

High-capacity Deterministic Secure Four-qubit W State Protocol for Quantum Communication Based on Order Rearrangement of Particle Pairs

Hao Yuan · Jun Song · Jun Zhou · Gang Zhang ·
Xiang-fei Wei

Received: 21 November 2010 / Accepted: 14 February 2011 / Published online: 4 March 2011
© Springer Science+Business Media, LLC 2011

Abstract A novel high-capacity protocol for deterministic secure quantum communication with four-qubit symmetric W state is proposed. In the presented protocol, the secret messages can be encoded on the four-qubit symmetric W states by employing four two-particle unitary operations and directly decoded by utilizing the corresponding measurements in Bell basis or single particle basis. It has a high capacity as each W state can carry two bits of secret information, and has a high intrinsic efficiency because almost all the instances are useful. The security of this communication can be ensured by the decoy photon checking technique and the order rearrangement of particle pairs technique. Furthermore, this protocol is feasible with present-day technique.

Keywords Deterministic secret quantum communication · Four-qubit W states · Decoy photon checking technique · Order rearrangement of particle pairs technique

1 Introduction

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.

This work is supported by the Key Project of the Education Department of Anhui Province under Grant No. KJ2010A323, the Talent Project of the Anhui Province for Outstanding Youth under Grant Nos. 2009SQRZ190, 2010SQRL186, 2010SQRL187 and 2011SQRL147, the Natural Science Research Programme of the Education Department of Anhui Province under Grant No. KJ2009B018Z.

H. Yuan (✉) · J. Song · J. Zhou · G. Zhang · X.-f. Wei
Department of Mathematics and Physics, West Anhui University, Lu' an 237012, China
e-mail: yuanhao@wxc.edu.cn

J. Song · J. Zhou
Department of Material Science and Engineering, University of Science and Technology of China,
Hefei 230026, China

Hence, since Bennett and Brassard presented the pioneering work in 1984 [1], a variety of QKD protocols have been proposed [1–10]. In these works, various properties of quantum mechanics, such as no-cloning theorem, uncertainty principle, indistinguishability of nonorthogonal states, and so on, are used to accomplish QKD tasks.

Subsequently, a new concept in quantum cryptography, i.e., quantum secure direct communication (QSDC) has been put forward [11]. With QSDC Alice and Bob can exchange the secret message directly without generating a private key in advance and then encrypting the message, which is different to QKD. Due to its instantaneous, QSDC may be used in some urgent circumstances. In 2002, by taking advantage of Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers, Boström and Felbinger [11] put forward the famous QSDC protocol referred to as the ping-pong protocol later. However, it is insecure in a noisy quantum channel as shown by Wójcik [12] and even can be attacked in an ideal quantum channel by Cai's denial-of-service (DoS) attack [13] and invisible photon attack [14]. In 2003, Deng et al. [15] proposed a two-step QSDC protocol using blocks of EPR pairs. In 2004, Cai et al. [16] firstly put forward a QSDC protocol only using single qubit in a mixed state. Later, Deng and Long [17] proposed another QSDC protocol only using a sequence of single photons. In 2005, Wang et al. presented a multi-step QSDC protocol using blocks of multi-particle maximally entangled state as quantum channel [18] and introduced a high-dimensional QSDC protocol [19]. In 2006, Deng et al. [20] presented two efficient QSDC network schemes with an N ordered Einstein-Podolsky-Rosen pairs. In 2007, Li et al. [21] proposed a new QSDC scheme with quantum encryption based on pure entangled states. Up to now, much attention has been focused on QSDC [11–26].

