Optics Communications 281 (2008) 4803–4806

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Improving the total efficiency of quantum key distribution by comparing Bell states

Hao Yuan [a,*], Jun Song [a], Lian-fang Han [b], Kui Hou [c], Shou-hua Shi [c]

[a] Department of Mathematics and Physics, West Anhui University, Lu'an 237012, China
[b] Teaching and Research Section of Physics, School of Basic Medical Science, Anhui Medical University, Hefei 230032, China
[c] School of Physics and Material Science, Anhui University, Hefei 230039, China

ARTICLE INFO

Article history:
Received 28 January 2008
Received in revised form 8 April 2008
Accepted 6 June 2008

PACS:
03.67.Dd
03.65.Ud

Keywords:
Quantum key distribution
Entanglement swapping
Bell states comparison
Total efficiency

ABSTRACT

A protocol for quantum key distribution by comparing Bell states [G. Gao, Opt. Commun. 281 (2008) 876] is recently proposed by Gan Gao. Gan Gao claimed that his protocol has the advantage of high total efficiency and its total efficiency is 50%. In this paper, by giving a little modification to the original one, we introduce an improved version of Gao's protocol, which can make the total efficiency of the communication come up to 100%.

The combination of the principles of quantum systems with cryptograph has produced a novel and interesting field named quantum cryptograph [1,2]. Quantum key distribution (QKD) is an important branch of quantum cryptograph, in which two remote legitimate users (Alice and Bob) can establish a shared secret key through the transmission of quantum signals. Its ultimate advantage is the unconditional security, the feat in cryptography. Hence, since Bennett and Brassard presented the pioneering work in 1984 [1], a variety of QKD protocols [1–12] have been proposed. For example, in 1992, Bennett et al. [2] proposed a famous QKD protocol named as BBM92 QKD protocol based on single particles. Latter, Bennett and Wiesner [3] put forward another QKD protocol via one- and two-particle operators on Einstein–Podolsky–Rosen (EPR) states. In 2000, Cabello presented a QKD protocol [4] using polarized photons and another QKD protocol [5] without alternative measurements based on entanglement swapping between EPR pairs. In 2002, Long and Liu [6] proposed a two-step highly efficient QKD protocol utilizing EPR pairs. In 2003, Deng and Long [7] put forward a novel QKD protocol based on the controlled order rearrangement operation. In 2004, Wang [8] proposed a prepare-and-measure QKD scheme with two-qubit quantum codes. Later Song [9] introduced two QKD schemes achieved by swapping quantum entanglement. In the same year, Deng and Long [10] presented a two-way QKD protocol with practical faint laser pulses. In 2005, Key et al. [11] proposed a new QKD scheme using the blind polarization basis.

Very recently, based on entanglement swapping, Gao [12] put forward a novel QKD protocol. The distinct advantage of Gao's QKD protocol is that during the final course of generating key, Alice (the preparer of quantum resource) possesses the initiative with some degree. However, in Gao's QKD protocol, the creating of a shared secret key must need some additional classical information and the total efficiency is only 50%. In this paper, by giving a little modification to Gao's QKD protocol, we introduce an improved version of Gao's QKD protocol. Different from the original Gao's QKD protocol, in the present improved protocol the two legitimate communicators can share a secret key without exchanging any classical information and the total efficiency of the communication can come up to 100%, twice as high as that in the original Gao's QKD protocol.

Before presenting the improved Gao's protocol, let us describe the property of the quantum entanglement swapping (ES) [5,9,12–28] simply which will be used later. Let $|0\rangle$ and $|1\rangle$ be the up and down eigenstates of the Pauli operator σ_z, and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ be the up and down eigenstates of the Pauli operator σ_x. $|0\rangle$ and $|1\rangle$ compose of $\mathscr{Z}$-basis and $|+\rangle$ and $|-\rangle$ compose of $\mathscr{X}$-basis. A typical kind of entanglement is the four Bell states ψ^+, ψ^-, ϕ^+ and ϕ^-, which are defined as follows:

* Corresponding author.
E-mail address: yuanhao@wxc.edu.cn (H. Yuan).

