$  spanning possibly distinct subspaces  $M(\mathcal{X})$  and  $M(\mathcal{Y})$ , respectively.  $\mathcal{X}$  is equivalent to  $\mathcal{Y}$ ,  $\mathcal{X} \equiv \mathcal{Y}$ , provided that  $\zeta_j Y_j = U X_j, \forall j = 1, 2, \dots, n$ , for some unitary  $U$  and  $|\zeta_j| = 1$ .

*Proposition 1.* Given the above definition for  $\mathcal{X} \equiv \mathcal{Y}$  for some  $n$ ,  $\mathcal{X}$  is unbiased with regards to a set  $\mathcal{Z} = \{Z_1, Z_2, \dots, Z_n\} \subset M(\mathcal{X})$  if and only if  $\mathcal{Y}$  is unbiased with regards to a set  $U\mathcal{Z} = \{U Z_1, U Z_2, \dots, U Z_n\} \subset M(\mathcal{Y})$ .

The above proposition is easily shown to be true by  $|\text{Tr}(X_j^\dagger Z_k)|^2 = |\text{Tr}[(U X_j)^\dagger U Z_k]|^2 = |\text{Tr}[(\zeta_j Y_j)^\dagger U Z_k]|^2 = |\text{Tr}[(Y_j)^\dagger U Z_k]|^2$ .

The case for  $n = 4$  here has  $M(\mathcal{X}) = M(\mathcal{Y})$  and is trivially the case of a changing basis in  $M(2, \mathbb{C})$ . Thus, one could begin with a basis containing arbitrary but pairwise orthogonal unitaries for  $M(2, \mathbb{C})$  and do a basis change by multiplying each element of the basis with some unitary operator (and ignoring possible overall phase factors) resulting in the basis  $\mathcal{B}_0 = \{\mathbb{I}_2, \sigma_1, \sigma_2, \sigma_3\}$ , where  $\mathbb{I}_2$  is the identity operator and  $\sigma_1, \sigma_2$ , and  $\sigma_3$  are the Pauli matrices given by

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5)$$

We can therefore consider the basis  $\mathcal{B}_0$  with no loss of generality. We next define a unitary element,  $U$ , as a linear combination of elements of  $\mathcal{B}_0$ ,

$$U = p_0 \mathbb{I}_2 + \sum_i^3 p_i \sigma_i. \quad (6)$$

Along with  $|\text{Tr}(\sigma_j U)|^2 = 4|p_j|, \forall j$ , and  $U^\dagger U = \mathbb{I}_2$ , we have  $|p_j|^2 = 1/4$ . On the other hand, a generic  $2 \times 2$  unitary matrix,  $U$ , may be written as

$$U = e^{i\alpha} \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \quad (7)$$

with  $|a|^2 + |b|^2 = 1$ . By comparing Eqs. (6) and (7) with regard to element  $e^{i\alpha} a$  and  $e^{i\alpha} a^*$ , we can write

$$e^{i\alpha} a = p_0 + p_3 \Rightarrow e^{i\alpha} a^* = e^{2i\alpha} (p_0^* + p_3^*), \quad (8)$$

$$e^{i\alpha} a^* = p_0 - p_3 \Rightarrow e^{i\alpha} a = e^{2i\alpha} (p_0^* - p_3^*). \quad (9)$$

The above equations give us

$$p_0^2 = -p_3^2 = e^{2i\alpha}/4. \quad (10)$$

Similar treatment for elements  $e^{i\alpha}b$  and  $-e^{i\alpha}b^*$  would result in

$$p_1^2 = p_2^2 = -e^{2i\alpha}/4. \quad (11)$$

There can only be two solutions for each  $p_i$  in the above equations. Representing the solutions for  $p_i$  to the above equations as a four-vector,  $(p_0, p_1, p_2, p_3)$ , one can have at most 16 sets of solutions for a given  $\alpha$ . As

$$|\text{Tr}[U_a^\dagger(e^{i\beta}U_b)]|^2 = |\text{Tr}[U_a^\dagger(U_b)]|^2, \quad (12)$$

we say  $e^{i\beta}U_b$  is equivalent to  $U_b$ ;  $e^{i\beta}$  acts like a ‘‘global phase factor’’ and is inconsequential in the context of MUUBs. Hence, the set  $(p_0, p_1, p_2, p_3)$  and  $(-p_0, -p_1, -p_2, -p_3)$  (the case where  $\beta = \pi$ ) would provide for equivalent matrices, then the number of nonequivalent solutions would be at most 8 for a given  $\alpha$ . As the factor  $\alpha$  itself has no effect on the equivalence of matrices, we conclude that there can be at most 8 matrices which are mutually unbiased with regards to all elements in  $\mathcal{B}_0$ . The 8 sets of solutions allow us to explicitly construct the vectors for bases  $\mathcal{B}_1$  and  $\mathcal{B}_2$  as

