# Quantum secure direct communication network with hyperentanglement*

Chang Ho Hong[a)b)], Jino Heo[a)b)], Jong In Lim[a)b)], and Hyung Jin Yang[a)b)c)d)†]

[a)] *Graduate School of Information Management and Security, Korea University, Seoul* 136-701, *Korea*
[b)] *Center for Information Security Technologies (CIST), Korea University, Seoul* 136-701, *Korea*
[c)] *Department of Physics, Korea University, Yeongi* 339-700, *Korea*
[d)] *Graduate School of Information Security (GSIS), Korea University, Seoul* 136-701, *Korea*

(Received 5 December 2013; revised manuscript received 8 April 2014; published online 9 July 2014)

We propose a quantum secure direct communication protocol with entanglement swapping and hyperentanglement. Any two users, Alice and Bob, can communicate with each other in a quantum network, even though there is no direct quantum channel between them. The trust center, Trent, who provides a quantum channel to link them by performing entanglement swapping, cannot eavesdrop on their communication. This protocol provides a high channel capacity because it uses hyperentanglement, which can be generated using a beta barium borate crystal.

**Keywords:** quantum secure direct communication, hyperentanglement

**PACS:** 03.67.Hk, 03.67.Ac, 03.65.Ud **DOI:** 10.1088/1674-1056/23/9/090309

## 1. Introduction

Quantum physics facilitates the secure communication. For example, the no-cloning theorem[1] of quantum mechanics provides communication security because an eavesdropper cannot fully steal the information transmitted from the sender to the receiver as an unknown quantum state cannot be perfectly copied. In 1984, the first quantum key distribution (QKD) protocol was developed by Bennett and Brassard[2] with nonorthogonal single polarization states. In that protocol, legitimate users, Alice and Bob, obtain the secure keys with a 50% success probability. In 1992, Bennett proposed a simplified QKD protocol[3] with two nonorthogonal states, however its success probability was decreased to 25%. The nonlocality of an entangled state provides a good medium for a secure quantum channel. For example, in 1991, Ekert[4] presented a QKD protocol with two qubits entangled states, i.e., Bell states, and its success probability was 50%. Although the qubits are usually assumed to be spatially separated, they exhibit perfect correlations. In 2004, Song[5] proposed two QKD schemes achieved by quantum entanglement swapping. Later, Deng and Long[6] proposed a two-way QKD protocol using practical faint laser pulses. Several such studies have recently been conducted[7–12] or are underway.

In contrast to the QKD, quantum secure direct communication (QSDC) enables direct sending of secret messages without generating any keys to encrypt them. The first QSDC protocol, which was proposed by Beige *et al.*[13] allows sending secret information that could be read by using additional classical information. That QSDC protocol is used to maintain a secure communication between users without key sharing. In 2002, the ping–pong protocol was proposed by Boström and Felbinger.[14] However, it was considered insecure because two legitimate users could not detect any eavesdropper before they encoded secret messages on the quantum states.[15] In 2004, Cai *et al.* presented a QSDC protocol with single photons, and Wang *et al.* proposed a QSDC protocol[16] with superdense coding and another multi-step QSDC protocol[17] with Greenberger–Horne–Zeilinger states in 2005. Since the advent of QSDC, many QSDC protocols have been proposed, such as schemes based on single particle states,[18–20] Bell states,[21,22] and multiparticle entangled states.[23,24]

In recent years, hyperentanglement has been the primary focus of research in this field. Hyperentanglement refers to the entanglement between several degrees of freedom of photons. It can be used to increase the channel capacity[25] and to complete the Bell-state measurements in the polarization degree of freedom of photons.[26,27] Walborn *et al.*[28] proposed a hyperentanglement-assisted Bell-state measurement in the polarization of photons, which was experimentally verified by Barbieri M *et al.*[29] In 2010, Sheng *et al.*[30] proposed a scheme for deterministic entanglement purification. They also presented the first protocol with hyperentanglement in the polarization, frequency, and spatial degrees of freedom. Recently, a complete hyperentangled-Bell-state analysis (CHBSA) scheme using the cross-Kerr nonlinearity was proposed.[31] Zhao *et al.*[25] also proposed a scheme for quantum superdense coding with a hyperentangled state.