0030-4018/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2008.06.010

$$\psi_{12}^{+} = (|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)/\sqrt{2} = (|+\rangle_1|+\rangle_2 - |-\rangle_1|-\rangle_2)/\sqrt{2}, \quad (1)$$

$$\psi_{12}^{-} = (|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2)/\sqrt{2} = (|-\rangle_1|+\rangle_2 - |+\rangle_1|-\rangle_2)/\sqrt{2}, \quad (2)$$

$$\phi_{12}^{+} = (|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)/\sqrt{2} = (|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2)/\sqrt{2}, \quad (3)$$

$$\phi_{12}^{-} = (|0\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2)/\sqrt{2} = (|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2)/\sqrt{2}, \quad (4)$$

where the subscripts 1 and 2 denote the two entangled photons. These four states form a complete orthogonal basis, i.e., Bell-basis. Incidently, it is easily verified that the four Bell states can be transformed into each other by performing the four local unitary operators U_{00}, U_{01}, U_{10} and U_{11} on any one photon of EPR pair in Bell state, where $U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_{01} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $U_{10} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and $U_{11} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Suppose the two distant parties, Alice and Bob, share two EPR pairs. Let the initial state of the two EPR pairs be the product of any two of the four Bell states, such as ψ_{12}^{-} and ϕ_{34}^{+}, Alice has photons 1 and 3, and Bob possesses 2 and 4. If Alice performs a Bell-basis measurement on photons 1 and 3 or Bob performs a Bell-basis measurement on photons 2 and 4, then the entanglement between photons 1 and 2, and 3 and 4 can be swapped into the entanglement between 1 and 3, and 2 and 4, which can been seen from the following process:

$$\begin{aligned}\psi_{12}^{-} \otimes \phi_{34}^{+} &= \frac{1}{2}(|01\rangle - |10\rangle)_{12}(|00\rangle + |11\rangle)_{34} \\ &= \frac{1}{2}(|0100\rangle + |0111\rangle - |1000\rangle - |1011\rangle)_{1234} \\ &= \frac{1}{2}(|0010\rangle + |0111\rangle - |1000\rangle - |1101\rangle)_{1324} \\ &= \frac{1}{2}(\phi_{13}^{-}\psi_{24}^{+} + \psi_{13}^{-}\phi_{24}^{+} - \phi_{13}^{+}\psi_{24}^{-} - \psi_{13}^{+}\phi_{24}^{-}). \end{aligned} \quad (5)$$

Obviously, the present state of the whole system is changed into one of the following states with equal possibility, i.e., $\phi_{13}^{-}\psi_{24}^{+}$, $\psi_{13}^{-}\phi_{24}^{+}$, $\phi_{13}^{+}\psi_{24}^{-}$ or $\psi_{13}^{+}\phi_{24}^{-}$. If Alice and Bob share other initial Bell states, the possible results of ES by similar deduction can be summarized in Table 1.