$$\mathcal{B}_k = \left\{ \frac{\mathbb{I}_2 + i \sum_{j=1}^3 d_j \sigma_j}{2} \mid d_j \in \{\pm 1\}, \prod_{j=1}^3 d_j = (-1)^k \right\} \quad (13)$$

for  $k = 1$  and  $2$ . It can easily be shown that both  $\mathcal{B}_1$  and  $\mathcal{B}_2$  span  $M(2, \mathbb{C})$  and

$$|\text{Tr}(U_a^\dagger U_b)|^2 = 1, \quad \forall U_a \in \mathcal{B}_1, U_b \in \mathcal{B}_2. \quad (14)$$

Thus the number of MUUBs for  $n = 4$  is three (including  $\mathcal{B}_0$ ). This maximal number is known to be achieved from Ref. [11].

### B. MUUBs for $n = 3$

As mentioned earlier, no MUUBs can exist in the case of  $n = 3$ . The proof is rather straightforward.

Beginning with an arbitrary basis  $\mathcal{V} = \{V_1, V_2, V_3\} \subset M(2, \mathbb{C})$  for a three-dimensional subspace of  $M(2, \mathbb{C})$ , it can always be mapped to  $\mathcal{S} = \{\mathbb{I}_2, \sigma_i, \sigma_j\}$ , for  $i \neq j$  where  $V_1^\dagger V_1 = \mathbb{I}_2$  and  $V_1^\dagger V_2 = \sigma_i$ . If we require  $\mathcal{V}$  to be unbiased with respect to  $\mathcal{S}$ ,  $V_1$  must be an element of the span of  $\mathcal{S}$  and  $V_1 = q_0 \mathbb{I}_2 + q_i \sigma_i + q_j \sigma_j$ , with  $|q_0|^2 = |q_1|^2 = |q_2|^2 = 1/3$ . Thus  $V_2 = V_1 \sigma_i = q_0 \sigma_i + q_i \mathbb{I}_2 + q_j \sigma_i \sigma_j$ . However,  $\sigma_i \sigma_j$  is not in the span of  $\mathcal{S}$ , hence  $\mathcal{V}$  cannot be an MUUB with respect to  $\mathcal{S}$  and we conclude no MUUBs exist for  $n = 3$ .

### C. MUUBs for $n = 2$

While all orthogonal (possibly distinct) bases of  $M(2, \mathbb{C})$  span the same space,  $M(2, \mathbb{C})$ , the case for  $n = 2$  suggests the possibility of considering a number of possible orthogonal bases of which each basis could very well span a distinct subspace. Hence, constructing MUUBs for one subspace naturally causes one to question whether the same number of MUUBs could be constructed in another subspace.

Referring to Definition 2 and Proposition 1, we are however assured that, if we consider an arbitrary orthogonal basis

defined by  $\{A, B\}$  for a two-dimensional subspace of  $M(2, \mathbb{C})$ , it is equivalent to the basis  $\mathcal{W}_0 = \{\mathbb{I}_2, \omega\}$ , where  $\omega = A^\dagger B$  and spans a subspace, say,  $M_1$ , which would have the same number of MUUBs for the subspace spanned by  $\{A, B\}$ . We then let  $\omega$  be represented by a generic matrix like Eq. (7) with the factor  $\alpha$  as  $\gamma$ .

Let  $W_0 = r_0 \mathbb{I}_2 + r_1 \omega \in M_1$  be a unitary matrix. With  $|\text{Tr}(\mathbb{I}_2 W_0)|^2 = |\text{Tr}(\omega W_0)|^2 = 4|r_j|^2, \forall j$  and  $W_0^\dagger W_0 = \mathbb{I}_2$ , we have  $|r_j|^2 = 1/2$ . Working with the same approach as we did for  $n = 4$ , where we compare  $W_0$  with a generic  $2 \times 2$  unitary matrix (say with a factor  $\alpha = \beta$ ), we have

$$r_0^2 = e^{2i\gamma}/2, \quad r_1^2 = e^{2i(\beta-\gamma)}/2. \quad (15)$$

The above admits only four sets of solutions for  $(r_0, r_1)$  and given that  $(r_0, r_1)$  and  $(-r_0, -r_1)$  provide for equivalent matrices, the number of MUUBs for  $n = 2$  is two. Explicit examples in terms of Pauli matrices are include  $\{\mathbb{I}_2, \sigma_2\}$  which is unbiased with respect to  $\{(\mathbb{I}_2 \pm i\sigma_2)/\sqrt{2}\}$  and  $\{\mathbb{I}_2, \sigma_3\}$  which is unbiased with respect to  $\{(\mathbb{I}_2 \pm i\sigma_3)/\sqrt{2}\}$ .

