Quantum Secret Sharing with Multi-level Mutually (Un-)Biased Bases

I-Ching Yu*, Feng-Li Lin† and Ching-Yu Huang‡
Department of Physics, National Taiwan Normal University, Taipei, 116, Taiwan

We construct general schemes for multi-partite quantum secret sharing using multi-level systems, and find that the consistent conditions for valid measurements can be summarized in two simple algebraic conditions. The scheme using the very high dimensional mutually unbiased bases can in principle achieve perfect security against intercept-resend attack; and for the scheme using mutually biased bases, it reaches the optimal but non-perfect security at 4-level system. We also address the security issue against the general attacks in the context of our multi-level schemes. Especially, we propose new protocol to enhance both the efficiency and the security against the entanglement-assisted participant's attack by incorporating quantum-key-distribution and measurement-basis-encrypted schemes so that its security is as robust as quantum-key-distribution.

I. INTRODUCTION

The security of quantum cryptography is ensured by the non-cloning theorem [1] so that the eavesdropping via physical means can always be detected. The schemes for quantum key distribution(QKD) and secret sharing were first proposed in [4, 5] and [6, 7], respectively. Both of the schemes can be thought as the quantum version of the classical threshold secret sharing (k, n)-scheme [2, 3]. The scheme is designed to distribute valuable information among n participants so that it can be reconstructed only if $k(\leq n)$ of them collaborate [18].

Although the quantum secret sharing(QSS) scheme is better than the classical one in detecting the error caused by an eavesdropper, it is not perfect. For the common intercept-resend attack, an eavesdropper can get hold of some participants' particles, perform the Bell-state measurement [13] and resend back. The probability of detecting such an attack is only 25 percent for the QSS scheme [6] using 2-level system. The detecting rate is quite low if the secret sharing is for some fatal event such as the release of warheads, for which we hope to have the perfect security, i.e., 100 percent detecting rate. Therefore, an important question for QSS is whether one can have a scheme with the perfect security for attacks such as intercept-resend. Surprisingly, despite many modified QSS schemes inspired by the original works [6, 7] in the past few years, as far as we know, there is no discussion for such an issue, even in principle.

One straightforward way to increase the detecting rate against the attacks is to use higher dimensional quantum systems to proceed the QSS. Intuitively, increasing the dimensions of the quantum bases will complicate the QSS protocol so that the eavesdropper has more difficulty to obtain correct information without being detected. Of course, we will pay the price for reducing the efficiency because we now use the higher dimensional bases to encode one bit information. This may also complicate the consistent conditions for the valid measurements of the protocol and make the QSS procedure more tedious. Moreover, the complication of the protocol may again pose security issues.

In this article we construct the QSS schemes using d-level systems and establish a security benchmark as a function of d against the common intercept-resend attack. The results show that in principle the perfect security against such an attack can be achieved by using very high dimensional mutually-unbiased bases(MUBs). Interestingly, we may wonder if the security or error-detecting rate will always increase by using the higher dimensional system. We will see that this is subtle, and we find a counterexample by using the mutually-biased bases(MBBs) for QSS, which reaches non-perfect optimal security at 4-level system. Our multi-level scheme is the generalization of [6] for 2-level case. It turns out that the consistent conditions for valid measurements of the higher dimensional protocol is quite simple and natural, and can be summarized in two algebraic conditions. Moreover, regarding the recent concern on the security of QSS [14], we will also address the issue in our multi-level schemes against more general and efficient attacks other than intercept-resend. We find that one can invalidate the entanglement-assited participant's attack devised in [14] by slightly modifying the protocol proposed in [6].

The paper is organized as follows: In the next section we will construct the QSS schemes by using the MUBs and MBBs, respectively. In section III we establish a security benchmark against the intercept-resend attack. In section IV we consider the security of our schemes against more general attacks. Especially, we give a proof of security against the attack by an outsider Eve with entangled probe. However, we comment that the original scheme [6] is vulnerable to the the entanglement-assited participant's attack devised in [14]. Finally we conclude our paper in section V by proposing an 100 percent efficient scheme against the entanglement-assited participant's attack by combining the quantum-key-distribution and measurement-basis-encrypted method.

