Robust quantum secure direct communication and authentication protocol against decoherence noise based on six-qubit DF state*

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

Department of Network Engineering, Chengdu University of Information Technology, Chengdu 610225, *China*

(Received 22 September 2014; revised manuscript received 26 November 2014; published online 27 March 2015)

By using six-qubit decoherence-free (DF) states as quantum carriers and decoy states, a robust quantum secure direct communication and authentication (QSDCA) protocol against decoherence noise is proposed. Four six-qubit DF states are used in the process of secret transmission, however only the $|0'\rangle$ state is prepared. The other three six-qubit DF states can be obtained by permuting the outputs of the setup for $|0'\rangle$. By using the $|0'\rangle$ state as the decoy state, the detection rate and the qubit error rate reach 81.3%, and they will not change with the noise level. The stability and security are much higher than those of the ping–pong protocol both in an ideal scenario and a decoherence noise scenario. Even if the eavesdropper measures several qubits, exploiting the coherent relationship between these qubits, she can gain one bit of secret information with probability 0.042.

Keywords: quantum secure direct communication, decoherence noise, authentication, six-qubit decohevence-free state

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.65.Ud **DOI:** 10.1088/1674-1056/24/5/050307

1. Introduction

Cryptography is the way to guarantee the safety of a secret message stored or communicated in the public environment. Both classical cryptosystems and quantum cryptography can solve the problems of security. However, the latter has shown the advantage of higher security because of the strong security basis assured by the physical principles. Therefore, quantum cryptography[1–16] is now attracting a great deal of attention.

Quantum secure direct communication (QSDC) is a new concept in quantum cryptography which exchanges secret information securely using a quantum system. In a QSDC protocol, the secret message is transmitted directly without first establishing a key to encrypt it. In 2000, Long and Liu[5] developed an efficient pioneer two-step QSDC protocol. In that protocol, an Einstein–Podolsky–Rosen (EPR) pair is selected as the carrier qubit, and the qubits are transmitted in blocks, which improves the efficiency of eavesdropping detection. Later, many QSDC protocols[5–16] were proposed. However, most researches about quantum secure communication are based on ideal scenarios.[1–16] Noise is inevitable in a real scenario, which affects the safety and fidelity of the information exchanged. Therefore, studies of quantum cryptography in noisy scenarios are needed.

Channel noise is attracting a lot of attention.[17–44] Researchers have found that the noises are usually caused by decoherence, which is caused by the coupling of a quantum system to its environment. Decoherence will make the quantum states fragile and easily destroyed, which leads to errors and leakage of secrets in the communication.[19] Collective decoherence is a kind of symmetry decoherence, which arises when the environment couples with the qubits without distinguishing between them.[19] For example, when the particles are delivered through some media such as the optical fiber, collective decoherence will appear. The alteration caused by collective decoherence can be described by a unitary operator $U(t)$, where t denotes the time of transmission and indicates a temporal dependence. As mentioned in Ref. [20], if the time delay between the photons is small enough, the effect of collective noise on an N-qubit state can be modeled approximately as

$$\rho_N \Rightarrow [U(t)]^{\otimes N}\rho_N[U(t)^{\dagger}]^{\otimes N},$$

where $[U(t)]^{\otimes N} = U(t)\otimes\cdots\otimes U(t)$ denotes the tensor product of N unitary transformations $U(t)$.

Many strategies have been proposed to decrease or eliminate the effect of decoherence noise, such as an error-correcting code (ECC),[21] quantum error correction,[22–26] entanglement purification,[27–31] entanglement concentration,[32–38] and quantum error rejection.[40] However, those methods will not work well when the interaction with the environment is not weak enough and the qubits are not affected with a low probability, such as, when the strong collective decoherence exists.[19]

Decoherence-free (DF) states are some interesting states which are invariant under collective decoherence no matter how strong the interaction is.[19] DF states have been applied

*Project supported by the National Natural Science Foundation of China (Grant No. 61402058), the Science and Technology Support Project of Sichuan Province of China (Grant No. 2013GZX0137), the Fund for Young Persons Project of Sichuan Province of 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

to the protection of quantum information in many researches. The invariance property of the DF state can be described by the following equation:

$$\rho_N = [U(t)]^{\otimes N}\rho_N[U(t)^{\dagger}]^{\otimes N}.$$

This immunity against $[U(t)]^{\otimes N}$ has been demonstrated in some studies.[20]

In this study, a robust QSDCA protocol against decoherence noise is proposed based on six-qubit DF states. The six-qubit DF states are used not only as the quantum carrier but also as the decoy state. In the process of secret transmission, four six-qubit DF states are used as the carrier, however only the $|0'\rangle$ state is prepared; the other three six-qubit DF states can be obtained by permuting the outputs of the setup for $|0'\rangle$. In the process of eavesdropping detection, the $|0'\rangle$ state is used as the decoy state; the detection rate and the qubit error rate reach 81.3%, which will not change with the noise level. The stability and security of the proposed protocol are much higher than those of the ping–pong protocol not only in an ideal scenario but also in the decoherence noise scenario. Most attacks including the man-in-the-middle attack, intercept-resend attack, Trojan horse attack, and coherent attack can be resisted in our protocol. If the eavesdropper performs the intercept-resend attack, he only has $7.86\times10^{-4}\%$ chance to know one bit of C, which will not lead to the leakage of M^1, unless K^{A} is leaked because of the improper storage by Alice and Bob. Even if the eavesdropper measures several qubits, exploiting the coherent relationship between these qubits, she can only gain one bit of secret information with probability 0.042.