## III. MUUBs AND MUBs OF MAXIMALLY ENTANGLED STATES

The study of unitary transformations, more generally quantum channels, is well known to be closely connected to that of maximally entangled states through the isomorphism between unitaries,  $U$  on a  $d$ -dimensional Hilbert space,  $\mathcal{H}_d$ , and vectors,  $|U\rangle\rangle$  (using the notation from Refs. [13,14]) in  $\mathcal{H}_d \otimes \mathcal{H}_d$ ,

$$U \equiv \sum_i \sum_j \langle j|U|i\rangle |i\rangle |j\rangle = |U\rangle\rangle \in \mathcal{H}_d \otimes \mathcal{H}_d \quad (16)$$

for some basis vectors  $|i\rangle$  and  $|j\rangle$  of  $\mathcal{H}_d$ . With  $|\langle\langle U_a|U_b\rangle\rangle|^2 = |\text{Tr}(U_a^\dagger U_b)|^2$  and  $|U\rangle\rangle/\sqrt{d}$  giving a maximally entangled state [15], the search for MUUBs is tantamount to looking for sets of maximally entangled states which not only form a basis for  $\mathcal{H}_d \otimes \mathcal{H}_d$  but are also mutually unbiased to one another. Thus, referring to the previous sections, the dimensionality of  $\mathcal{H}_2 \otimes \mathcal{H}_2$  is 4; i.e., states are mutually unbiased if the absolute value of their inner product is given by  $1/2$ . Hence, with  $|\mathbb{I}_2\rangle\rangle/\sqrt{2} = |\Phi^+\rangle, |\sigma_1\rangle\rangle/\sqrt{2} = |\Psi^+\rangle, |\sigma_2\rangle\rangle/\sqrt{2} = |\Psi^-\rangle, \text{ and } |\sigma_3\rangle\rangle/\sqrt{2} = |\Phi^-\rangle$ , the maximal number of such MUBs is three and they are

$$\mathfrak{B}_0 = \{|\Phi^+\rangle, |\Psi^+\rangle, |\Psi^-\rangle, |\Phi^-\rangle\},$$

$$\mathfrak{B}_k = \left\{ \frac{|E_0\rangle + \sum_{j=1}^3 c_j |E_j\rangle}{2} \mid c_j \in \{\pm 1\}, \prod_{j=1}^3 c_j = (-1)^k \right\}, \quad (17)$$

for  $k = 1$  and  $2$  with  $|E_0\rangle = |\Phi^+\rangle, |E_1\rangle = i|\Psi^+\rangle, |E_2\rangle = |\Psi^-\rangle, \text{ and } |E_3\rangle = i|\Phi^-\rangle$  (also known as a ‘‘magic basis’’ [16]). It is worth noting that the requirement for entangled states as a basis would not allow for the construction of the maximal number of MUBs for a four-dimensional system (which would be five). It was noted in Ref. [17] that, in constructing MUBs for two-qubit states, if one begins by constructing three Bell-type bases which are mutually unbiased, then one cannot construct two additional basis sets.

This connection can be extended to the case of MUUBs for  $n = 2$  as the dimension of the subspace is two where mutually unbiased states have the absolute value of their inner product as  $1/\sqrt{2}$ . The absolute value of the inner product between maximally entangled states, say  $|U_a\rangle/\sqrt{2}$  and  $|U_b\rangle/\sqrt{2}$ , derived from differing MUUBs in this case would result in  $|\langle U_b|U_a\rangle|/2 = |\text{Tr}(U_b^\dagger U_a)|/2 = 1/\sqrt{2}$ .

#### IV. MUUBs FOR PRIME NUMBERED DIMENSIONAL QUANTUM SYSTEMS

It is natural to consider the construction of MUUBs on higher-dimensional systems,  $\mathcal{H}_d$ , and much is hinted at from the qubit scenario. We begin with the issue of subspaces of  $M(d, \mathbb{C})$  which may admit MUUBs (or rather those that do not). To this end, we provide the following theorem.

*Theorem 1.* Consider a subspace of  $M(d, \mathbb{C})$  and let its dimensionality be  $n$ . If  $n$  is neither  $d$  nor  $d^2$ , then no MUUB can exist for such a subspace.

