Faithful deterministic secure quantum communication and authentication protocol based on hyperentanglement against collective noise*

Chang Yan(昌 燕)†, Zhang Shi-Bin(张仕斌), Yan Li-Li(闫丽丽), and Han Gui-Hua(韩桂华)

College of Information Security Engineering, Chengdu University of Information Technology, Chengdu 610225, *China*

(Received 6 January 2015; revised manuscript received 2 February 2015; published online 20 June 2015)

Higher channel capacity and security are difficult to reach in a noisy channel. The loss of photons and the distortion of the qubit state are caused by noise. To solve these problems, in our study, a hyperentangled Bell state is used to design faithful deterministic secure quantum communication and authentication protocol over collective-rotation and collective-dephasing noisy channel, which doubles the channel capacity compared with using an ordinary Bell state as a carrier; a logical hyperentangled Bell state immune to collective-rotation and collective-dephasing noise is constructed. The secret message is divided into several parts to transmit, however the identity strings of Alice and Bob are reused. Unitary operations are not used.

Keywords: collective noise, hyperentanglement, channel capacity

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/24/8/080306

1. Introduction

The principle of quantum mechanics provides the theoretical basis for exchanging information in an unconditionally secure manner. However, channel noise may make information be exchanged in an unsafe way and with low fidelity. A high qubit error rate (QER) caused by channel noise has become an obstacle restricting the further development of quantum communication. The existence of channel noise not only reduces the fidelity of information, but also gives eavesdroppers chances to steal secret information beneath the mask of noise.

In the past two decades, quantum secure communication has developed rapidly. Since Bennett and Brassard[1] proposed the first quantum key distribution (QKD[1–6]) protocol, another important branch in quantum communication–QSDC[7–19] has been investigated by many groups. So far, many important protocols have been proposed. In 2002, Long and Liu[7] put forward the first QSDC protocol, in which the secret message is transmitted directly. In 2003, Deng *et al.*[8] published the famous two-step QSDC protocol (called the two-step protocol). In the two-step protocol, the way of designing the protocol for direct communication of a secret message was given clearly and it was put forward for the first time that QSDC should be performed with a quantum data block. In 2004, the first QSDC based on a sequence of single photons (called the DL04 protocol) was given by Deng and Long.[9] In 2005, the first QSDC protocol based on super-dense coding was developed by Wang *et al.*[10] In the same year, Wang *et al.*[11] proposed a QSDC scheme using multi-particle entanglement. In 2007, Li *et al.*[12] presented a QSDC protocol with quantum encryption. In 2011, the first QSDC protocol based on photonic polarization-spatial hyperentanglement was presented by Wang *et al.*[13] Meanwhile, many interesting and valuable QSDC schemes with special characteristics were published. Gu *et al.* put forward a robust QSDC protocol based on a quantum one-time pad over a collective-noise channel[14] and a two-step QSDC scheme with hyperentanglement.[15] Liu *et al.*[16] proposed a high-capacity QSDC scheme with single photons in both polarization and spatial-mode degrees of freedom. Sun *et al.*[17] developed a QSDC scheme with two-photon four-qubit cluster states. Ren *et al.*[18] published a robust QSDC protocol based on the spatial-mode entanglement of a two-photon system. Gu *et al.*[19] proposed a robust QSDC protocol with spatial quantum states of single photons.

In recent investigations, some researches about quantum secure communication under noisy conditions were reported.[20–45] These researches focused on the following aspects. (i) How were the effects of noise reduced? Entanglement purification[25,26,38,39,42] and entanglement concentration[29,32,33,40,41,43,44] were respectively utilized to reduce the effects of noise. (ii) How is the communication immune to noise? The fault tolerant quantum secure communication was implemented by constructing a decoherence-free subspace (which is immune to noise) and transmitting secret information in the subspace.[21,22,24,30,31,35] (iii) How is the influence of noise sidestepped? The quantum states were de-

*Project supported by the National Natural Science Foundation of China (Grant No. 61402058), the Science and Technology Support Project of Sichuan Province, China (Grant No. 2013GZX0137), the Fund for Young Persons Project of Sichuan Province, China (Grant No. 12ZB017), and the Foundation of Cyberspace Security Key Laboratory of Sichuan Higher Education Institutions, China (Grant No. szjj2014-074).

†Corresponding author. E-mail: cyttkl@cuit.edu.cn

© 2015 Chinese Physical Society and IOP Publishing Ltd

livered in spatial-mode degrees of freedom or frequency degrees of freedom, which suffers little effect of noise.[34,36] (iv) How are the errors corrected after communication? Quantum error correction[27,45] was used to correct error caused by noise. Besides these methods, Li *et al.*[20] and Deng *et al.*[28] also proposed self-error-rejecting methods to resist the effect of collective noise. However, to reduce or eliminate the influence of noise, the auxiliary particles were introduced and delivered through the quantum channel,[21,22,24,30–33,35,38] which reduced the channel capacity inevitably. Also in references,[25,26,34,36] only how to reduce or sidestep the influence of noise was considered, no attention was paid to increasing the channel capacity. Therefore, more attention should be paid to the research about high channel capacity quantum secure communication under noisy conditions.

Supper-dense coding is the primary way to increase the channel capacity. Its essential idea is to encode as much information as possible with the minimum number of particles. The principal methods to implement supper-dense coding are to use entanglement states, high-dimensional entanglement states or hyperentanglement states as quantum carriers and combine sublime designing ideas. In most supper-dense coding protocols which are based on entanglement states, the sender encodes secret information on ordinary entanglement states such as Bell states and GHZ states, and the receiver analyzes the Bell states or GHZ states. The receiver decrypts the secret information by distinguishing four Bell states or eight GHZ states. Yet the experiment indicated that in polarization degrees of freedom we cannot completely distinguish Bell states nor GHZ states with linear optical elements.[46] Therefore, the channel capacity cannot achieve theoretical values. Furthermore, although some probabilistic schemes can distinguish Bell states or GHZ states completely, the maximum success chances of these schemes are only 0.5 and 0.25 respectively.[46] Thus, the channel capacity is not increased either. High-dimensional entanglement state is a state in d-dimensional ($d > 2$) Hilbert space, which can increase the channel capacity greatly, because one high-dimensional particle can carry more than one bit of classical information. For example, the highest channel capacity of supper-dense coding protocol based on d-dimensional ($d > 2$) Bell states can reach $\log_2 d^2$.[10] However, because high-dimensional entanglement states are difficult to prepare and measure, supper-dense coding protocols based on high-dimensional[10] entanglement states are more difficult to implement.

