Vol 16 No 12, December 2007
1009-1963/2007/16(12)/3553-07

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Economical quantum secure direct communication network with single photons*

Deng Fu-Guo(邓富国)[a)b)c)†], Li Xi-Han(李熙涵)[a)b)], Li Chun-Yan(李春燕)[a)b)], Zhou Ping(周 萍)[a)b)], and Zhou Hong-Yu(周宏余)[a)b)c)]

[a)] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing* 100875, *China*
[b)] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing* 100875, *China*
[c)] *Beijing Radiation Center, Beijing* 100875, *China*

(Received 24 February 2007; revised manuscript received 31 March 2007)

In this paper a scheme for quantum secure direct communication (QSDC) network is proposed with a sequence of polarized single photons. The single photons are prepared originally in the same state $|0\rangle$ by the servers on the network, which will reduce the difficulty for the legitimate users to check eavesdropping largely. The users code the information on the single photons with two unitary operations which do not change their measuring bases. Some decoy photons, which are produced by operating the sample photons with a Hadamard, are used for preventing a potentially dishonest server from eavesdropping the quantum lines freely. This scheme is an economical one as it is the easiest way for QSDC network communication securely.

Keywords: quantum secure direct communication, network, single photons
PACC: 0155, 0365B

1. Introduction

The combination of the principles in quantum mechanics and the theory of information produces some novel applications, such as quantum computer and quantum communication.[1] Quantum key distribution (QKD)[2] provides a secure way for two remote parties, Bob and Charlie, to create a private key with which they can communicate securely by using the Vernam one-time pad crypto-system. The non-cloning theorem and the quantum correlation of an entangled quantum system ensure the security of QKD. In 1984, Bennett and Brassard (BB84)[3] proposed an original point-to-point QKD scheme based on the non-cloning theorem. As the state of each single photon is produced by choosing randomly one of the two measuring bases (MBs), the rectilinear basis σ_z and the diagonal basis σ_x, a vicious eavesdropper, Eve, will inevitably disturb the quantum systems and leave a mark in the results if she eavesdrops the quantum line. Moreover, she cannot obtain all the information about the single-photon state because an unknown quantum state cannot be cloned. Now, there have been some point-to-point QKD schemes proposed.[2−9]

Recently, a novel concept, quantum secure direct communication (QSDC) was prosed and actively pursued by some groups.[10−31] With QSDC, the two authorized users, say the sender Bob and the receiver Charlie, can exchange their secret message directly without creating a private key to encrypting the message. There are two types of QSDC schemes. One is based on entangled states, such as those in Refs.[10–26]. The other is based on single photons. Typical such QSDC protocols are the ones presented in Refs.[27–30]. Obviously, the ones with single photons are more convenient for the users at the aspect of measurements than those with entangled states. The message in the two point-to-point QSDC protocols proposed by Schimizu and Imoto[27] and Beige *et al*[28] cannot be read out until an additional classical bit is transmitted for each qubit. We[29] proposed a QSDC scheme with a sequence of single photons, and Cai and Li[30] introduced a QSDC protocol with a single photon following some ideas in Bennett 1992 QKD protocol.[32]

A general case of practical applications of QSDC

*Project supported by the National Natural Science Foundation of China (Grant Nos 10604008 and 10435020) and the Beijing Education Committee (Grant No XK100270454).
†E-mail: fgdeng@bnu.edu.cn

requires that an authorized user on a network can exchange the secret message directly with another one. That is, QSDC network schemes are useful in practice. There are some servers who provide the service for preparing and measuring the quantum signal for the legitimate users (the number is much larger than that of the servers), which will make the quantum communication between the legitimate users more convenient than those in point-to-point QSDC protocols[10−31] as it reduces the setups for the normal users, the same as that in a classical communication network. Although there exist a few QSDC network schemes based on entanglements,[33−35] none with single photons. Certainly, an ideal single-photon source is not available for a practical application at present, but people believe that it can be produced without difficulty in the near future with the development of technology.[36] Thus, it is interesting, in theory, to study the model for QSDC network with single photons.