In this paper, we propose a QSDC network protocol with

*Project supported by the Ministry of Knowledge Economy, Korea, under the Information Technology Research Center (ITRC) support program (NIPA-2013-H0301-13-3007) supervised by the National IT Industry Promotion Agency, and the Research Foundation of Korea University.

†Corresponding author. E-mail: yangh@korea.ac.kr

© 2014 Chinese Physical Society and IOP Publishing Ltd 

hyperentanglement. Trent and Alice (Trent and Bob) share a hyperentangled photon pair. Alice and Bob can securely communicate with each other, after Trent establishes a quantum communication channel between them through entanglement swapping. Trent cannot access the secret message even though he establishes the quantum channel between the users. This is because he does not know the legitimate user's collapsed state after measurement, and there is no quantum channel between Trent and Alice or between Trent and Bob.

## 2. QSDC network

A hyperentanglement in the polarization and spatial mode degrees of freedom can be created using a beta barium borate (BBO) crystal and a mirror.[17,32,33] Ultraviolet light passes through the BBO crystal twice due to the presence of the mirror and produces the hyperentanglement. In the first process, correlated pairs of photons are divided into spatial modes $s_1$ and $s_2$. In the second process, the reflected correlated pairs of photons are divided into spatial modes $s_3$ and $s_4$. The process is shown in Fig. 1. The Hamiltonian of hyperentanglement reads[17,32–34]

$$H=\gamma[(s_{1\mathrm{H}}^{+}s_{2\mathrm{H}}^{+}+s_{1\mathrm{V}}^{+}s_{2\mathrm{V}}^{+})+r\mathrm{e}^{\mathrm{i}\phi}(s_{3\mathrm{H}}^{+}s_{4\mathrm{H}}^{+}+s_{3\mathrm{V}}^{+}s_{4\mathrm{V}}^{+})]+\mathrm{H.c.}, \quad (1)$$

where the subscripts H and V represent the horizontal and the vertical polarizations, respectively, $r$ is the relative probability of emission of photons into the lower modes, and $\phi$ is the phase difference between the two possibilities. We assume the ideal conditions to be $r=1$ and $\phi=0$.[17,32–34] Then, the state can be rewritten as $(s_{1\mathrm{H}}^{+}s_{2\mathrm{H}}^{+}+s_{1\mathrm{V}}^{+}s_{2\mathrm{V}}^{+}+s_{3\mathrm{H}}^{+}s_{4\mathrm{H}}^{+}+s_{3\mathrm{V}}^{+}s_{4\mathrm{V}}^{+})|0\rangle$. It can be described as

$$|\Psi_{ab}^{+}\rangle_{\mathrm{PS}}=\frac{1}{2}[(|HH\rangle+|VV\rangle)_{\mathrm{P}}\otimes(|s_1s_2\rangle+|s_3s_4\rangle)_{\mathrm{S}}]_{ab}, \quad (2)$$

where the subscripts P and S represent the polarization and the spatial mode degrees of freedom, respectively, and $s_1$, $s_2$, $s_3$, and $s_4$ represent the spatial modes for photons $a$ and $b$.

In 2010, Sheng *et al.*[31] proposed the CHBSA protocol for quantum communication by using cross-Kerr nonlinearity to construct a quantum detector. The CHBSA, which involves a complete Bell-state measurement as its name suggests, enables entanglement swapping using hyperentangled states. We suppose that pairs $A$, $B$ and $C$, $D$ are in the following hyperentangled states:

$$|\Phi_{A,B}^{+}\rangle_{\mathrm{PS}}=\frac{1}{2}[(|HH\rangle+|VV\rangle)_{\mathrm{P}}\otimes(|s_{a1}s_{b1}\rangle+|s_{a2}s_{b2}\rangle)_{\mathrm{S}}]_{A,B}, \quad (3)$$

$$|\Phi_{C,D}^{+}\rangle_{\mathrm{PS}}=\frac{1}{2}[(|HH\rangle+|VV\rangle)_{\mathrm{P}}\otimes(|s_{c1}s_{d1}\rangle+|s_{c2}s_{d2}\rangle)_{\mathrm{S}}]_{C,D}. \quad (4)$$

The subscript P denotes the polarization mode of the hyperentangled state, and the subscript S denotes the spatial mode. If Trent shares a photon pair $A$, $B$ with Alice and a pair $C$, $D$ with Bob, his CHBSA of the two particles $B$ and $C$ causes an entanglement swapping effect on the particles $A$ and $D$, as shown in Fig. 2.

