Commun. Theor. Phys. **56** (2011) 831–836 Vol. 56, No. 5, November 15, 2011

Quantum Secure Direct Communication by Using Three-Dimensional Hyperentanglement*

SHI Jin (施锦),[1,2] GONG Yan-Xiao (龚彦晓),[1] XU Ping (徐平),[1,†] ZHU Shi-Ning (祝世宁),[1] and ZHAN You-Bang (詹佑邦)[2,‡]

[1]National Laboratory of Solid State Microstructures, Department of Physics, Nanjing University, Nanjing 210093, China

[2]School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huaian 223300, China

(Received May 13, 2011; revised manuscript received July 11, 2011)

Abstract *We propose two schemes for realizing quantum secure direct communication (QSDC) by using a set of ordered two-photon three-dimensional hyperentangled states entangled in two degrees of freedom (DOFs) as quantum information channels. In the first scheme, the photons from Bob to Alice are transmitted only once. After insuring the security of the quantum channels, Bob encodes the secret message on his photons. Then Alice performs single-photon two-DOF Bell bases measurements on her photons. This scheme has better security than former QSDC protocols. In the second scheme, Bob transmits photons to Alice twice. After insuring the security of the quantum channels, Bob encodes the secret message on his photons. Then Alice performs two-photon Bell bases measurements on each DOF. The scheme has more information capacity than former QSDC protocols.*

PACS numbers: 03.67.Hk, 03.67.Dd, 03.65.Ud, 42.50.Dv
Key words: quantum secure direct communication, hyperentanglement, Bell bases measurement

1 Introduction

Quantum communication provides a new technique for secure high-capacity information transmission. Quantum cryptography is one of the most striking developments in quantum communication, including quantum key distribution (QKD),[1−2] quantum secret sharing,[3−6] quantum dialogue,[7−8] quantum secure direct communication (QSDC)[9−29] and so on. Quantum key distribution was first proposed by Bennett and Brassard[1] in 1984, in which two remote legitimate users, say Alice and Bob, establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) the secret messages. This protocol has been proven to be unconditionally secure.[30−31]

Quantum secure direct communication[9−29] is another remarkable branch of quantum cryptography, which allows the sender to transmit deterministic secret information to the receiver directly without establishing random keys first. The QSDC protocol proposed by Beige *et al.*[9] is a scheme with one communication in the quantum channel and another communication in the classical channel, which is later called deterministic secure quantum communication (DSQC).[12,14] Boström and Felbinger put forward a ping-pong QSDC protocol following the idea of quantum dense coding with EPR pairs. It is a quasi-secure direct communication protocol.[10] It has stimulated wide interests for direct quantum communication though it was not secure on a lossy quantum channel.[11] Deng *et al.*[12] introduced the concept of quantum data block into quantum communication and proposed a QSDC scheme based on entangled quantum systems. Wang *et al.*[13] proposed a QSDC protocol with quantum superdense coding in high-dimensional Hilbert space. Zhan *et al.*[17] proposed a QSDC protocol by using entangled qutrits and entanglement swapping. The most typical protocols of QSDC are ping-pong protocol[10] and one-time pad protocol.[19] In Ref. [21], QSDC protocol based on hyperdense coding with hyperentangled qubits is given. This protocol has the advantage of higher capacity than the QSDC protocols with a qubit system. More recently, many QSDC protocols under the noise condition were proposed.[24−29]

Hyperentanglement[32−36] means simultaneous entanglement in more than one degree of freedom (DOF), such as polarization-momentum, polarization-frequency, path-orbit angular momentum (OAM)-polarization and so on. Hyperentangled two-photon states have been used to enhance the channel capacity and have considerable putative robustness in superdense coding.[36] Hyperentanglement is less affected by decoherence than single-DOF multipartite entanglement.[34,40] Hyperentangled states can be used to assist complete Bell-state discrimination,[37−39] efficient construction of entangled states,[40−41] quantum key distribution,[42] entanglement purification protocols,[43−44] enhanced violation of local

*Supported by the National Natural Science Foundations of China under Grant Nos. 10904066 and 11004096, and the State Key Program for Basic Research of China under Grant No. 2011CBA00205

†Corresponding author, E-mail: pingxu520@nju.edu.cn
‡E-mail: ybzhan@hytc.edu.cn

realism,[45] quantum communication,[46] and multiqubit logic gates.[47] Many quantum systems have been used to produce hyperentanglement.[48−52]

In this paper, we propose two QSDC schemes where the carriers of information are two-photon three-dimensional hyperentangled states entangled in two DOFs. We show the QSDC schemes provide higher capacity than the QSDC taking two-dimensional one-DOF photon pairs as quantum channel. And also the communication is proved to be more secure under usual attacks.