Now, let us start with the brief description of Gao's QKD protocol. In Gao's QKD protocol, there are two legitimate parties, say Alice and Bob. Alice prepares a batch of ordered EPR pairs and each EPR pair may be randomly in one of the four Bell states. She takes one photon from each EPR pair to form an ordered photon sequence, say S_h. The remaining EPR partner photons form another ordered photon sequence, say S_t. Alice sends S_t to Bob and retains S_h in her site. After receiving S_t, Bob selects randomly a number of the photons from S_t and tells Alice which photons he has chosen. Then Bob chooses randomly one of the two measuring bases, i.e., $\mathscr{Z}$-basis or $\mathscr{X}$-basis, to measure the chosen photons. Subsequently, Bob tells Alice which measuring basis he has chosen for each photon and the results of his measurements. Alice uses the same measuring basis as Bob to measure the corresponding photons in the S_h and checks with the results of Bob. According to Eqs. (1)–(4), their measurement results should be correlated. If the error rate is high, Alice and Bob discard their transmission and abort the communication. Otherwise, they continue to next communication procedure. That is, Alice and Bob take two EPR pairs to form one group and divide these remaining EPR pairs into several groups. Suppose two EPR pairs in one group are prepared in ψ_{12}^{-} and ϕ_{34}^{+}, respectively. The photons 1 and 3 belong to Alice and the photons 2 and 4 belong to Bob. Alice and Bob performs Bell state measurements on the photons 1 and 3, and 2 and 4, respectively. The measurement results may be one of the four states $\phi_{13}^{-}\psi_{24}^{+}$, $\psi_{13}^{-}\phi_{24}^{+}$, $\phi_{13}^{+}\psi_{24}^{-}$ and $\psi_{13}^{+}\phi_{24}^{-}$. Without loss of generality, assuming their measurement results are ψ_{13}^{+} and ϕ_{24}^{-}, respectively. Then Alice publicly tells Bob one of the two initial states ψ_{12}^{-} or ϕ_{34}^{+}. Suppose the published state is ψ_{12}^{-}, then Bob can get a relation between the published state ψ_{12}^{-} and his measurement result ϕ_{24}^{-}, i.e., $\psi^{-} \leftrightarrow U_{01}\phi^{-}$. Similarly, Alice can get a relation between the un-published state ϕ_{34}^{+} and her measurement result ψ_{13}^{+}, i.e., $\phi^{+} \leftrightarrow U_{01}\psi^{+}$. Obviously, the comparison outcomes between published (un-published) state and measurement results on both sides are entirely identical. Alice and Bob agree on beforehand that the four local unitary operators U_{00}, U_{01}, U_{10} and U_{11} are encoded into the two-bit classical information 00, 01, 10 and 11, respectively. Therefore, the secret key 01 has been shared between Alice and Bob. The other case can be deduced by the similar way.

From the above brief review of Gao's QKD protocol, one can see that the quantum resources are all prepared by Alice and Alice's publications of one of her initial Bell states in a group to Bob are necessary. To simplify the process and improve the efficiency of Gao's QKD protocol, we make a modification on it. In the present modified protocol, the quantum resources are prepared by both Alice and Bob together, and no additional classical information (except for that used to check eavesdropping) are required. Now let us describe the details of the improved Gao's QKD protocol. Suppose there are two remote legitimate communicators, Alice and Bob. They want to share n two-bit secret key in the ideal quantum channel, which may be implemented by the following five-step scheme.

Step 1 : Alice prepares a sequence of $n + \delta$ ordered EPR pairs $\mathscr{A}$. Each EPR pair is randomly in one of the four Bell states, which is only known to Alice herself. We denote the $n + \delta$ ordered EPR pairs in the sequence $\mathscr{A}$ with $\{(a_1^1, a_2^1), (a_1^2, a_2^2), \ldots, (a_1^{n+\delta}, a_2^{n+\delta})\}$, here the superscripts 1, 2, …, $n + \delta$ indicate the order of each EPR photon pair in the sequence $\mathscr{A}$, and the subscripts 1 and 2 represent the different photons in any one EPR pair, respectively. Subsequently, Alice takes the photon 1 from each EPR pairs in the sequence $\mathscr{A}$ to form an ordered photon sequence, say, $\{a_1^1, a_1^2, \ldots, a_1^{n+\delta}\}$. It is called the sequence $\mathscr{A}_1$. The remaining partner photon compose of another ordered photon sequence $\{a_2^1, a_2^2, \ldots, a_2^{n+\delta}\}$, say sequence $\mathscr{A}_2$. Bob also prepares an ordered $n + \delta$ EPR pair sequence, say, $\{(b_1^1, b_2^1), (b_1^2, b_2^2), \ldots, (b_1^{n+\delta}, b_2^{n+\delta})\}$. It is called sequence $\mathscr{B}$. Each EPR pair in the sequence $\mathscr{B}$ may be in arbitrary Bell state, and none but Bob himself knows the states of his prepared EPR pairs. Then Bob takes a photon from each EPR pair to form two ordered photon sequence $\mathscr{B}_1$ and $\mathscr{B}_2$, e.g. $\mathscr{B}_1 = \{b_1^1, b_1^2, \cdots, b_1^{n+\delta}\}$ and $\mathscr{B}_2 = \{b_2^1, b_2^2, \cdots, b_2^{n+\delta}\}$.