Similar to QSDC, another class of quantum cryptography is called deterministic secure quantum communication (DSQC) [27]. In the framework of DSQC, the receiver can read out the secret message only after the transmission of at least one bit of additional classical information for each qubit, different from QSDC in which the secret message can be read out directly without exchanging any classical information. Comparing with QKD, DSQC can be used to obtain deterministic information, not a randomly binary string. So far, DSQC has been actively pursued by some groups [27–42]. For example, in 2002, Beige et al. [28] first proposed a DSQC scheme based on single-photon two-qubit states. In 2004, Yan and Zhang [29] proposed a DSQC scheme based on EPR pairs and quantum teleportation. Later, Zhang et al. [30] proposed a DSQC protocol by taking advantage of the property of quantum entanglement swapping of two photon pairs. In 2005, Gao et al. [31] and Man et al. [32] proposed two DSQC protocols also based on entanglement swapping. In 2006, Zhu et al. [33] proposed a DSQC protocol with EPR pairs based on the encryption on the order of the transmission of the particles. However, this protocol has a vital loophole founded by Li et al. [34]. Soon later, Wang et al. [35] revised this DSQC protocol with single photons. Lee et al. [36] proposed a protocol for controlled DSQC with Greenberger-Horne-Zeilinger (GHZ) states. Cao et al. [37] put forward a DSQC scheme based on a block of four-qubit symmetric W states. In 2009, Xiu et al. [38] proposed a controlled DSQC scheme using five-qubit entangled states and two-step security test. Dong et al. [39] put forward a protocol for DSQC against collective-dephasing noise by using EPR pairs and auxiliary photons. In 2010, Zhou et al. [40] proposed two DSQC protocols by utilizing Bell states and GHZ states respectively. Recently, Chen et al. [41] proposed a new efficient DSQC scheme which allows a group of mutually distrustful players to perform the summation computation.

In this paper, we will present a novel high-capacity DSQC protocol using the same four-qubit symmetric W states as the scheme [37] used. Incidentally, the communication expounded in the scheme [37] can be eavesdropped by adopting the intercept-measure-resend attack [42]. On the other hand, each W state can only carry one bit of information in the

scheme [37]. It will be shown that the present protocol has a high capacity as each W state can carry two bits of secret messages. Moreover, the security of the scheme [37] mainly relies on the property of entanglement, which will waste a large amount of entanglement resource. While the present protocol exploits the decoy photon checking technique [7, 20] and the order rearrangement of particle pairs technique [5, 33–35] to ensure the security of the communication, which makes the checking process become simple.

2 High-Capacity DSQC Protocol with Four Qubit Symmetric W State

Now, let us describe the details of our DSQC protocol. Suppose there are two remote legitimate communicators, Alice and Bob. Alice wants to transmit n two-bit secret classical messages to Bob, which may be implemented by the following nine-step protocol.

(I) *Preparing a quartet sequence P .* Alice prepares a sequence of n ordered quartets of entangled particles P . Each quartet is in the four-qubit symmetric W state $|W\rangle$,

$$|W\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)_{a_1 a_2 b_1 b_2}, \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of the σ_z , and the subscript a_1, a_2, b_1 and b_2 represent the four particles of one W state. We denote the ordered n quartet in the sequence P with $[\mathcal{P}_1(a_1, a_2, b_1, b_2), \mathcal{P}_2(a_1, a_2, b_1, b_2), \dots, \mathcal{P}_n(a_1, a_2, b_1, b_2)]$, here the subscript $1, 2, \dots, n$ indicate the order of each particle quartet in the sequence P , respectively.

(II) *Encoding secret information on the sequence P .* Alice performs one of the four unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ on the particles b_1 and b_2 of each quartet in the sequence P to encode her secret messages $\{00, 01, 10, 11\}$, where

$$U_{00} = I \otimes I, \quad U_{01} = I \otimes i\sigma_y, \quad U_{10} = \sigma_x \otimes I, \quad U_{11} = \sigma_x \otimes i\sigma_y, \tag{2}$$

and

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1|, & \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ i\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|, & \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|. \end{aligned} \tag{3}$$

The operation U_{ij} ($i, j \in \{0, 1\}$) will transform the state $|W\rangle$ into the state $|W_{ij}\rangle$, where

$$\begin{aligned} |W_{00}\rangle &= \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)_{a_1 a_2 b_1 b_2} \\ &= \frac{1}{2}[\sqrt{2}|00\rangle_{a_1 a_2} |\psi^+\rangle_{b_1 b_2} + (|01\rangle + |10\rangle)_{a_1 a_2} |00\rangle_{b_1 b_2}], \end{aligned} \tag{4}$$