The proof for this follows from that of Sec. II B by having one basis consisting of the identity and some Pauli matrices and then demanding another which is a MUUB to it to contain elements which are in the span of the former. Let a basis  $\mathcal{D}$  be defined (unitary operator basis [18]) by

$$\{X^{a_i} Z^{b_j} | i \in [0, m], j \in [0, n]\} \quad (18)$$

for  $m, n, a_i, b_j \in \mathbb{Z}_d$  and with  $X$  and  $Z$  as the generalized Pauli operators for the  $d$ -dimensional system given in Ref. [19]. We fix  $a_0 = b_0 = 0$  so that  $\mathcal{D}$  includes  $\mathbb{I}_d$ . We can represent this set by the set of pairs,

$$C_{\mathcal{D}} = \{(i, j) | i \in [0, m], j \in [0, n]\}. \quad (19)$$

Consider an element  $E_1$  from another basis  $\mathcal{E}$  such that

$$E_1 = \sum_i^m \sum_j^n q_{ij} X^{a_i} Z^{b_j} \in \text{span}(\mathcal{D}) \quad (20)$$

for  $q_{ij} \in \mathbb{C}$ . Another element, say,  $E_2 \in \mathcal{E}$ , can then be written as

$$\begin{aligned} E_2 &= \left( \sum_i^m \sum_j^n q_{ij} X^{a_i} Z^{b_j} \right) X^{a_k} Z^{b_l} \\ &= \sum_i^m \sum_j^n q_{ij} \eta_d X^{a_i+a_k} Z^{b_j+b_l} \end{aligned} \quad (21)$$

for some element  $X^{a_k} Z^{b_l} \in \mathcal{D}$  and  $\eta_d = \exp(2\pi i/d)$ . Requiring  $\mathcal{E}$  be the MUUB to  $\mathcal{D}$ , we require  $E_2 \in \text{span}(\mathcal{D})$  implying  $X^{a_i+a_k} Z^{b_j+b_l} \in \mathcal{D}$  or  $(i+k, j+l) \in C_{\mathcal{D}}$  for all  $i, k \in [0, m]$  and  $j, l \in [0, n]$ . It is obvious to note that  $E_2 \in \text{span}(\mathcal{D})$  only if  $C_{\mathcal{D}}$  is closed under addition mod  $d$  which gives  $|\mathcal{D}| = d$  or  $d^2$ .

While this tells us about the nonexistence of MUUBs in certain subspaces, it does not promise the existence of MUUBs for the remaining subspaces. To this extent, we only verify the existence of MUUBs operating on  $\mathcal{H}_d$  for the  $d^2$ -dimensional subspace with  $d$  being a prime number by noting the existence of MUB for maximally entangled states in  $\mathcal{H}_d \otimes \mathcal{H}_d$ . Given the recipe for constructing MUBs for maximally entangled states in Ref. [20], we write a basis of maximally entangled

states for  $\mathcal{H}_d \otimes \mathcal{H}_d$  as  $\{|U_d^{0,0}\rangle, \dots, |U_d^{d-1,d-1}\rangle\}$ , with  $|U_d^{n,m}\rangle$  given by

$$|U_d^{n,m}\rangle = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} \eta_d^{np} |(p+m) \bmod d\rangle |p'\rangle \quad (22)$$

for  $n, m = 0, 1, \dots, d-1$ , and  $|(p+m) \bmod d\rangle$  and  $|p'\rangle$  refer to states, each being elements of the orthonormal bases of their respective Hilbert spaces. A basis mutually unbiased with respect to the above could be one with elements given by  $\mathbb{I}_d \otimes U_p |U_d^{n,m}\rangle$  with  $U_p |p'\rangle \rightarrow |p''\rangle$ , where  $|\langle p'|p''\rangle| = 1/\sqrt{d}$  (hence  $|\langle U_d^{n,m} | U_p |U_d^{n,m}\rangle| = 1/d$ ). As there would be only  $d+1$  MUBs for a  $d$ -dimensional system, we can conclude that this recipe provides for  $d+1$  MUBs for the maximally entangled states from  $\mathcal{H}_d \otimes \mathcal{H}_d$ , thus implying the same number for MUUBs acting on  $\mathcal{H}_d$  for the  $d^2$ -dimensional subspace. This obviously provides for the minimal number of such MUUBs. It was noted in Ref. [11] that the maximal number that such a MUUB can possibly have is  $d^2 - 1$ , though it remains unclear if this is saturated for all prime  $d$ . Given all these factors, we have the following proposition.

*Proposition 2.* The maximal and minimal numbers of MUUBs for a subspace of  $M(d, \mathbb{C})$  with dimensionality  $d^2$  are  $d^2 - 1$  and  $d + 1$ , respectively, for a prime number  $d$ .

In the specific case of  $d = 2$  ( $n = 4$ ), the minimal number of MUUBs is in fact also the maximal, i.e., three.

