A two-step quantum secure direct communication protocol with hyperentanglement*

Gu Bin(顾 斌)[a)b)†], Huang Yu-Gai(黄余改)[c)], Fang Xia(方 夏)[c)], and Zhang Cheng-Yi(张成义)[a)b)]

[a)] *College of Mathematics and Physics, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*
[b)] *The Photonic Technology Laboratory, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*
[c)] *Jiangsu Institute of Education, Nanjing* 210013, *China*

(Received 26 April 2011; revised manuscript received 20 May 2011)

We propose a two-step quantum secure direct communication (QSDC) protocol with hyperentanglement in both the spatial-mode and the polarization degrees of freedom of photon pairs which can in principle be produced with a beta barium borate crystal. The secret message can be encoded on the photon pairs with unitary operations in these two degrees of freedom independently. This QSDC protocol has a higher capacity than the original two-step QSDC protocol as each photon pair can carry 4 bits of information. Compared with the QSDC protocol based on hyperdense coding, this QSDC protocol has the immunity to Trojan horse attack strategies with the process for determining the number of the photons in each quantum signal as it is a one-way quantum communication protocol.

Keywords: quantum secure direct communication, two-step, hyperentanglement, high capacity

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.1088/1674-1056/20/10/100309

Quantum communication is a wonderful technique in the security of information transmission and has attracted a lot of attention in the last 2 decades. For example, quantum key distribution (QKD) provides an absolutely secure tool for two legitimate users to produce a private key.[1−4] Recently, quantum secure direct communication (QSDC), a new concept, was proposed[4,5] and pursued.[6−33] The Long–Liu quantum communication protocol[4] (the efficient-QSDC protocol) proposed in 2002 is the first QSDC protocol where secret message can be transmitted directly, and another QSDC protocol, the two-step scheme, was proposed by Deng, Long, and Liu[5] in 2003 exploiting the quantum dense coding operations. Also, they refer to the branch of quantum communication in a deterministic way as quantum secure direct communication clearly in the two-step scheme.[5] Moreover, Deng and Long gave a criterion for QSDC.[5,6,11,13] According to Deng–Long criterion,[13] the ping–pong protocol proposed by Boström and Felbinger[7] in 2002 is insecure and its insecurity comes from the fact that the two legitimate users cannot find an eavesdropper, say Eve before they encode the secret message on the quantum states. In 2003, Wójcik[34] showed that the ping–pong scheme can be attacked when the transmission efficiencies are low. In 2004, Cai and Li[18] proposed a deterministic quantum communication protocol with single photons. In 2004, Deng and Long[6] introduced a secure communication protocol with a quantum one-time pad based on a sequence of single-photon polarization states. In 2005, Wang *et al.* proposed a QSDC protocol[9] with superdense coding and another multi-step QSDC protocol[10] with Greenberger–Horne–Zeilinger (GHZ) states. The former is the generalization of the two-step QSDC protocol[5] into a high-dimensional entangled system. In 2007, Li *et al.*[12] proposed a QSDC with quantum encryption. In 2009, Qin *et al.*[14] proposed a QSDC protocol over collective amplitude damping channel. Recently, we[15] proposed a robust quantum one-time-pad scheme over a collective noise. There is another branch of quantum direct communication, named deterministic secure quantum communication (DSQC),[13] which is also considered as QSDC in previous works.[16−33] With some other quantum techniques,[35−38] QSDC may be very useful in future.

In recent years, hyperentanglement, the entanglement of photons in several degrees of freedom, has attracted a great deal of attention. For example, in 2002

*Project supported by the Natural Science Foundation of Jiangsu Provincial Universities, China (Grant No. 10KJB180004).
†Corresponding author. E-mail: gubin@nuist.edu.cn
© 2011 Chinese Physical Society and IOP Publishing Ltd