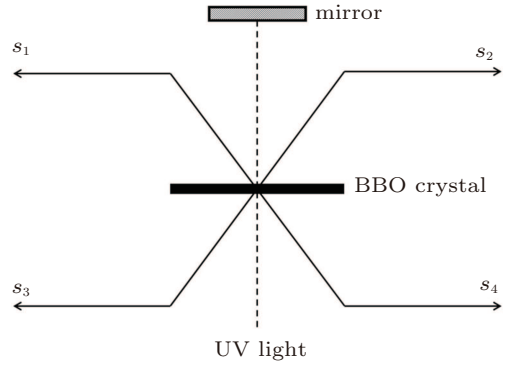



**Fig. 1.** Process for generating a hyperentanglement.

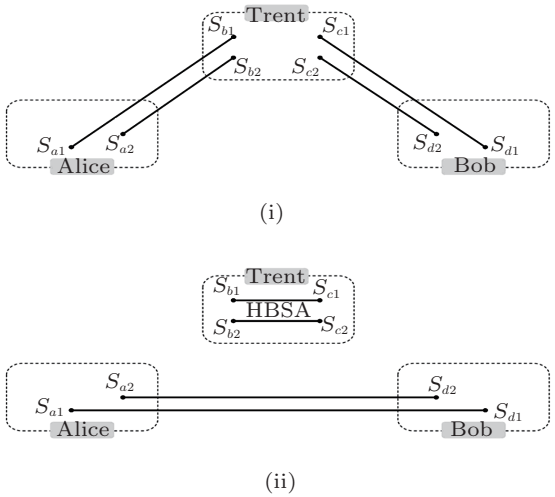



**Fig. 2.** Schematic expression of hyperentanglement swapping. The bold line denotes a hyperentangled state. After Trent's CHBSA of particles $B$ and $C$, Alice and Bob have a hyperentangled state between photons $A$ and $D$.

The total state evolves as

$$\begin{aligned}|\Phi_{A,B}^{+}\rangle_{\mathrm{PS}}\otimes|\Phi_{C,D}^{+}\rangle_{\mathrm{PS}} &= \frac{1}{4}(|HHHH\rangle+|HHVV\rangle+|VVHH\rangle+|VVVV\rangle)_{A,B,C,D}\otimes(|S_{a1}S_{b1}S_{c1}S_{d1}\rangle+|S_{a2}S_{b2}S_{c2}S_{d2}\rangle\\ &\quad+|S_{a1}S_{b1}S_{c2}S_{d2}\rangle+|S_{a2}S_{b2}S_{c1}S_{d1}\rangle)_{A,B,C,D}\\ &\xrightarrow{\mathrm{ES}}\frac{1}{4}\Big[\Big(|\phi^{+}\rangle_{\mathrm{P}}^{A,D}|\phi^{+}\rangle_{\mathrm{P}}^{B,C}+|\phi^{-}\rangle_{\mathrm{P}}^{A,D}|\phi^{-}\rangle_{\mathrm{P}}^{B,C}+|\psi^{+}\rangle_{\mathrm{P}}^{A,D}|\psi^{+}\rangle_{\mathrm{P}}^{B,C}+|\psi^{-}\rangle_{\mathrm{P}}^{A,D}|\psi^{-}\rangle_{\mathrm{P}}^{B,C}\Big)\\ &\quad\otimes\Big(|\phi^{+}\rangle_{\mathrm{S}}^{A,D}|\phi^{+}\rangle_{\mathrm{S}}^{B,C}+|\phi^{-}\rangle_{\mathrm{S}}^{A,D}|\phi^{-}\rangle_{\mathrm{S}}^{B,C}+|\psi^{+}\rangle_{\mathrm{S}}^{A,D}|\psi^{+}\rangle_{\mathrm{S}}^{B,C}+|\psi^{-}\rangle_{\mathrm{S}}^{A,D}|\psi^{-}\rangle_{\mathrm{S}}^{B,C}\Big)\Big], \end{aligned} \quad (5)$$

