Commun. Theor. Phys. **63** (2015) 285–290 Vol. 63, No. 3, March 1, 2015

Controlled Deterministic Secure Quantum Communication Protocol Based on Three-Particle GHZ States in X-Basis*

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 September 1, 2014; revised manuscript received January 14, 2015)

Abstract *A controlled deterministic secure quantum communication (CDSQC) protocol is proposed based on three-particle GHZ state in X-basis. Only X-basis and $Z_1Z_2X_3$-basis (composed of Z-basis and X-basis) measurement are required, which makes the scheme more convenient than others in practical applications. By distributing a random key between both sides of the communication and performing classical XOR operation, we realize a one-time-pad scheme, therefore our protocol achieves unconditional secure. Because only user with legitimate identity string can decrypt the secret, our protocol can resist man-in-the middle attack. The three-particle GHZ state in X-basis is used as decoy photons to detect eavesdropping. The detection rate reaches 75% per qubit.*

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.-a
Key words: deterministic secure quantum communication, eavesdropping detection, classical XOR operation

1 Introduction

Cryptosystem is the backbone of information security. With the rapid development of quantum technology, especially the advent of quantum computation, the classical cryptosystem was unable to meet the security needs of informationization. Therefore, quantum cryptosystem which is based on quantum mechanics and aims to exchange information absolutely safe in theory has attracted more and more attention.

In the past two decades, quantum secure communication developed rapidly. Quantum key distribution (QKD)[1−7] is one of the important braches in quantum secure communication. Many scholars have studied QKD and proposed some important ideas and protocols. For example, in 1984, Bennett and Brassard[1] proposed the first QKD scheme; later, in 2003, Deng and Long[4] gave the idea of order rearrangement and presented the first QKD protocol based on order rearrangement, which supplies new method for improving communication security; after a year, Deng and Long[5] put forward the first two-way QKD scheme; and Hwang[6] proposed the first QKD with decoy state; in 2008, Li *et al.*[7] proposed a robust QKD to collective noise , which make the QKD meets the actual practical application better.

QSDC,[8−24] as another important branch in quantum communication has been investigated by many groups in recent years. QSDC is much different from QKD. In a QSDC protocol, the secret information is transmitted in quantum channel directly. There is no need to establish a key first and encrypt the secret with the key. By far, many important protocols have been proposed. In 2000, Long and Liu[8] put forward the first QSDC protocol, in which the secret message is transmitted directly. In 2003, Deng *et al.*[9] published the famous two-step QSDC protocol (called two-step protocol). In the two-step protocol, the way for designing the protocol for direct communication of secret message was given clearly and it pointed out that QSDC should be performed with quantum data block in the first time. In 2004, the first QSDC based on a sequence of single photons (called DL04 protocol) was given by Deng and Long.[10] In 2005, the first QSDC protocol based on super-dense coding was developed by Wang *et al.*[11] In 2011, the first QSDC protocol based on photonic polarization-spatial hyperentanglement was presented by Wang *et al.*[14] Meanwhile, many interesting and valuable QSDC scheme with special characteristics were published. Wang *et al.*[12] proposed a QSDC scheme using multi-particle entanglement. Li *et al.*[13] presented a QSDC protocol with quantum encryption. Gu *et al.* put forward a robust QSDC protocol based on a quantum one-time pad over a collective-noise channel[15] and a two-step QSDC scheme with hyperentanglement.[16] Liu, Chen, and Jiang[17] proposed a high-capacity QSDC scheme with single photons in both polarization and spatial-mode degrees of freedom. Sun *et al.*[18] developed a QSDC scheme with two-photon four-qubit cluster states. Ren *et al.*[19] published a robust QSDC protocol based on the spatial-mode entanglement of two-photon systems. Zhang *et al.*[21] presented a QSDC protocol with four-qubit cluster states. Chang *et al.*[22] put forward a QSDC protocol with single photons and authentication.