Step 2 : Alice sends sequence $\mathscr{A}_2$ to Bob and retains sequence $\mathscr{A}_1$ in her site. Similarly, Bob sends sequence $\mathscr{B}_1$ to Alice and retains sequence $\mathscr{B}_2$ in his site. Then Alice and Bob each publicly confirm that the other received the qubits.

Step 3 : To guarantee the security of the whole communication process, Alice and Bob should check whether the sequences $\mathscr{A}_2$ and $\mathscr{B}_1$ are eavesdropped during the

Table 1
The corresponding relations between the two initial Bell states (TIBSs) and the two possible output Bell states (TPOBSs) after the ES

TIBSs				TPOBSs			
$\{\psi_{12}^{+}, \psi_{34}^{+}\}$	$(\{\psi_{12}^{-}, \psi_{34}^{-}\},$	$\{\phi_{12}^{+}, \phi_{34}^{+}\},$	$\{\phi_{12}^{-}, \phi_{34}^{-}\})$	$\{\psi_{13}^{+}, \psi_{24}^{+}\}$	$\{\psi_{13}^{-}, \psi_{24}^{-}\}$	$\{\phi_{13}^{+}, \phi_{24}^{+}\}$	$\{\phi_{13}^{-}, \phi_{24}^{-}\}$
$\{\psi_{12}^{+}, \psi_{34}^{-}\}$	$(\{\psi_{12}^{-}, \psi_{34}^{+}\},$	$\{\phi_{12}^{+}, \phi_{34}^{-}\},$	$\{\phi_{12}^{-}, \phi_{34}^{+}\})$	$\{\psi_{13}^{+}, \psi_{24}^{-}\}$	$\{\psi_{13}^{-}, \psi_{24}^{+}\}$	$\{\phi_{13}^{+}, \phi_{24}^{-}\}$	$\{\phi_{13}^{-}, \phi_{24}^{+}\}$
$\{\psi_{12}^{+}, \phi_{34}^{+}\}$	$(\{\psi_{12}^{-}, \phi_{34}^{-}\},$	$\{\phi_{12}^{+}, \psi_{34}^{+}\},$	$\{\phi_{12}^{-}, \psi_{34}^{-}\})$	$\{\psi_{13}^{+}, \phi_{24}^{+}\}$	$\{\psi_{13}^{-}, \phi_{24}^{-}\}$	$\{\phi_{13}^{+}, \psi_{24}^{+}\}$	$\{\phi_{13}^{-}, \psi_{24}^{-}\}$
$\{\psi_{12}^{+}, \phi_{34}^{-}\}$	$(\{\psi_{12}^{-}, \phi_{34}^{+}\},$	$\{\phi_{12}^{+}, \psi_{34}^{-}\},$	$\{\phi_{12}^{-}, \psi_{34}^{+}\})$	$\{\psi_{13}^{+}, \phi_{24}^{-}\}$	$\{\psi_{13}^{-}, \phi_{24}^{+}\}$	$\{\phi_{13}^{+}, \psi_{24}^{-}\}$	$\{\phi_{13}^{-}, \psi_{24}^{+}\}$