where

$$|\phi^{\pm}\rangle_{\rm P}^{x,y} = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle),$$
$$|\psi^{\pm}\rangle_{\rm P}^{x,y} = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$
$$|\phi^{\pm}\rangle_{\rm S}^{x,y} = \frac{1}{\sqrt{2}}(|S_{x1}S_{y1}\rangle \pm |S_{x2}S_{y2}\rangle),$$
$$|\psi^{\pm}\rangle_{\rm S}^{x,y} = \frac{1}{\sqrt{2}}(|S_{x1}S_{y2}\rangle \pm |S_{x2}S_{y1}\rangle).$$

For example, if Trent obtains the outcome $|\phi^-\rangle_{\rm P}^{B,C}|\psi^+\rangle_{\rm S}^{B,C}$, the state between Alice and Bob will be in the hyperentangled state $|\phi^-\rangle_{\rm P}^{A,D}|\psi^+\rangle_{\rm S}^{A,D}$. On the basis of this CHBSA and entanglement swapping of hyperentanglement,[31] we propose a QSDC network protocol.

Any two users among $n$ users in the network system can communicate with each other without any quantum channel linking them. This is possible because Trent's measurement entangles the quantum states of the two users and thus establishes a quantum connection between them. However, Trent, who performs entanglement swapping, cannot eavesdrop on the information of the communication between the two users. Our QSDC network protocol is explained as follows.

(i) Trent shares a sequence of ordered hyperentangled states with the legitimate users of the quantum network. For example, Trent shares $n$ hyperentanglements with Alice

$$|\Psi_{TA,A}^{+}\rangle_{\rm PS} = \frac{1}{2}[(|HH\rangle + |VV\rangle)_{\rm P} \otimes (|s_{a1}s_{a2}\rangle + |s_{a3}s_{a4}\rangle)_{\rm S}]_{TA,A}, \quad (6)$$

where $TA$ represents Trent's photons and $A$ represents Alice's photons. Trent and Bob share the state $|\Psi_{TB,B}^{+}\rangle_{\rm PS}$ in the same way as described above. The shared state between Trent and Bob is

$$|\Psi_{TB,B}^{+}\rangle_{\rm PS} = \frac{1}{2}[(|HH\rangle + |VV\rangle)_{\rm P} \otimes (|s_{b1}s_{b2}\rangle + |s_{b3}s_{b4}\rangle)_{\rm S}]_{TB,B}, \quad (7)$$

where the subscript $TB$ represents Trent's photons and the subscript $B$ represents Bob's photon. Figure 3 shows the schematic structure of the quantum network.

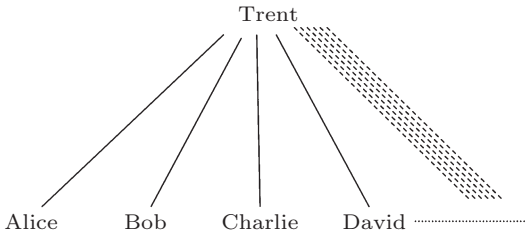



**Fig. 3.** Schematic diagram of quantum network. Each bold line represents a hyperentanglement installed between Trent and a user in the quantum network system.

(ii) Alice (Bob) requests Trent to communicate with Bob (Alice).