Simon and Pan[39] exploited the hyperentanglement in the spatial-mode and the polarization degrees of freedom to purify the polarization entanglement of a photon pair from a parametric down-conversion (PDC) source. In 2009, Sheng *et al.*[40] also exploited the hyperentanglement in the spatial-mode and the polarization degrees of freedom to purify a PDC source. Xiao *et al.*[41] and Wang *et al.*[42] exploited the entanglement in frequency degree of freedom to purify the entanglement in a polarization degree of freedom. In 2010, Sheng and Deng[43,44] proposed two deterministic entanglement purification protocols with hyperentanglement. With the hyperentangled state in both polarization and orbital angular momentum, Barreiro *et al.*[45] overcame the channel capacity limit for superdense coding in 2008. In 2009, Wang *et al.*[46] proposed a high-capacity QKD protocol using both polarization and differential phase shifts of photons. In 2010, Sheng *et al.*[47] proposed a complete hyperentangled-Bell-state analysis (CHBSA) protocol for quantum communication, by resorting to cross-Kerr nonlinearity to construct a quantum nondemolition detector. More recently, Wang *et al.*[48] proposed a hyperdense coding protocol and a QSDC protocol with hyperentanglement and CHBSA.

In the present paper, we propose a two-step QSDC with hyperentanglement in both the spatial-mode and the polarization degrees of freedom of photon pairs by following some ideas in the original two-step QSDC scheme.[5] The hyperentanglement can in principle be produced with a beta barium borate (BBO) crystal and a mirror. A sequence of photon pairs in a hyperentangled Bell state is divided into two photon sequences. Each sequence is composed of photons chosen from each photon pair. The sender, Alice, encodes her secret message independently on the photon pairs with unitary operations in the spatial-mode and the polarization degrees of freedom. This QSDC protocol has a higher capacity than the original two-step QSDC protocol[15] as each photon pair can carry four bits of information. Compared with the QSDC protocol based on hyperdense coding,[48] this protocol is immune to Trojan horse attack strategies as it is a one-way quantum communication protocol.

As pointed out in Refs. [39], [40], and [44], a hyperentangled state in the polarization and the spatial-mode degrees of freedom can in principle be produced with a BBO crystal. In detail, a pump pulse of ultraviolet light passes through the crystal and produces correlated pairs of photons into the spatial modes a_1 and b_1; it is then reflected and traverses the crystal a second time, which produces correlated pairs of photons into the spatial modes a_2 and b_2. Its principle is shown in Fig. 1. The Hamiltonian can be approximately described as[39,40,44]

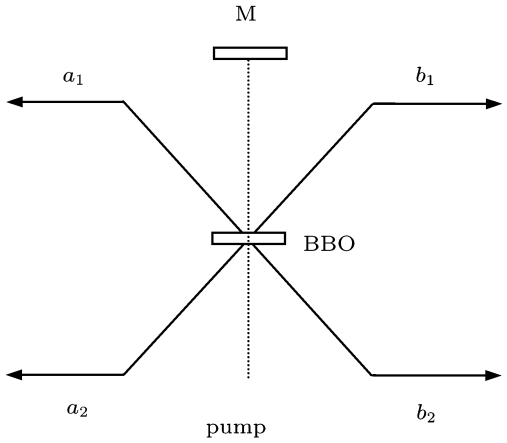


Fig. 1. Principle for producing a hyperentangled photon pair in the polarization and spatial degrees of freedom. BBO and pump represent a beta barium borate crystal and a pump pulse of ultraviolet light, respectively. M is a mirror which is used to reflect the light. a_1, a_2, b_1, and b_2 are the spatial modes for the two photons a and b.

$$H_{\rm PDC} = \gamma[(a_{1H}^{\dagger}b_{1H}^{\dagger} + a_{1V}^{\dagger}b_{1V}^{\dagger}) + r\,{\rm e}^{{\rm i}\,\phi}(a_{2H}^{\dagger}b_{2H}^{\dagger} + a_{2V}^{\dagger}b_{2V}^{\dagger})] + {\rm H.c.} \quad (1)$$

Here γ is the probability with which the nonlinear process in the BBO crystal for producing entangled photon pairs takes place, r denotes the relative probability of emission of photons between the lower spatial mode and the upper spatial mode, and ϕ is the phase between these two possibilities.[39,40,44] As indicated in Refs. [39], [40], and [44], in a simple case we assume $r = 1$ and $\phi = 0$. So the state of the photon pair can be described by $(a_{1H}^{\dagger}b_{1H}^{\dagger}+a_{1V}^{\dagger}b_{1V}^{\dagger}+a_{2H}^{\dagger}b_{2H}^{\dagger}+a_{2V}^{\dagger}b_{2V}^{\dagger})|0\rangle$. It can also be written as

$$|\Phi_{ab}^{+}\rangle_{\rm SP} = \frac{1}{2}(|a_1b_1\rangle + |a_2b_2\rangle)_{ab} \otimes (|HH\rangle + |VV\rangle)_{ab}. \quad (2)$$

