Quantum secret sharing with multilevel mutually (un)biased bases

I-Ching Yu,* Feng-Li Lin,† and Ching-Yu Huang‡
Department of Physics, National Taiwan Normal University, Taipei 116, Taiwan
(Received 27 November 2007; published 23 July 2008)

We construct general schemes for multipartite quantum secret sharing using multilevel systems, and find that the consistency conditions for valid measurements can be summarized in two simple algebraic conditions. The scheme using 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 nonperfect security at the four-level system. We also address the security issue against general attacks in the context of our multilevel schemes. In particular, we propose a protocol to enhance both the efficiency and the security against an 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.

DOI: 10.1103/PhysRevA.78.012344 PACS number(s): 03.67.Dd

I. INTRODUCTION

The security of quantum cryptography is ensured by the no-cloning theorem [1] so that eavesdropping via physical means can always be detected. Schemes for quantum-key distribution(QKD) and secret sharing were first proposed in [2,3] and [4,5], respectively. Both of the schemes can be thought of as the quantum versions of the classical threshold secret sharing (k,n) scheme [6,7]. 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.[1]

Although the quantum secret sharing (QSS) scheme is better than the classical one in detecting errors caused by an eavesdropper, it is not perfect. For the common intercept-resend attack, an eavesdropper can get hold of some participants' particle, perform a Bell-state measurement [9], and send it back. The probability of detecting such an attack is only 25% for the QSS scheme [4] using a two-level system. The detection 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 perfect security, i.e., 100% detection rate. Therefore, an important question for QSS is whether one can have a scheme with perfect security for attacks such as intercept-resend. Surprisingly, despite many modified QSS schemes inspired by the original works [4,5] in the past few years, as far as we know, there has been no discussion for such an issue, even in principle.

One straightforward way to increase the detection rate against attacks is to use higher-dimensional quantum systems for the QSS. Intuitively, increasing the dimensions of the quantum bases will complicate the QSS protocol so that the eavesdropper has more difficulty in obtaining correct information without being detected. Of course, we will pay the price for reducing efficiency because we now use the higher-dimensional bases to encode one bit of information. This may also complicate the consistency conditions needed for 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 paper, we construct 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 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-detection rate will always be increased by using a higher-dimensional system. We will see that this is subtle, and we find a counterexample by using mutually biased bases (MBBs) for QSS, which reaches nonperfect optimal security for a four-level system. Our multilevel scheme is the generalization of [4] for the two-level case. It turns out that consistency 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 about the security of QSS [10], we will also address the issue in our multilevel schemes of security against more general and efficient attacks other than intercept-resend. We find that one can invalidate the entanglement-assisted participant's attack devised in [9] by slightly modifying the protocol proposed in [4].

The paper is organized as follows: In the next section we will construct QSS schemes by using MUBs and MBBs, respectively. In Sec. III we establish a security benchmark against the intercept-resend attack. In Sec. IV we consider the security of our schemes against more general attacks. In particular, we give a proof of security against attack by an outsider, Eve, with an entangled probe. However, we comment that the original scheme [4] is vulnerable to the entanglement-assisted participant's attack devised in [9]. Finally, we conclude our paper in Sec. V by proposing a 100% efficient scheme against the entanglement-assisted participant's attack by combining the quantum-key-distribution and measurement-basis-encrypted methods.

II. QUANTUM SECRET SHARING WITH MUTUALLY UNBIASED BASES

We first consider the (2,3) scheme for QSS using multilevel MUBs, and later generalize it to the multipartite cases.

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

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

The (2,3) scheme is for Alice to distribute the secret key to both Bob and Charlie, and use the QSS protocol via local operations and classical communication (LOCC).

We start with the d-level Greenberger-Horne-Zeilinger (GHZ) state [11], which is shared among Alice, Bob, and Charlie,

$$|\mathrm{GHZ}_3\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} |jjj\rangle; \tag{1}$$

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 the outcomes of their measurements, they know Alice's.