(iii) Trent performs the CHBSA on the two photons $TA$ and $TB$ in both polarization and spatial mode degrees of freedom. The whole state evolves as

$$\begin{aligned}|\Psi_{TA,A}^{+}\rangle_{\rm PS} \otimes |\Psi_{TB,B}^{+}\rangle_{\rm PS} &= \frac{1}{4}(|HHHH\rangle + |VVVV\rangle + |HHVV\rangle + |VVHH\rangle)_{TA,A,TB,B} \otimes (|s_{a1}s_{a2}s_{b1}s_{b2}\rangle + |s_{a3}s_{a4}s_{b3}s_{b4}\rangle \\ &\quad + |s_{a1}s_{a2}s_{b3}s_{b4}\rangle + |s_{a3}s_{a4}s_{b1}s_{b2}\rangle)_{TA,A,TB,B} \\ &\xrightarrow{\text{HBSA(ES)}} \frac{1}{4}\left(|\phi^+\rangle_{\rm P}^{TA,TB}|\phi^+\rangle_{\rm P}^{A,B} + |\phi^-\rangle_{\rm P}^{TA,TB}|\phi^-\rangle_{\rm P}^{A,B} + |\psi^+\rangle_{\rm P}^{TA,TB}|\psi^+\rangle_{\rm P}^{A,B} + |\psi^-\rangle_{\rm P}^{TA,TB}|\psi^-\rangle_{\rm P}^{A,B}\right) \\ &\quad \otimes \left(|\phi^+\rangle_{\rm S}^{TA,TB}|\phi^+\rangle_{\rm S}^{A,B} + |\phi^-\rangle_{\rm S}^{TA,TB}|\phi^-\rangle_{\rm S}^{A,B} + |\psi^+\rangle_{\rm S}^{TA,TB}|\psi^+\rangle_{\rm S}^{A,B} + |\psi^-\rangle_{\rm S}^{TA,TB}|\psi^-\rangle_{\rm S}^{A,B}\right). \quad (8)\end{aligned}$$

We denote the two-photon entangled states in the polarization and spatial mode degrees of freedom as

$$|\phi^{\pm}\rangle_{\rm P}^{TA,TA(A,B)} = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle),$$
$$|\psi^{\pm}\rangle_{\rm P}^{TA,TA(A,B)} = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$
$$|\phi^{\pm}\rangle_{\rm S}^{TA,TB(A,B)} = \frac{1}{\sqrt{2}}(|s_{a1(a2)}s_{b1(b2)}\rangle \pm |s_{a3(a4)}s_{b3(b4)}\rangle),$$
$$|\psi^{\pm}\rangle_{\rm S}^{TA,TB(A,B)} = \frac{1}{\sqrt{2}}(|s_{a1(a2)}s_{b3(b4)}\rangle \pm |s_{a3(a4)}s_{b1(b2)}\rangle). \quad (9)$$

If Trent's outcome of entanglement swapping is $|\phi^+\rangle_{\rm P}^{TA,TB}|\psi^+\rangle_{\rm S}^{TA,TB}$, the quantum state of the channel between Alice and Bob will be in the hyperentangled state $|\phi^+\rangle_{\rm P}^{A,B}|\psi^+\rangle_{\rm S}^{A,B}$.

(iv) Trent, Alice, and Bob check the security of the quantum channels. Bob randomly chooses some photons from his photon pool and measures them using one of the two measuring bases, say, $Z$ and $X$. Here, $Z = Z_{\rm P} \otimes Z_{\rm S}$ and $X = X_{\rm S} \otimes X_{\rm P}$ with $Z_{\rm P} = \{|H\rangle, |V\rangle\}$, $Z_{\rm S} = \{|s_{b2}\rangle, |s_{b4}\rangle\}$, $X_{\rm P} = \{(|H\rangle \pm |V\rangle)/\sqrt{2}\}$, and $X_{\rm S} = \{(|s_{b2}\rangle \pm |s_{b4}\rangle)/\sqrt{2}\}$, as described in Ref. [35]. After Bob has measured the checking photons, he publicly announces his outcomes and measuring basis. Trent reveals the corresponding pair's CHBSA outcomes. Then, Alice chooses the same measuring basis as Bob's to measure her photons, which are correlated to the photons measured by Bob. Alice estimates the error rate of the checking photons to determine whether there is an eavesdropper. If their outcomes correlate, they can continue to the next

step in the QSDC protocol. Otherwise, they abort their communication.