2 QSDC by Using Three-Dimensional Hyperentanglement

Alice and Bob are provided with a pair of photons A and B simultaneously entangled in two DOFs, for example, in their space and frequency DOFs or in their orbital angular momentum and time-bin DOFs and so on. In general, we denote the state of the two photons entangled in a-DOF and b-DOF as

$$\begin{aligned}|\Psi^{00}\rangle_{AB} &= |\phi^{00}\rangle_{AB}^{aa}\otimes|\phi^{00}\rangle_{AB}^{bb}\\ &= \frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{AB}^{aa}\\ &\quad\otimes\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{AB}^{bb}.\end{aligned}\tag{1}$$

Bell bases are defined as

$$|\phi^{nm}\rangle^{k_1k_2}=\sum_j\frac{1}{\sqrt{3}}\,\mathrm{e}^{2\pi\mathrm{i}nj/3}|j\rangle^{k_1}|j+m\mod 3\rangle^{k_2}.\tag{2}$$

Following the method of Ref. [53], we introduce other two three-dimensional measurement bases. We denote X-bases and Z-bases as

$$\begin{aligned}|X^{nm}\rangle^{k_1k_2} &= \frac{1}{\sqrt{3}}(\,\mathrm{e}^{2\pi\mathrm{i}/3}|0\rangle|m\rangle\\ &\quad+\sum_{j=1}^{2}\mathrm{e}^{2\pi\mathrm{i}nj/3}|j\rangle|j+m\mod 3\rangle)^{k_1k_2},\end{aligned}\tag{3}$$

$$|Z^{nm}\rangle^{k_1k_2}=|nm\rangle^{k_1k_2}.\tag{4}$$

Here $n,m,j=0,1,2$. If k_1, k_2 denote different DOFs, they are single-photon two-DOF bases. If k_1, k_2 denote the same DOF, they are two-photon bases. The unitary operations

$$U_0^{nm}=\sum_{j=0}^{2}\mathrm{e}^{2\pi\mathrm{i}jn/3}|j+m\mod 3\rangle\langle j|,\tag{5}$$

can transform $U_0^{nm}|\phi^{00}\rangle=|\phi^{nm}\rangle$. Bob can perform unitary operations U_1^{nm} on his photon B and transform $U_1^{nm}|\phi^{00}\rangle=|X^{nm}\rangle$,

$$U_1^{nm}=\mathrm{e}^{2\pi\mathrm{i}/3}|m\rangle\langle 0|+\sum_{j=1}^{2}\mathrm{e}^{2\pi\mathrm{i}nj/3}|j+m\mod 3\rangle\langle j|.\tag{6}$$

Alice can perform unitary operations U_1^{nm} on her photon A and the transform results are shown in Table 1.

Table 1 Results of U_1^{nm} transforming $|\phi^{00}\rangle$ on photon A.

U_1^{00}	U_1^{10}	U_1^{20}	U_1^{01}	U_1^{11}	U_1^{21}	U_1^{02}	U_1^{12}	U_1^{22}
X^{00}	X^{10}	X^{20}	X^{22}	X^{02}	X^{12}	X^{11}	X^{21}	X^{01}

2.1 *QSDC by Using Single-Photon Two-DOF Bell Bases Measurement with Hyperentanglement*

The states resulting from Bob's encoding can be rewritten as superpositions of the single-photon two-DOF Bell states as

$$\begin{aligned}|\Psi^{nm}\rangle &= |\phi^{nm}\rangle_{AB}^{aa}\otimes|\phi^{00}\rangle_{AB}^{bb}=\frac{1}{3}\sum_{j,j'}(|\phi^{j,j'}\rangle_A^{ab}\\ &\quad\otimes|\phi^{(3+n-j)\mod 3,(3-m+j')\mod 3}\rangle_B^{ab},\end{aligned}\tag{7}$$

where $n,m,j,j'=0,1,2$. In our first scheme, we consider QSDC by using single-photon two-DOF Bell bases measurements on three-dimensional hyperentanglement. Bob is the sender of messages and Alice is the receiver. The concrete steps are described as follows:

(i) Bob first prepares a large enough number (N) of two-DOF entangled states in

$$\begin{aligned}|\Psi\rangle_{A_nB_n} &= \frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A_nB_n}^{aa}\\ &\quad\otimes\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A_nB_n}^{bb},\end{aligned}\tag{8}$$

where $n=1,2,\ldots,N$. He takes one photon from each state to form an ordered qutrits $[B_1,B_2,\ldots,B_N]$ called $\mathrm{S_B}$ sequence. The remaining qutrits $[A_1,A_2,\ldots,A_N]$ called $\mathrm{S_A}$ sequence.