In this paper, we introduce an economical QSDC network scheme with single photons. The server provides the service for preparing and measuring the quantum signals, a sequence of single photons S, which will simplify the authorized users' setups for secret communication largely. Different from QKD network protocols, the server first sends the quantum signals to the receiver who encrypts them with local unitary operations and then sends them to the sender. The secret message is encoded directly on the single photons after confirming their security. All the parties, including the servers, agree that the initial states of the single photons are $|0\rangle$, which will reduce the difficulty for the users to check eavesdropping. This QSDC network protocol is an optimal one.

2. QSDC network with single photons

Although a QSDC network is a composite system, its subsystem can be simplified to three parts, the server (Alice), the sender (Bob) and the receiver (Charlie), similar to QKD network.[37−42] That is, a great number of these subsystems compose the whole network. Similar to the classical network communication, for each request of the legitimate users, the server analyses it and then performs a relevant operation, for example, connecting the user to another one on the network or sending a sequence of single photons to the user. Moreover, all the users and the servers agree that the server of the branch with the receiver provides the service for preparing and measuring the quantum signal, and all other servers only provide the service for connecting the quantum line for these two legitimate users in a curtain time slot if the sender and the receiver do not exist in a branch of the network. Thus, a QSDC network scheme is explicit if the principle of its subsystem is described clearly.

The subsystem in our QSDC network scheme is shown in Fig.1. Alice provides the service for preparing and measuring the polarized single photons. The single photons S_0 are prepared initially in the same states $|+z\rangle \equiv |0\rangle$. Here $|+z\rangle$ is an eigenvector of the MB σ_z. Alice sends the photons S_0 first to the receiver Charlie who stores them and checks the security of the transmission. The procedure for checking eavesdropping includes two parts. One is used to check whether the sample photons are in the same state $|0\rangle$ or not, which can be completed by measuring half the samples with the MB σ_z. The other is used to check whether there are more than one photon in each signal. That is, Charlie should forbid others eavesdrop the quantum communication with a multi-photon fake signal attack.[43] This task can be accomplished with some photon beam splitters (PBSs), similar to Ref.[43]. In detail, Charlie splits each signal in the half of the samples remaining with three PBSs, shown in Fig.2, and then measures each signal with a single-photon detector. If there is only one photon in the initial signal, only one detector will be clicked in theory. Otherwise, the number of the detectors clicked is more than one with a large probability.

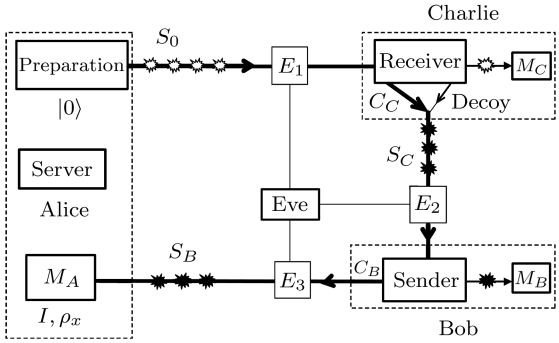


Fig.1. The subsystem of the present QSDC network. M_A, M_B and M_C represent the measurements done by Alice, Bob and Charlie respectively; E_1–E_3 represent the eavesdropping done by Eve in different processes. C_B and C_C are the codes done by Bob and Charlie respectively.

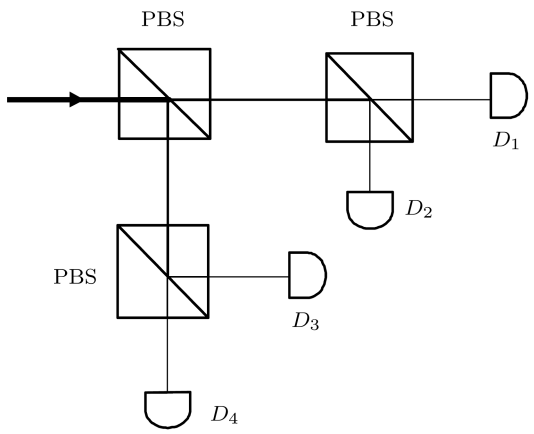


Fig.2. The principle of the check against multiphoton fake signal attack, similar to Ref.[43]. PBS presents a photon beam splitter 50/50, and D_i ($i = 1, 2, 3, 4$) are four single-photon detectors.