Here the subscripts a and b represent the two photons in the hyperentangled state; the subscript S is the spatial-mode degree of freedom and P denotes the polarization degree of freedom; H and V are the horizontal and the vertical polarizations of photons, respectively; a_1 (b_1) and a_2 (b_2) are the spatial modes for photon a (b). If the pump pulse is faint, the four-photon state produced by this PDC source is negligible, which means that the source will produce a photon pair in the hyperentangled state $|\Phi_{ab}^{+}\rangle_{\rm SP}$.

We can describe a set of orthogonal Bell states with hyperentanglement in both the spatial-mode and the polarization degrees of freedom as follows:

$$|\Theta_{ab}\rangle_{\rm SP} = |\zeta\rangle_{\rm S} \otimes |\xi\rangle_{\rm P}, \tag{3}$$

where $|\zeta\rangle_{\rm S}$ represents one of the four Bell states in the spatial-mode degree of freedom of a photon pair, i.e.,

$$\begin{aligned} |\Phi^{\pm}\rangle_{\rm S} &= \frac{1}{\sqrt{2}}(|a_1b_1\rangle \pm |a_2b_2\rangle)_{ab}, \\ |\Psi^{\pm}\rangle_{\rm S} &= \frac{1}{\sqrt{2}}(|a_1b_2\rangle \pm |a_2b_1\rangle)_{ab}. \end{aligned} \tag{4}$$

Here, $|\xi\rangle_{\rm P}$ represents one of the four Bell states in the polarization degree of freedom of a photon pair, i.e.,

$$\begin{aligned} |\phi^{\pm}\rangle_{P} &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)_{ab}, \\ |\psi^{\pm}\rangle_{P} &= \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)_{ab}. \end{aligned} \tag{5}$$

As pointed out by Wang *et al.*,[48] one of the 16 Bell states $|\Theta_{ab}\rangle_{\rm SP}$ can be transferred into the other with one of the 16 unitary operations on one photon. That is, the 16 unitary operation can be chosen as $U_{ij} = U_i^{\rm S} \otimes U_j^{\rm P}$ $(i, j = 1, 2, 3, 4)$, where $U_i^{\rm S}$ and $U_j^{\rm P}$ are the unitary operations on the photon a in the spatial-mode degree of freedom and the polarization degree of freedom, respectively. Here

$$\begin{aligned} U_1^{\rm S} &= |a_1\rangle\langle a_1| + |a_2\rangle\langle a_2|, \\ U_2^{\rm S} &= |a_2\rangle\langle a_1| + |a_1\rangle\langle a_2|, \\ U_3^{\rm S} &= |a_1\rangle\langle a_1| - |a_2\rangle\langle a_2|, \\ U_4^{\rm S} &= |a_2\rangle\langle a_1| - |a_1\rangle\langle a_2|, \\ U_1^{\rm P} &= |H\rangle\langle H| + |V\rangle\langle V|, \\ U_2^{\rm P} &= |V\rangle\langle H| + |H\rangle\langle V|, \\ U_3^{\rm P} &= |H\rangle\langle H| - |V\rangle\langle V|, \\ U_4^{\rm P} &= |V\rangle\langle H| - |H\rangle\langle V|. \end{aligned} \tag{6}$$

The four unitary operations in the polarization-mode degree of freedom can be completed with linear optical elements, such as a $\lambda/2$ wave plate or a $\lambda/4$ wave plate. The bit-flip operation $U_2^{\rm S}$ and the phase-flip operation $U_3^{\rm S}$ in the spatial-mode degree of freedom can be accomplished by exchanging the two fibre channels (a_1 and a_2) and by adding a $\lambda/2$ wave plate to the spatial mode a_2, respectively.[48]

With the hyperentangled states shown in Eq. (3), the principle of our two-step QSDC protocol with hyperentanglement can be described as follows.