(v) Alice encodes her secret message on photon $A$ in the polarization degree of freedom, and Bob does the same on photon $B$ in the spatial mode degree of freedom. The encoding operations are $U_i^{\rm P}$ and $U_j^{\rm S}$ $(i,j=0,1)$, respectively. Here,

$$\begin{aligned} U_0^{\rm P} &= |H\rangle\langle H| + |V\rangle\langle V|, \\ U_1^{\rm P} &= |H\rangle\langle V| + |V\rangle\langle H|, \\ U_0^{\rm S} &= |s_{b2}\rangle\langle s_{b2}| + |s_{b4}\rangle\langle s_{b4}|, \\ U_1^{\rm S} &= |s_{b2}\rangle\langle s_{b4}| + |s_{b4}\rangle\langle s_{b2}|. \end{aligned} \tag{10}$$

(vi) Alice and Bob measure their own photons using the measuring basis $Z = Z_{\rm P} \otimes Z_{\rm S}$. Alice reveals her measurement's outcome only in the polarization degree of freedom to Bob, and in turn, Bob reveals his results only in the spatial mode degree of freedom to Alice. Finally, both Alice and Bob can recover each other's messages using their own encoding operations and the announced information.

For example, let us suppose that Alice's message is "0", Bob's message is "1", and Trent's CHBSA result is

$$\begin{aligned} &|\psi^-\rangle_{\rm P}^{TA,TB}|\phi^-\rangle_{\rm S}^{TA,TB} \\ &= \frac{1}{2}(|HV\rangle - |VH\rangle)_{\rm P}^{TA,TB} \otimes (|s_{a1}s_{b1}\rangle - |s_{a3}s_{b3}\rangle)_{\rm S}. \end{aligned} \tag{11}$$

Then, the channel state between Alice and Bob is

$$\begin{aligned} &|\psi^-\rangle_{\rm P}^{A,B}|\phi^-\rangle_{\rm S}^{A,B} \\ &= \frac{1}{2}(|HV\rangle - |VH\rangle)_{\rm P}^{A,B} \otimes (|s_{a2}s_{b2}\rangle - |s_{a4}s_{b4}\rangle)_{\rm S}. \end{aligned} \tag{12}$$

When Alice's announced outcome is $|H\rangle_{\rm P}$, Bob deduces her message "0" with his own measurement result $|V\rangle_{\rm P}$. Similarly, Alice infers Bob's message "1" using her own outcome $|s_{b2}\rangle_{\rm S}$ and Bob's published result $|s_{a4}\rangle_{\rm S}$.

The security checking method in step (iv) is similar to the procedures employed in the BBM92 protocol[36] in which the legitimate users can check the security of the channels using single-photon measurements. The unconditional security of the BBM92 protocol in both ideal and practical conditions has been proved in Refs. [37] and [38]. In principle, the security of our protocol is the same as that of the BBM92 protocol. Furthermore, the network center, Trent, cannot acquire any information about the user's messages because he does not know Alice's and Bob's collapsed outcomes obtained using single-photon measurements. That is, our network protocol is secure in principle. If the noise in quantum channels intervenes, the QSDC protocol requires additional techniques for security. In noisy environments, the prepared states are generally only partially entangled. It is important to reduce the effects of noise and decoherence on communication systems. There are two ways to recoup maximally entangled channels from partially entangled states: entanglement purification[16,30,31,39–43] and entanglement concentration.[44–49] Recently, a hyperentanglement purification and concentration protocol using linear optics was proposed[50] by Ren and Deng. Luo *et al.*[51] also presented a practical hyperentanglement concentration scheme. Because communicating users are spatially separated, after preparation and distribution, the parties may share an ensemble of noisy hyperentangled states. In order to share a perfect quantum channel, the noisy hyperentangled states are first purified using a hyperentanglement purification and concentration protocol, followed by some tests on the security of the quantum channel, as in step (iv). Once the security of the quantum channel is guaranteed, then no information is leaked to an eavesdropper.