Hyperentanglement[46–62] is a state that is simultaneously entangled in multiple degrees of freedom. One hyperentanglement particle can also carry more than one bit of classical information. Compared with high-dimensional entanglement, hyperentanglement is easy to prepare and measure;[50] based on hyperentanglement, the receiver can easily distinguish all Bell states and GHZ states completely. In 2003, Walborn *et al.*[47] proposed a protocol based on momentum and polarization degrees of freedom, which distinguishes four Bell states completely. In 2007, the conclusion was verified experimentally.[48] In 2011, Wang *et al.* put forward a supper-dense coding protocol based on hyperentanglement, and the channel capacity achieved four bits of classical information per particle.[50] Recently, also other scholars were involved in the preparation and analysis of hyperentanglement in multiple degrees of freedom,[47–49,52,55–57] quantum communication protocols based on hyperentanglement[50,51] and quantum information processing.[49,53,54,58–62] Sheng *et al.*[49] discussed the applications in the quantum teleportation of a particle in an unknown state in two different degrees of freedom and in the entanglement swapping of hyperentangled states. In 2012, Ren *et al.*[53] and Wang *et al.*[54] studied complete hyperentangled Bell-state analysis for photon systems. Ren *et al.* studied deterministic photonic spatial-polarization hyper-controlled-not gate assisted by a quantum dot[58] and hyper-parallel photonic quantum computation.[60] Ren *et al.* proposed a hyperentanglement purification scheme assisted by diamond nitrogen–vacancy (NV) centers inside a photonic crystal cavity[59] and two-step hyperentanglement purification with the quantum-state-joining method.[62] Ren *et al.*[60] also developed a hyperentanglement concentration scheme for two-photon four-qubit system with linear optics. All these researches laid the foundation for the research of quantum secure communication. However, these supper-dense coding studies are under ideal condition without noise.

In this study, two protocols based on a hyperentanglement state are proposed over a collective-rotation and a collective-dephasing noisy channel respectively. The two protocols are immune to collective-rotation noise and collective-dephasing noise respectively. In the whole process, with hyperentangled Bell state $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ or $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{dp}}$ as carriers respectively, Alice and Bob transmit two bits of classical information by delivering two particles once over the collective-rotation and collective-dephasing noisy channel respectively. A man-in-the-middle attack can be resisted in our protocols. The secret message is divided into several parts to transmit, however the identity string of Alice and Bob is reused. Unitary operations are not used.

2. Description of hyperentanglement

Hyperentanglement is a state that is simultaneously entangled in multiple degrees of freedom. A photon has multiple quantum degrees of freedom. Each degree of freedom can define a qubit under proper conditions. Theoretically, different degrees of freedom can form entanglement, which is called hyperentanglement. For example, a photon with two degrees

of freedom can entangle another photon with two degrees of freedom, therefore, a photon can be used as two qubits.

A hyperentangled Bell state in polarization and spatial-mode degrees of freedom can be described as follows:

$$\left|\Phi_{AB}^{-}\right\rangle_{PS}=\frac{1}{2}(|00\rangle-|11\rangle)_{AB}\otimes(|a_1b_1\rangle-|a_2b_2\rangle)_{AB}. \quad (1)$$

Here $|0\rangle$ and $|1\rangle$ denote the horizontal and the vertical polarizations of photons respectively. The subscripts A and B represent the two photons in the hyperentangled state, a_1 (b_1) and a_2 (b_2) are the different spatial modes for photons A and B. The subscript P denotes the polarization degree of freedom and S is the spatial-mode degree of freedom. A pump pulse of ultraviolet light passes through a beta barium borate (BBO) crystal and produces correlated pairs of photons in the modes a_1 and b_1. Then it is reflected and traverses the crystal a second time and produces correlated pairs of photons in the modes a_2 and b_2. Figure 1 is the elementary diagram of hyperentanglement in polarization and spatial-mode degrees of freedom.

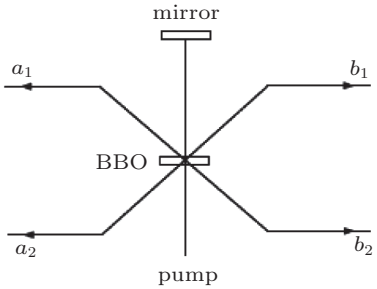


Fig. 1. Elementary diagram of hyperentanglement in polarization and spatial-mode degrees of freedom.

For a hyperentangled Bell state in polarization and spatial-mode degrees of freedom, there are 16 Bell states, which can be denoted as

$$|\xi_{AB}\rangle_{PS}=|\Theta\rangle_P\otimes|\Xi\rangle_S. \quad (2)$$

Here $|\Theta\rangle_P$ denotes one of the following four Bell states in polarization degree of freedom:

$$\left|\phi^{\pm}\right\rangle_P=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)_{AB}, \quad (3)$$

$$\left|\psi^{\pm}\right\rangle_P=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)_{AB}. \quad (4)$$

$|\Xi\rangle_S$ denotes one of the following four Bell states in spatial-mode degree of freedom:

$$\left|\phi^{\pm}\right\rangle_S=\frac{1}{\sqrt{2}}(|a_1b_1\rangle\pm|a_2b_2\rangle)_{AB}, \quad (5)$$

$$\left|\psi^{\pm}\right\rangle_S=\frac{1}{\sqrt{2}}(|a_1b_2\rangle\pm|a_2b_1\rangle)_{AB}. \quad (6)$$

By using CHBSA,[49] 16 hyperentangled Bell states can be distinguished completely. $Z^P=\{|0\rangle,|1\rangle\}$ and

$$X^P=\left\{|+\rangle_P=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\,|-\rangle_P=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right\}$$

can be selected as two non-orthodox measurement bases in the polarization degree of freedom. $Z^S=\{|a_1\rangle,|a_2\rangle\}$ and

$$X^S=\left\{|+\rangle_S=\frac{1}{\sqrt{2}}(|a_1\rangle+|a_2\rangle),\quad |-\rangle_S=\frac{1}{\sqrt{2}}(|a_1\rangle-|a_2\rangle)\right\}$$

can be selected as two non-orthodox measurement bases in the spatial-mode degree of freedom.