If the receiver Charlie confirms that there is no eavesdropper monitoring the quantum line between the server and him, he operates each photon in the sequence S_0 with one of the two local operations $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U_1 = |0\rangle\langle 1| - |1\rangle\langle 0|$ randomly. He keeps the secret about his operations C_C. In order to check eavesdropping efficiently, he should also insert some decoy photons in the sequence S_0. That is, Charlie picks up randomly some sample photons (the number is not very large, just enough for doing the error rate analysis, about the number of samples for eavesdropping check in BB84 QKD protocol), say $S_{\rm e}$ from the sequence S_0 after his operations with U_0 and U_1, and performs a Hadamard (H) operation on each one. The H operation will make the photons in S_e in the state $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $|-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. That is, the states of the photons in the sequence S_0 are nonorthogonal, which will forbid the eavesdroppers to eavesdrop the information on the states freely. After these operations, Charlie sends the sequence S_C (the sequence S_0 after Charlie's operations) to the sender Bob.

After Bob receives the sequence S_C, Charlie chooses randomly some photons from the sequence S_C as the samples for checking eavesdropping and tells their positions to Bob. The samples include all the photons operated with a H operation $S_{\rm e}$ and some other photons with only the operation U_0 or U_1. Charlie tells Bob the MBs of the samples and requires him to announce his outcomes obtained by measuring the samples with the same MBs as those of Charlie. Simultaneously, Bob can also use the same way as Charlie's to determine whether there are more than one photons in each sample. The error rate analysis on the samples can be accomplished by the receiver Charlie. That is, he compares the outcomes published by Bob with his own operations on the samples. If they believe that the quantum line is secure, Bob codes his secret message C_B on the photons remaining in the sequence S_C by choosing the operation U_0 or U_1 according to the bit is 0 or 1 respectively. Certainly, Bob should add a small trick in the sequence S_C before he sends it out. That is, he should select some photons in the sequence S_C as the samples for checking the security of the transmission between him and the server Alice, and operates them with U_0 or U_1 randomly. Then he sends the photons encoded, say S_B, to Alice who measures them with the MB σ_z. Alice announces the outcomes of her measurements in public, i.e., $C_A = C_C \oplus C_B$. After Bob and Charlie check eavesdropping with the photons operated by Bob using U_0 and U_1 randomly, Charlie can read out the secret message $C_B = C_A \oplus C_C$ directly if the transmission of whole quantum communication is secure.

3. Security analysis

3.1. The relation between the information leaked and the probability detected

In this QSDC network scheme, there are three processes for checking eavesdropping: i.e., one for the transmission between the server Alice and the receiver Charlie, one between Charlie and the sender Bob, and the other one between Bob and Alice. Although an eavesdropper, say Eve (including a dishonest server Alice), can eavesdrop the quantum communication between the two parties of the transmission in each process, say E_1, E_2 and E_3 (see Fig.1), the eavesdropping checks can forbid her to monitor the quantum line freely, as the process of each transmission is similar to that in BB84 QKD protocol[3] which is proven unconditionally secure with error correction and privacy amplification.[44] That is, Eve's action will be detected by Charlie and Bob before Bob encodes his message on the photons.

In detail, with the eavesdropping E_1, Eve can only obtain the information about the initial states of the

photons, which is known to every one, not a secret. If Eve wants to steal the information about the operations C_C, she should insert some Trojan-horse photons in the original signal or intercept the photons operated by Charlie and measure them. Obviously, her actions will inevitably leave a trace in the first or second process for eavesdropping check. The reason is that the Trojan-horse photons will be found out when Charlie measures the samples with some PBSs as there are more than one detector clicked for each original signal received from Alice. If Eve exploits the intercept–resending attack to steal the information about Charlie's operations C_C, her action will introduce some errors in the outcomes of the measurements on the samples in the second process for eavesdropping check, the same as that in BB84 protocol.[3] The eavesdropping on the last stage E_3 (the transmission between Bob and Alice) will give Eve nothing about the message C_B as it is encrypted by the operations C_C.[2,29] In a word, Eve cannot steal the information about the secret message C_B freely in an ideal condition. If the noise in the quantum line is not very small, the case is different. We discuss it as follows.