*896410029@ntnu.edu.tw
†linfengli@phy.ntnu.edu.tw, correspondent author
‡896410093@ntnu.edu.tw

II. QUANTUM SECRET SHARING WITH MUTUALLY UNBIASED BASES

We first consider the $(2,3)$-scheme for QSS using the multi-level MUBs, and later generalize it to the multipartite cases. The $(2,3)$-scheme is for Alice to distribute the secret key to both Bob and Charlie, and proceed the QSS protocol via the local operations and classical communication(LOCC).

We start with the d-level GHZ state [9], which is shared among Alice, Bob and Charlie,

$$|GHZ_3\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jjj\rangle \tag{1}$$

each holds one particle in it. The GHZ state is a maximally entangled state, and is used for QSS such that the measurement outcomes of Alice, Bob and Charlie for their own particles are correlated. Once Bob and Charlie combine their outcomes of measurements, they can know Alice's.

A typical QSS protocol runs as following [6, 7]. (i) Alice prepares the GHZ state, and then distributes the corresponding particles to Bob and Charlie, respectively. (ii) Alice, Bob and Charlie perform the local measurements on their own particles by randomly choosing the measurement bases. (iii) Bob and Charlie then announce their measurement bases publicly to Alice, but not their outcomes. (iv) Alice then determines if the measurement bases satisfy the consistent conditions encoded by the GHZ state, which can be summarized in a lookup table. If so, they keep the outcomes as the useful key and examine further if there is eavesdropping. If there is, then just discard the results. (v) Repeat the above procedure to collect enough outcomes for the secret information. When necessary, Bob and Charlie can collaborate to reproduce Alice's information.

We will adopt the above protocol for the QSS using d-level GHZ state (1). However, in the end we will modify this protocol to enhance both the security and efficiency of QSS. The modification will incorporate both QKD and measurement-basis-encrypted scheme [15].

As noted in [10, 11], it is possible to find $d+1$ MUBs in d dimensions only if d is (any power of) an odd prime. Besides the canonical basis $\{|j\rangle, j=0,...,d-1\}$, the explicit forms of the remaining d sets of MUBs are

$$|P_p\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\phi(Pj^2+pj)}|j\rangle, \quad \phi = \frac{2\pi}{d} \tag{2}$$

where P (runs from 1 to d) denotes the basis and p (runs from 0 to $d-1$) labels the vector in a given orthonormal basis [19]. They are mutually unbiased because the overlap is

$$|\langle P_p|P'_{p'}\rangle| = \frac{1}{\sqrt{d}} \quad \text{for} \quad P \neq P', \tag{3}$$

which follows from the Gauss sums of number theory valid for odd prime d.

From (3) we can derive the consistent conditions for a valid measurement. To arrive that, let us assume that Bob and Charlie hold the states $|B_b\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi(Bj^2+bj)}|j\rangle$ and $|C_c\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi(Cj^2+cj)}|j\rangle$, respectively. Then, take the inner product between the GHZ state and the 2-particle state $|B_b\rangle|C_c\rangle$, we obtain

$$(\langle B_b|\langle C_c|)|GHZ_3\rangle = \frac{1}{d\sqrt{d}} \sum_{j=0}^{d-1} e^{-i\phi((B+C)j^2+(b+c)j)}|j\rangle$$

which after normalization should match with Alice's state $|A_a\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{i\phi(Aj^2+aj)}|j\rangle$ in order to make a valid measurement for secret sharing. This then implies the following consistent conditions:

$$A+B+C = 0 \ (\text{mod } d), \tag{4}$$

$$a+b+c = 0 \ (\text{mod } d). \tag{5}$$

According to these, we can write down a $d^2 \times d^2$ lookup table for the use of QSS protocol using the d-level system. This is the straightforward generalization for the $d=2$ case. In QSS protocol[6, 7], one first checks if condition (4) satisfies or not by LOCC. If yes, it is a valid measurement and (5) follows; otherwise, the measurement will be discarded. Importantly, the conciseness of conditions (4) and (5) helps to simplify the practical en/de-coding procedures in QSS. On the other hand, condition (4) implies that the efficiency is $1/d$ since only one out of d cases makes a valid measurement, and condition (5) can be used to detect eavesdropping for valid measurements.