Constructing a maximal set of MUUB for any  $d$  dimensional is obviously a challenge, and following the construction for the qubit case, we consider the following. If a basis is given by Eq. (18) with  $m = n = d - 1$ , and a unitary  $U$  is taken from a MUUB containing  $X^{a_i} Z^{b_j}$ , then, with  $U^\dagger U = \mathbb{I}_d$  and  $|\text{Tr}(U^\dagger X^{a_i} Z^{b_j})|^2 = |\text{Tr}(U^\dagger X^{a_k} Z^{b_l})|^2, \forall i, j, k, l \in \mathbb{Z}_d$ , we have

$$U = \sum q_{ij} X^{a_i} Z^{b_j} \Rightarrow |q_{ij}| = 1/d^2, \quad (23)$$

and because  $|\text{Tr}(U^\dagger X^{a_i} Z^{b_j})|^2 = |q_{ij} \text{Tr}(\mathbb{I}_d)|^2$ , we see that this reduces to the definition given for such unitaries in Ref. [11]. It is now not difficult to consider a numerical search where one selects  $q_{ij} = \exp(2\pi i/d)^{t_{ij}}$  for some  $t_{ij} \in \mathbb{Z}_d$  and searches through all possible values for the possibilities of unitaries that fulfill the relevant criterion. Carrying this out for the case of  $M(3, \mathbb{C})$ , for example, we begin with a set of unitary matrices that span  $M(3, \mathbb{C})$ , constructed from a set of unitary operator bases [18] containing the identity  $\mathbb{I}_3$  and the generalized Pauli matrices for qutrits,

$$\mathcal{B}_{30} = \{X_3^j Z_3^k | j, k = 0, 1, 2\}, \quad (24)$$

with  $X_3$  and  $Z_3$  being the generalized Pauli operators for qutrits (explicitly given in Ref. [19]). We then find the following MUUBs,

$$\mathcal{B}_{3l} = \{R_l X^j Z^k | j, k = 0, 1, 2\}, \quad (25)$$

for  $l = 1, \dots, 7$  with

$$\begin{aligned} R_1 &= \mathbb{I} + \eta_3 X + \eta_3^2 X^2 + \eta_3 Z + \eta_3^2 Z^2 \\ &\quad + \eta_3 XZ + \eta_3^2 (XZ)^2 + \eta_3 XZ^2 + \eta_3^2 (XZ^2)^2 \\ R_2 &= \mathbb{I} + X + \eta_3 X^2 + Z + \eta_3 Z^2 \\ &\quad + \eta_3^2 XZ + (XZ)^2 + \eta_3^2 XZ^2 + (XZ^2)^2 \end{aligned}$$

$$\begin{aligned}
 R_3 &= \mathbb{I} + X + \eta_3 X^2 + Z + \eta_3^2 Z^2 \\
 &\quad + XZ + \eta_3^2 (XZ)^2 + \eta_3^2 XZ^2 + \eta_3^2 (XZ^2)^2 \\
 R_4 &= \mathbb{I} + X + \eta_3 X^2 + Z + \eta_3^2 Z^2 \\
 &\quad + \eta_3 XZ + (XZ)^2 + \eta_3 XZ^2 + \eta_3 (XZ^2)^2 \\
 R_5 &= \mathbb{I} + X + \eta_3^2 X^2 + Z + \eta_3 Z^2 \\
 &\quad + XZ + \eta_3^2 (XZ)^2 + \eta_3 XZ^2 + (XZ^2)^2 \\
 R_6 &= \mathbb{I} + X + \eta_3^2 X^2 + Z + \eta_3 Z^2 \\
 &\quad + \eta_3 XZ + (XZ)^2 + XZ^2 + \eta_3^2 (XZ^2)^2 \\
 R_7 &= \mathbb{I} + X + \eta_3^2 X^2 + Z + \eta_3^2 Z^2 \\
 &\quad + \eta_3^2 XZ + \eta_3^2 (XZ)^2 + XZ^2 + \eta_3 (XZ^2)^2. \quad (26)
 \end{aligned}$$

This saturates the maximal number of eight that has been showed to be achieved in Ref. [11]. As for the subspace of dimension 3, we are able to construct three MUUBs. Beginning with say  $\mathcal{D}_0 = \{\mathbb{I}_3, A, A^2\}$ , where  $A \in \mathcal{B}_{30} - \{\mathbb{I}_3\}$ , we can construct two sets of MUUBs,  $\mathcal{D}_1$  and  $\mathcal{D}_2$  given by

$$\mathcal{D}_j = \{D, DA, DA^2\}, \quad (27)$$

where  $D = \mathbb{I}_3 + \eta_3^j A + \eta_3^j A^2$  for  $j = 1$  and  $2$ .