Similar to Ref.[33,45], we can also use the relation of the error rate and the correspondent maximal amount of information obtainable for an eavesdropper from a photon with E_2 to demonstrate the security of the quantum channel between Charlie and Bob. As Bob checks eavesdropping by choosing the two MBs σ_z and σ_x for the samples, the same as the BB84 QKD protocol,[3] the eavesdropping done by Eve can be realized by a unitary operation, say $\hat{E}$, on a larger Hilbert space. That is, Eve can perform the unitary transformation $\hat{E}$ on the photon sent by Charlie (say photon C) and the ancilla whose state is initially in $|0\rangle$[33,45]

$$\hat{E}|0\rangle_C|0\rangle = \sqrt{F}|0\rangle|e_{00}\rangle + \sqrt{D}|1\rangle|e_{01}\rangle, \quad (1)$$

$$\hat{E}|1\rangle_C|0\rangle = \sqrt{D}|0\rangle|e_{10}\rangle + \sqrt{F}|1\rangle|e_{11}\rangle, \quad (2)$$

$$\hat{E}|+x\rangle_C|0\rangle = \frac{1}{\sqrt{2}}[\sqrt{F}(|0\rangle|e_{00}\rangle + |1\rangle|e_{11}\rangle) + \sqrt{D}(|1\rangle|e_{01}\rangle + |0\rangle|e_{10}\rangle)], \quad (3)$$

$$\hat{E}|-x\rangle_C|0\rangle = \frac{1}{\sqrt{2}}[\sqrt{F}(|0\rangle|e_{00}\rangle + |1\rangle|e_{11}\rangle) - \sqrt{D}(|1\rangle|e_{01}\rangle + |0\rangle|e_{10}\rangle)], \quad (4)$$

where F is the fidelity of the state of the photon C after the eavesdropping, D is the probability that Bob and Charlie can detect Eve's action. As the operation $\hat{E}$ is a unitary one, we have the relations as follows:

$$\langle e_{00}|e_{00}\rangle + \langle e_{01}|e_{01}\rangle = F + D = 1, \quad (5)$$

$$\langle e_{10}|e_{10}\rangle + \langle e_{11}|e_{11}\rangle = D + F = 1, \quad (6)$$

$$\langle e_{00}|e_{10}\rangle + \langle e_{01}|e_{11}\rangle = 0. \quad (7)$$

After the eavesdropping check, Bob encodes his message on the photons in the eigenvectors of the MB σ_z with the operations U_0 and U_1. As the states of the samples are random for any eavesdropper, the photon C is in the state $\rho_C = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. After the unitary operation $\hat{E}$, the final state of the photon B and the ancilla e is described as follows:[33,46]

$$\varepsilon(\rho_C) = P_0\varepsilon_{U_0}(\rho_C) + P_1\varepsilon_{U_1}(\rho_C), \quad (8)$$

where P_0 and P_1 are the probabilities encoded with the operation U_0 and U_1, ε_{U_0} and ε_{U_1} are quantum operations describing the evolution of the initial state ρ_C, i.e.

$$\varepsilon_{U_i}(\rho_C) = U_i\hat{E}\rho_C \otimes |e\rangle\langle e|\hat{E}^+U_i^+. \quad (9)$$

The accessible information extracted from the state $\varepsilon(\rho_C)$ is no more than the Holevo bound[11,33,46], i.e.

$$I_{\rm Eve} \le S(\varepsilon(\rho_C)) - [P_0S(\varepsilon_{U_0}(\rho_C)) + P_1S(\varepsilon_{U_1}(\rho_C))] \equiv I_{\max}, \quad (10)$$

where $S(\rho)$ is the von-Neumann entropy of the state ρ, i.e.,

$$S(\rho) = -{\rm Tr}\{\rho\log_2\rho\} = \sum_{i=0}^{3} -\lambda_i\log_2\lambda_i, \quad (11)$$

where λ_i are the roots of the characteristic polynomial $\det(\rho - \lambda I)$.[11]

Suppose that Bob chooses the same probability for choosing the two operations U_0 and U_1, i.e., $P_0 = P_1 = 1/2$, we can obtain the relation between $I_{\max}$ and the probability D as follows when Eve measures the composite system with the basis $\{|0\rangle|e_{00}\rangle, |0\rangle|e_{01}\rangle, |1\rangle|e_{00}\rangle, |1\rangle|e_{01}\rangle\}$ which spans the generic subspace of the Hilbert space $H_C \otimes H_e$ support of $\varepsilon(\hat{\rho}_C)$

$$I_{\max} = -D\log_2 D - (1-D)\log_2(1-D). \quad (12)$$

That is, the probability of being detected D will increase if Eve wants to steal more information about the secret message. If the error rate introduced by noise is not zero, Bob should exploit the single-photon quantum privacy amplification method[47] to reduce the leakage greatly.