## 3. Conclusion

In summary, we proposed a QSDC network with hyperentanglement in the polarization and the spatial mode degrees of freedom. Our protocol can be used to exchange secret messages simultaneously. It uses a two-photon entangled state to transmit two bits of information. The prominent feature of our protocol is that any two users among $n$ members can communicate with each other without a quantum channel linking them directly. This is possible because the communication center, Trent, can establish quantum connections between those two users through entanglement swapping. Trent, who generates the quantum channels, cannot eavesdrop on the communication between two users. Any subscriber of the network needs only the single-photon measurement for decoding. Trent's CHBSA ability is also experimentally feasible.[31]

## References


[1] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[2] Bennett C H and Brassad G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, December 10–12, 1984 Bangalore, India p. 175
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 66
[5] Song D 2004 *Phys. Rev. A* **69** 034301
[6] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311
[7] Gisin N, Ribordy R, Tittel W and Zbindenet H 2002 *Rev. Mod. Phys.* **74** 145
[8] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[9] Ling G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[10] Hong C H, Heo J O, Khym G L, Lim J I, Hong S K and Yang H J 2010 *Opt. Commun.* **283** 2644
[11] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[12] Deng F G, Xiao L and Long G L 2002 *Chin. Phys. Lett.* **19** 893
[13] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol. A* **101** 357
[14] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[15] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. Chin.* **2** 251
[16] Wang C, Deng F G, Li Y S, Zhou P and Zhou H Y 2005 *Phys. Rev. A* **71** 044305
[17] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

[18] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[19] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[20] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett. A* **358** 256
[21] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[22] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev. A* **73** 022338
[23] Lee H Y, Lim J I and Yang H J 2006 *Phys. Rev. A* **73** 042305
[24] Jin X R, Ji X, Zhang Y Q, Zhang S, Hong S K, Yeon K H and Um C I 2006 *Phys. Lett. A* **354** 67
[25] Zhao R T, Guo Q, Chen L, Wang H F and Zhang S 2012 *Chin. Phys. B* **21** 080303
[26] Wei T C, Barreiro J T and Kwiat P G 2007 *Phys. Rev. A* **75** 060305
[27] Schuck C, Huber G, Kurtsiefer C and Weinfurter H 2006 *Phys. Rev. Lett.* **96** 190501
[28] Walborn S P, Padua S and Monken C H 2003 *Phys. Rev. A* **68** 042313
[29] Barbieri M, Vallone G, Mataloni P and Martini F D 2007 *Phys. Rev. A* **75** 042317
[30] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **81** 032307
[31] Sheng Y B, Deng F G and Long G L 2010 *Phys. Rev. A* **82** 032318
[32] Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **77** 042308
[33] Simon C and Pan J W 2002 *Phys. Rev. Lett.* **89** 257901
[34] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[35] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[36] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[37] Waks E, Zeevi A and Yamamoto Y 2002 *Phys. Rev. A* **65** 052310
[38] Inamori H, Rallan L and Vedral V 2001 *J. Phys. A* **34** 6913
[39] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
[40] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[41] Deng F G 2011 *Phys. Rev. A* **83** 062316
[42] Sheng Y B, Zhou L and Long G L 2013 *Phys. Rev. A* **88** 022302
[43] Zheng Y Z, Guo G C and Ye P 2004 *Chin. Phys. Lett.* **21** 9
[44] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 *Phys. Rev. A* **53** 2046
[45] Yamamoto T, Koashi M and Imoto N 2001 *Phys. Rev. A* **64** 012304
[46] Zhao Z, Yang T, Chen Y A, Zhang A N and Pan J W 2003 *Phys. Rev. Lett.* **90** 207901
[47] Deng F G 2012 *Phys. Rev. A* **85** 022311
[48] Du F F, Li T, Ren B C, Wei H R and Deng F G 2012 *J. Opt. Soc. Am. B* **29** 1399
[49] Wang T J and Long G L 2013 *2013 J. Opt. Soc. Am. B* **30** 1069
[50] Ren B C and Deng F G 2013 *Laser Phys. Lett.* **10** 115201
[51] Luo M X, Chen X B, Yang Y X, Qu Z G and Wang X 2014 *J. Opt. Soc. Am. B* **31** 67