2. Description of QSDCA based on DF state

In this section, four 6-qubit DF states[41–44] are selected as the carrier qubits. They are in the forms of

$$\begin{aligned}
|0'\rangle &= |\psi^-\rangle_{12}\otimes\frac{1}{2\sqrt{3}}(2|0011\rangle-|0101\rangle-|0110\rangle-|1001\rangle\\
&\quad-|1010\rangle+2|1100\rangle)_{3456}\\
&= \frac{1}{2\sqrt{6}}(2|010011\rangle-|010101\rangle-|010110\rangle-|011001\rangle\\
&\quad-|011010\rangle+2|011100\rangle-2|100011\rangle+|100101\rangle\\
&\quad+|100110\rangle+|101001\rangle\\
&\quad+|101010\rangle-2|101100\rangle)_{123456},\\
|1'\rangle &= P_{1\leftrightarrow3,2\leftrightarrow4}|0'\rangle\\
&= |\psi^-\rangle_{34}\otimes\frac{1}{2\sqrt{3}}(2|0011\rangle-|0101\rangle-|0110\rangle\\
&\quad-|1001\rangle-|1010\rangle+2|1100\rangle)_{1256},\\
|+'\rangle &= P_{1\leftrightarrow3}|0'\rangle\\
&= |\psi^-\rangle_{32}\otimes\frac{1}{2\sqrt{3}}(2|0011\rangle-|0101\rangle-|0110\rangle\\
&\quad-|1001\rangle-|1010\rangle+2|1100\rangle)_{1456},\\
|-'\rangle &= P_{2\leftrightarrow4}|0'\rangle\\
&= |\psi^-\rangle_{14}\otimes\frac{1}{2\sqrt{3}}(2|0011\rangle-|0101\rangle-|0110\rangle\\
&\quad-|1001\rangle-|1010\rangle+2|1100\rangle)_{3256},
\end{aligned}\tag{1}$$

where $|\psi^-\rangle=(|01\rangle-|10\rangle)/\sqrt{2}$, and $P_{i\leftrightarrow j}$ denotes permuting the i-th qubit and the j-th qubit in the quantum state. These four states satisfy

$$\langle0'|1'\rangle=\langle+'|-'\rangle=0,\tag{2}$$

$$|\langle0'|+'\rangle|^2=|\langle0'|-'\rangle|^2=|\langle1'|+'\rangle|^2=|\langle1'|-'\rangle|^2=\frac{1}{2}.\tag{3}$$

Here, $\{|0'\rangle,|1'\rangle\}$ and $\{|+'\rangle,|-'\rangle\}$ construct two orthogonal bases in the 6-qubit DF state space. Indeed, one can prepare these four mutually orthogonal 6-qubit DF states just by combining the two setups of Ref. [41]. By using six single-qubit measurements $Z_1Z_2X_3X_4Z_5Z_6$ ($X_1Z_2Z_3X_4Z_5Z_6$), we can distinguish $|0'\rangle$ and $|1'\rangle$ ($|+'\rangle$ and $|-'\rangle$), where X_i (Z_i) ($i=1,\ldots,6$) denotes measuring the i-th qubit in the X basis (Z basis).

Assume that Alice wants to send a secret message directly to Bob. The protocol is designed to help Alice and Bob finish their task safely. Alice and Bob share keys K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and K^{B} (k_1^{B}, k_2^{B}, …, k_N^{B}) with length N in advance, where k_i^{A} and $k_i^{\mathrm{B}}\in\{0,1\}$. The K^{A} and K^{B} represent Alice and Bob's identities, respectively. Alice's secret message is denoted as $M(m_1, m_2, \ldots, m_S)$, where $m_s\in\{0,1\}$. Alice breaks up her secret message into k substrings (where parameter k is a natural number), the length of each substring is N.

Step 1 By adding K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and (m_1, m_2, …, m_N) bitwise, Alice obtains C (c_1, c_2, …, c_N) with length N.

Step 2 Alice prepares photon sequence S_C according to $C(c_1, c_2, \ldots, c_N)$. Firstly, Alice prepares N $|0'\rangle$ states, which form qubit sequence S. If c_i is 0, Alice randomly performs $1\leftrightarrow3$ operation or nothing on the i-th $|0'\rangle$ state in S; if c_i is 1, Alice randomly performs $1\leftrightarrow3$ and $2\leftrightarrow4$ operations or $2\leftrightarrow4$ operation on the i-th $|0'\rangle$ state in S.

Step 3 Alice prepares other N $|0'\rangle$ states, which form a decoy photon sequence S_{T}. To detect the eavesdropping, Alice mixes S_{T} into S_C according to a rule and sends the mixed sequence S_C^* to Bob. The rule is: if k_i^{B} is 0, Alice inserts the i-th 6-qubit DF state of S_{T} behind the i-th 6-qubit DF state of S_C; if k_i^{B} is 1, Alice inserts the i-th 6-qubit DF state of S_{T} before the i-th 6-qubit DF state of S_C.

Step 4 After Bob receives S_C^*, Bob can extract S_{T} from S_C^*, because he knows K^{B} (k_1^{B}, k_2^{B}, …, k_N^{B}). Bob measures the extracted S_{T} with six single-qubit measurements $Z_1Z_2Z_3Z_4Z_5Z_6$. In the ideal case, every result should be in any of the 12 states: $|010011\rangle_{123456}$, $|010101\rangle_{123456}$, $|010110\rangle_{123456}$, $|011001\rangle_{123456}$, $|011010\rangle_{123456}$, $|011100\rangle_{123456}$, $|100011\rangle_{123456}$, $|100101\rangle_{123456}$, $|100110\rangle_{123456}$, $|101001\rangle_{123456}$, $|101010\rangle_{123456}$, $|101100\rangle_{123456}$. 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 5 If eavesdropping does not exist, Alice publicly announces the correct basis $Z_1Z_2X_3X_4Z_5Z_6$ or $X_1Z_2Z_3X_4Z_5Z_6$ of each 6-DF state in S_C. Then Bob can measureS_C correctly. According to the measurement result, Bob can restore C (c_1, c_2, …, c_N). Then Bob obtains the secret message sent by Alice by adding K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and (c_1, c_2, …, c_N) bitwise.