3.2. Quantum privacy amplification for single qubits

In brief, the principle of the quantum privacy amplification for two single photons can be described as follows.[47] It includes two controlled-not (CNOT) gates and an H gate, shown in Fig.3. Suppose the original states of the photon 1 and photon 2 are $|\varphi\rangle_1 = a_1|0\rangle + b_1|1\rangle$ and $|\varphi\rangle_2 = a_2|0\rangle + b_2|1\rangle$, respectively. After the operation, the qubit 2 is measured with the MB σ_z and the information of its original state is incorporated into photon 1 as

$$\begin{aligned}|\psi\rangle_{\text{out}} = & \frac{1}{\sqrt{2}}\{(a_1a_2 + b_1b_2)\,|0\rangle_1 \\ & +(a_1b_2 - b_1a_2)\,|1\rangle_1\}\,|0\rangle_2 \\ & +\frac{1}{\sqrt{2}}\{(a_1a_2 - b_1b_2)\,|1\rangle_1 \\ & +(a_1b_2 + b_1a_2)\,|0\rangle_1\}\,|1\rangle_2\,. \end{aligned} \tag{13}$$

This means that the state of the control qubit $|\varphi\rangle_1$ will contain the information of the state of the original target qubit no matter what the result obtained by Bob is. In this way, the probability that Eve gets the complete information about the output state is reduced to r^2. Here r is the original probability that Eve obtains the information about the qubits in a noisy channel.

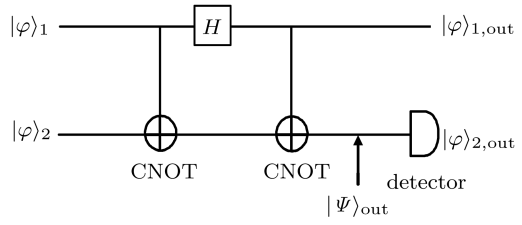


Fig.3. Quantum privacy amplification operation for two qubits.[47]

If the noise in the quantum line somewhat depolarizes the single photons, the legitimate users can purify the polarized single photons[48] and then perform quantum privacy amplification on them for eliminating the information leaked to Eve.[47] These two operations will eliminate the effect of the noise. In this way, the security of this QSDC network scheme is the same as that with an ideal quantum line. Of course, if the noise or the loss in the quantum line is not small, this scheme is not good for transmitting the secret message directly, but for creating a private key efficiently.

4. Discussion and summary

It is of interest to point out the advantage that the sequence S_0 is first sent to the receiver Charlie, not the sender Bob. As the secret message C_B cannot be discarded, different from the outcomes in QKD, the users have to confirm whether the quantum line between them is secure or not.[12,29] Only when the quantum line is secure, the sender Bob would encode his message on the quantum information carriers, a sequence of polarized single photons. The operations done by Charlie C_C carry nothing about the message before Bob codes the photons. That is, C_C is just a raw key, same as that in QKD before Bob and Charlie confirm the security of the transmission between them, and can be discarded. But after the confirmation is done by Bob and Charlie, the operations C_C become the unique private key for decrypting the message C_B. This order of the transmissions ensures that the message C_B is not revealed to Eve even though she monitors the quantum lines. Moreover, the two users, in this time, can exploit quantum privacy amplification to reduce the leakage to a low level as the photons do not carry the secret message.

Another character of this QSDC network scheme is that the initial states prepared by the server Alice are all $|0\rangle$. It will reduce the difficulty for the parties to check eavesdropping. In detail, Bob and Charlie can complete their eavesdropping check without the Alice's help, which can prevent Alice from attacking the communication with a fake signal and cheating.[49] Moreover, Charlie can use a H operation to change a photon into a decoy one efficiently.