A typical QSS protocol runs as follows [4,5]. (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 consistency conditions encoded by the GHZ state, which can be summarized in a lookup table. If so, they keep the outcomes as a useful key and examine further if there is eavesdropping. If there is, then they just discard the results. (v) They 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 the 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 quantum-key-distribution (QKD) and measurement-basis-encrypted schemes [12].

As noted in [13,14], 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 $\{|j\rangle,\ j=0,\ldots,d-1\}$, 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 (running from 1 to d) denotes the basis and p (running from 0 to $d-1$) labels the vector in a given orthonormal basis.[2] 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 consistency conditions for a valid measurement. To arrive at them, 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, taking the inner product between the GHZ state and the two-particle state $|B_b\rangle|C_c\rangle$, we obtain

$$(\langle B_b|\langle C_c|)|\mathrm{GHZ}_3\rangle = \frac{1}{d\sqrt{d}}\sum_{j=0}^{d-1} e^{-i\phi[(B+C)j^2+(b+c)j]}|j\rangle$$

which after normalization should match 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 consistency conditions:

$$A + B + C = 0 \pmod d, \tag{4}$$

$$a + b + c = 0 \pmod d. \tag{5}$$

According to these, we can write down a $d^2 \times d^2$ lookup table for the use of the QSS protocol using the d-level system. This is a straightforward generalization for the $d=2$ case. In a QSS protocol [4,5], one first checks if condition (4) is satisfied 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- and decoding 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 [4,5] using MUBs. Now we look for a scheme using MBBs which has not been discussed before in the literature.

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

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

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 $P=0,\ldots,d-1$, $p=0,\ldots,d-1$. 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 $\{|P_p\rangle,\ p=0,\ldots,d-1\}$ 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 the $d=3$ case, which is the same as for $d=3$ 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 $(\langle B_b|\langle C_c|)|\mathrm{GHZ}_3\rangle$ 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

[2] The $d=3$ MUB was used in [15] for quantum key distribution.

yields the same consistency conditions (4) and (5) for a valid measurement as for MUBs.

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

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

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

$$|A_a\rangle = (\langle B_b|\langle C_c|\langle D_d|\cdots\langle \Omega_\omega|)|\mathrm{GHZ}_n\rangle,$$

which yields the following consistency conditions:

$$A + B + C + \cdots + \Omega = 0 \pmod d, \tag{9}$$

$$a + b + c + \cdots + \omega = 0 \pmod d. \tag{10}$$

These are straightforward generalizations 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 wish to give a benchmark formula for the detection rate against the very common intercept-resend attack as a function of dimension d. The attack goes as follows for the tripartite case. The dishonest Charlie* gets hold of Bob's particle and performs a general Bell-state measurement on his two-particle state, and 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 of getting 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 a detectable error.

The detection rate against 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., $\langle A_a|\mathrm{GHZ}_3\rangle = \Sigma_{a'=0}^{d-1}\langle A_a|A'_{a'}\rangle\langle A'_{a'}|\mathrm{GHZ}_3\rangle$. 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 detection 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 detection rate (11) is

$$P_{E,\mathrm{MUB}}(d) = \left(\frac{d-1}{d}\right)^2. \tag{12}$$

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

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

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

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

Estimating the detecting rate in the multipartite 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 others' particles and the more secure the scheme is.

IV. SECURITY AGAINST GENERAL EAVESDROPPERS

Enforcing the security of the cryptography is state of the art, and so is its attack strategy. After establishing a security benchmark against the common intercept-resend attack, we wish 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 the GHZ state. Then the QSS scheme is secure provided that the GHZ state is the only state satisfying the consistency conditions (9) and (10). Otherwise, there will be a set of fake key states $\{|\mathrm{FK}\rangle\}$ other than the GHZ state satisfying (9) and (10), and Eve can use the ancilla states $\{|E\rangle_{\mathrm{FK}}\}$ and $|E\rangle_{\mathrm{GHZ}}$ to form the entangled state

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

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

The proof constructed for the two-level scheme is given in [4] by showing that all the states orthogonal to the GHZ state do not satisfy the consistency conditions (9) and (10). This procedure will be far more involved for the multilevel case. Instead, we directly show that

$$|\langle\Lambda|\Phi\rangle| < |\langle\Lambda|\mathrm{GHZ}_n\rangle| \tag{15}$$