3. DSQC scheme with authentication against a collective-rotation noise

3.1. Protocol

A collective-rotation noise can be described as

$$\begin{aligned}U_r|0\rangle&=\cos\theta|0\rangle+\sin\theta|1\rangle,\\ U_r|1\rangle&=-\sin\theta|0\rangle+\cos\theta|1\rangle.\end{aligned} \quad (7)$$

Here θ is the noise parameter, which fluctuates with time. That is, if a $|0\rangle$ state is delivered through channel with collective-rotation noise, the state will change into $\cos\theta|0\rangle+\sin\theta|1\rangle$; while, a $|1\rangle$ state will change into $-\sin\theta|0\rangle+\cos\theta|1\rangle$. For collective-rotation noise, $|\phi^+\rangle$ and $|\psi^-\rangle$ are invariant. Therefore, logical qubits immune to collective-rotation noise are described respectively as

$$|0\rangle_L\equiv\left|\phi^+\right\rangle,\quad |1\rangle_L\equiv\left|\psi^-\right\rangle. \quad (8)$$

Now let us briefly describe the DSQC protocol based on hyperentanglement against collective-rotation noise. We suppose that the sender, Bob, wants to transmit his secret message to the legitimate receiver, say Alice. Alice and Bob have the secret w-bit string identity (ID) representing their identities. Suppose that Bob's secret message is a series of classical 0 or 1 numbers in order, called M.

For a hyperentangled Bell state

$$\left|\Phi_{AB}^{-}\right\rangle_{PS}=\frac{1}{2}(|00\rangle-|11\rangle)_{AB}\otimes(|a_1b_1\rangle-|a_2b_2\rangle)_{AB},$$

if particle B is delivered through quantum channel with collective- rotation noise, to resist the effect of noise, the sender should represent particle B as a logical quantum state, that is $|\phi^+,|0\rangle_B$ should be expressed as $|\phi^+\rangle_{B_1B_2}$, and $|1\rangle_B$ is expressed as $|\psi^-\rangle_{B_1B_2}$. Therefore, the logical hyperentangled Bell state should be expressed as

$$\begin{aligned}&\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}=\frac{1}{2}(|0\rangle_A\left|\phi^+\right\rangle_{B_1B_2}-|1\rangle_A\left|\psi^-\right\rangle_{B_1B_2})\\ &\otimes(|a_1b_1c_1\rangle-|a_2b_2c_2\rangle)_{AB_1B_2}\\ =&\frac{1}{2\sqrt{2}}[|0\rangle_A(|00\rangle_{B_1B_2}+|11\rangle_{B_1B_2})\\ &-|1\rangle_A(|01\rangle_{B_1B_2}-|10\rangle_{B_1B_2})]\\ &\otimes(|a_1b_1c_1\rangle-|a_2b_2c_2\rangle)_{AB_1B_2}\end{aligned}$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle + |011\rangle - |101\rangle + |110\rangle)_{AB_1B_2} \otimes (|a_1b_1c_1\rangle - |a_2b_2c_2\rangle)_{AB_1B_2}. \quad (9)$$

Step 1 Alice prepares N ordered $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ states. We denote the ordered $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ states as $\{[P_1(A),P_1(B_1),\ P_1(B_2)],\ [P_2(A),P_2(B_1),\ P_2(B_2)],\ldots,[P_N(A),\ P_N(B_1),P_N(B_2)]\}$, where the subscript indicates the order of each state in the sequence, and A, B_1, B_2 represent the three particles of each state. Alice takes particle A from each state to form an ordered particle sequence $\{P_1(A),\ P_2(A),\ldots,\ P_N(A)\}$, called the S_A sequence. The remaining particles constitute an S_B sequence, denoted as $\{P_1(B_1),\ P_1(B_2),\ P_2(B_1),\ P_2(B_2),\ldots,\ P_N(B_1),\ P_N(B_2)\}$. The idea of block transmission is similar to the original protocol.[7] Alice prepares another $2N/3$ ordered $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ states, which form a sequence S_{T}. The S_T is denoted as $\{T_1(A),T_1(B_1),\ T_1(B_2),\ T_2(A),T_2(B_1),\ T_2(B_2),\ldots,\ T_N(A),T_N(B_1),\ T_N(B_2)\}$, which is used as decoy photons.

Step 2 Alice inserts the decoy photons S_T into sequence S_B according to ID, forming a new sequence S_B'. For example, if the i-th bit of ID is 0, Alice inserts the i-th photon of S_T behind the i-th photon of S_B; if the i-th bit of ID is 1, Alice inserts the i-th photon of S_T before the i-th photon of S_B. Only Alice and Bob know the positions of these decoy photons. Then Alice sends S_B' to Bob.

Step 3 After Bob receives S_B', Bob extracts the decoy photons from S_B' according to ID. Bob performs three single-qubit measurements $Z_A^P Z_{B_1}^P Z_{B_2}^{\mathrm{P}}$ on the S_T extracted respectively. In the ideal cases, each result should be in one of the four $|000\rangle$, $|011\rangle$, $|101\rangle$, $|110\rangle$ states with equal probability. If the error rate is low enough Bob believes that Alice is legal and no eavesdropping exists. In this condition, the communication goes on. Otherwise Bob interrupts it.

Step 4 Alice and Bob perform $S\otimes S\otimes S$ and $H\otimes H\otimes H$ operations on particles AB_1B_2 in turn respectively. Then the combined system of AB_1B_2 will change into

$$\begin{aligned}\left|\Phi_{AB}^{-}\right\rangle_{\mathrm{PS}}^{\mathrm{r}'} &= \frac{1}{2}(|1\rangle_A|10\rangle_{B_1B_2} - |0\rangle_A|01\rangle_{B_1B_2}) \otimes (|a_1b_1c_1\rangle - |a_2b_2c_2\rangle)_{AB_1B_2} \\ &= \frac{1}{2}(|{+}{+}{-}\rangle + |{-}{-}{-}\rangle - |{+}{-}{+}\rangle - |{-}{+}{+}\rangle)_{AB_1B_2} \otimes (|a_1b_1c_1\rangle - |a_2b_2c_2\rangle)_{AB_1B_2}. \quad (10)\end{aligned}$$

Here, the phase gate S and Hadamard gate H are represented respectively as

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (11)$$

Step 5 Bob publishes the photons that he does not receive in S_B, Alice discards the corresponding photons in S_A. Therefore, photons in S_B will be always one-to-one matching with photons in S_A.