(i) Alice prepares a sequence of hyperentangled photon pairs in the hyperentangled state $|\Phi_{ab}^{+}\rangle_{\rm SP}$. She divides them into two photon sequences, say S_a and S_b. That is, S_a is composed of all the photons a in the photon pairs ab and S_b is made up of all the photons b in the photon pairs, as in Refs. [4], [5], [9], and [48].

(ii) Alice sends the sequence S_b to Bob and he keeps the sequence S_a.

(iii) Alice and Bob perform the first security check for the transmission of the photon sequence S_b. This task can be completed with the same process as the original two-step QSDC protocol.[5] In detail, Bob randomly chooses some photons from his sequence S_b and measures them with one of two measuring bases, say, Z and X, as done in Ref. [48]. Here $Z = Z_S \otimes Z_{\rm P}$ and $X = X_S \otimes X_{\rm P}$, with $Z_S = \{|b_1\rangle, |b_2\rangle\}$, $X_S = \{\frac{1}{\sqrt{2}}(|b_1\rangle \pm |b_2\rangle)\}$, $Z_{\rm P} = \{|H\rangle, |V\rangle\}$, and $X_{\rm P} = \{\frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\}$. After his measurements on the samples, Bob tells Alice his outcomes, i.e., the state of each sample with his single-photon measurement. Alice chooses the same measuring basis as Bob's to measure the photon in the sequence S_a, correlated to the photon measured by Bob in the sequence S_b. Alice analyses the error rate of the samples and judges whether the transmission is secure. If she confirms that the transmission of the sequence S_b is secure, Alice tells Bob to perform the next step for QSDC; otherwise, Alice and Bob abort their quantum communication and abandon the photons transmitted.

(iv) Alice encodes her secret message on the sequence S_a with the 16 unitary operations U_{ij} $(i, j = 1, 2, 3, 4)$ which can represent 16 different secret binary strings. In order to complete the second security check, she should choose some of the photons in the sequence S_a as the samples for analysing the error rate of the transmission of this sequence. Alice encodes some random codes on the samples. She sends the sequence S_a to Bob after her encoding.

(v) After Bob receives the sequence S_a, he performs hyperentangled Bell-state analysis[47] on all the photon pairs, including those acting as the samples for the second security check; then Alice tells Bob the samples for the second security check.

(vi) After the measurements with hyperentangled Bell-state analysis, Bob requires Alice to tell him the information about the samples for the security check and he judges whether their transmission succeeds by analysing the error rate of the samples.

(vii) If their transmission is secure, Bob will read out the secret message directly; otherwise, he should discard the outcomes and request Alice to repeat their quantum communication from the first step.

Unlike the QSDC protocol based on hyperdense coding,[48] our QSDC protocol is immune to attack by an eavesdropper with a Trojan horse as it is a one-way quantum communication protocol, not a two-way one, the same as the two-step QSDC protocol.[15] That is, this QSDC protocol does not require the user to have photon number splitters. It requires the receiver Bob to have the ability to determine whether there is a photon in each quantum signal in the sequence S_b when our QSDC protocol is used over a noisy channel. In the two-step QSDC protocol,[5] this task is accomplished using entanglement swapping. However, entanglement swapping will at least consume a photon pair in a hyperentangled Bell state prepared by the receiver (Bob). Although hyperentanglement swapping is in principle feasible with nonlinear optics, as shown in Ref. [47], it is not the most efficient method for this QSDC protocol. With nonlinear optics, Bob can design a quantum nondemolition detector (QND) in the same way as described in Ref. [47]. Bob can in principle judge whether there is a photon in each quantum signal in the sequence S_b with a QND, which makes this QSDC protocol more practical than the two-step QSDC protocol.[5]

In general, the security of our QSDC protocol is the same as that of the two-step QSDC protocol since they have the same topological structure. As shown by Deng *et al.*, the two-step QSDC protocol is, in principle, secure both in an ideal condition and in a noisy one. That is, our QSDC protocol is also secure in principle. If the noise in the quantum channels is unreasonably large, this QSDC protocol is not suitable for two users in quantum communication to transmit their secret message directly. In this case, it can be used to produce a private key and act as a high-capacity QKD protocol.