Quantum secret sharing with mutually biased bases.— The above generalizes the QSS scheme of [6, 7] using MUBs. Now we look for the scheme using MBBs which has not been discussed before in literatures.

Our construction of the d-level MBBs for QSS is as follows. Start with the Fourier transform of the canonical basis

$$|u_k\rangle_F = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{ikj\phi}|j\rangle, \quad k=0,..,d-1, \quad \phi = \frac{2\pi}{d}.$$

We then introduce the following d MBBs

$$|P_p\rangle = |u_p\rangle_F + \frac{1}{\sqrt{d}}(e^{iP\phi}-1)|0\rangle \tag{6}$$

for $P=0,..,d-1, p=0,..,d-1$. Note that $|0_j\rangle = |u_j\rangle_F$. For simplicity, here and hereafter we use the same notation as for MUBs.

We now show that these bases will form a consistent lookup table for QSS. Note that the overlap

$$\langle P_p|P'_{p'}\rangle = \delta_{pp'} + \frac{1}{d}[e^{i(P'-P)\phi}-1]. \tag{7}$$

Thus, each basis $\{|P_p\rangle, p = 0,..,d-1\}$ is orthonormal and complete, and the overlap $|\langle P_p|P'_{p'}\rangle|$ between different bases will depend on $P'-P$ and so is called biased except for $d=3$ case, which is the same as $d=3$ MUBs'.

Similar to the case for MUBs, if Bob and Charlie hold the states $|B_b\rangle = |u_b\rangle_F + \frac{1}{\sqrt{d}}(e^{iB\phi}-1)|0\rangle$ and $|C_c\rangle = |u_c\rangle_F + \frac{1}{\sqrt{d}}(e^{iC\phi}-1)|0\rangle$ respectively, we should require the state $(\langle B_b|\langle C_c|)|GHZ_3\rangle$ to match Alice's state $|A_a\rangle = |u_a\rangle_F + \frac{1}{\sqrt{d}}(e^{iA\phi}-1)|0\rangle$ for a valid measurement. This then yields the same consistent conditions (4) and (5) for a valid measurement as for MUBs.

It is straightforward to generalize the above tri-partite scheme to the multi-partite one. We just start with the n-partite GHZ state

$$|GHZ_n\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|jjj...j\rangle_{123...n}. \tag{8}$$

Each party measures her/his own particle and obtains the outcome in one of the d bases, say $\{|P_p\rangle\}$. To have a consistent lookup table for n-partite case, we should require (up to some normalization factor)

$$|A_a\rangle = (\langle B_b|\langle C_c|\langle D_d|\cdots\langle \Omega_\omega|)|GHZ_n\rangle$$

which yields the following consistent conditions

$$A+B+C+...+\Omega = 0 \ (\mathrm{mod}\ d), \tag{9}$$
$$a+b+c+...+\omega = 0 \ (\mathrm{mod}\ d). \tag{10}$$

These are straightforward generalization of (4) and (5), respectively. Note that because of (3) or (7), condition (9) implies (10) but not vice versa.

III. DETECTING THE INTERCEPT-RESEND ATTACK

We like to give a benchmark formula for the detecting rate against the very common intercept-resend attack as a function of dimension d. The attack goes as follows for tri-partite case: the dishonest Charlie* gets hold of Bob's particle and performs the general Bell-state measurement on his two-particle state, then resends one particle to Bob. Since Charlie* does not know Alice's measurement basis, he may use the wrong base for his Bell-state measurement but still has some probability to get the right result. On the other hand, if Charlie* happens to use the right base, he will then know Bob's measurement outcome and then Alice's after LOCC without making detectable error.