Step 6 Alice takes the next N bits of the secret message and begins the next transmission until all secret messages are sent.

3. Analysis

3.1. Correctness analysis

3.1.1. Correctness in the ideal scenario

In step 1, by adding K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and M^1 (m_1, m_2, …, m_N) bitwise, Alice obtains C (c_1, c_2, …, c_N),

$$C = M^1 \tilde{\oplus} K^{\mathrm{A}}, \tag{4}$$

where $\tilde{\oplus}$ denotes the bitwise adding operation. Then Alice encodes the message C on N $|0'\rangle$ states by permuting operations, therefore Alice forms a qubit sequence S_C,

$$S_C = P_C(S), \tag{5}$$

where P_C denotes the permuting operations denominated by C, and S denotes the qubit sequence consisting of N $|0'\rangle$ states. After, Alice inserts decoy sequence S_{T} to S_C and obtains S_C^*,

$$S_C^* = Z(S_C,\ S_{\mathrm{T}},\ K^{\mathrm{B}}), \tag{6}$$

where Z denotes inserting S_{T} to S_C according to K^{B}.

After Bob receives S_C^*, he recovers S_C by extracting S_{T} from S_C^* according to K^{B},

$$S_C = Z^{-1}(S_C^*,\ S_{\mathrm{T}},\ K^{\mathrm{B}}), \tag{7}$$

where Z^{-1} denotes extracting S_{T} from S_C^* according to K^{B}. By measuring S_C with correct bases, Bob obtains

$$C = M_{\mathrm{s}}(S_C), \tag{8}$$

where M_{s} denotes measuring S_C with bases $Z_1Z_2X_3X_4Z_5Z_6$ or $X_1Z_2Z_3X_4Z_5Z_6$. Bob obtains the secret message by adding K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and $C(c_1, c_2, \ldots, c_N)$ bitwise,

$$M^1 = C \tilde{\oplus} K^{\mathrm{A}}. \tag{9}$$

Obviously, the protocol is correct in the ideal scenario.

3.1.2. Correctness in decoherence noise scenario

With the use of DF states, the collective decoherence noise will not lead to errors in the protocol. So only the noise other than collective decoherence needs to be considered. These noises might appear in all of the quantum preparation setups, quantum channels, and measurement equipment. Therefore, to protect our protocol from these non-collective decoherence noises, we can add an error-correcting code (ECC) in our protocol.

Alice and Bob select an $[s, N]$ error-correcting code,[21] which uses an s bits codeword to encode an N bits word using generator matrix $G(x^N)$ and can correct t codeword error bits with the error-correcting function $D(y^s)$.

In step 1, after Alice obtains C, she calculates the corresponding bits codeword W=(w_1, w_2, …, w_s), where

$$W = C \cdot G,\ \ C = W \cdot D. \tag{10}$$

In step 2, Alice performs permuting operations on $|0'\rangle$ states according to W and forms a new qubit sequence S_W,

$$S_W = P_W(S), \tag{11}$$

where P_W denotes the permuting operations denominated by W, and S denotes the qubit sequence consisting of s $|0'\rangle$ states. After Alice inserts decoy sequence S_{T} to S_W, she obtains

$$S_W^* = Z(S_W,\ S_{\mathrm{T}},\ K^{\mathrm{B}}), \tag{12}$$

where Z denotes inserting S_{T} to S_W according to K^{B}.

After Bob receives S_W^*, he recovers S_W by extracting S_{T} from S_W^* according to K^{B},

$$S_W = Z^{-1}(S_W^*,\ S_{\mathrm{T}},\ K^{\mathrm{B}}), \tag{13}$$

where Z^{-1} denotes extracting S_{T} from S_W^* according to K^{B}. By measuring S_W with correct bases, Bob obtains

$$W = M_{\mathrm{s}}(S_W), \tag{14}$$

where M_{s} denotes measuring S_W with bases $Z_1Z_2X_3X_4Z_5Z_6$ or $X_1Z_2Z_3X_4Z_5Z_6$.

Suppose that the non-collective decoherence noises appear in the courses of $W(w_1, w_2, \ldots, w_s)$ as $O = (o_1, o_2, \ldots, o_s)$, where $o_i = 0$ or 1 represents whether an error is existent or not in w_i. Then Bob obtains bit string W' as

$$W' = W \tilde{\oplus} O. \tag{15}$$

The C can be obtained by using the error-correcting function $D(y^s)$ on W',

$$C = W' \cdot D = (W \tilde{\oplus} O) \cdot D. \tag{16}$$

When the error rate does not exceed a rational threshold, the number of "1" in bit string O does not exceed t, therefore,

$$C = W \cdot D. \tag{17}$$

Bob obtains the secret message by adding K^{A} (k_1^{A}, k_2^{A}, …, k_N^{A}) and $C(c_1, c_2, \ldots, c_N)$ bitwise,

$$M^1 = C \tilde{\oplus} K^{\mathrm{A}}. \tag{18}$$

That is, the protocol is correct in the decoherence noise scenario too.