transmission. Here, we only give the checking procedure of sequence $\mathscr{A}_2$. The checking procedure of sequence $\mathscr{B}_1$ is similar to that of sequence $\mathscr{A}_2$. The detailed checking procedure of sequence $\mathscr{A}_2$ is: (i) Bob chooses δ photons randomly in the sequence $\mathscr{A}_2$ and tells Bob the positions of chosen photons via the classical channel. (ii) For each of the δ chosen photons, Bob measures it in $\mathscr{Z}$ basis or $\mathscr{X}$ basis at random. (iii) Bob tells Alice which measuring basis he has chosen for each photon and the outcomes of his measurements. (iv) Alice uses the same measuring basis as Bob to measure the corresponding photons in the partner sequence $\mathscr{A}_1$ and checks with the results of Bob. According to Eqs. (1)–(4), their measurement results should be completely correlated if no eavesdropping exists. By comparing the outcomes of their measurements, Alice can then evaluate the error rate of the transmission of the sequence $\mathscr{A}_2$. If the error rate exceeds the threshold, they discard the transmission and the repeat quantum communication from the beginning. Otherwise, they continue to the next step.

Step 4 : Alice and Bob divide all the remaining $2n$ EPR pairs into n ordered groups $\{a_1^1, a_2^1, b_1^1, b_2^1\}$, $\{a_1^2, a_2^2, b_1^2, b_2^2\}$, …, $\{a_1^n, a_2^n, b_1^n, b_2^n\}$, and denote $\{a_1^k, a_2^k, b_1^k, b_2^k\}$ ($k = 1,2, \ldots,n$) for the four photons of the two EPR pairs in each group. Alice holds the photons a_1^k and b_1^k, and Bob holds the photons a_2^k and b_2^k.

Step 5 : Alice and Bob performs Bell-basis measurements on photons a_1^k and b_1^k, and a_2^k and b_2^k in each group, respectively. Assume Φ_{APS}, Φ_{AMR}, Φ_{BPS} and Φ_{BMR} mean Alice's preparing state, Alice's measurement result, Bob's preparing state and Bob's measurement result, respectively, in each group, then it is easily verified that if $\Phi_{\mathrm{APS}} \leftrightarrow U_{ij}\Phi_{\mathrm{AMR}}$ then $\Phi_{\mathrm{BPS}} \leftrightarrow U_{ij}\Phi_{\mathrm{BMR}}$, where U_{ij} ($i,j = 0, 1$) represents the above mentioned four local unitary operations. That is to say, by comparing the initial state and the measurement result in each group, Alice and Bob can deduce the identical unitary operation U_{ij}. Therefore, if the operation U_{ij} represents the two-bit classical secret information ij, then a new protocol for quantum key distribution can be generated.

For example, suppose Alice initially prepared $\phi^+_{a_1a_2}$ while Bob prepared $\psi^+_{b_1b_2}$. Alice and Bob performs Bell-basis measurements on photons a_1 and b_1, and a_2 and b_2, respectively. From Table 1, one can find out that there are four possible Bell measurement results: $\{\phi^+_{a_1b_1}, \psi^+_{a_2b_2}\}$, $\{\phi^-_{a_1b_1}, \psi^-_{a_2b_2}\}$, $\{\psi^+_{a_1b_1}, \phi^+_{a_2b_2}\}$ and $\{\psi^-_{a_1b_1}, \phi^-_{a_2b_2}\}$. Without loss of generality, suppose their measurements is $\phi^+_{a_1b_1}$ and $\psi^+_{a_2b_2}$. By comparing the initial preparing state $\phi^+_{a_1a_2}$ and measurement result $\phi^+_{a_1b_1}$, Alice can get the relation that $\phi^+ \leftrightarrow U_{00}\phi^+$. Similarly, Bob can get the relation that $\psi^+ \leftrightarrow U_{00}\psi^+$. Therefore, Alice and Bob will share the secret key bit "00". If the measurement result is other than $\phi^+_{a_1b_1}\psi^+_{a_2b_2}$, we can obtain the possible shared secret key (see Table 2) by the similar deduction.