Step 6 Alice measures photons in S_A with basis $Z^S = \{|a_1\rangle, |a_2\rangle\}$ (measurement basis in spatial-mode degree of freedom). Then according to ID, Alice measures photons in S_A with basis $Z^P = \{|0\rangle, |1\rangle\}$ or $X^P = \{|+\rangle_P,\ |-\rangle_P\}$ (non-orthodox measurement basis in polarization degree of freedom) in order. That is, if the bit of ID is "0", Alice measures the corresponding photon of S_A with the Z^P basis; otherwise, Alice uses the X^P basis. If the measurement result is $|0\rangle$ or $|+\rangle$, Alice refers to the result as "0"; otherwise, Alice refers to the result as "1". By measuring photons in S_A with the basis in spatial-mode and polarization degree of freedom, Alice will obtain the measurement result $|a_1 0\rangle$, $|a_2 0\rangle$, $|a_1 1\rangle$, $|a_2 1\rangle$ or $|a_1+\rangle$, $|a_2+\rangle$, $|a_1-\rangle$, $|a_2-\rangle$ with equal probability. At the same time the states of particles B_1B_2 are fixed: they are $|b_1c_1\rangle|01\rangle$, $|b_2c_2\rangle|01\rangle$, $|b_1c_1\rangle|10\rangle$, $|b_2c_2\rangle|10\rangle$ or $|b_1c_1\rangle|+-\rangle(|-+\rangle)$, $|b_2c_2\rangle|+-\rangle(|-+\rangle)$, $|b_1c_1\rangle|++\rangle(|--\rangle)$, $|b_2c_2\rangle|++\rangle(|--\rangle)$ respectively. And if the measurement result of Alice is $|a_1 0\rangle$, $|a_2 0\rangle$, $|a_1 1\rangle$, $|a_2 1\rangle$, the measurement result of Bob must be $|b_1c_1\rangle|01\rangle$, $|b_2c_2\rangle|01\rangle$, $|b_1c_1\rangle|10\rangle$, $|b_2c_2\rangle|10\rangle$ respectively; and if the measurement result of Alice is $|a_1+\rangle$, $|a_2+\rangle$, $|a_1-\rangle$, $|a_2-\rangle$, the measurement result of Bob must be $|b_1c_1\rangle|+-\rangle(|-+\rangle)$, $|b_2c_2\rangle|+-\rangle(|-+\rangle)$, $|b_1c_1\rangle|++\rangle(|--\rangle)$, $|b_2c_2\rangle|++\rangle(|--\rangle)$ respectively. If we use binary string $\{00,\ 01,\ 10,\ 11\}$ to express $\{|a_1 0\rangle,\ |a_2 0\rangle,\ |a_1 1\rangle,\ |a_2 1\rangle\}$, $\{|a_1+\rangle,\ |a_2+\rangle,\ |a_1-\rangle,\ |a_2-\rangle\}$, $\{|b_1c_1\rangle|01\rangle,\ |b_2c_2\rangle|01\rangle,\ |b_1c_1\rangle|10\rangle,\ |b_2c_2\rangle|10\rangle\}$ or $\{|b_1c_1\rangle|+-\rangle(|-+\rangle),\ |b_2c_2\rangle|+-\rangle(|-+\rangle),\ |b_1c_1\rangle|++\rangle(|--\rangle),\ |b_2c_2\rangle|++\rangle(|--\rangle)\}$, Alice and Bob will obtain an identical binary string C, which is a real random number.

Step 7 Bob also measures photons B_1B_2 with the same method as Alice. If the measurement result is $|01\rangle$, $|+-\rangle$ or $|-+\rangle$, Bob denotes it as "0"; otherwise as "1". By doing so, Bob will obtain C.

Step 8 Assuming the length of C to be L, Bob divides the secret message M into several parts. Each part is termed M_i $(i = 1,2,\ldots)$, which includes the classical secret information about L bits. Bob encrypts the secret message M_1 with C bit by bit using XOR operation and obtains C_1. That is, $C_1 = M_1$ XOR C. Bob publishes C_1.

Step 9 Alice decrypts C_1 with C bit by bit using XOR operation and obtains M_1. That is, $M_1 = C_1$ XOR C.

Step 10 Alice stores secret message M_1.

Step 11 Alice and Bob begin the next transmission, until all secret messages are finished.

3.2. Security analysis

Because the DSQC scheme is designed to be immune to collective-rotation noise, the eavesdropping will be found more easily. Thus, the security of the protocol is mainly guaranteed by the identity string ID (shared by Alice and Bob) and the eavesdropping detection strategy based on $\left|\Phi_{AB}^{-}\right\rangle_{P}^{\mathrm{r}} =$

$\frac{1}{2}(|000\rangle+|011\rangle-|101\rangle+|110\rangle)_{AB_1B_2}$ ($\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ in polarization degree of freedom). Because identity authentication is implemented based on the identity string, the protocol will not be threatened by a man-in-the-middle attack. Next, we analyze the eavesdropping detection rate of the protocol.

3.2.1. Analysis of the detection rate

In the DSQC scheme immune to collective-rotation noise, to reduce the state one needs to prepare the

$$\left|\Phi_{AB}^{-}\right\rangle_{P}^{\mathrm{r}}=\frac{1}{2}(|000\rangle+|011\rangle-|101\rangle+|110\rangle)_{AB_1B_2}$$

state that is used as decoy photons to detect eavesdropping (that is, only one state is needed). Because the positions of decoy photons are secret, Eve cannot discriminate between decoy photons and information photons (photons in S_B).