3.2. Security analysis

With the use of DF states, the protocol is immune to collective decoherence noise, therefore, the eavesdropping will be found more easily. The cryptanalysis of the QSDCA protocol boils down to two aspects: (i) how to analyze the eavesdropping detection rate if Eve eavesdrops; (ii) whether the protocol resists some common attack strategies, such as the intercept-resend attack, man-in-the-middle attack, Trojan horse attack, and coherent attack, or not. Because the identity authentication is implemented based on identity string K^{B}, the protocol will not be threatened by the man-in-the-middle attack. Next we analyze the eavesdropping detection rate of the protocol and how the protocol resists some common attack strategies, such as the intercept-resend attack, Trojan horse attack, and coherent attack.

3.2.1. Analysis of the eavesdropping detection rate

In the protocol, state $|0'\rangle$ is used as the decoy state to detect eavesdropping. Because the positions of decoy particles are secret, Eve cannot discriminate between decoy particles and information particles (particles in S_C). Under this circumstance, Eve usually performs the same attack operation on all particles. We term the attack that Eve performs on each particle as E. Eve's attack will make the state $|0\rangle$ change to $|\tilde{0}\rangle = E\otimes|0x\rangle = a|0x_0\rangle + b|1x_1\rangle$; and the state $|1\rangle$ change to $|\tilde{1}\rangle = E\otimes|1x\rangle = m|0y_0\rangle + n|1y_1\rangle$. Here $|a|^2+|b|^2=1$ and $|m|^2+|n|^2=1$.

Because of Eve's attack, the combined system changes to

$$
\begin{aligned}
|\psi\rangle_{\mathrm{Eve}} \;=\; & E\otimes E\otimes E\otimes E\otimes E\otimes E\otimes\Bigg[\frac{1}{2\sqrt{6}}(2|0x1x0x0x1x1x\rangle-|0x1x0x1x0x1x\rangle-|0x1x0x1x1x0x\rangle-|0x1x1x0x0x1x\rangle\\
& -|0x1x1x0x1x0x\rangle+2|0x1x1x1x0x0x\rangle-2|1x0x0x0x1x1x\rangle+|1x0x0x1x0x1x\rangle+|1x0x0x1x1x0x\rangle\\
& +|1x0x1x0x0x1x\rangle+|1x0x1x0x1x0x\rangle-2|1x0x1x1x0x0x\rangle)_{123456}\Bigg], \qquad (19)
\end{aligned}
$$

$$
\begin{aligned}
& |0x1x0x0x1x1x\rangle\\
=\;& (a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
=\;& a^3m^3|0x_00y_00x_00x_00y_00y_00y_0\rangle\\
& +a^3m^2n|0x_01y_10x_00x_00y_00y_0\rangle+ba^2m^3|1x_10y_00x_00x_00y_00y_0\rangle+ba^2nm^2|1x_11y_10x_00x_00y_00y_0\rangle\\
& +a^2m^3b|0x_00y_01x_10x_00y_00y_0\rangle+a^2nbm^2|0x_01y_11x_10x_00y_00y_0\rangle+b^2m^3a|1x_10y_01x_10x_00y_00y_0\rangle\\
& +b^2nam^2|1x_11y_11x_10x_00y_00y_0\rangle+a^2m^3b|0x_00y_00x_01x_10y_00y_0\rangle+a^2nbm^2|0x_01y_10x_01x_10y_00y_0\rangle\\
& +b^2am^3|1x_10y_00x_01x_10y_00y_0\rangle+b^2anm^2|1x_11y_10x_01x_10y_00y_0\rangle+am^3b^2|0x_00y_01x_11x_10y_00y_0\rangle\\
& +anb^2m^2|0x_01y_11x_11x_10y_00y_0\rangle+b^3m^3|1x_10y_01x_11x_10y_00y_0\rangle+b^3nm^2|1x_11y_11x_11x_10y_00y_0\rangle\\
& +a^3m^2n|0x_00y_00x_00x_01y_10y_0\rangle+a^3n^2m|0x_01y_10x_00x_01y_10y_0\rangle+ba^2m^2n|1x_10y_00x_00x_01y_10y_0\rangle\\
& +ba^2n^2m|1x_11y_10x_00x_01y_10y_0\rangle+a^2m^2bn|0x_00y_01x_10x_01y_10y_0\rangle+a^2n^2bm|0x_01y_11x_10x_01y_10y_0\rangle\\
& +b^2m^2an|1x_10y_01x_10x_01y_10y_0\rangle+b^2n^2am|1x_11y_11x_10x_01y_10y_0\rangle+a^2m^2bn|0x_00y_00x_01x_11y_10y_0\rangle\\
& +a^2n^2bm|0x_01y_10x_01x_11y_10y_0\rangle+b^2am^2n|1x_10y_00x_01x_11y_10y_0\rangle+b^2an^2m|1x_11y_10x_01x_11y_10y_0\rangle\\
& +am^2b^2n|0x_00y_01x_11x_11y_10y_0\rangle+an^2b^2m|0x_01y_11x_11x_11y_10y_0\rangle+b^3m^2n|1x_10y_01x_11x_11y_10y_0\rangle\\
& +b^3n^2m|1x_11y_11x_11x_11y_10y_0\rangle+a^3m^2n|0x_00y_00x_00x_00y_01y_1\rangle+a^3n^2m|0x_01y_10x_00x_00y_01y_1\rangle\\
& +ba^2m^2n|1x_10y_00x_00x_00y_01y_1\rangle+ba^2n^2m|1x_11y_10x_00x_00y_01y_1\rangle+a^2m^2bn|0x_00y_01x_10x_00y_01y_1\rangle\\
& +a^2n^2bm|0x_01y_11x_10x_00y_01y_1\rangle+b^2m^2an|1x_10y_01x_10x_00y_01y_1\rangle+b^2n^2am|1x_11y_11x_10x_00y_01y_1\rangle\\
& +a^2m^2bn|0x_00y_00x_01x_10y_01y_1\rangle+a^2n^2bm|0x_01y_10x_01x_10y_01y_1\rangle+b^2am^2n|1x_10y_00x_01x_10y_01y_1\rangle\\
& +b^2an^2m|1x_11y_10x_01x_10y_01y_1\rangle+am^2b^2n|0x_00y_01x_11x_10y_01y_1\rangle+an^2b^2m|0x_01y_11x_11x_10y_01y_1\rangle\\
& +b^3m^2n|1x_10y_01x_11x_10y_01y_1\rangle+b^3n^2m|1x_11y_11x_11x_10y_01y_1\rangle+a^3mn^2|0x_00y_00x_00x_01y_11y_1\rangle\\
& +a^3n^3|0x_01y_10x_00x_01y_11y_1\rangle+ba^2mn^2|1x_10y_00x_00x_01y_11y_1\rangle+ba^2n^3|1x_11y_10x_00x_01y_11y_1\rangle\\
& +a^2mbn^2|0x_00y_01x_10x_01y_11y_1\rangle+a^2n^3b|0x_01y_11x_10x_01y_11y_1\rangle+b^2man^2|1x_10y_01x_10x_01y_11y_1\rangle\\
& +b^2n^3a|1x_11y_11x_10x_01y_11y_1\rangle+a^2mbn^2|0x_00y_00x_01x_11y_11y_1\rangle+a^2n^3b|0x_01y_10x_01x_11y_11y_1\rangle\\
& +b^2amn^2|1x_10y_00x_01x_11y_11y_1\rangle+b^2an^3|1x_11y_10x_01x_11y_11y_1\rangle+amb^2n^2|0x_00y_01x_11x_11y_11y_1\rangle\\
& +an^3b^2|0x_01y_11x_11x_11y_11y_1\rangle+b^3mn^2|1x_10y_01x_11x_11y_11y_1\rangle+b^3n^3|1x_11y_11x_11x_11y_11y_1\rangle, \qquad (20)
\end{aligned}
$$