## V. APPLICATIONS

Analogous to MUBs which set constraints on state distinguishability, we consider in this section the issue of distinguishability of unitaries selected from a set of MUUBs on  $\mathcal{H}_2$  and then proceed to consider its use in a QKD setup.

### A. Distinguishability of unitaries

In distinguishing between unitaries selected randomly from the set  $SU(d)$ , Refs. [3,21,22] consider a black box executing the unitary transformation, where one may submit a particular quantum state (which may comprise a qubit entangled with an ancillary system), through the black box and the resulting state may be measured to provide information of the transformation. Given a single use of the box, the task requires not only an optimal input but also an optimal measurement of the output state. If one considers the set  $\{U_g\}$  as a (projective) irreducible representation of a group  $G$ , a pure maximally entangled state,  $|\Gamma\rangle$ , may be used as an optimal input [15] and the issue of discriminating between unitaries  $U_g$  reduces to one of discriminating states in the group orbit [21]

$$\{|\Gamma_g\rangle\langle\Gamma_g| = (U_g \otimes \mathbb{I}_R)|\Gamma\rangle\langle\Gamma|(U_g \otimes \mathbb{I}_R)^\dagger |g \in G\}. \quad (28)$$

It is necessary though to subscribe to the minimal discriminating requirement of Ref. [21] where  $U_g = \lambda U_k \Rightarrow g = k$  for  $\lambda \in \mathbb{C}, g, k \in G$ .

In considering the discrimination between elements of MUUBs, we apply the same method above, though we restrict our study to the case of  $n = 4$ . More precisely, let us consider the scenario of selecting a unitary transformation randomly from the set of unitaries  $\cup_{i=0}^2 \mathcal{B}_i$  and let us choose for the input state  $|\Psi\rangle = \sum_{i=0}^1 |i, i\rangle / \sqrt{2} \in \mathcal{H}_2 \otimes \mathcal{H}_2$ .<sup>1</sup> It is easy to check

that

$$\forall |\psi\rangle \in \mathfrak{B}_i, \forall U \in \mathcal{B}_j, U \otimes I |\psi\rangle \in \mathfrak{B}_{(i+j) \bmod 2} \quad (29)$$

and the problem of discriminating between unitaries selected from the set  $\cup_{i=0}^2 \mathcal{B}_i$  reduces to an optimal discrimination of maximally entangled states forming mutually unbiased bases; i.e., the group orbit here is  $\{|\Gamma_g\rangle\langle\Gamma_g| | |\Gamma_g\rangle \in \cup_{i=0}^2 \mathfrak{B}_i\}$ .

In discriminating between the maximally entangled states above, we apply quite directly the method and use of extremal covariant measurements in Ref. [23] for quantum states of prime powered dimensions. Let us rewrite the states of  $\mathfrak{B}_0$  with  $|\Phi^+\rangle \equiv |0\rangle$ ,  $|\Psi^+\rangle \equiv |1\rangle$ ,  $|\Psi^-\rangle \equiv |2\rangle$ , and  $|\Phi^-\rangle \equiv |3\rangle$  with  $\{|i\rangle, i \in \mathbb{F}_4\}$  as the ‘‘computational basis’’ in  $\mathcal{H}_4$ , where  $\mathbb{F}_4$  is the finite field of cardinality 4. Let us then consider the projective representation of the Abelian group  $G = \mathbb{F}_4 \times \mathbb{F}_4$  as [23]

$$R(G) = \{\mathcal{U}_q \mathcal{V}_w | (q, w) \in \mathbb{F}_4 \times \mathbb{F}_4\}, \quad (30)$$

where  $\mathcal{U}_q |i\rangle = |i \oplus q\rangle$  and  $\mathcal{V}_w |i\rangle = \langle w, i | i \rangle$ , with  $\langle w, i \rangle = \chi(w \odot i)$ , where  $\chi(x)$  is a nontrivial character of the additive group  $\mathbb{F}_4$ . The operations  $\oplus$  and  $\odot$  are of course field addition and multiplication, respectively. Writing  $x$  as a tuple  $(s_1, s_2), s_i \in \{0, 1\}$ , we choose  $\chi(x)$  as  $\exp(\pi i s_1)$  [24]. Considering the state (call it initial)  $|0\rangle\langle 0|$ , it can be easily checked that its orbit under  $R(G)$  is indeed  $\{|i\rangle\langle i|, i \in \mathbb{F}_4\}$ . This holds similarly for the states from  $\mathfrak{B}_1$  and  $\mathfrak{B}_2$  where the orbits under  $R(G)$  for any one ‘‘initial’’ state in one basis are the set of all states from the respective bases and the stability groups for the initial states are nontrivial. From Ref. [23], with  $R(G)$  being irreducible, an extremal positive operator valued measure is the group orbit of a single operator, and we may conclude that, with the choice of basis,  $\mathfrak{B}_0$ ,  $\mathfrak{B}_1$ , and  $\mathfrak{B}_2$  being equally probable, the optimal measurement operator is the orthogonal measurement onto any one of the bases. The average estimation fidelity [3] in discriminating these states can then be written as