Another class of quantum communication protocols used to transmit a secret message is called deterministic secure quantum communication (DSQC).[25−30] Cer-

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

tainly, the receiver can read out the secret message only after he exchanges at least one bit of classical information for each qubit with the sender in a DSQC protocol, which is different from QSDC. DSQC is similar to QKD, but it can be used to obtain deterministic information, not a random binary string. In 2005, Gao *et al.*[25] presented a DSQC scheme with GHZ states and swapping quantum entanglement. Man *et al.*[26] also developed a DSQC protocol based on swapping quantum entanglement of Bell states and local unitary operations. Shaari *et al.*[27] proposed a two-way deterministic protocol for quantum communication using six mutually unbiased states in the Poincare sphere. Li *et al.*[28] proposed two DSQC schemes, one based on pure entangled states and the other on d-dimensional single-photon states. Huang *et al.*[30] presented a DSQC scheme with collective detection using single photons.

Controlled quantum secure direct communication (CQSDC)[31−39] is a new concept different from QSDC. In this circumstance, except for the sender and the receiver, there is still at least one controller. Only with the permission of controller can the receiver read the secret from the sender. By far, there are several schemes for CQSDC with GHZ states have been proposed, even with GHZ-like states. In 2006, Man *et al.* developed a bidirectional CQSDC scheme with GHZ state.[31] Man's scheme can exchange four bits of information (two from Alice and two from Bob) in all, however, in 2013, Liu *et al.*[32] found that three bits are leaked out unintentionally (without any active attack) and only 1 ($-\log(1/2) = 1$) bit of information is secretly kept. In 2013, Ye *et al.*[33] put forward two approaches to improve Man's protocol. One is to modify the encoding rule of Man's protocol. The other is to use a Bell state as the quantum resource instead of a GHZ state. Wang *et al.*[34] proposed a one-way dense coding scheme for CQSDC with GHZ state. In Wang's protocol three bits of secret message are transmitted, however, in 2010, Gao *et al.*[35] found that Wang's protocol could not defend correlation-elicitation (double-CNOT) attack and the receiver can illegally obtain 33.3% of the sender's secret without any controller's permission. Gao *et al.* also proposed an improved protocol for Wang's protocol by introducing an additional random sampling to avoid the weakness. Though Gao's improvement overcomes the information leakage problem, the qubit efficiency is decreased, due to the introduction of an additional random sampling.[36] In 2011, Kao *et al.*[36] overcome the information leakage problem by introducing the base changing technique to the random sampling in Wang's protocol and provide better qubit efficiency. Dong Jian *et al.*[37] presented a multiparty CQSDC scheme based on GHZ state and teleportation. In Dong Jian's protocol, secret message of d-dimensional is transmitted through teleportation and some measurements, such as d-dimensional Bell state measurement (DBM) and X-basis or Z-basis measurement. Dong Li *et al.*[38] also presented a one-way three-party CQSDC protocol with GHZ-like state by using controlled quantum teleportation. Dong's protocol is tolerant of some noise effects and is feasible by using the present optical technique because of imperfect Bell-state measurement based on Bell-state analyzer of Bouwmeester *et al.*[40] Li *et al.*[39] proposed an experimentally feasible protocol for implementing controlled dense coding by using a three-atom GHZ-type state in cavity quantum electrodynamics (QED).