Compared with the existing QSDC network schemes,[33−35] a sequence of polarized single photons is enough, not entanglements. The users on the network only need to have the capability of performing single-photon measurement and local unitary operations, not multipartite joint measurements. Moreover, it is unnecessary for the users to have an ideal single-photon source as the quantum signals are prepared by the server, which will simplify the devices of the users on the network. Same as the point-to-point QSDC scheme,[29] almost all the photons can be used to carry the useful information in theory. That is, the efficiency for qubits η_q approaches 100%. Except for checking eavesdropping, it is unnecessary for the users to exchange the classical information. Thus this QSDC network scheme is an economical one.

Certainly, on the one hand, if the sender Bob has a perfect device for measuring a sequence of single photons, he can send no photon to the server Alice and he measures them himself in this network scheme. In this way, the server Alice has more space for dealing with other users' request. In essence, the server Alice only provides the service for preparing a sequence of single photons in this modified network scheme. On the other hand, if a perfect device for measuring single photons is very expensive in a practical application, the sender Bob can send the photon sequence to the server Alice for determining their states. This structure will reduce the requirements on the users' devices largely at the expense of Alice's resource.

In summary, we have presented a new QSDC network scheme with a sequence of polarized single photons S. In this scheme, the server prepares all the quantum signals initially in the same state $|0\rangle$, which will reduce the difficulty for the parties to check eavesdropping. After confirming the security of the single photons encrypted by the receiver, the sender encodes his secret message directly on them. After the server announces the combined operations on the photons, the receiver can read out the message directly. This scheme is an economical one as it is the easiest way for QSDC network communication securely. If the noise or the loss in the quantum line is not small, the parties can use this model for creating a private key efficiently, not exchanging the secret message.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum computation and quantum information* (Cambridge: Cambridge University Press)

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

[3] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE) p 175

[4] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

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

[6] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[7] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097

[8] Ma H Q, Li Y L, Zhao H and Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)

[9] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese)

[10] Shimizu K and Imoto N 1999 *Phys. Rev.* A **60** 157

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

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

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

[14] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

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

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

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

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

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

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

[21] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 277

[22] Nguyen B A 2004 *Phys. Lett.* A **328** 6

[23] Deng F G, Li X H, Li C Y, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676

[24] Lee H, Lim J and Yang H 2006 *Phys. Rev.* A **73** 042305

[25] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys. Lett.* **24** 23

[26] 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

[27] Shimizu K and Imoto N 2000 *Phys. Rev.* A **62** 054303

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

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

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

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

[32] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

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

[34] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y and Deng F G 2006 *Chin. Phys. Lett.* **23** 1080

[35] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys. Lett.* **22** 2473

[36] Michler P, Kiraz A, Becher C, Schoenfeld WV, Petroff P M, Zhang L D, Hu E and Imamoglu A 2000 *Science* **290** 2282
Yuan Z L, Kardynal B E, Stevenson R M, Shields A J, Lobo C J, Cooper K, Beattie N S, Ritchie D A and Pepper M 2002 *Science* **295** 102

[37] Phoenix S J D, Barnett S M, Townsend P D and Blow K J 1995 *J. Mod. Opt.* **42** 1155

[38] Townsend P D 1997 *Nature* **385** 47

[39] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651

[40] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317

[41] Deng F G, Liu X S, Ma Y J, Xiao L and Long G L 2002 *Chin. Phys. Lett.* **19** 893

[42] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896
[43] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
Deng F G, Li X H, Zhou H Y and Zhang Z J 2006 *Phys. Rev.* A **73** 049901
[44] Lo H K and Chau H F 1999 *Science* **283** 2050
Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[45] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[46] Degiovanni I P, Berchera I R, Castelletto S, Rastello M L, Bovino F A, Colla A M and Castagnoli G 2005 *Phys. Rev.* A **71** 016302
[47] Deng F G and Long G L 2006 *Commun. Theor. Phys.* **46** 443
[48] Cirac J I, Ekert A K and Macchiavello C 1999 *Phys. Rev. Lett.* **82** 4344
Ricci M, Martini F D, Cerf N J, Filip R, Fiurasek J and Macchiavello C 2004 *Phys. Rev. Lett.* **93** 170501
[49] Deng F G, Li X H, Chen P, Li C Y and Zhou H Y 2006 quant-ph/0604060