$$\frac{1}{12} \sum_{u,s} P(|s\rangle\langle s| | u\rangle\langle u|) |\langle s | u \rangle|^2, \quad (31)$$

where  $P(|s\rangle\langle s| | u\rangle\langle u|)$  is the probability of a measurement of state  $|u\rangle$  resulting in  $|s\rangle$ . It is easy to show that the average fidelity of discriminating between states selected randomly from  $\cup_{i=0}^2 \mathfrak{B}_i$  is really  $1/2$ . This is in fact the same maximal value for the average estimation fidelity of a completely unknown maximally entangled states in  $\mathcal{H}_2 \otimes \mathcal{H}_2$  immediately calculated from Ref. [3] as well as that of a completely unknown unitary in  $SU(2)$  as from Ref. [9].

### B. MUUBs in a quantum key distribution setup

The idea of ‘‘bases’’ for unitary transformation was mentioned in Ref. [9] and later also used in Ref. [10] to highlight richer points as opposed to a prepare and measure type QKD scheme. From the above sections describing the ‘‘unbiasedness’’ of such bases in a more precise way, applying it to two-way QKDs is the most natural step in generalizing such protocols to include all MUUBs. The basic structure of the protocol remains; Bob would submit a qubit prepared in a particular basis to Alice who would encode on it with a

<sup>1</sup>According to Ref. [11],  $\cup_{i=0}^2 \mathcal{B}_i$  forms a 2-design.

unitary transformation before sending the qubit back to Bob for measurements.

For the sake of clarity, we propose a protocol which is a generalization (in terms of the encoding) of one proposed and analyzed in Ref. [25]. For encoding purposes, Alice randomly selects an operator from her “bases”  $\mathcal{B}_0$ ,  $\mathcal{B}_1$ , and  $\mathcal{B}_2$ . Binary values are assigned to each operator in  $\mathcal{B}_0$  as in Ref. [25], i.e., 0,1,1,0 to  $\mathbb{I}_2, \sigma_1, \sigma_2, \sigma_3$ , respectively, which can be done as well for  $\mathcal{B}_1$  and  $\mathcal{B}_2$ . Bob submits a qubit prepared in one of two MUBs and measures the returned qubit in a randomly selected basis; either the same as the one he prepared in or one mutually unbiased to it. While  $\mathcal{B}_0$  retains the bases of Bob’s qubit states,  $\mathcal{B}_1$  and  $\mathcal{B}_2$  shift them to a basis mutually unbiased. At the end of the protocol, Alice announces (on a public channel) which of the “bases” she used for a given round of the protocol. Alice further discloses if she used either one of two subsets from her basis choice where each subset contains elements that can be distinguished perfectly by Bob’s measurements (subject to Bob measuring the qubit in the correct basis). As a quick example from Ref. [25], we give the subsets  $\{\mathbb{I}_2, \sigma_2\}$  and  $\{\sigma_1, \sigma_3\}$ . Hence, 1/3 of the time Bob retains his measurements where he can determine Alice’s encoding conclusively for key purposes while discarding the rest (instances where he measures a qubit in a wrong basis).

To provide an insight into the security of such a protocol, we consider the simplest strategy for an eavesdropper, Eve, to ascertain Alice’s encoding. She would hijack Bob’s qubit en route, submit a Bell state to Alice instead to estimate the unitary used, and then apply her estimation on Bob’s qubit before returning to him. Subsequent to Alice’s disclosure, Eve’s gain would only be 1/3 while inducing an equal amount of error. While obviously a more involved strategy should be considered, for an error less than 1/2 between Alice and Bob, Eve’s gain would never achieve unity due to the inability to distinguish between MUUBs perfectly for a single use. A proper security analysis is, however, beyond the scope of this work.

## VI. CONCLUSION

Generalizing the notion of MUUBs formalized in Ref. [11], we provide a definition for sets of unitary transformations forming bases for subspaces of  $M(d, \mathbb{C})$ , such that the elements in one basis are mutually unbiased with respect to elements in

another. The essence of the definition is in capturing the notion of distinguishability between unitary transformations based on their actions on quantum states. We explicitly construct such bases for the qubit case and show how such a construction gives the maximal number of such bases as three for the four-dimensional vector space of  $M(2, \mathbb{C})$  and two for a two-dimensional subspace of  $M(2, \mathbb{C})$ . Subsequent to that, we consider the case for unitary operators acting on prime numbered dimensional systems and prove the nonexistence of MUUBs for subspaces of  $M(d, \mathbb{C})$  of dimensionality other than  $d$  or  $d^2$ . Subscribing to a simple numerical search, we construct MUUBs for qutrits in all possible subspaces.