(ii) Bob chooses several subsets randomly to constitute a sufficiently large subset in the $\mathrm{S_B}$ sequence as a checking set, called $\mathrm{C_B}$ set. The remaining qutrits in $\mathrm{S_B}$ sequence are taken as encoding-decoding set, called $\mathrm{M_B}$ set. Then Bob selects randomly unitary operations U_1^{nm} on one DOF of his qutrits in $\mathrm{C_B}$ set and sends $\mathrm{S_A}$ sequence to Alice.

(iii) After verifying that Alice has received all qutrits of $\mathrm{S_A}$ sequence, Bob announces the position and the DOF on which he performs unitary operations for each checking photon of $\mathrm{C_B}$ set. Alice takes the corresponding photons in $\mathrm{S_A}$ sequence to form an ordered checking set, called $\mathrm{C_A}$ set. The remaining photons in $\mathrm{S_A}$ sequence are taken as encoding-decoding set, namely $\mathrm{M_A}$ set. Alice performs randomly unitary operations U_1^{nm} on the other DOF of her qutrits in Eq. (8). Then she measures her qutrits by using single-photon two-DOF X-bases and single-photon two-DOF Z-bases randomly on all the checking photons in $\mathrm{C_A}$ set and announces measurement bases for each checking photon of $\mathrm{C_A}$ set.

(iv) After Bob performs the single-photon measurement on all the checking photons in his C_B set by using the same measurement bases as Alice′s, Alice announces her measurement results and unitary operations of all the checking photons. Bob compares his outcomes with Alice′s to determine whether there is an eavesdropper in the channel. For example, if Bob performs unitary operation U_1^{21} on a-DOF of qutrit j in $\mathrm{C_B}$ set at step (ii) and Alice performs unitary operation U_1^{21} on b-DOF and X-bases measures of qutrit j in C_A set at step (iii), the state of the system including qutrits of checking photons j in $\mathrm{C_B}$ and $\mathrm{C_A}$ sets can be written as

$$|X^{21}\rangle_{AB}^{aa}\otimes|X^{12}\rangle_{AB}^{bb}=\frac{1}{3}(\,\mathrm{e}^{2\pi\mathrm{i}/3}|01\rangle+\mathrm{e}^{4\pi\mathrm{i}/3}|12\rangle+\mathrm{e}^{2\pi\mathrm{i}/3}|20\rangle)_{AB}^{aa}$$
$$\otimes(\,\mathrm{e}^{2\pi\mathrm{i}/3}|02\rangle+\mathrm{e}^{2\pi\mathrm{i}/3}|10\rangle+\mathrm{e}^{4\pi\mathrm{i}/3}|21\rangle)_{AB}^{bb}=\frac{1}{3}(\,\mathrm{e}^{4\pi\mathrm{i}/3}|X^{12}\rangle_{A}^{ab}\otimes|X^{00}\rangle_{B}^{ab}+\mathrm{e}^{2\pi\mathrm{i}/3}|X^{02}\rangle_{A}^{ab}$$
$$\otimes|X^{10}\rangle_{B}^{ab}+\mathrm{e}^{2\pi\mathrm{i}/3}|X^{22}\rangle_{A}^{ab}\otimes|X^{20}\rangle_{B}^{ab}+\mathrm{e}^{2\pi\mathrm{i}/3}|X^{20}\rangle_{A}^{ab}\otimes|X^{01}\rangle_{B}^{ab}+|X^{10}\rangle_{A}^{ab}\otimes|X^{11}\rangle_{B}^{ab}+|X^{00}\rangle_{A}^{ab}$$
$$\otimes|X^{21}\rangle_{B}^{ab}+\mathrm{e}^{2\pi\mathrm{i}/3}|X^{01}\rangle_{A}^{ab}\otimes|X^{02}\rangle_{B}^{ab}+|X^{21}\rangle_{A}^{ab}\otimes|X^{12}\rangle_{B}^{ab}+\mathrm{e}^{4\pi\mathrm{i}/3}|X^{11}\rangle_{A}^{ab}\otimes|X^{22}\rangle_{B}^{ab}\,). \quad (9)$$

It is clear that if Alice's measurement result is $|X^{00}\rangle_{A}^{ab}$ when she performs X-bases measurement on the checking photon j in $\mathrm{C_A}$ set, and if no eavesdropping exists, then Bob's measurement outcome should be $|X^{21}\rangle_{B}^{ab}$ when he performs X-bases measurements on the corresponding photon j in $\mathrm{C_B}$ set. After security checking process, if the error rate is high, Bob concludes that the channel is not secure, and aborts the communication. Otherwise, they continue to execute the next step.