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

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

with the states' labels satisfying (9) and (10). This implies that none of the states in $V_{\mathrm{GHZ}}^{\perp}$ 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 $V_{\mathrm{GHZ}}^{\perp}$ in terms of the canonical basis $\{|ijk\cdots\rangle\}$ via the Gram-Schmidt orthonormalization process. Then we have 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 states, i.e.,

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

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

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

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

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

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

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

$$\langle\Lambda|\mathrm{GHZ}_n\rangle = d^{1-n/2}. \tag{17}$$

These two equations 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 $\langle\Lambda|\Phi\rangle_{\perp,2} = d^{-n/2}\Sigma_{j=0}^{d-1} c_j = 0$ 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 $\{|\mathrm{FK}\rangle\}$ in (14). On the other hand, from (17) for the first kind of basis vectors we have $|\langle\Lambda|\Phi\rangle_{\perp,1}| = d^{-n/2} < \langle\Lambda|\mathrm{GHZ}_n\rangle$ for any conditional state $|\Lambda\rangle$ so that they are also excluded from the set $\{|\mathrm{FK}\rangle\}$ in (14). This then completes our proof.

However, the uniqueness of the GHZ state does not guarantee security of QSS 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 [10], an explicit attack scheme via manipulation of the GHZ state with an ancilla was devised so that AB's and CE's states are maximally entangled:[3]

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

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 bases $\bar{A}$ 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 bases, 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 a detectable error as shown in [10]. In a sense, the multilevel QSS scheme using the protocol of [4] is highly insecure.

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

We now propose a modified protocol to remedy the above security loophole. Moreover, it will enhance the efficiency of QSS from $1/d$ to 100%. The modification is twofold. One is to adopt the measurement-basis-encrypted efficient QSS scheme proposed in [12] as follows. Instead of the participants announcing their measurement basis in order to verify if it satisfies (9) for 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 valid measurements as seen from (9) and (10). This yields 100% efficiency. Moreover, since Charlie* does not know about others' chosen bases and thus cannot take advantage of the entangled state (18), he has no way to extract others' measurement outcomes from such a state $|\psi_{ab}^{(\bar{A}\bar{B})}\rangle_{CE}$. By guessing, he has only a $1/d$ chance to get it right. The remaining modification is to ensure that the first run can be a valid measurement without announcing the measurement basis. This can be done by using multilevel QKD for Alice to distribute a valid set of measurement bases to each participant separately. The eavesdropper can of course attack QKD, too. However, QKD security is more robust than that of QSS and has been studied extensively, e.g., see [16]. An alternative against the attack of [10] was considered in [17] for multilevel QSS recently.

In this paper, we have generalized the QSS scheme for qubits to multilevel 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.

ACKNOWLEDGMENTS

We would like to thank Ming-Che Chang, Li-Yi Hsu, and I-Ming Tsai for valuable comments. This work was supported by Taiwan NSC Grant No. 96-2112-M-003-014.

[3] In [10] the authors consider the $d=2$ case; it is straightforward to generalize to d-level cases for both MUBs and MBBs by using the d-level Hadamard and controlled-NOT gates. Also note that the form of (18) is maximally entangled in Schmidt's decomposition between two parties AB and CE.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[2] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984* (IEEE Computer Society Press, Los Alamitos, CA, 1985), p. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] M. Hillery, V. B ŭ zek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[5] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[6] G. R. Blakley, in *Proceedings of the National Computer Conference*, Arlington, VA, 1979 (American Federation of Information Processing, Montvale, NJ, 1979), pp.313–317.
[7] A. Shamir, Commun. ACM **22**, 612 (1979).
[8] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[9] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **53**, R1209 (1996).
[10] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Rev. A **76**, 062324 (2007).
[11] D. Greenberger, M. Horne, and A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer Academic, Dordrecht, 1989).
[12] L. Xiao, G.-L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).
[13] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).
[14] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[15] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[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, and S.-J. Lee, e-print arXiv:0801.0177.