$$
\begin{aligned}
&|0x1x0x1x0x1x\rangle\\
=\ &(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle), \qquad (21)\\
&|0x1x0x1x1x0x\rangle\\
=\ &(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle), \qquad (22)\\
&|0x1x1x0x0x1x\rangle\\
=\ &(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle), \qquad (23)\\
&|0x1x1x0x1x0x\rangle\\
=\ &(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle), \qquad (24)\\
&|0x1x1x1x0x0x\rangle\\
=\ &(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle), \qquad (25)\\
&|1x0x0x0x1x1x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(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)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle), \qquad (26)\\
&|1x0x0x1x0x1x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle), \qquad (27)\\
&|1x0x0x1x1x0x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle), \qquad (28)\\
&|1x0x1x0x0x1x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle), \qquad (29)\\
&|1x0x1x0x1x0x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle), \qquad (30)\\
&|1x0x1x1x0x0x\rangle\\
=\ &(m|0y_0\rangle+n|1y_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle)\\
&\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\\
&\otimes(a|0x_0\rangle+b|1x_1\rangle)\otimes(a|0x_0\rangle+b|1x_1\rangle). \qquad (31)
\end{aligned}
$$

Obviously, after Bob receives S_C^* (mixture of S_C and S_T), Bob extracts S_T and performs six single-qubit measurements $Z_1Z_2Z_3Z_4Z_5Z_6$ on S_T. The probability without an eavesdropper is

$$
\begin{aligned}
p(|\psi_E\rangle) = \frac{1}{24}&(|2a^3n^3|^2+|2a^2n^2mb|^2+|2a^2n^2mb|^2\\
&+|2a^2n^2mb|^2+|2a^2n^2mb|^2+|2anm^2b^2|^2\\
&+|2a^2n^2mb|^2+|2anm^2b^2|^2+|2anm^2b^2|^2\\
&+|2anm^2b^2|^2+|2anm^2b^2|^2+|2anm^2b^2|^2\\
&+|anm^2b^2|^2+|m^3b^3|^2+|anm^2b^2|^2+|anm^2b^2|^2\\
&+|a^2n^2mb|^2+|anm^2b^2|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2\\
&+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|a^2n^2mb|^2+|m^3b^3|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|anm^2b^2|^2+|anm^2b^2|^2\\
&+|a^2n^2mb|^2+|m^3b^3|^2+|anm^2b^2|^2+|anm^2b^2|^2\\
&+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2+|anm^2b^2|^2\\
&+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2\\
&+|a^2n^2mb|^2+|anm^2b^2|^2+|\mathrm{m}^3b^3|^2+|anm^2b^2|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|anm^2b^2|^2\\
&+|2a^2n^2mb|^2+|2anm^2b^2|^2+|2anm^2b^2|^2\\
&+|2anm^2b^2|^2+|2anm^2b^2|^2+|2m^3b^3|^2+|2a^3n^3|^2\\
&+|2a^2n^2mb|^2+|2a^2n^2mb|^2+|2a^2n^2mb|^2\\
&+|2a^2n^2mb|^2+|2a^2n^2mb|^2+|2a^2n^2mb|^2\\
&+|2anm^2b^2|^2+|2anm^2b^2|^2+|2anm^2b^2|^2\\
&+|2anm^2b^2|^2+|2b^3m^3|^2+|2a^3n^3|^2\\
&+|2a^2n^2mb|^2+|2a^2n^2mb|^2+|2a^2n^2mb|^2\\
&+|2a^2n^2mb|^2+|2anm^2b^2|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2\\
&+|a^2n^2mb|^2+|anm^2b^2|^2+|b^3m^3|^2+|anm^2b^2|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|anm^2b^2|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|a^2n^2mb|^2+|b^3m^3|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|a^2n^2mb|^2\\
&+|a^2n^2mb|^2+|a^3n^3|^2+|anm^2b^2|^2+|a^2n^2mb|^2\\
&+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|a^2n^2mb|^2+|b^3m^3|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|anm^2b^2|^2+|b^3m^3|^2\\
&+|anm^2b^2|^2+|anm^2b^2|^2+|a^2n^2mb|^2\\
&+|anm^2b^2|^2+|a^2n^2mb|^2+|anm^2b^2|^2\\
&+|a^2n^2mb|^2+|a^2n^2mb|^2+|a^3n^3|^2+|a^2n^2mb|^2
\end{aligned}
$$