In a bid to see MUUBs in action beyond their construction, we note that in the case for qubits, estimating a unitary selected randomly from the full set of MUUBs is equivalent to the estimation of a maximally entangled states selected randomly from the maximal number of MUBs with the average estimation fidelity as 1/2, i.e., equal to the case for estimating a completely unknown maximally entangled state or a completely unknown unitary from  $SU(2)$ . We then consider this in a QKD setup. These in fact would be beyond the role that MUUBs have been shown to play in unitary 2-designs [11].

There are obviously various other interesting directions this work may be extended to, including an information-disturbance tradeoff in the estimation of such unitaries (or its isomorphic equivalent of maximally entangled states), a more specific scenario of Refs. [9,26]), and a proper understanding of possible entropic bounds in such estimations. Immediate applications of such studies include a possibly more thorough study of quantum cryptography as described in Sec. V. More immediate issues would include a deeper understanding of MUUBs acting on higher-dimensional quantum systems.

## ACKNOWLEDGMENTS

J.S.S. would like to thank H. Zainuddin and S. Karumanchi for fruitful discussions. He is grateful to the University of Camerino for the kind hospitality during the time this work was conceived and for financial support by Ministry of Higher Education (Malaysia), Fundamental Research Grant Scheme FRGS14-152-0393. J.S.S. is also grateful the University’s Research Management Centre for their assistance.

- 
- [1] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, *Int. J. Quantum Inf.* **08**, 535 (2010).
  - [2] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
  - [3] A. Acín, E. Jané, and G. Vidal, *Phys. Rev. A* **64**, 050302(R) (2001).
  - [4] G. Chiribella, G. M. D’Ariano, P. Perinotti, and M. F. Sacchi, *Phys. Rev. Lett.* **93**, 180503 (2004).
  - [5] K. Boström and T. Felbinger, *Phys. Rev. Lett.* **89**, 187902 (2002).
  - [6] M. Lucamarini and S. Mancini, *Phys. Rev. Lett.* **94**, 140501 (2005).
  - [7] M. Lucamarini and S. Mancini, *Theor. Comput. Sci.* **560**, 46 (2014).
  - [8] G. Chiribella, G. M. D’Ariano, and P. Perinotti, *Phys. Rev. Lett.* **101**, 180504 (2008).
  - [9] A. Bisio, G. Chiribella, G. M. D’Ariano, and P. Perinotti, *Phys. Rev. A* **82**, 062305 (2010).
  - [10] J. S. Shaari, *Phys. Lett. A* **378**, 863 (2014).
  - [11] A. J. Scott, *J. Phys. A* **41**, 055308 (2008).
  - [12] A. Roy and A. J. Scott, *Des., Codes Cryptogr.* **53**, 1 (2009).
  - [13] G. M. D’Ariano, P. Lo Presti, and M. F. Sacchi, *Phys. Lett. A* **272**, 32 (2000).
  - [14] G. M. D’Ariano, P. Lo Presti, and M. G. A. Paris, *Phys. Rev. Lett.* **87**, 270404 (2001).
  - [15] G. M. D’Ariano, P. Lo Presti, and M. G. A. Paris, *J. Opt. B* **4**, S273 (2002).
  - [16] S. Hill and W. K. Wootters, *Phys. Rev. Lett.* **78**, 5022 (1997).
  - [17] J. Lawrence, Č. Brukner, and A. Zeilinger, *Phys. Rev. A* **65**, 032320 (2002).

- [18] D. Gottesman, A. Kitaev, and J. Preskill, *Phys. Rev. A* **64**, 012310 (2001).
- [19] J. Hall, Ph.D. thesis, RMIT University, 2011.
- [20] Y.-H. Tao, H. Nan, J. Zhang, and S.-M. Fei, *Quantum Inf. Proc.* **14**, 2291 (2015).
- [21] G. Chiribella, Ph.D. thesis, Università Degli Studi Di Pavia, 2006.
- [22] G. Chiribella, *J. Phys.: Conf. Ser.* **284**, 012001 (2011).
- [23] G. Chiribella and G. M. D'Ariano, *J. Math. Phys.* **47**, 092107 (2006).
- [24] K. R. Parthasarathy, [arXiv:quant-ph/0408069](https://arxiv.org/abs/quant-ph/0408069).
- [25] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, *Phys. Rev. A* **88**, 062302 (2013).
- [26] M. F. Sacchi, *Phys. Rev. Lett.* **96**, 220502 (2006).