(v) After insuring the security of the quantum channel, Alice and Bob perform their secure direct communication. In order to encode the secret message, they agree that the unitary operations $U_0^{00},U_0^{10},U_0^{20},U_0^{01},U_0^{11},U_0^{21},U_0^{02},U_0^{12},U_0^{22}$, represent the secret messages 00, 10, 20, 01, 11, 21, 02, 12, and 22, respectively. In accord with the encoding-decoding photons ordering, Bob performs his two-bit encoding via U_0^{nm} operations on a-DOF of the encoding-decoding photons according to his bit strings to be transmitted this time.

(vi) Bob performs single-photon two-DOF Bell measurements and publicly announces his measurement outcomes, then Alice measures her encoding-decoding photons in M_A sequence by using single-photon two-DOF Bell bases. After she compares each of Bob's measurement outcomes and her measurement results with photon orders, she can identify the exact unitary operation U_0^{nm} performed by Bob on each encoding-decoding photon. Thus, Alice can read $\log_2 9$ bits information.

We now discuss the security for our QSDC protocol. There is an eavesdropper Eve with unlimited powers, whose technology is confined only by the laws of quantum mechanics. To gain useful secret messages, Eve must attack the quantum channel during the hyperentangled states transmission process. Firstly, we consider the intercept-and-resend attack. Eve prepares a series of ordered photons pairs, which are in the state

$$|\Psi\rangle_{A'_nB'_n}=\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A'_nB'_n}^{aa}$$
$$\otimes\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A'_nB'_n}^{bb}.$$

Eve divides them into two sequences, the $\mathrm{S_{A'}}$ sequence and the $\mathrm{S_{B'}}$ sequence. When Bob sends the $\mathrm{S_A}$ sequence to Alice, Eve intercepts $\mathrm{S_A}$ sequence and sends her fake sequence $\mathrm{S_{A'}}$ to Alice. Then Alice would take $\mathrm{S_{A'}}$ sequence for $\mathrm{S_A}$ sequence and performs the single-photon bases measurements as described above. In accordance with the order of qutrits in $\mathrm{C_B}$ set, Eve can take the corresponding photons in $\mathrm{S_{B'}}$ sequence to form an ordered set, called $\mathrm{C_{B'}}$. After Alice announces her measurement bases and measurement results for each photon in $\mathrm{C_{A'}}$, Eve performs the same bases measurement on the corresponding photons in $\mathrm{C_A}$ set. Since the photons are transmitted only once, if Eve is not detected in the security checking process, Eve will get the whole secret messages in the process of secret message transmission. However, in our protocol Bob performs randomly unitary operations U_1^{nm} on one DOF of checking qutrits in $\mathrm{C_B}$ set before sending $\mathrm{S_A}$ sequence to Alice, so Eve can only guess randomly and only has 1/9 chance to choose the right unitary operation for one time. Alice performs randomly unitary operations U_1^{nm} on the other DOF of checking qutrits in C_A set and announces her measurement results after Bob finishes measurements, so Eve has only 1/9 chance to choose the right unitary operations. Hence, the intercept-and-resend attack can be detected when Bob compares their measurement outcomes.

Secondly, we consider the entangle-and-measure attacks. Eve prepares a series of ordered photon pairs, which are in the state

$$|\Psi\rangle_{A'_nB'_n}=\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A'_nB'_n}^{aa}$$
$$\otimes\frac{1}{\sqrt{3}}(|00\rangle+|11\rangle+|22\rangle)_{A'_nB'_n}^{bb}.$$