According to Stingspring dilation theorem, Eve's eavesdropping can be implemented by a unitary operation E acting on a bigger Hilbert space $H_{AB_1B_2}\otimes H_E$. The eavesdropping can be represented as

$$\begin{aligned}E\otimes|0\rangle|x\rangle_E&=a|0\rangle|x_0\rangle_E+b|1\rangle|x_1\rangle_E,\\ E\otimes|1\rangle|x\rangle_E&=n|0\rangle|y_0\rangle_E+m|1\rangle|y_1\rangle_E.\end{aligned}\tag{12}$$

Here, $|x\rangle_E$ is the initial state of Eve's auxiliary particle and $|a|^2+|b|^2=1$, $|m|^2+|n|^2=1$. $|x_0\rangle_E$, $|x_1\rangle_E$, $|y_0\rangle_E$, $|y_1\rangle_E$ are pure states uniquely determined by unitary operation E.

The unitary operation E of Eve can be represented as

$$E=\begin{pmatrix}a & n\\ b & m\end{pmatrix}.\tag{13}$$

The complex numbers a, b, m, n satisfy $EE^{\dagger}=I$. Therefore, $|a|^2=|m|^2$ and $|b|^2=|n|^2$ can be obtained.

After Eve's eavesdropping, the combined system changes into

$$\begin{aligned}|\psi\rangle_{\mathrm{Eve}}=&\ E\otimes E\otimes E\otimes[\frac{1}{2}(|0x0x0x\rangle\\ &+|0x1x1x\rangle-|1x0x1x\rangle+|1x1x0x\rangle)]\\ =&\ \frac{1}{2}[(a|0x_0\rangle+b|1x_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\ &\otimes(a|0x_0\rangle+b|1x_1\rangle)+(a|0x_0\rangle+b|1x_1\rangle)\\ &\otimes(n|0y_0\rangle+m|1y_1\rangle)\otimes(n|0y_0\rangle+m|1y_1\rangle)\\ &-(n|0y_0\rangle+m|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\ &\otimes(n|0y_0\rangle+m|1y_1\rangle)+(n|0y_0\rangle+m|1y_1\rangle)\\ &\otimes(n|0y_0\rangle+m|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)]\\ =&\ \frac{1}{2}[a^3|0x_00x_00x_0\rangle+a^2b|0x_00x_01x_1\rangle\\ &+a^2b|0x_01x_10x_0\rangle+ab^2|0x_01x_11x_1\rangle\\ &+a^2b|1x_10x_00x_0\rangle+b^2a|1x_10x_01x_1\rangle\\ &+b^2a|1x_11x_10x_0\rangle+b^3|1x_11x_11x_1\rangle\\ &+an^2|0x_00y_00y_0\rangle+amn|0x_00y_01y_1\rangle\\ &+anm|0x_01y_10y_0\rangle+am^2|0x_01y_11y_1\rangle\\ &+bn^2|1x_10y_00y_0\rangle+bmn|1x_10y_01y_1\rangle\\ &+bnm|1x_11y_10y_0\rangle+bm^2|1x_11y_11y_1\rangle\\ &-an^2|0y_00x_00y_0\rangle-amn|0y_00x_01y_1\rangle\\ &-n^2b|0y_01x_10y_0\rangle-mbn|0y_01x_11y_1\rangle\\ &-amn|1y_10x_00y_0\rangle-am^2|1y_10x_01y_1\rangle\\ &-nbm|1y_11x_10y_0\rangle-m^2b|1y_11x_11y_1\rangle\\ &+an^2|0y_00y_00x_0\rangle+bn^2|0y_00y_01x_1\rangle\\ &+nam|0y_01y_10x_0\rangle+mnb|0y_01y_11x_1\rangle\\ &+amn|1y_10y_00x_0\rangle+bmn|1y_10y_01x_1\rangle\\ &+m^2a|1y_11y_10x_0\rangle+m^2b|1y_11y_11x_1\rangle].\end{aligned}\tag{14}$$

After Bob receives S_B' (mixture of S_B and S_T), Bob extracts S_T and performs three single-qubit measurements $Z_A^PZ_{B_1}^PZ_{B_2}^P$ on S_T. The probability without an eavesdropper is

$$\begin{aligned}p(|\psi_{\mathrm{E}}\rangle)=&\ \frac{1}{4}(3|n^2a|^2+3|b^2a|^2+3|m^2a|^2\\ &+6|mnb|^2+|a^3|^2).\end{aligned}\tag{15}$$

Because $|a|^2=|m|^2$ and $|b|^2=|n|^2$, then

$$p(|\psi_{\mathrm{E}}\rangle)=|a|^6+3|a|^2|b|^4.\tag{16}$$

Let $|a|^2=s$ and $|b|^2=t$, then $t+s=1$, we can obtain

$$p(|\psi_E\rangle)=|a|^6+3|a|^2|b|^4=4s^3-6s^2+3s.$$

Therefore, the error rate of each qubit is

$$\sigma=1-p(|\psi_E\rangle)=1-4s^3+6s^2-3s,\tag{17}$$

which can also be seen as the lower bound of the detection rate of each qubit eavesdropped:

$$d=1-p(|\psi_{\mathrm{E}}\rangle)=1-4s^3+6s^2-3s.\tag{18}$$

According to the theory of von Neumann entropy, the maximum amount of information contained in qubit $|0\rangle$ is termed

$$I_{|0\rangle}=-s\log_2 s-(1-s)\log_2(1-s)=H(s).\tag{19}$$

And the maximum amount of information contained in qubit $|1\rangle$ is termed

$$I_{|1\rangle}=-t\log_2 t-(1-t)\log_2(1-t)=H(t).\tag{20}$$

For a qubit transmitting in a quantum channel, it will be in $|0\rangle$ or $|1\rangle$ state with equal probability ($p=0.5$); therefore, the total information that Eve can eavesdrop in a qubit will be

$$I=\frac{1}{2}(I_{|0\rangle}+I_{|1\rangle})=\frac{1}{2}[H(s)+H(t)]=H(s).\tag{21}$$

According to Eq. (18), we obtain the relationship between s and d as follows:

$$-4s^3+6s^2-3s+1-d=0.\tag{22}$$

Let

$$s = Y - \frac{6}{3*(-4)} = Y + \frac{1}{2},$$

and substitute s into Eq. (22), then we will obtain that

$$-4Y^3 + \frac{1}{2} - d = 0, \tag{23}$$

and

$$Y = \sqrt[3]{\frac{1-2d}{8}}. \tag{24}$$

Therefore,

$$s = \sqrt[3]{\frac{1-2d}{8}} + \frac{1}{2}. \tag{25}$$

We obtain the relationship between I (the maximum amount of information) and d (the detection rate) as follows:

$$I(d) = H(s) = H\left(\sqrt[3]{\frac{1-2d}{8}} + \frac{1}{2}\right). \tag{26}$$

From Fig. 2 we find that when $d = 0.5$, then $I = 1$, which is the maximum amount of information Eve can eavesdrop. That is, if Eve performs an attack by using ancillary particles, when she obtains the maximum amount of information on one qubit, the detection rate or qubit error rate reaches 50%.