$$+|2a^3n^3|^2+|2a^2n^2mb|^2+|2a^2n^2mb|^2$$
$$+|2a^2n^2mb|^2+|2a^2n^2mb|^2+|2anm^2b^2|^2). \quad (32)$$

Suppose $|a|^2=s$, $|b|^2=t$, $a=m$, and $b=n$, then

$$p(|\psi_{\rm E}\rangle)=12s^3t^3. \quad (33)$$

Because $|a|^2+|b|^2=1$ and $|m|^2+|n|^2=1$, $p(|\psi_{\rm E}\rangle)=-12s^6+36s^5-36s^4+12s^3$ can be obtained. Therefore, the error rate of each qubit due to eavesdropping is

$$\sigma=1-p(|\psi_{\rm E}\rangle)=1+12s^6-36s^5+36s^4-12s^3, \quad (34)$$

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

$$d=1-p(|\psi_{\rm E}\rangle)=1+12s^6-36s^5+36s^4-12s^3. \quad (35)$$

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

$$I_{|0\rangle}=-s\log_2 s-(1-s)\log_2(1-s)=H(s), \quad (36)$$

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

$$I_{|1\rangle}=-t\log_2 t-(1-t)\log_2(1-t)=H(t). \quad (37)$$

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

$$I=\frac{1}{2}(I_{|0\rangle}+I_{|1\rangle})=\frac{1}{2}[H(s)+H(t)]=H(s). \quad (38)$$

By calculating, when $I=1$, $d=0.813$ is obtained. Also $\sigma=0.813$ can be obtained. That is, eavesdropping to obtain the whole message on one qubit will lead to an 81.3% qubit-error rate, whatever the noise level is. In Ref. [18], Li analyzed the security of the ping–pong protocol in the presence of collective-rotation noise (a major collective decoherence noise). According to Li's analysis, when the noise level is 0, the qubit-error rate caused by eavesdropping to obtain the whole message on one qubit is 0.5; when the noise level is 6%, the qubit-error rate is 0.18; and when the noise level is 11%, the qubit-error rate is 0.11. By comparing, we find that, when $I=1$, the qubit-error rate in our protocol is always 81.3% whatever the noise level is; however, the qubit-error rate in the ping–pong protocol decreases dramatically with the increase of the noise level. Even when the noise level is 0, the qubit-error rate of the ping–pong protocol is only 0.5, which is much lower than that in our protocol. Therefore, the eavesdroppers will be found more easily in our protocol both in the ideal condition and the noisy condition. Even in the noisy condition, our protocol can display a better eavesdropping detection rate than the ping–pong protocol.

3.2.2. Intercept-resend attack

In an intercept-resend attack, when Alice sends particles to Bob, Eve intercepts some particles; Eve measures these individual particles and resends them to Bob. Eve intents to obtain some information by performing the intercept-resend attack. In this protocol, if Eve intercepts some particles, Eve has an 18.7% chance to guess the purpose of the particle right (for eavesdropping detection or transmitting secret information) and an 81.3% chance to guess wrong. If Eve guesses wrong, she cannot obtain any secret information contained in the qubit and is sure to be found. If Eve guesses right, Eve will have a 50% chance to choose the correct basis to measure the particle. Therefore, in this case, Eve has a 9.4% chance to know one qubit. Because six qubits contribute to one bit of C, Eve can know one bit of C with probability $(9.4\%)^6\approx 6.89\times10^{-5}\%$. However, because C is the result of M^1 bitwise adding with $K^{\rm A}$, Eve cannot obtain the corresponding bit of M^1 (the secret message) without $K^{\rm A}$ ($K^{\rm A}$ is secret to anyone else except Alice and Bob).

On the other hand, if Eve guesses right, but she chooses the wrong basis, Bob will have a 50% chance to obtain wrong information and Eve has a 50% chance to obtain the information. Under this circumstance, Eve has a 4.7% (18.7% × 50% × 50%) chance to know one qubit. Therefore, the total rate that Eve knows one qubit is 14.1% (9.4 %+4.7%). Then Eve can know one bit of C with probability $(14.1\%)^6\approx 7.86\times10^{-4}\%$, which will not lead to leakage of M^1, unless $K^{\rm A}$ is leaked because of improper storage by Alice and Bob. Even if $K^{\rm A}$ is leaked completely, Eve will have a $7.86\times10^{-4}\%$ chance to know the secret message on one qubit, which is much smaller than that in the ping–pong protocol (37.5%).