When Bob sends the $\mathrm{S_A}$ sequence to Alice, Eve captures $\mathrm{S_A}$ sequence and performs the two-photon Bell measurement on the qutrits (A_n,A'_n). If Bob has not randomly performed unitary operations U_1^{nm} on the checking groups in $\mathrm{C_B}$ set at step (ii), the state of the whole system will be described as

$$|\Psi^{00}\rangle_{A_nB_n}\otimes|\Psi^{00}\rangle_{A'_nB'_n}=|\phi^{00}\rangle_{A_nB_n}^{aa}\otimes|\phi^{00}\rangle_{A_nB_n}^{bb}\otimes|\phi^{00}\rangle_{A'_nB'_n}^{aa}\otimes|\phi^{00}\rangle_{A'_nB'_n}^{bb}$$
$$=\frac{1}{9}\sum_{(j,j')}(|\phi^{j,j'}\rangle_{B_nB'_n}^{aa}\otimes|\phi^{(3-j)\ \bmod 3,(3+j')\ \bmod 3}\rangle_{B_nB'_n}^{bb}\otimes|\phi^{j,j'}\rangle_{A_nA'_n}^{aa}$$
$$\otimes|\phi^{(3-j)\ \bmod 3,(3+j')\ \bmod 3}\rangle_{A_nA'_n}^{bb}.$$

After two-photon (A_n, A'_n) Bell-measurement by Eve, the entanglement between qutrits (A_n, B_n) disappears and the new entanglement between qutrits A_n and A'_n (B_n and B'_n) is set up. Then Eve sends the S_A sequence to Alice. According to the public announcement of Bob as above, Alice proceeds as usual. Then Eve can perform the single-photon two-DOF Bell-measurement on the corresponding qutrits in $S_{A'}$ sequence to get the information of unitary operations performed by Alice, and make the same unitary operations on the corresponding groups in the $S_{B'}$ sequence. As a result, Eve will not be detected, and can get the whole secret messages in the process of secret message transmission. However, as Bob randomly performs unitary operations at step (ii), Eve cannot perform correct unitary operations U_1^{nm} on the corresponding groups in $S_{B'}$ qutrit sequence, and therefore the Eve's eavesdropping can be detected by Alice and Bob in the security checking process. Finally, we consider the Trojan horse attack strategy.[2] The primary Trojan horse attack strategies include a multi-photon-signal attack,[54] an invisible-photon attack,[55] and a delay-photon attack.[56] Since this protocol transmits photons only once, it is secure for Trojan horse attack strategies.

2.2 *QSDC by Using Hyperdense Coding with Hyperentanglement*

In our second scheme, we consider QSDC by using hyperdense coding with three-dimensional hyperentanglement. We can write 81 three-dimensional unitary operations as

$$\begin{aligned} U^{nm} &= (U^{n'm'}) \otimes (U^{n''m''}) \\ &= \sum_j \mathrm{e}^{2\pi \mathrm{i} j n'/3} |j + m' \mod 3\rangle^a \langle j|^a \\ &\quad \otimes \sum_{j'} \mathrm{e}^{2\pi \mathrm{i} j' n''/3} |j' + m'' \mod 3\rangle^b \langle j'|^b , \end{aligned} \tag{10}$$

where $U^{n'm'}$ can transform $U^{n'm'}|\phi^{00}\rangle^{aa} = |\phi^{n'm'}\rangle^{aa}$ and $U^{n''m''}$ can transform $U^{n''m''}|\phi^{00}\rangle^{bb} = |\phi^{n''m''}\rangle^{bb}$. where $j, j', n', m', n'', m'' = 0, 1, 2$. Now, let us describe our second QSDC protocol where Bob is the sender of messages and Alice is the receiver.

(i) Bob first prepares a large enough number (N) of two-DOF entangled states $|\Psi\rangle_{A_n B_n}$ in Eq. (8). He takes one photon from each state to form an ordered S_B sequence. The remaining qutrits called S_A sequence.

(ii) Bob chooses several subsets randomly to constitute two sufficiently large subset in the S_B sequence as the first checking set C_B^1 and the second checking set C_B^2. The remaining qutrits in S_B sequence are taken as encoding-decoding set, called M_B set. Then Bob performs randomly unitary operations U_1^{nm} on one DOF of his qutrits to perform all the checking photons in C_B^1 set and sends S_A sequence to Alice.

(iii) After verifying that Alice has received all qutrits of S_A sequence, Bob announces the position and the DOF on which he performs unitary operations for each checking photon of C_B^1 set in S_B sequence. Alice takes the corresponding photons in S_A sequence to form an ordered checking set, called C_A^1 set. Then, Alice performs randomly unitary operations U_1^{nm} on the other DOF and single-photon two-DOF bases measurements by using single-photon two-DOF X-bases and Z-bases randomly on all the checking photons in C_A^1 set and announces measurement bases.