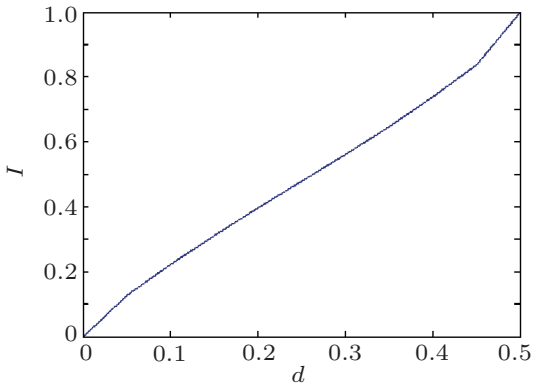


Fig. 2. (color online) Relationship between I and d.

3.2.2. Security of ID

The ID is shared by Alice and Bob previously. They can share it by executing the QKD protocol; therefore the QKD protocol can guarantee the security of the ID in the process of quantum key distribution. In the process of secret transmission in our protocol, the ID will not be delivered in a classical channel in any form. Therefore, in the process of a secret transmission, the ID will be safe. The only unsafe factor is the improper storage of Alice and Bob. Thus, without considering the unsafe factor of improper storage, the ID can be reused in an unconditionally safe manner.

3.3. Discussion

The original decoy photon idea is proposed by Li *et al*. in Refs. [63] and [64]. In Refs. [63] and [64], a group of non-orthodox photons are used as decoy photons. In our protocol, the unique qubits

$$\left|\Phi_{AB}^{-}\right\rangle_P^{\mathrm{r}} = \frac{1}{2}(|000\rangle + |011\rangle - |101\rangle + |110\rangle)_{AB_1B_2}$$

are used as decoy photons. However, the unique qubits $\left|\Phi_{AB}^{-}\right\rangle_P^{\mathrm{r}}$ will not reduce the security of this detection strategy, the reasons are shown as follows: i) because the position of S_T in S_B' is secret, Eve cannot obtain the secret by any measurement; ii) because Alice and Bob measure the information photons (S_B) with Z^P or X^P basis according to ID (which is shared by Alice and Bob only), the decoy photons will be measured with three single-qubit measurements $Z_A^P Z_{B_1}^P Z_{B_2}^P$, to eavesdrop on the secret, Eve may run a great risk of measuring decoy photons with the X^P basis. That is, to eavesdrop on the secret, Eve has to measure photons with the X^P basis sometimes, however, because Eve does not know which photons should be measured with the X^P basis and which photons should be measured with the Z^P basis, she may measure decoy photons with the X^P basis by mistake, which will be found by Alice and Bob easily.

4. DSQC scheme with authentication against a collective-dephasing noise

4.1. Protocol

A collective-dephasing noise can be described as

$$U_d|0\rangle = |0\rangle \quad U_d|1\rangle = \mathrm{e}^{\mathrm{i}\phi}|1\rangle. \tag{27}$$

Here ϕ is the noise parameter, which fluctuates with time. That is, if a $|0\rangle$ state is delivered through the channel with collective-dephasing noise, the state will not change; while a $|1\rangle$ state will change into $\mathrm{e}^{\mathrm{i}\phi}|1\rangle$. Because two physical qubits with anti-parallel parity obtain the same phase factor $\mathrm{i}\phi$, to defend against collective-dephasing noise, two anti-parallel qubits can form a logical qubit. The logical qubits immune to collective-dephasing noise can be described by Eq. (8), and given as

$$|0\rangle_L \equiv |0\rangle|1\rangle \quad \text{and} \quad |1\rangle_L \equiv |1\rangle|0\rangle. \tag{28}$$

Now we briefly describe the DSQC protocol based on hyperentanglement against a collective-dephasing noise. Suppose that Bob is the sender and Alice is the legitimate receiver. Alice and Bob have the secret w-bit string ID representing their identities. Bob's secret message is a series of classical 0 or 1 numbers in order, called M.

For a hyperentangled Bell state

$$\left|\Phi_{AB}^{-}\right\rangle_{PS} = \frac{1}{2}(|00\rangle - |11\rangle)_{AB} \otimes (|a_1b_1\rangle - |a_2b_2\rangle)_{AB},$$

if particle B is delivered through the quantum channel with collective-dephasing noise, to resist the effect of noise, the sender should represent particle B as a logical quantum state, that is, $|0\rangle_B$ should be expressed as $|0\rangle_{B_1}|1\rangle_{B_2}$; $|1\rangle_B$ is expressed as $|1\rangle_{B_1}|0\rangle_{B_2}$. Therefore, the logical hyperentangled Bell state should be expressed as

$$\begin{aligned}\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{dp}} &= \frac{1}{2}(|0\rangle_A|01\rangle_{B_1B_2}-|1\rangle_A|10\rangle_{B_1B_2})\\ &\quad\otimes(|a_1b_1c_1\rangle-|a_2b_2c_2\rangle)_{AB_1B_2}\\ &= \frac{1}{2}(|{+}{+}{-}\rangle+|{-}{-}{-}\rangle\\ &\quad-|{+}{-}{+}\rangle-|{-}{+}{+}\rangle)_{AB_1B_2}\\ &\quad\otimes(|a_1b_1c_1\rangle-|a_2b_2c_2\rangle)_{AB_1B_2}. \end{aligned}\tag{29}$$

Step 1 Alice prepares N ordered $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{dp}}$ states. We denote the ordered $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{dp}}$ states as $\{[P_1(A),P_1(B_1),P_1(B_2)]$, $[P_2(A),P_2(B_1),P_2(B_2)]$, …, $[P_N(A),P_N(B_1),P_N(B_2)]\}$. Alice takes particle A from each state to form an ordered particle sequence S_A sequence. The remaining particles constitute an S_B sequence. It is similar to the original protocol.[7]

Step 2 According to the ID, Alice prepares a qubit sequence S_T. As did in Refs. [63] and [64], Alice uses S_T as decoy photons. The rule is that she randomly prepares the i-th qubit of S_T in $|0\rangle$ or $|1\rangle$ state if the i-th bit of the ID is 0; or else, she randomly prepares the qubit in $|+\rangle$ or $|-\rangle$ state. Alice inserts the decoy sequence S_T into the sequence S_B according to the ID, forming a new sequence S_B', which is similar to Step 2 in the DSQC scheme against collective-rotation noise. Only Alice and Bob know the positions of these decoy photons. Then Alice sends S_B' to Bob.