3.2.3. Security of $K^{\rm A}$ and $K^{\rm B}$

The $K^{\rm A}$ and $K^{\rm B}$ are shared by Alice and Bob by executing the QKD protocol, therefore $K^{\rm A}$ and $K^{\rm B}$ are safe in the process of quantum key distribution. In the process of secret transmission, $K^{\rm A}$ and $K^{\rm B}$ will never be delivered in classical form but in qubit form which will be unconditionally safe because of quantum mechanics. The only unsafe factor is improper storage of $K^{\rm A}$ and $K^{\rm B}$ by Alice and Bob. However, the loss of $K^{\rm A}$ will lead to leakage of the secret message on one qubit with probability $7.86\times10^{-4}\%$. The loss of $K^{\rm B}$ will not lead to leakage of the secret message in this transmission but give Eve a chance to obtain $K^{\rm A}$ by exhaustive attack, which will make leakage of the secret in the following transmission. Therefore, the loss of $K^{\rm B}$ or both $K^{\rm B}$ and $K^{\rm A}$ will cause leakage of the secret.

3.2.4. Trojan horse attack

The Trojan horse attack is performed by using spy photons. The spy photons are usually some invisible photons with a different wavelength or delay photons, which cannot be found by the legitimate users. Usually, Eve inserts spy

photons to the legitimate photons. Because Bob cannot find the spy photons, Bob will encode the secret message on the spy photon, then Eve has the chance to obtain the secret message. In our protocol, Eve cannot obtain any secret message by performing a Trojan horse attack, because our protocol is a one-way protocol, Bob will not encode the secret message on photons.

3.2.5. Coherent attack

In our protocol, $|0'\rangle$ and $|1'\rangle$ ($|+'\rangle$ and $|-'\rangle$) are distinguished by six single-qubit measurements $Z_1Z_2X_3X_4Z_5Z_6$ ($X_1Z_2Z_3X_4Z_5Z_6$). Bob measures 6-DF states in S_C with basis $Z_1Z_2X_3X_4Z_5Z_6$ or $X_1Z_2Z_3X_4Z_5Z_6$. The decoy qubits mixed in S_C are measured with basis $Z_1Z_2Z_3Z_4Z_5Z_6$. For measurements $Z_1\boldsymbol{Z_2}X_3X_4\boldsymbol{Z_5Z_6}$, $X_1\boldsymbol{Z_2}Z_3X_4\boldsymbol{Z_5Z_6}$, and $Z_1\boldsymbol{Z_2}Z_3Z_4\boldsymbol{Z_5Z_6}$, we can find that three single-qubit measurements, which are marked in bold, remain unaltered. If Eve wants to get some valuable information and escape from being detected, she can intercept all the states sent from Alice and only measure the qubits with $\boldsymbol{Z_2Z_5Z_6}$ except for the first, the third, and the fourth ones in each state.

Table 1. All possible measurement results obtained by Eve with $Z_2Z_5Z_6$ in her attack.

The original state	The possible result
$\|0'\rangle$	$\|0\rangle_2\|0\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|0\rangle_6$
	$\|0\rangle_2\|0\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|0\rangle_6$
$\|1'\rangle$	$\|0\rangle_2\|1\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|0\rangle_6$
	$\|0\rangle_2\|0\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|0\rangle_6$
$\|+'\rangle$	$\|0\rangle_2\|0\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|0\rangle_6$
	$\|0\rangle_2\|0\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|0\rangle_6$
$\|-'\rangle$	$\|0\rangle_2\|1\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|0\rangle_6$
	$\|0\rangle_2\|0\rangle_5\|1\rangle_6, \|1\rangle_2\|0\rangle_5\|1\rangle_6$
	$\|0\rangle_2\|1\rangle_5\|0\rangle_6, \|1\rangle_2\|1\rangle_5\|0\rangle_6$

All the possible measurement results obtained by Eve in this attack are shown in Table 1. From Table 1, we can see that when Alice sends $|0'\rangle$ and $|+'\rangle$, Eve may obtain some results which will never appear in the cases $|1'\rangle$ and $|-'\rangle$, i.e., $|0\rangle_2|0\rangle_5|0\rangle_6$ and $|1\rangle_2|1\rangle_5|1\rangle_6$. Here $\rho^0_{256} \neq \rho^1_{256}$ and $\rho^{0'}_{256} \neq \rho^{1'}_{256}$, where ρ^0_{256}, ρ^1_{256}, $\rho^{0'}_{256}$, and $\rho^{1'}_{256}$ denote the reduced density matrices of quantum systems shown in Eq. (1). If Alice sends $|0'\rangle$ and $|+'\rangle$, we can find that both $|0\rangle_2|0\rangle_5|0\rangle_6$ and $|1\rangle_2|1\rangle_5|1\rangle_6$ appear with a probability of 1/6 in either $|0'\rangle$ or $|+'\rangle$ state. Alice sends $|0'\rangle$ or $|+'\rangle$ with probability 1/2, and Eve has good judgment of the purpose of the photon (decoy photon or secret carriers) with probability 1/2, therefore, Eve can gain one bit of the information of C with probability $1/6\times2\times1/2\times1/2=1/12$. To obtain one bit of the secret information, Eve has to know the corresponding bit of K^{A} with probability 1/2. Thus, Eve can gain one bit of the secret information with probability $1/12\times1/2=1/24\approx0.042$. When the number of bits transmitted in one transmission is $N=50$ (the length of K^{A}), the probability that Eve obtains the secret information approaches zero.