Though the above protocols exhibit significant advantages in theory, they need to perform one or several kinds of measurements with certain difficulty in technology, such as three-particle or multi-particle GHZ state measurement, imperfect Bell-state measurement, d-dimensional Bell state measurement (DBM), or the combination of one of above measurements with X-basis and Z-basis measurement, which increase the difficulty of realization. Furthermore, for lack of identity authentication, the above protocols may be threatened with man-in-the middle attack. We proposed a controlled deterministic secure quantum communication (CDSQC) protocol based on three-particle GHZ state in X-basis. In our protocol, only X-basis and $Z_1Z_2X_3$-basis (composed of Z-basis and X-basis) measurement is needed; therefore our protocol is easier to implement. Besides, by distributing a random key between both sides of the communication and performing classical XOR operation, we realize a one-time-pad scheme, therefore our protocol achieves unconditional secure. Because only legitimate user with correct identity string ID_B can recover C_3 and decrypt the secret, our protocol can resist man-in-the middle attack. The three-particle GHZ state in X-basis is used as decoy photons to detect eavesdropping. The detection rate reaches 75%.

2 Description of Protocol

In classical cryptography, it is generally accepted that the Vernam cipher (one-time pad),[41] which utilizes a previously shared secret key to encrypt the message transmitted in the public channel, is the only cryptosystem with proved security.[42] In 2002, Leung[43] firstly proposed and analyzed a quantum analog of the Vernam cipher (quantum one-time pad). The quantum Vernam cipher may also be called quantum Vernam algorithm and it is similar to the classic Vernam algorithm. But it is not limited by the so-called "one-time" characteristic which is necessary in the classic Vernam algorithm for its security. Actually, in some quantum Vernam algorithms the shared key between communicators might be employed repeatedly since its quantum nature.[44] The advantage of the quantum Vernam algorithm is apparent because the difficulty of the key management in the quantum Vernam algorithm goes away. In addition, the quantum Vernam algorithm can encode quantum messages as well as classic messages, and the optimal length of the key may be the same as the plaintext.[44]

Now let us briefly describe the three-particle GHZ state in X basis and quantum one-time pad protocol. We suppose that the sender, Alice, transmits her secret message to the legitimate receiver, say Bob. But Bob could not read out the message without the permission of the

controller, say Charlie. Bob has the secret N-bit string ID_B representing his identity. Alice shares ID_B. Suppose that Alice's secret message is a series of classical 0 or 1 numbers in order, called M.

Step 1 Alice prepares N ordered three-particle GHZ states in X basis used to transmit secret information, each of which is in the state:

$$|\psi\rangle=\frac{1}{2\sqrt{2}}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123}\,. \quad (1)$$

The ordered $|\psi\rangle$ state sequence is expressed as $\{[P_1(1), P_1(2), P_1(3)], [P_2(1), P_2(2), P_2(3)], \ldots, [P_N(1), P_N(2), P_N(3)]\}$. Alice takes photons 1 from each state to construct S_1 sequence, which is an ordered photon sequence: $\{P_1(1), P_2(1), \ldots, P_N(1)\}$; the remaining photons 2 and 3 construct S_2 and S_3 sequences respectively, which are ordered photon sequences: $\{P_1(2), P_2(2), \ldots, P_N(2)\}$ and $\{P_1(3), P_2(3), \ldots, P_N(3)\}$. It is similar with the block transmission technique first proposed by Long and Liu,[45] which realizes efficient quantum communication.

Step 2 According to ID_B, Alice performs one of the two unitary operations,

$$I=|+\rangle\langle+|+|-\rangle\langle-|\,, \quad U=\mathrm{i}\sigma_y=|+\rangle\langle-|-|-\rangle\langle+|\,, \quad (2)$$

on photons 3 in S_3 sequence and gets S_{3U}. The rule is that, if ID_B is "0" ("1"), she performs operation$I$ (U) on photon 3.

Step 3 Alice prepares another two M ordered $|\psi\rangle$ states used as decoy photons. The ordered $|\psi\rangle$ states are denoted as $\{T_1(1), T_1(2), T_1(3), T_2(1), T_2(2), T_2(3), \ldots, T_M(1), T_M(2), T_M(3)\}$, termed as S_T sequence. The decoy photons technique comes from the works by Li *et al.*[46−47]

Step 4 Alice randomly mixes the two S_T to S_2 and S_{3U} respectively (forms S_2' and S_{3U}'). Only Alice knows the positions of these decoy photons in S_2' and in S_{3U}'. Then, Alice transmits S_2' and S_{3U}' to Bob and Charlie respectively.