Step 3 After Bob receives S_B', Bob extracts decoy photons from S_B' and measures it with $Z^P=\{|0\rangle,|1\rangle\}$ or $X^P=\{|+\rangle_P,|-\rangle_P\}$ basis according to the ID. If the error rate is low enough Bob believes that Alice is legal and no eavesdropping exists. In this condition, the communication goes on. Otherwise Bob interrupts it.

Step 4 Bob publishes the photons that he does not receive in S_B, Alice discards the corresponding photons in S_A.

Step 5 Alice first measures photons in S_A with basis $Z^S=\{|a_1\rangle,|a_2\rangle\}$. Then according to the ID, Alice measures photons in S_A with basis $Z^P=\{|0\rangle,|1\rangle\}$ or $X^P=\{|+\rangle_P,|-\rangle_P\}$. Like Step 6 in the DSQC scheme against collective-rotation noise, Alice and Bob will obtain an identical binary string C, which is a real random number.

Step 6 The next steps are the same as Steps 7–11 in the DSQC scheme against collective-rotation noise, which will not be described further here.

4.2. Security analysis

Because the DSQC scheme is designed to be immune to collective-dephasing noise, the eavesdropping will be found more easily. Thus, the security of the protocol is mainly guaranteed by the identity string ID (shared by Alice and Bob) and the eavesdropping detection strategy based on $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ states. Because identity authentication is implemented based on the identity string, the protocol will not be threatened by a man-in-the-middle attack. Next, we analyze the eavesdropping detection rate of the protocol.

4.2.1. Analysis of the detection rate

In the DSQC scheme immune to collective-dephasing noise, $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ states are used as decoy photons to detect eavesdropping. Because the positions of decoy photons are secret, Eve cannot discriminate between decoy photons and information photons (photons in S_B).

According to Stingspring dilation theorem, Eve's eavesdropping can be implemented by a unitary operation E acting on a bigger Hilbert space. The eavesdropping can be represented as

$$\begin{aligned}E\otimes|0\rangle|x\rangle_E &= a|0\rangle|x_0\rangle_E+b|1\rangle|x_1\rangle_E,\\ E\otimes|1\rangle|x\rangle_E &= n|0\rangle|y_0\rangle_E+m|1\rangle|y_1\rangle_E,\\ E\otimes|+\rangle|x\rangle_E &= \frac{1}{\sqrt{2}}(a|0\rangle|x_0\rangle_E+b|1\rangle|x_1\rangle_E\\ &\quad+n|0\rangle|y_0\rangle_E+m|1\rangle|y_1\rangle_E)\\ &= \frac{1}{2}[|+\rangle(a|x_0\rangle_E+b|x_1\rangle_E+n|y_0\rangle_E+m|y_1\rangle_E)\\ &\quad+|-\rangle(a|x_0\rangle_E-b|x_1\rangle_E+n|y_0\rangle_E-m|y_1\rangle_E)],\\ E\otimes|-\rangle|x\rangle_E &= \frac{1}{\sqrt{2}}(a|0\rangle|x_0\rangle_E+b|1\rangle|x_1\rangle_E\\ &\quad-n|0\rangle|y_0\rangle_E-m|1\rangle|y_1\rangle_E)\\ &= \frac{1}{2}[|+\rangle(a|x_0\rangle_E+b|x_1\rangle_E-n|y_0\rangle_E-m|y_1\rangle_E)\\ &\quad+|-\rangle(a|x_0\rangle_E-b|x_1\rangle_E\\ &\quad-n|y_0\rangle_E+m|y_1\rangle_E)].\end{aligned}\tag{30}$$

Here $|x\rangle_E$ is the initial state of Eve's auxiliary particle and $|a|^2+|b|^2=1$, $|m|^2+|n|^2=1$. $|x_0\rangle_E$, $|x_1\rangle_E$, $|y_0\rangle_E$, $|y_1\rangle_E$ are pure states uniquely determined by unitary operation E.

The unitary operation E of Eve can be represented as

$$E=\begin{pmatrix}a & n\\ b & m\end{pmatrix}.\tag{31}$$

The complex numbers a, b, m, and n satisfy $EE^{\dagger}=I$. Therefore, $|a|^2=|m|^2$ and $|b|^2=|n|^2$ can be obtained. The error rate of each qubit is

$$\sigma=1-|a|^2.\tag{32}$$

Let $|a|^2=s$, then we will obtain

$$\sigma=1-s,\tag{33}$$

which can be seen as the detection rate:

$$d=1-s.\tag{34}$$

Like that in the collective-rotation noise scheme, the total information that Eve can eavesdrop in a qubit will be

$$I = H(s) = H(1-d). \tag{35}$$

We can calculate that when $I = 1$, $d = 0.5$. That is, if Eve performs an attack by using ancillary particles, when she obtains the full information, the detection rate or qubit error rate reaches 50%.

4.2.2. Discussion

Like that in the collective-rotation noise scheme, the ID is shared by Alice and Bob previously. The only unsafe factor is the improper storage of Alice and Bob. Thus, without considering the unsafe factor of improper storage, the ID can be reused in an unconditionally safe manner. In our protocol, a group of non-orthodox photons ($|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$) are used as decoy photons, which are nearly the same as the modus operandi of the original decoy photons idea proposed by Li *et al.* in Refs. [63] and [64]. However, the non-orthodox decoy photons in our protocol are prepared according to the identity string ID, which is secret to others. The special detection strategy implements not only eavesdropping detection in a lure approach, but also identity authentication.

5. Conclusions

In this study, the two protocols by using hyperentangled Bell state $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{r}}$ or $\left|\Phi_{AB}^{-}\right\rangle_{PS}^{\mathrm{dp}}$ are secure in theory, which are immune to collective-rotation noise and collective-dephasing noise respectively. Compared with the existing schemes, our protocol has the following differences.