(iv) After Bob performs single-photon measurements on all the checking photons in his C_B^1 set by using the same measurement bases as Alice's, Alice announces her measurement results and unitary operations of all the checking photons. Bob compares his outcomes with Alice's to determine whether there is an eavesdropper in the channel. If the error rate is high, Bob concludes that the channel is not secure, and aborts the communication. Otherwise, they continue to execute the next step.

(v) After insuring the security of the quantum channel, Alice and Bob perform their secure direct communication. In order to encode the secret message, they agree that the 81 unitary operations $(U^{aa}_{n'm'}) \otimes (U^{bb}_{n''m''}), (n', m', n'', m'' = 0, 1, 2)$, represent the secret messages 0000, 0001, 0002, ..., and 2222 respectively. In accord with the encoding-decoding photons order, Bob performs his three-dimensional four-bit encoding via local unitary operations $(U^{aa}_{n'm'}) \otimes (U^{bb}_{n''m''})$ on two DOFs of the encoding-decoding photons according to his bit strings to be transmitted this time. In order to insure the security of the quantum channel, Bob selects randomly unitary operations U_1^{nm} on two DOFs of his qutrits in Eq. (8) to perform all the checking photons in C_B^2 set and sends S_B sequence to Alice.

(vi) After verifying that Alice has received all qutrits of S_B sequence, Bob announces the positions of each checking photon of C_B^2 set and encoding-decoding photons M_B set in S_B sequence. Alice takes the corresponding photons in S_A sequence to form an ordered checking set, called C_A^2 set and an ordered encoding-decoding M_A set. Alice performs the two-photon measurement on all the checking photons in C_A^2 set and C_B^2 set randomly in above two-photon X-bases or two-photon Z-bases on each DOF. Alice announces her two-photon measurement bases and measurement results of all the checking photons. Bob can determine whether there is any eavesdropping in the channel. If the error rate is high, Bob concludes that the channel is not secure, and aborts the communication. Otherwise, they continue to execute the next step.

(vii) Then Alice measures corresponding two-photon by using two-photon Bell bases on each DOF of all the encoding-decoding set. She can identify the exact unitary operations $U^{aa}_{n'm'} \otimes U^{bb}_{n''m''}$ performed by Bob on each encoding-decoding photon. Thus, Alice can read the $\log_2 81$ bits information.

Our second QSDC protocol requires two security analysis. The first security analysis is similar to that for our first QSDC protocol. We now discuss the second security analysis when Bob sends the S_B sequence to Alice. Firstly, we consider the intercept-and-resend attack. Eve prepares

a series of ordered hyperentanglement pairs, which are in the state

$$|\Psi\rangle_{A'_nB'_n} = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)^{aa}_{A'_nB'_n} \otimes \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)^{bb}_{A'_nB'_n}.$$

Eve divides them into two sequences, the $S_{A'}$ sequence and the $S_{B'}$ sequence. When Bob sends the S_B sequence to Alice, Eve intercepts S_B sequence and sends her fake sequence $S_{B'}$ to Alice, and Alice would take $S_{B'}$ sequence for S_B sequence. In accordance with the order of qutrits in C^2_B set by Bob from his public announcement, Alice can take the corresponding photons in $S_{B'}$ sequence to form an ordered set, call $C^2_{B'}$ set and perform the two-photon bases measurement as described above. However, in our protocol Bob performs randomly unitary operations U^{nm}_1 on two DOFs of checking qutrits in C^2_B set before sending S_B sequence to Alice, and Alice performs two-photon measurements on all the checking photons in C^2_A and C^2_B randomly by using two-photon X-bases or Z-bases. So Eve can only guess and has only 1/9 chance to choose the right unitary operation each time. Hence, the intercept-and-resend attack can be detected when Bob compares their measurement outcomes. Secondly, we consider the entangle-and-measure attacks. Similarly, as Bob randomly performs unitary operations at step (ii), Eve cannot perform correct unitary operations U^{nm}_1 on the corresponding groups in the $S_{B'}$ sequence, so the Eve's eavesdropping can be detected by Alice and Bob in the security checking process. Finally, after receiving the qutrits sequence, Alice first adds a filter before the devices with which she operates the photons by performing unitary operations and measurements to prevent Trojan horse attack strategies. It is worth pointing out that when Bob sends the S_B sequence to Alice, particles carry the secret messages between two legitimate users, Eve can not get secret messages even by eavesdroping in the second checking procedure, because the secret messages can be only obtained by Alice's joint two-photon Bell-measurement on each DOF.