The detecting rate against the attack can be derived as follows. Let us assume that Alice's measurement outcome is $|A_a\rangle$, However, Charlie* thinks Alice was using the base $\{|A'_{a'}\rangle\}$ and expands his two-particle state in such a base, i.e., $\langle A_a|GHZ_3\rangle = \sum_{a'=0}^{d-1}\langle A_a|A'_{a'}\rangle\langle A'_{a'}|GHZ_3\rangle$. A detectable error occurs if the condition (4) holds but (5) is violated, and its rate is $1-|\langle A'_{a'}|A_a\rangle|^2$. Then, the average detecting rate over the configurations satisfying (4) but not (5) is

$$P_E := \sum_{A-A'=1}^{d-1}\frac{1}{d}\sum_{a'=0}^{d-1}|\langle A_a|A'_{a'}\rangle|^2(1-|\langle A'_{a'}|A_a\rangle|^2). \tag{11}$$

For the scheme using MUBs, by (3) the detecting rate (11) is

$$P_{E,MUBs}(d) = (\frac{d-1}{d})^2. \tag{12}$$

It is a monotonically increasing function of d so that higher dimensional system is more secure. Especially, it approaches unity as d goes to infinity and implies perfect security, in principle.

For the cases using MBBs, by (7) we find that

$$P_{E,MBBs}(d) = \frac{4d^2-10d+6}{d^3}. \tag{13}$$

In contrast to MUBs' case, it is not a monotonic function of d because of the weighted overlap between bases. Instead, it reaches the maximal at $d=4$ with $P_{E,MBBs}(d=4) = \frac{15}{32}$, and then decreases to zero monotonically for $d>4$. Moreover, $P_{E,MUBs}(d=3) = P_{E,MBBs}(d=3) = \frac{4}{9}$ as expected because our MUBs and MBBs are the same for $d=3$. Recall that the detecting rate for the 2-level scheme of [6] is only 1/4, so even the lower $d(>2)$ schemes using MBBs have higher security than the 2-level case. Since the MUBs' scheme is only available for odd prime d, the $d=4$ MBBs' case can be considered as the optimal scheme for a compromise between the degree of security and the efficiency. Practically, one can physically realize the $d=4$ system by combining two 2-level systems to carry out the optimal MBBs' scheme; for example, the para- and ortho-helium spectra can be seen as a $d=4$ system by appropriately adjusting the external magnetic/electric fields.

Estimating the detecting rate in the multi-partite system is more complicated, we will not discuss the details here. However, the more persons share the entangled key, the more difficult it is for the eavesdropper to collect all the other's particles and the more secure the scheme is.

IV. SECURITY AGAINST GENERAL EAVESDROPPERS

Enforcing the security of the cryptography is state-of-the-art, so is its attack strategy. After establishing a security benchmark against the common intercept-resend attack, we like to address the issue for more general attacks which could be more efficient than expected for an eavesdropper (called Eve) using the ancilla probe.

First, we consider the case that Eve is not the member sharing the secret via GHZ state. Then, the QSS scheme is secure provided that GHZ state is the only state satisfying the consistent conditions (9) and (10). Otherwise, there will be a set of fake key states $\{|FK\rangle\}$ other than the GHZ satisfying (9) and (10), and Eve can use the ancilla states $\{|E\rangle_{FK}\}$ and $|E\rangle_{GHZ}$ to form the entangled state

$$|\Psi\rangle = |GHZ_n\rangle|E\rangle_{GHZ} + \sum_{\{|FK\rangle\}} |FK\rangle|E\rangle_{FK}. \tag{14}$$

She can then extract the encoded secret information in the GHZ state by performing the general Bell-state measurement without making detectable errors. We now show that GHZ state is indeed the unique one satisfying (9) and (10).