$$\begin{aligned} |W_{01}\rangle &= \frac{1}{2}(|0000\rangle - |0011\rangle - |0101\rangle - |1001\rangle)_{a_1 a_2 b_1 b_2} \\ &= \frac{1}{2}[\sqrt{2}|00\rangle_{a_1 a_2} |\phi^-\rangle_{b_1 b_2} - (|01\rangle + |10\rangle)_{a_1 a_2} |01\rangle_{b_1 b_2}], \end{aligned} \tag{5}$$

$$\begin{aligned} |W_{10}\rangle &= \frac{1}{2}(|0011\rangle + |0000\rangle + |0110\rangle + |1010\rangle)_{a_1 a_2 b_1 b_2} \\ &= \frac{1}{2}[\sqrt{2}|00\rangle_{a_1 a_2} |\phi^+\rangle_{b_1 b_2} + (|01\rangle + |10\rangle)_{a_1 a_2} |10\rangle_{b_1 b_2}], \end{aligned} \tag{6}$$

$$\begin{aligned}
 |W_{11}\rangle &= \frac{1}{2}(|0010\rangle - |0001\rangle - |0111\rangle - |1011\rangle)_{a_1 a_2 b_1 b_2} \\
 &= -\frac{1}{2}[\sqrt{2}|00\rangle_{a_1 a_2} |\psi^-\rangle_{b_1 b_2} + (|01\rangle + |10\rangle)_{a_1 a_2} |11\rangle_{b_1 b_2}], \tag{7}
 \end{aligned}$$

here $|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle$ and $|\phi^-\rangle$ are the four Bell states, which are defined as the follows,

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle), \quad |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle), \tag{8}$$

they compose of \mathcal{B} -basis.

(III) *Distributing the particles in the sequence P .* Alice takes the particles a_1 and a_2 from each quartet in the sequence P to form an ordered particle pair sequence, say, $[\mathcal{P}_1(a_1, a_2), \mathcal{P}_2(a_1, a_2), \dots, \mathcal{P}_n(a_1, a_2)]$. It is called the P_A sequence. The remaining partner particle pairs form another ordered sequence $[\mathcal{P}_1(b_1, b_2), \mathcal{P}_2(b_1, b_2), \dots, \mathcal{P}_n(b_1, b_2)]$. It is called the P_B sequence.

(IV) *Disturbing the order of the particle pairs in the sequence P_B .* Alice disturbs the order of the particle pairs in the P_B sequence and generates a rearranged particle pair sequence, called P'_B sequence $[\mathcal{P}'_1(b_1, b_2), \mathcal{P}'_2(b_1, b_2), \dots, \mathcal{P}'_n(b_1, b_2)]$. The order of P'_B sequence is completely secret to others but Alice herself, which ensures the security of the present scheme.

(V) *Adding some decoy photons into the sequence P'_B .* Before sending the P'_B sequence to Bob, Alice has to add some decoy photons in it. The purpose of this step is to check for eavesdropping in the transmission of the sequence P'_B subsequently. The detail process is as follows. Alice prepares k ($k \ll n$) decoy photons each randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, here $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are the up and down eigenstates of the σ_x . Then she randomly inserts the k decoy photons into the P'_B sequence. Thus, a new sequence P'_{B+k} is formed. Since the states and the positions of the decoy photons are only known for Alice herself, the eavesdropping done by an eavesdropper will inevitably disturb these decoy photons and will be detected.

(VI) *Transmitting the P'_{B+k} sequence.* Alice sends the P'_{B+k} sequence to Bob and keeps the P_A sequence in her site.

(VII) *Checking the quantum channel from Alice to Bob.* After confirming Bob has received the P'_{B+k} sequence, Alice announces publicly the positions and the states of the k decoy photons. Then Bob performs a suitable measurement on each decoy photon with the same basis as Alice chose for preparing it. By comparing his measurement results with Alice's announcement, Bob can then evaluate the error rate of the transmission of the P'_B sequence. If the error rate exceeds the threshold, they abort this communication and repeat the procedures from the beginning. Otherwise, they continue to the next step.

(VIII) *Recovering the disturbed sequence P'_B back to its original sequence P_B .* Alice exposes the secret transmitted order of the P'_B sequence. According to this information Bob can adjust the disturbed sequence P'_B to it's original sequence P_B .