3.3. Discussion

In many cases, six-qubit entangled states are very difficult to prepare and manipulate in an experiment. However, in our protocol, the 6-DF state $|0'\rangle$ can be prepared with a setup[43,44] that can be designed by combining the two apparatuses of Ref. [41], and the other three states $|1'\rangle$, $|+'\rangle$, and $|-'\rangle$ can be prepared by permuting the outputs of the setup for $|0'\rangle$.[42] The measurements of $|0'\rangle$, $|1'\rangle$, $|+'\rangle$, or $|-'\rangle$ may be very difficult, however, six single-qubit measurements $Z_1Z_2X_3X_4Z_5Z_6$ ($X_1Z_2Z_3X_4Z_5Z_6$) cannot only distinguish $|0'\rangle$ and $|1'\rangle$ ($|+'\rangle$ and $|-'\rangle$), but also decrease the difficulty of measurement in an experiment. Therefore, our protocol is practical in an experiment.

4. Conclusion

We present a QSDCA protocol based on four six-qubit DF states. Because of the features of the four six-qubit DF states, only the state $|0'\rangle$ needs a setup and the other three states can be prepared by permuting the outputs of the setup for $|0'\rangle$.[42] The protocol is verified as secure in the ideal scenario and the noise scenario. The four six-qubit DF states are immune to collective decoherence noise, however, they may be affected by some non-collective decoherence noises. To protect our protocol from these non-collective decoherence noises, we add an error-correcting code (ECC) in our protocol. The six-qubit DF state is not only used as the carrier to transmit a secret securely but also used as the decoy state to detect an eavesdropper. The detection rate (qubit error rate) reaches 81.3% per-qubit. Compared with the ping–pong protocol, the qubit error rate is much higher and is not effected by the noise level. The qubit-error rate in the ping–pong protocol decreases dramatically with the increase of the noise level. Most attacks including the man-in-the-middle attack, intercept-resend attack, Trojan horse attack, and coherent attack can be resisted in our protocol. If the eavesdropper performs an intercept-resend attack, he only has a $7.86\times10^{-4}\%$ chance to know one bit of C, which will not lead to the leakage of M^1, unless K^{A} is leaked because of improper storage by Alice and Bob. Even if the eavesdropper measures several qubits, exploiting the coherent relationship between these qubits, she can gain one bit of secret information with probability 0.042.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Processing* (New York: IEEE) p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[5] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[6] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[7] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[8] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[9] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev. A* **74** 054302
[10] Long G L, Deng F G, Wang C and Li X H 2007 *Front Phys. China* **2** 251
[11] Gao F, Qin S J and Guo F Z 2011 *Chin. Phys. Lett.* **28** 020303
[12] Chang Y, Xu C X, Zhang S B and Yan L L 2014 *Chin. Phys. B* **23** 010305
[13] Gao F, Liu B and Wen Q Y 2012 *Opt. Express* **20** 17411
[14] Zou X F and Qiu D W 2014 *Sci. China-Phys. Mech. Astron.* **57** 1696
[15] Zheng C and Long G F 2014 *Sci. China-Phys. Mech. Astron.* **57** 1238
[16] Chang Y, Xu C X, Zhang S B and Yan L L 2014 *Chin. Sci. Bull.* **59** 2541
[17] Pei C X, Han B B and Zhao N 2009 *Acta Photon. Sin.* **38** 422
[18] Li J, Li L Y, Jin H F and Li R F 2013 *Phys. Lett. A* **377** 2729
[19] Li Y B and Qin S J 2013 *Quantum Inf. Process* **12** 2191
[20] Chen T Y, Zhang J, Boileau J C, Jin X M, Yang B, Zhang Q, Yang T, Laflamme R and Pan J W 2006 *Phys. Rev. Lett.* **96** 150504
[21] MacWilliams F J and Sloane N J A 1977 *The Theory of Error-Correcting* Codes (New York: Noth-Holland)
[22] Shor P W 1995 *Phys. Rev. A* **52** R2493
[23] Laflamme R, Miquel C, Paz J P and Zurek W H 1996 *Phys. Rev. Lett.* **77** 198
[24] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
[25] Wen K and Long G L 2010 *Int. J. Quant. Inf.* **8** 697
[26] Zhang C M and Song X T 2014 *Chin Sci. Bull.* **59** 2825
[27] Li X H 2010 *Phys. Rev. A* **82** 044304
[28] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **81** 042332
[29] Xia Y, Fan L L and Hao S Y 2013 *Quantum Inf. Process* **12** 3553
[30] Sheng Y B, Zhou L and Long G L 2013 *Phys. Rev. A* **88** 022302
[31] Hou S Y, Sheng Y B, Feng G R and Long G L 2014 *Quantum Information Processor*
[32] Wang C, Zhang Y and Jin G S 2011 *Phys. Rev. A* **84** 032307
[33] Sheng Y B, Zhou L, Zhao S M and Zheng B Y 2012 *Phys. Rev. A* **85** 012307
[34] Du F F, Li T, Ren B C, Wei H R and Deng F G 2012 *J. Opt. Soc. Am. B* **29** 1399
[35] Ren B C, Du F F and Deng F G 2013 *Phys. Rev. A* **88** 012302
[36] Wang T J and Long G L 2013 *J. Opt. Soc. Am. B* **30** 1069
[37] Zhang R, Zhou S H, Cao C 2014 *Sci. China-Phys. Mech. Astron.* **57** 1511
[38] Ren B C and Long G L 2014 *Opt. Express* **22** 6547
[39] Xu G F and Long G L 2014 *Scientific Reports* **4** 6814
[40] Wang X B 2004 *Phys. Rev. A* **69** 022320
[41] Bourennane M, Eibl M and Gaertner S 2004 *Phys. Rev. Lett.* **92** 107901
[42] Ji C H and Yee Y 2004 *IEEE J. Sel. Top Quantum Electron.* **10** 545
[43] Cabello A 2007 *Phys. Rev. A* **75** 020301
[44] Sun Y, Wen Q Y, Gao F and Zhu F C 2009 *Phys. Rev. A* **80** 032321