The proof constructed for the 2-level scheme is given in [6] by showing that all the states orthogonal to the GHZ state do not satisfy the consistent conditions (9) and (10). This procedure will be far more involved for the multi-level case. Instead, we directly show

$$|\langle\Lambda|\Phi\rangle| < |\langle\Lambda|GHZ_n\rangle| \tag{15}$$

for any state $|\Phi\rangle$ belonging to the vector space $V_{GHZ}^{\perp}$ which is orthogonal to GHZ state, and the conditional states $|\Lambda\rangle$'s representing the consistent conditions (9) and (10), i.e.,

$$|\Lambda\rangle = |A_a\rangle|B_b\rangle|C_c\rangle...|\Omega_\omega\rangle,$$

with the states' labels satisfying (9) and (10). This implies that none of the states in $V_{GHZ}^{\perp}$ will satisfy all the d^{n-1} conditions given by (9) and (10). The state $|\Psi\rangle$ in (14) will then reduce to the product of GHZ and ancilla states so that Eve cannot obtain useful information through entanglement without making detectable errors.

We start the proof by constructing the basis vectors for $V_{GHZ}^{\perp}$ in terms of the canonical basis $\{|ijk\cdots\rangle\}$ via Gram-Schmidt orthonormalization process. Then, there arrive two kinds of basis states: (1) there are $d^n - d$ unit vectors in the canonical basis which do not belong to the subset made of GHZ state, i.e.,

$$|\Phi\rangle_{\perp,1} := |ijk\cdots\rangle \neq |\ell\ell\ell\cdots\rangle$$

with $i, j, k, \ell\cdots = 0, 1, 2, \ldots, d-1$; (2) there are the other $d-1$ basis vectors taking the following form

$$|\Phi\rangle_{\perp,2} = \sum_{j=0}^{d-1} c_j |jjj\cdots\rangle,$$

and the orthogonality to GHZ state requires $\sum_{j=0}^{d-1} c_j = 0$ besides the normalization condition $\sum_{j=0}^{d-1} |c_j|^2 = 1$.

Before we check if states $|\Phi\rangle_{\perp,1}$ and $|\Phi\rangle_{\perp,2}$ satisfy (15), we note that

$$\langle\Lambda|jjj\cdots\rangle = d^{-\frac{n}{2}} \tag{16}$$

for any conditional state $|\Lambda\rangle$ so that

$$\langle\Lambda|GHZ_n\rangle = d^{1-\frac{n}{2}}. \tag{17}$$

These two imply that while checking (15) we can treat all the d^{n-1} conditional states equally, it then helps to simplify the task. Condition (16) then yields $\langle\Lambda|\Phi\rangle_{\perp,2} = d^{-\frac{n}{2}} \sum_{j=0}^{d-1} c_j = 0$ for any $|\Lambda\rangle$ so that the second type of basis vectors are orthogonal to all the conditional states and thus are excluded from the set $\{|FK\rangle\}$ in (14). On the other hand, from (17) for the first kind of basis vectors we have $|\langle\Lambda|\Phi\rangle_{\perp,1}| = d^{-\frac{n}{2}} < \langle\Lambda|GHZ_n\rangle$ for any conditional state $|\Lambda\rangle$ so that they are also excluded from the set $\{|FK\rangle\}$ in (14). This then completes our proof.

However, the uniqueness of GHZ state does not guarantee QSS' security if Charlie* is dishonest with the help of an ancilla Eve to entangle with Bob's particle. This is the entanglement-assisted participant's attack. In [14], an explicit attacking scheme via manipulating GHZ state with ancilla was devised so that AB's and CE's states are maximally entangled [20]

$$|\Psi\rangle_{ABCE} = \frac{1}{d}\sum_{a,b=0}^{d-1} |\bar{A}_a\rangle|\bar{B}_b\rangle \otimes |\psi_{ab}^{(\bar{A}\bar{B})}\rangle_{CE} \tag{18}$$