Compared with the two-step QSDC protocol,[5] our QSDC protocol has the advantage of higher capacity as each photon pair in a hyperentangled Bell state can carry four bits of information, the same as that in Ref. [48]. Compared with the QSDC protocol based on hyperdense coding,[48] this protocol does not require two users in quantum communication to prevent an eavesdropper from eavesdropping on their communication using Trojan horse attack strategies. Certainly, the two users will pay the price of performing a QDN on each quantum signal in the sequence S_b in order to have such immunity.

In summary, we have introduced a two-step quantum secure direct communication protocol with hyperentanglment in both the spatial-mode and the polarization degrees of freedom of photon pairs. A secret message can be encoded on the photon pairs with unitary operations in the spatial-mode and the polarization degrees of freedom independently. This QSDC protocol has a higher capacity than the original two-step QSDC protocol[5] as each photon pair can carry four bits of information. Compared with the QSDC protocol based on hyperdense coding,[48] this QSDC protocol does not require the two users in quantum communication to prevent an eavesdropper from eavesdropping on their communication with Trojan horse attack strategies.

References

[1] Bennett C H and Brassad G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* Bangalore, India (New York: IEEE) p. 175

[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Li X H, Duan X J, Sheng Y B, Zhou H Y and Deng F G 2009 *Chin. Phys.* B **18** 3710

[4] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[5] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[6] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[7] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[8] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[9] Wang C, Deng F G, Li Y S, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **71** 044305

[10] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

[11] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **359** 359

[12] Li X H, Li C Y, Deng F G, Zhou P, Liang Y and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[13] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. Chin.* **2** 251

[14] Qin S J, Wen Q Y, Meng L M and Zhu F C 2009 *Sci. Chin.* G **52** 1208

[15] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. Chin.* G **54** 942

[16] Beige A, Englert B G, Kurtsiefer C and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[17] Yan F L and Zhang X 2004 *Eur. Phys. J.* B **41** 75

[18] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento Della Societa Italiana Di Fisica* B **119** 313

[19] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18

[20] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[21] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A: *Math. Gen.* **38** 5761

[22] Gao T, Yan F L and Wang Z X 2005 *Int. J. Mod. Phys.* C **16** 1293

[23] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290

[24] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[25] Zhu A D, Xia Y, Fan Q B and Zhang S L 2006 *Phys. Rev.* A **73** 022338

[26] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302

[27] Wang C, Li Y S and Long G L 2006 *Commun. Theor. Phys.* **46** 440

[28] Yang J, Wang C and Zhang R 2010 *Chin. Phys.* B **19** 110306

[29] Zhang X L, Zhang Y X and Wei H 2009 *Chin. Phys.* B **18** 435

[30] Liu W J, Chen H W, Ma T H, Li Z Q, Liu Z H and Hu W B 2009 *Chin. Phys.* B **18** 4105

[31] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[32] Gu B, Pei S X, Song B and Zhong K 2009 *Sci. Chin.* G **52** 1913

[33] Cao W F, Yang Y G and Wen Q Y 2010 *Sci. Chin.* G **53** 1271

[34] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[35] Wang W Y, Wang C, Zhang G Y and Long G L 2009 *Chin. Sci. Bull.* **54** 158

[36] Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443

[37] Hao L, Wang C and Long G L 2010 *J. Phys.* B **43** 125502

[38] Wen K and Long G L 2010 *Int. J. Quantum Inform.* **8** 697

[39] Simon C and Pan J W 2002 *Phys. Rev. Lett.* **89** 257901

[40] Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **77** 042308

[41] Xiao L, Wang C, Zhang W, Huang Y D, Peng J D and Long G L 2008 *Phys. Rev.* A **77** 042315

[42] Wang C, Sheng Y B, Li X H, Deng F G, Zhang W and Long G L 2009 *Sci. Chin.: Tech. Sci.* **52** 3464

[43] Sheng Y B and Deng F G 2010 *Phys. Rev.* A **81** 032307

[44] Sheng Y B and Deng F G 2010 *Phys. Rev.* A **82** 044305

[45] Barreiro J T, Wei T C and Kwiat P G 2008 *Nature Phys.* **4** 282

[46] Wang W Y, Wang C and Long G L 2009 *Int. J. Quantum Inform.* **7** 529

[47] Sheng Y B, Deng F G and Long G L 2010 *Phys. Rev.* A **82** 032318

[48] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305, arXiv: 1103.0471