(IX) *Extracting secret information from the sequence P_B .* Alice performs $\mathcal{Z} \otimes \mathcal{Z}$ basis measurements on her particle pairs (i.e., the particles a_1 and a_2) in the P_A sequence, where $\mathcal{Z} = \{|0\rangle, |1\rangle\}$ and $\mathcal{Z} \otimes \mathcal{Z}$ represents a local measurement on each qubit of the particle pairs in \mathcal{Z} -basis. If her measurement result is $|00\rangle_{a_1 a_2}$, then Alice sends classical information 0 to Bob, otherwise 1 is sent. According to Alice's announcement, Bob chooses one of the two bases, i.e., \mathcal{Z} -basis or \mathcal{B} -basis to measure the partner particles b_1 and b_2 in the sequence P_B . That is, if Alice's announcement is 0, then Bob measures the partner particles b_1 and b_2 in \mathcal{B} -basis, otherwise, he measures the partner particles in $\mathcal{Z} \otimes \mathcal{Z}$ basis. Once obtaining the

Table 1 Corresponding relations among Alice’s measurement results (AMR), Alice’s classical information (ACI), Bob’s measurement results (BMR) and the secret messages in the presented DSQC scheme

AMR	ACI	BMR			
$ 00\rangle_{a_1a_2}$	0	$ \psi^+\rangle_{b_1b_2}$	$ \phi^-\rangle_{b_1b_2}$	$ \phi^+\rangle_{b_1b_2}$	$ \psi^-\rangle_{b_1b_2}$
$ 01\rangle_{a_1a_2}$ or $ 10\rangle_{a_1a_2}$	1	$ 00\rangle_{b_1b_2}$	$ 01\rangle_{b_1b_2}$	$ 10\rangle_{b_1b_2}$	$ 11\rangle_{b_1b_2}$
Secret messages		00	01	10	11

measurement result, Bob can deduce the secret message according to (4) to (7). Table 1 shows the joint correlations of the results for measurements made by Alice and Bob and all possible cases of quantum communication in the present DSQC protocol.

To explicitly demonstrate the decoding process in our protocol, let us show an example. Suppose Alice’s measurement results are $\{|00\rangle_{a_1a_2}, |01\rangle_{a_1a_2}, |10\rangle_{a_1a_2}, |00\rangle_{a_1a_2}, \dots\}$, then she sends the classical bit sequence $\{0, 1, 1, 0, \dots\}$ to Bob. After receiving Alice’s announcement, Bob chooses the bases $\{\mathcal{B}, \mathcal{Z} \otimes \mathcal{Z}, \mathcal{Z} \otimes \mathcal{Z}, \mathcal{B}, \dots\}$ to measure his partner particles in the sequence P_B , respectively. Assumed the measurement results are $\{|\phi^+\rangle_{b_1b_2}, |01\rangle_{b_1b_2}, |11\rangle_{b_1b_2}, |\psi^-\rangle_{b_1b_2}, \dots\}$, then Bob can deduce the secret messages are $\{10, 01, 11, 11, \dots\}$ according to Table 1.

So far we have expatiated a high-capacity DSQC protocol with the four-qubit symmetric W state.

3 Security Analysis

Now we discuss the security for the present protocol. Since the secret messages are encoded on the four-qubit symmetric W states, if eavesdropper Eve wants to wiretap some secret messages, she has to access the quantum channel and execute her evil action by manipulating it. she may use some types of man-in-the-middle attack strategy, such as (1) Measure-resend attack: Eve measures the qubits emerging from Alice and then resends them to Bob. (2) Entangle-measure attack: Eve entangles her ancilla with the particle pair $\mathcal{P}_i(b_1, b_2)$ ($i \in \{1, 2, \dots, n\}$) before $\mathcal{P}_i(b_1, b_2)$ reaches Bob. After Bob measures his particle pair $\mathcal{P}_i(b_1, b_2)$, Eve does so with her ancilla and deduce Bob’s measurement result. (3) Denial-service attack: When the sequence P_B is traveling from Alice to Bob, Eve intercepts it and uses some methods to destroy the states of the particle pairs $\mathcal{P}_1(b_1, b_2), \mathcal{P}_2(b_1, b_2), \dots$ and $\mathcal{P}_n(b_1, b_2)$. By doing so, Eve, though can not gain any information, is able to make the protocol to be denial of service. Unfortunately, all of the above types of attack can be forbidden by the decoy-particle checking procedure explained in the preceding section, i.e., the step (VII). In our protocol, each decoy photon is prepared randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and is distributed in the sequence P_B randomly. That is to say, the states and the positions of the decoy photons are unknown for Eve. Hence, Once Eve manipulates the particle pairs in the sequence P_B , she will inevitably disturb these decoy photons and be easily detected by the authorized users.