where the bar quantity means its value is chosen and fixed, and $\{|\psi_{ab}^{(\bar{A}\bar{B})}\rangle_{CE}\}$ is an orthonormal complete set for Alice's and Bob's chosen basis $\bar{A}$ and $\bar{B}$, respectively. After Alice and Bob measure their particles in bases $\bar{A}$ and $\bar{B}$ with the outcomes $a = \bar{a}$ and $b = \bar{b}$ respectively, then the state (18) collapses to $|\psi_{\bar{a}\bar{b}}^{(\bar{A}\bar{B})}\rangle_{CE}$. Since $\{|\psi_{ab}^{(\bar{A}\bar{B})}\rangle_{CE}\}$ is orthonormal and Charile* knows Alice's and Bob's measurement basis, he can perform local unitary transformations to extract the $\bar{a}$ and $\bar{b}$ from $|\psi_{\bar{a}\bar{b}}^{(\bar{A}\bar{B})}\rangle_{CE}$ without making detectable error as shown in [14]. In a sense, the multi-level QSS scheme using protocol of [6] is highly insecure.

V. AN EFFICIENT SCHEME AGAINST ENTANGLEMENT-ASSISTED PARTICIPANT'S ATTACK

We now propose a modified protocol to remedy the above security loop-hole. Moreover, it will enhance the efficiency of QSS from $1/d$ to 100 percent. The modification is two-fold. One is to adopt the measurement-basis-encrypted efficient QSS scheme proposed in [15] as follows: Instead for the participants to announce their measurement basis in order to verify if they satisfy (9) for the valid measurements, they will use their measurement outcomes as the measurement basis for the next run. As long as the first run is a valid measurement, then all the subsequent runs will be automatically the valid measurements as seen from (9) and (10). This yields 100 percent efficiency. Moreover, since Charile* does not know about others' chosen bases and thus cannot take advantage of the entangled state (18), he has no way to extract other's measurement outcomes from such a state $|\psi_{ab}^{(\bar{A}\bar{B})}\rangle_{CE}$. By guess, he has only $1/d$ chance to do it right. The remaining modification is to ensure the first run can be a valid measurement without announcing the measurement basis. This can be done by using multi-level QKD for Alice to distribute a valid set of measurement basis to each participant separately. The eavesdropper can of course attack QKD, too. However, the QKD security is more robust than QSS's and has been studied extensively, e.g. see [16]. An alternative against the attack of [14] is considered in [17] for multi-level QSS recently.

In this paper, we have generalized the QSS scheme for qubits to the multi-level cases with both MUBs and MBBs. We also discuss the security issues for general attacks. Finally we propose an efficient and secure protocol which could be relevant to the physical realization of QSS.

Acknowledgement: We would like to thank Ming-Che Chang, Li-Yi Hsu and I-Ming Tsai for valuable comments. This work was supported by Taiwan's NSC grant 96-2112-M-003-014.

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982). D. Dieks, Physics Letters A, **92**271 (1982).

[2] G. R. Blakley, in Proceedings of the American Federation of Information Processing 1979 National Computer Conference (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317.

[3] A. Shamir, Commun. ACM **22**, 612 (1979).

[4] C. Bennett and G. Brassard in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India 1984) p. 175.

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661(1991).

[6] M. Hillery, V. Bŭzek, and A. Berthiaume, Phys. Rev. A **59**, 1829(1999).

[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83** 648 (1999).

[9] D. Greenberger, M. Horne, and A. Zeilinger in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer Academic, Dordrecht, 1989).

[10] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).

[11] W. K. Wootters and B. D. Fields, Annals of Physics, **191**, 363 (1989).

[12] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).

[13] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209(1996).

[14] S.-J. Qin, F. Gao, Q.-Y. Wen, F.-C. Zhu, Phys. Rev. A **76**, 062324(2007).

[15] L. Xiao, G.-L. Long, F.-G. Deng, J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).

[16] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[17] D.-P. Chi, J.-W. Choi, J.-S. Kim, T.-W. Kim, S.-J Lee, arXiv:0801.0177.

[18] See also [8] for deriving the constraint $k > n/2$ on the existence of threshold schemes.

[19] The $d = 3$ MUBs has been used in [12] for quantum key distribution.

[20] In [14] the authors consider $d = 2$ case, it is straightforward to generalize to d-level cases for both MUBs and MBBs by using the d-level Hadamard and CNOT gates. Also note that the form of (18) is maximally entangled in Schmidt's decomposition between two parties AB and CE.