3 Conclusion

In summary, we have proposed two QSDC protocols by using two-photon three-dimensional hyperentangled states entangled in two DOFs as quantum channels. In our first scheme, we have realized checking steps by using two different single-photon measurement bases and realized encoding-decoding by using single-photon two-DOF Bell measurements with the information capacity $\log_2 9$. In our second scheme, we have realized encoding-decoding by using two-photon general Bell-measurement, the information capacity is $2\log_2 9$, showing higher information capacity. We have showed that the two schemes are both secure under usual attacks. In the first scheme, the photons are transmitted only one time, so one security analysis is required. While, as photons are transmitted two times in the second scheme, we are required to make two security analysis. Practically, there are noises and losses in quantum channels, which will threaten the security of quantum communication since Eve can hide her eavesdropping in the noises. But with the help of quantum error correction and the quantum repeater technique, the protocols can also be acted securely.

Since spontaneous parametric down-conversion (SPDC) in a nonlinear crystal is the most widely used method to prepare entangled photon pairs, we can use a single nonlinear crystal to produce high-dimensional entanglement[57−59] such as frequency, path, orbit angular momentum (OAM) and time-bin DOF. Generation and application of two-dimensional and high-dimensional hyperentanglement have rapid development both experimentally and theoretically.[21,33−39,51,60−61] So we believe our protocols are feasible in the future. Compared with previous QSDC protocols, our protocols have several advantages. Firstly, the quantum channel is different. The three-dimensional two DOFs hyperentangled states are substituted for the usual one DOF entangled states as quantum channel. Entanglement in more than one DOF can provide a significantly larger channel capacity and a putative robustness. Secondly, the present protocols provide better security. In our QSDC protocols, as two legitimate users randomly perform unitary operations during the checking steps, the probability for Eve guessing the right unitary operation is 1/9 each time, which is smaller than that of the schemes using two-dimensional entangled state as quantum channels. Thirdly, our protocols have higher information capacity. For two-dimensional quantum channel, one particle can carry 2 bits of information, while in the three-dimensional quantum channel the capacity is $\log_2 9$. Especially when Bob encodes the secret messages on two-DOF respectively, the capacity is $2\log_2 9$. Finally, our schemes can be easily generalized to QSDC based on d-dimensional hyperentangled states entangled in multi-DOF, which may be exploited for higher capacity and more secure quantum communication. Moreover, our approaches may stimulate approaches on high-dimensional hyperentanglement generation and applications.

References

[1] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computer, Systems and Signal Proceesing*, Bangalore, India IEEE, New York (1984) 175.

[2] A. Gisin, G. Ribordy, W. Tittle, and H. Zbinden, Rev. Mod. Phys. **74** (2002) 145.

[3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59** (1999) 1829.

[4] R. Cleve, D. Gottesman, and H.K. Lo, Phys. Rev. Lett. **83** (1999) 648.

[5] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98** (2007) 020503.

[6] R.H. Shi, Q. Su, Y. Guo, and M.H. Lee, Commun. Theor. Phys. **55** (2011) 573.

[7] B.A. Nguyen, Phys. Lett. A **328** (2004) 6.

[8] Y.B. Zhan, L.L. Zhang, *et al.*, Commun. Theor. Phys. **53** (2010) 648.

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

[10] K. Boström and T. Felbinger, Phys. Rev. Lett. **89(18)** (2002) 187902.

[11] Q.Y. Cai, Phys. Rev. Lett. **91** (2003) 109801.

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

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

[14] G.L. Long, F.G. Deng, C. Wang, *et al.*, Front. Phys. China **2** (2007) 251.

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

[16] S. Lin, Q.Y. Wen, F. Gao, and F.C. Zhu, Phys. Rev. A **78** (2008) 064304.

[17] Y.B. Zhan, L.L. Zhang, and Q.Y. Zhang, Opt. Commun. **282** (2009) 4633.

[18] S.J. Qin, F. Gao, Q.Y. Wen, and F.C. Zhu, Optics. Commun. **283** (2010) 1566.

[19] F.G. Deng and G.L. Long, Phys. Rev. A **69** (2004) 052319.

[20] H. Hoffmann, K. Boström, and T. Felbinger, Phys. Rev. A **72** (2005) 016301.

[21] T.J. Wang, T. Li, F.F. Du, and F.G. Deng, Chin. Phys. Lett. **28** (2011) 040305.