(I) Man-in-the-middle attack can be resisted in our protocol.

(II) For two classical bits, only two carrier qubits need to be transmitted once; compared with the two-step protocol, our protocol reduces not only the transmission of carrier qubits but also the number of decoy photons; compared with the protocol based on an ordinary Bell state, in the sense of being immune to collective-rotation noise or collective-dephasing noise, our protocol doubles the channel capacity.

(III) The secret message is divided into several parts to transmit, however the identity string of Alice and Bob is reused.

(IV) Unitary operations are not used.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Deng F G and Long G L 2003 *Phys. Rev. A* **68** 042315
[5] Deng F G and Long G L 2004 *Phys. Rev. A* **70** 012311
[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[7] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[8] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[9] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[10] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[11] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15
[12] Li X H, Li C Y and Deng F G, *et al.* 2007 *Chin. Phys.* **16** 2149
[13] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[14] Gu B, Zhang C Y, Cheng G S and Huang Y G 2011 *Sci. China: Phys. Mech. Astron.* **54** 942
[15] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[16] Liu D, Chen J L and Jiang W 2012 *Int. J. Theor. Phys.* **51** 2923
[17] Sun Z W, Du R G and Long D Y 2012 *Int. J. Theor. Phys.* **51** 1946
[18] Ren B C *et al.* 2013 *Eur. Phys. J. D* **67** 30
[19] Gu B *et al.* 2013 *Int. J. Theor. Phys.* **52** 4461
[20] Li X H, Deng F G and Zhou H Y 2007 *Appl. Phys. Lett.* **91** 144101
[21] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **78** 022321
[22] Li X H, Zhao B K, Sheng Y B, Deng F G and Zhou H Y 2009 *Int. J. Quantum Inform.* **7** 1479
[23] Pei C X, Han B B and Zhao N 2009 *Acta Photon. Sin.* **38** 422
[24] Yang J, Wang C and Zhang R 2010 *Chin. Phys. B* **19** 110306
[25] Li X H 2010 *Phys. Rev. A* **82** 044304
[26] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **81** 042332
[27] Wen K and Long G L 2010 *Int. J. Quantum Inform.* **8** 697
[28] Deng F G, Li X H and Zhou H Y 2011 *Quantum Inform. Comput.* **11** 913
[29] Wang C, Zhang Y and Jin G S 2011 *Phys. Rev. A* **84** 032307
[30] Yang C W, Tsai C W and Hwang T 2011 *Sci. China-Phys. Mech. Astron.* **54** 496
[31] Huang W, Wen Q Y and Jia H Y 2012 *Chin. Phys. B* **21** 100308
[32] Sheng Y B, Zhou L, Zhao S M and Zheng B Y 2012 *Phys. Rev. A* **85** 012307
[33] Du F F, Li T, Ren B C, Wei H R and Deng F G 2012 *J. Opt. Soc. Am. B* **29** 1399
[34] Niu H C, Ren B C and Wang T J 2012 *Int. J. Theor. Phys.* **51** 2346
[35] Yang C W and Hwang T 2013 *Quantum Inform. Process.* **12** 3495
[36] Gu B, Huang Y G, Fang X and Chen Y L 2013 *Int. J. Theor. Phys.* **52** 4461
[37] Li J, Li L Y, Jin H F and Li R F 2013 *Phys. Lett. A* **377** 2729
[38] Xia Y, Fan L L and Hao S Y 2013 *Quantum Inform. Process.* **12** 3553
[39] Sheng Y B, Zhou L and Long G L 2013 *Phys. Rev. A* **88** 022302
[40] Ren B C, Du F F and Deng F G 2013 *Phys. Rev. A* **88** 012302
[41] Wang T J and Long G L 2013 *J. Opt. Soc. Am. B* **30** 1069
[42] Hou S Y, Sheng Y B, Feng G R and Long G L 2014 *Quantum Inform. Process.* DOI: 10.1038/ srep06857
[43] Zhang R, Zhou S H and Cao C 2014 *Sci. China-Phys. Mech. Astron.* **57** 1511
[44] Ren B C and Long G L 2014 *Opt. Express* **22** 6547
[45] Zhang C M, Song X T, Treeviriyanupab P, Li M, Wang C, Li H W, Yin Z Q, Chen W and Han Z F 2014 *Chin. Sci. Bull.* **59** 2825
[46] Pan J W and Zeilinger A 1998 *Phys. Rev. A* **57** 2208
[47] Walborn S P, Padua S and Monken C H 2003 *Phys. Rev. A* **68** 042313
[48] Barbieri M, Vallone G, Mataloni P and Martini F D 2007 *Phys. Rev. A* **75** 042317
[49] Sheng Y B, Deng F G and Long G L 2010 *Phys. Rev. A* **82** 032318
[50] Wang T J, Li T, Du F F and Deng F G 2011 *Chin. Phys. Lett.* **28** 040305
[51] Zhao R T, Guo Q and Chen L 2012 *Chin. Phys. B* **21** 080303
[52] Wang T J, Song S Y and Long G L 2012 arXiv: 1211.0082v2[quant-ph]
[53] Ren B C, Wei H R, Hua M, Li T and Deng F G 2012 *Opt. Express* **20** 24664
[54] Wang T J, Lu Y and Long G L 2012 *Phys. Rev. A* **86** 042337
[55] Wang T J and Wang C 2013 *J. Opt. Soc. Am. B* **30** 2689
[56] Ren B C, Wei H R and Deng F G 2013 arXiv: 1303.0056v2[quant-ph]
[57] Graham T M, Barreiro J T, Mohseni M and Kwiat P G 2013 *Phys. Rev. Lett.* **110** 060404
[58] Ren B C, Wei H R and Deng F G 2013 *Laser Phys. Lett.* **10** 095202
[59] Ren B C and Deng F G 2013 *Laser Phys. Lett.* **10** 115201
[60] Ren B C, Du F F and Deng F G 2013 *Phys. Rev. A* **88** 012302
[61] Ren B C and Deng F G 2014 *Sci. Rep.* **4** 4623
[62] Ren B C, Du F F and Deng F G 2014 *Phys. Rev. A* **90** 052309
[63] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[64] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2897