So far we have expatiated an improved Gao's QKD scheme. Now we discuss it's security. The present scheme uses EPR pairs as quantum channel and it's proof for the security is based on the security for the transmission of the sequences $\mathscr{A}_1$ and $\mathscr{B}_1$. One can easily find that the transmission and the security check of the sequence $\mathscr{A}_1$ or $\mathscr{B}_2$ in the present improved scheme is in fact identical to that in BBM92 QKD protocol. The proofs of security for BBM92 in ideal condition and in practical conditions have been given in Refs. [29,30]. Therefore, our scheme is also secure.

Let us see the advantages in the present improved scheme compared to Gao's QKD protocol. In Gao's QKD protocol, in order to establish the random secret key, Alice must publish one of the two initial states of her prepared EPR pairs in each group, which will waste a large amount of classical information. However, no any additional classical information (except for the one that exchanged during checking eavesdropping) is necessary in the present improved scheme. That leads the total efficiency in the present improved scheme is higher than that in Gao's QKD protocol, which can be seen from the following calculations. For convenience of the comparing, here, we also employ the Cabello's definition of QKD efficiency [4]: $\eta = b_s/(q_t + b_t)$, where η denotes the total efficiency of a quantum communication scheme, b_s is the excepted number of the shared secret bits, q_t and b_t are the numbers of qubits transmitted and the classical bits exchanged, respectively. In the present improved scheme, $b_s = 2$, $q_t = 2$ and $b_t = 0$, as the legitimate users Alice and Bob can share two bits of secret key, while only send one photon to each other and no additional classical bits is necessary except for the one that used to check eavesdropping. Therefore, its total efficiency is $\eta_{\mathrm{our}} = 2/(2 + 0) = 100\%$ in theory. While in Gao's QKD protocol, as Gao says, since Alice must publish one of four Bell states each time, b_t should also equal to 2 bits, so the total efficiency is only $\eta_{\mathrm{Gao}} = 2/(2 + 2) = 50\%$. Obviously, $\eta_{\mathrm{our}} = 2\eta_{\mathrm{Gao}}$. Incidently, Gao claimed that the high efficiency is the advantage of his QKD protocol, i.e., the efficiency in his QKD protocol is relatively higher than the one in Ref. [9], whose total efficiency is η Ref. [9] = 33.3%. Clearly, $\eta_{\mathrm{our}} = 3\eta$ Ref. [9]. That is to say, the present improved scheme is actually more efficient.

To summarize, an improvement on Gao's QKD protocol, which makes the original version of Gao's QKD protocol become more efficient is presented. In the original version of Gao's QKD protocol, all of the qubits are only prepared by Alice herself. Different from that, in the present improved scheme, the legitimate parties, Alice and Bob collaborate with each other to produce the quantum resource. With this modification, it is not necessary for Alice to publish one of four Bell states each time, which makes the efficiency in the improved scheme come up to 100%, twice as high as that in the original version of Gao's QKD protocol.

Table 2
If Alice's preparing state (APS) is $\phi^+_{a_1a_2}$ and Bob's preparing state (BPS) is $\psi^+_{b_1b_2}$, then the possible Alice's measurement result (AMR) and Bob's measurement result (BMS), and the corresponding relations among Alice's comparison outcome (ACO), Bob's comparison outcome (BCO), and the shared secret key (SSK) can be summarized as follows