[22] J. Yang, C. Wang, and R. Zhang, Commun. Theor. Phys. **54** (2010) 829.

[23] Z.Y. Wang, Commun. Theor. Phys. **54** (2010) 997.

[24] S.J. Qin, F. Gao, Q.Y. Wen, *et al.*, Commun. Theor. Phys. **53** (2010) 645.

[25] J. Yang, C.A. Wang, and R. Zhang, Chin. Phys. B, **19** (2010) 110306.

[26] H. Yuan, J. Song, Q. He, *et al.*, Commun. Theor. Phys. **50** (2008) 627.

[27] B. Gu, C.Y. Zhang, G.S. Cheng, *et al.*, Science China-Phys. Mechanics & Astronomy **54** (2011) 942.

[28] S. Salemian and S. Mohammadnejad, Chinese Science Bulletin **56** (2011) 618.

[29] C.W. Yang, C.W. Tsai, and T.L. Hwang, Science China-Phys. Mechanics & Astronomy **54** (2011) 496.

[30] H.K. Lo and H.F. Chau, Science **283** (1999) 2050.

[31] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85** (2000) 441.

[32] P.G. Kwiat, J. Mod. Opt. **44** (1997) 2173.

[33] J.T. Barreiro, N.K. Langford, N.A. Peters, and P.G. Kwiat, Phys. Rev. Lett. **95** (2005) 260501.

[34] C.M. Li, K. Chen, A. Reingruber, Y.N. Chen, and J.W. Pan, Phys. Rev. Lett. **105** (2010) 210504.

[35] M. Barbieri, C. Cinelli, P. Mataloni, and F.D. Martini, Phys. Rev. A **72** (2005) 052110.

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

[37] S.P. Walborn, S. Pádua, and C.H. Monken, Phys. Rev. A **68** (2003) 042313.

[38] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **96** (2006) 190501.

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

[40] K. Chen, C.M. Li, Q. Zhang, Y.A. Chen, A. Goebel, S. Chen, A. Mair, and J.W. Pan, Phys. Rev. Lett. **99** (2007) 120503.

[41] G. Vallone, E. Pomarico, F.D. Martini, and P. Mataloni, Phys. Rev. Lett. **100** (2008) 160502.

[42] Y. Sun, Q.Y. Wen, and Z. Yuan, Opt. Commun. **284** (2011) 527.

[43] Simon and J.W. Pan, Phys. Rev. Lett. **89** (2002) 257901.

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

[45] M. Barbieri, M. Martini, F.D. Mataloni, *et al.*, Phys. Rev. Lett. **97** (2006) 140407.

[46] L.X. Chen and W.L. She, Phys. Rev. A **83** (2011) 032305.

[47] B.P. Lanyon, *et al.*, Nature Phys. **5** (2009) 134.

[48] J. Chen, J.Y. Fan, M.D. Eisaman, and A. Migdall, Phys. Rev. A **77** (2008) 053812.

[49] G. Vallone, R. Ceccarelli, F.D. Martini, and P. Mataloni, Phys. Rev. A **79** (2009) 030301.

[50] B.L. Hu and Y.B. Zhan, Phys. Rev. A **82** (2010) 054301.

[51] H. Yan, S.C. Zhang, J.F. Chen, M.M.T. Loy, G.K.L. Wong, and S.W. Du, Phys. Rev. Lett. **106** (2011) 033601.

[52] W.B. Gao, C.Y. Lu, *et al.*, Nature Phys. **6** (2010) 331.

[53] B.P. Helle and A. Peres, Phys. Rev. Lett. **85** (2000) 3313.

[54] F.G. Deng, X.H. Li, H.Y. Zhou, and Z.J. Zhang, Phys. Rev. A **72** (2005) 044302.

[55] Q.Y. Cai, Phys. Lett. A **351** (2006) 23.

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

[57] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89** (2002) 240401.

[58] X.Q. Yu, P. Xu, Z.D. Xie, *et al.*, Phys. Rev. Lett. **101** (2008) 233601.

[59] N.K. Langford, R.B. Dalton, M.D. Harvey, *et al.*, Phys. Rev. Lett. **93** (2004) 053601.

[60] A.K. Jha, J. Leach, B. Jack, *et al.*, Phys. Rev. Lett. **104** (2010) 010501.

[61] J. Lugani, S. Ghosh, and K. Thyagarjan, Phys. Rev. A **83** (2011) 062333.