It is should be noticed that in addition to have the ability to detect eavesdropping, the two legitimate users must can ensure the secret message do not leak to eavesdropper before she is detected. As a matter of fact, if only exploiting the decoy photon checking technique while not using the order rearrangement technique, then some useful information may be eavesdropped by Eve in the present protocol. In such case, the best attack strategy that Eve uses is the intercept-resend attack strategy. Under this kind of attack, Eve intercepts the

sequence P_{B+k} and stores it, and then sends a fake sequence P_{B+k}^* to Bob. When Alice publicly announces the positions and the states of the k decoy photons, Eve can also obtain the classical information easily. Subsequently, Eve takes out the decoy photons from the sequence P_{B+k}^* . Incidentally, for each particle in the fake sequence P_{B+k}^* , its state is prepared completely randomly and have no correlation with the state of the particle in the sequence P_{B+k} at all. Therefore, by using the checking procedure mentioned in Step (VII), Alice and Bob can easily detect Eve's attack and discard the communication immediately. Obviously, Alice do not continue to measure her particle pairs in the sequence P_A and not to mention announcing her measurement results publicly. Seen from the surface, Alice and Bob do not leak any useful information to Eve. However, only by measuring the particle pairs (i.e., particles b_1 and b_2) in the P_B sequence, Eve can still successfully deduce 75% secret messages. Fortunately, in the present scheme, before sending the sequence P_{B+k} to Bob, Alice disturbs the order of particle pairs. In such case, Eve only obtain the disturbed sequence P_B' . Without the correct order of the particle pair sequence, Eve can only obtain a batch of meaningless date.

From the above analysis, one can see clearly that the decoy photon checking technique and the order rearrangement of particle pairs technique can ensure the security of the present scheme. The decoy photon checking technique can decide whether a potential eavesdropper Eve is online, and the secret transmitting order of particle pairs is used to prevent Eve from obtaining secret message. Incidentally, since the classical communication channel is used in our protocol, which have been assumed highly authentic, Eve do not pretend to be Bob to get Alice's secret messages or pretend to be Alice to send fake secret messages to Bob.

4 Summary

To summarize, we have presented a high-capacity DSQC protocol using the four-qubit symmetric W states in blocks. In the presented protocol, the sender Alice exploits four two-particle unitary operations to encode her secret messages, and the receiver Bob can infer the secret messages directly by utilizing some assistant classical information and the corresponding measurements in \mathcal{B} -basis or $\mathcal{Z} \otimes \mathcal{Z}$ basis. To check the eavesdropping in the transmission process, Alice inserts some decoy photons in the transmitting particle pair sequence, which can forbid the eavesdropper to eavesdrop the quantum channel freely. Our protocol has the advantage of high capacity as each W state can carry two bits of secret messages, two times than that of the scheme [37], and high intrinsic efficiency as almost all the instances are useful except for the decoy photons used to check eavesdropping. Furthermore, a majority of measurements are in the \mathcal{Z} -basis in the present protocol, while all of the measurements are in the \mathcal{B} -basis in the scheme [37]. That leads our protocol is simpler than the scheme [37].

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, p. 175. IEEE, New York (1984)
2. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
3. Cabello, A.: Phys. Rev. Lett. **85**, 5635 (2000)
4. Long, G.L., Liu, X.S.: Phys. Rev. A **65**, 032302 (2002)
5. Deng, F.G., Long, G.L.: Phys. Rev. A **68**, 042315 (2003)
6. Deng, F.G., Long, G.L., Wang, Y., Xiao, L.: Chin. Phys. Lett. **21**, 2097 (2004)
7. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Chin. Phys. Lett. **22**, 1049 (2005)