APS	AMR	ACO	BPS	BMR	BCO	SSK
$\phi^+_{a_1a_2}$	$\phi^+_{a_1b_1}$	$\phi^+ \leftrightarrow U_{00}\phi^+$	$\psi^+_{b_1b_2}$	$\psi^+_{a_2b_2}$	$\psi^+ \leftrightarrow U_{00}\psi^+$	00
$\phi^+_{a_1a_2}$	$\psi^+_{a_1b_1}$	$\phi^+ \leftrightarrow U_{01}\psi^+$	$\psi^+_{b_1b_2}$	$\phi^-_{a_2b_2}$	$\psi^+ \leftrightarrow U_{01}\phi^-$	01
$\phi^+_{a_1a_2}$	$\psi^-_{a_1b_1}$	$\phi^+ \leftrightarrow U_{10}\psi^-$	$\psi^+_{b_1b_2}$	$\phi^+_{a_2b_2}$	$\psi^+ \leftrightarrow U_{10}\phi^+$	10
$\phi^+_{a_1a_2}$	$\phi^-_{a_1b_1}$	$\phi^+ \leftrightarrow U_{11}\phi^-$	$\psi^+_{b_1b_2}$	$\psi^-_{a_2b_2}$	$\psi^+ \leftrightarrow U_{11}\psi^-$	11

References

[1] C.H. Bennett, G. Brassard, in: Proceedings of the IEEE International Conference on Computers Systems and Signal Processings, Bangalore, India, IEEE, New York, 1984, p. 175.
[2] C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. 68 (1992) 557.
[3] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881.
[4] A. Cabello, Phys. Rev. Lett. 85 (2000) 5635.
[5] A. Cabello, Phys. Rev. A 61 (2000) 052312.
[6] G.L. Long, X.S. Liu, Phys. Rev. A 65 (2002) 032302.
[7] F.G. Deng, G.L. Long, Phys. Rev. A 68 (2003) 042315.
[8] X.B. Wang, Phys. Rev. Lett. 92 (2004) 077902.
[9] D. Song, Phys. Rev. A 69 (2004) 034301.
[10] F.G. Deng, G.L. Long, Phys. Rev. A 70 (2004) 012311.
[11] W.H. Kye, C.M. Kim, M.S. Kim, Y.J. Park, Phys. Rev. Lett. 95 (2005) 040501.
[12] G. Gao, Opt. Commun. 281 (2008) 876.
[13] M. Zukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. 71 (1993) 4287.
[14] M. Koashi, N. Imoto, Phys. Rev. Lett. 79 (1997) 2383.
[15] S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A 57 (1998) 822.
[16] L. Hardy, D. Song, Phys. Rev. A 62 (2000) 052315.
[17] A. Cabello, Phys. Rev. A 64 (2001) 024301.
[18] Y.S. Zhang, C.F. Li, G.C. Guo, Phys. Rev. A 63 (2001) 036301.
[19] J.W. Pan, M. Daniell, S. Gasparoni, G. Weihs, A. Zeilinger, Phys. Rev. Lett. 86 (2001) 4435.

[20] J. Lee, S. Lee, J. Kim, S.D. Oh, Phys. Rev. A 70 (2004) 032305.
[21] Z.J. Zhang, Z.X. Man, Int. J. Quantum Inf. 2 (2004) 521.
[22] Z.X. Man, Z.J. Zhang, Y. Li, Chin. Phys. Lett. 22 (2005) 18.
[23] Z.J. Zhang, Y.M. Liu, Z.X. Man, Commun. Theor. Phys. 44 (2005) 847.
[24] Z.J. Zhang, J. Yang, Z.X. Man, Y. Li, Eur. Phys. J. D 33 (2005) 133.
[25] Z.J. Zhang, Z.X. Man, Phys. Rev. A 72 (2005) 022303.
[26] Z.X. Man, Y.J. Xia, J. Phys. B39 (2006) 3855.
[27] Y. Chen, Z.X. Man, Y.J. Xia, Chin. Phys. Lett. 24 (2007) 19.
[28] Z.X. Man, Y.J. Xia, J. Phys. B 40 (2007) 1767.
[29] H. Inamori, L. Rallan, V. Vedral, J. Phys. A 34 (2001) 6913.
[30] E. Waks, A. Zeevi, Y. Yamamoto, Phys. Rev. A 65 (2002) 052310.