8. Kye, W.H., Kim, C.M., Kim, M.S., Park, Y.J.: *Phys. Rev. Lett.* **95**, 040501 (2005)
9. Liu, X.B., Liao, C.J., Tang, Z.L., Wang, J.D., Liu, S.H.: *Chin. Phys. Lett.* **25**, 3856 (2008)
10. Li, X.H., Deng, F.G., Zhou, H.Y.: *Phys. Rev. A* **78**, 022321 (2008)
11. Boström, K., Felbinger, T.: *Phys. Rev. Lett.* **89**, 187902 (2002)
12. Wójcik, A.: *Phys. Rev. Lett.* **90**, 157901 (2003)
13. Cai, Q.Y.: *Phys. Rev. Lett.* **91**, 109801 (2003)
14. Cai, Q.Y.: *Phys. Lett. A* **351**, 23 (2006)
15. Deng, F.G., Long, G.L., Liu, X.S.: *Phys. Rev. A* **68**, 042317 (2003)
16. Cai, Q.Y., Li, B.W.: *Chin. Phys. Lett.* **21**, 601 (2004)
17. Deng, F.G., Long, G.L.: *Phys. Rev. A* **69**, 052319 (2004)
18. Wang, C., Deng, F.G., Long, G.L.: *Opt. Commun.* **253**, 15 (2005)
19. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: *Phys. Rev. A* **71**, 044305 (2005)
20. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: *Phys. Lett. A* **359**, 359 (2006)
21. Li, X.H., Li, C.Y., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: *Chin. Phys.* **16**, 2149 (2007)
22. Long, G.L., Deng, F.G., Wang, C., Li, X.H., Wen, K., Wang, W.Y.: *Front. Phys. China* **2**, 251 (2007)
23. Liu, W.J., Chen, H.W., Li, Z.Q., Liu, Z.H.: *Chin. Phys. Lett.* **25**, 2354 (2008)
24. Yi, X.J., Nie, Y.Y., Zhou, N.N., Huang, Y.B., Hong, Z.H.: *Int. J. Theor. Phys.* **47**, 3401 (2008)
25. Liu, D., Pei, C.X., Quan, D.X., Zhao, N.: *Chin. Phys. Lett.* **27**, 050306 (2010)
26. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: *Opt. Commun.* **283**, 192 (2010)
27. Li, X.H., Deng, F.G., Li, C.Y., Liang, Y.J., Zhou, P., Zhou, H.Y.: *J. Korean Phys. Soc.* **49**, 1354 (2006)
28. Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: *Acta Phys. Pol. A* **101**, 357 (2002)
29. Yan, F.L., Zhang, X.Q.: *Eur. Phys. J. B* **41**, 75 (2004)
30. Zhang, Z.J., Man, Z.X., Li, Y.: *Int. J. Quant. Infom.* **2**, 521 (2004)
31. Gao, T., Yan, F.L., Wang, Z.X.: *J. Phys. A* **38**, 5761 (2005)
32. Man, Z.X., Zhang, Z.J., Li, Y.: *Chin. Phys. Lett.* **22**, 18 (2005)
33. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: *Phys. Rev. A* **73**, 022338 (2006)
34. Li, X.H., Deng, F.G., Zhou, H.Y.: *Phys. Rev. A* **74**, 054302 (2006)
35. Wang, J., Zhang, Q., Tang, C.J.: *Phys. Lett. A* **358**, 256 (2006)
36. Lee, H., Lim, J., Yang, H.: *Phys. Rev. A* **73**, 042305 (2006)
37. Cao, H.J., Song, H.S.: *Chin. Phys. Lett.* **23**, 290 (2006)
38. Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: *Opt. Commun.* **282**, 333 (2009)
39. Dong, L., Xiu, X.M., Gao, Y.J., Chi, F.: *Opt. Commun.* **282**, 1688 (2009)
40. Zhou, N.R., Wang, L.J., Ding, J., Gong, L.H., Zuo, X.W.: *Int. J. Theor. Phys.* **40**, 2035 (2010) (QDSC)
41. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: *Int. J. Theor. Phys.* **49**, 2793 (2010)
42. Liu, J., Liu, Y.M., Cao, H.J., Shi, S.H., Zhang, Z.J.: *Chin. Phys. Lett.* **23**, 2652 (2006)