Step 5 After Alice has confirmed that Bob and Charlie have received photons successfully, Alice publishes the positions two S_T in S_2' and S_{3U}' respectively. According to the positions Alice published, Bob and Charlie extract the two S_T from S_2' and S_{3U}' respectively. Bob and Charlie perform three single-qubit measurements $Z_1Z_2X_3$ on the S_T extracted respectively. In the ideal cases, every result should be in one of the four $|00+\rangle$ $|11+\rangle$, $|00-\rangle$, $|11-\rangle$ states with equal probability. If the error rate is low enough it means no eavesdropping exists. In this condition, the communication goes on. Otherwise Bob or Charlie interrupts it.

Step 6 If Charlie allows Bob recover the secret message, Charlie measures photons in S_{3U} sequence with X-basis in order; if state $|+\rangle$ is denoted as "0" and $|-\rangle$ as "1", Charlie can get a series of classical numbers C_{3U} in order; Charlie publishes C_{3U}.

Step 7 Bob measures photons in S_2 sequence with X-basis in order. According to the rule: "0" expresses states $|+\rangle$ and "1" denotes $|-\rangle$, he gets an ordered classical numbers sequence C_2. Bob and Charlie publicly announce which photons in S_2 and S_{3U} they lost respectively. Alice, Bob and Charlie make their phones (S_1, S_2 and S_{3U}) one-to-one matching by discarding the one-to-one photons not received by anyone. For instance, if Bob loses the second photon in S_2, then Alice discards the second in S_1 and Charlie discards the second in S_{3U}.

Step 8 Alice measures the remaining photons in S_1 in order with X-basis and constructs an ordered classical numbers sequence C_1. It is similar to the delayed measurement technique in Ref. [48]. On assumption that the number of bits in C_1 is N_1, Alice takes the first N_1 bits from secret message M (called M_1) and encrypts it with C_1 bit by bit using XOR operation (M_1 XOR $C_1 \to C$). Then Alice publishes C.

Step 9 Bob recovers C_3 according to C_{3U} and ID_B. Because the operation U flips the state in X-basis, as

$$U|+\rangle=-|-\rangle\,, \quad U|-\rangle=|+\rangle\,. \quad (3)$$

Therefore, if the bit of ID_B is "1", the one-to-one bit of C_3 can be obtained by performing logical negation on the one-to-one bit of $C_{3U}(C_3=\overline{C_{3U}})$; if the bit of ID_B is "0", the one-to-one bit of C_3 is equal to the bit of C_{3U}. Therefore, if Bob is not a legitimate user, he can not recover C_3.

Step 10 According to C_3, Bob decrypts C with C_2 bit by bit using XOR operation. We denote the possible states of S_1, S_2 and S_3 as

$$\begin{bmatrix} S_1 & S_2 & S_3 \\ |+\rangle & |+\rangle & |+\rangle \\ |+\rangle & |-\rangle & |-\rangle \\ |-\rangle & |+\rangle & |-\rangle \\ |-\rangle & |-\rangle & |+\rangle \end{bmatrix}. \quad (4)$$

Obviously, if the photon 3 is in state $|+\rangle$, the state of photon 1 is the same with the state of photons 2; if the photon 3 is in state $|-\rangle$, the state of photon 1 is quite opposite to the state of photons 2. Therefore, if the bit of C_3 is "0", the bit of C_2 is equal to the one-to-one bit of C_1; otherwise the bit of C_2 is opposite to the one-to-one bit of C_1. Thus, to read out the secret message M_1, if the bit of C_3 is "0", Bob gets M_1 by performing C_2 XOR $C \to M_1$; if the bit of C_3 is "1", Bob gets M_1 by performing $\bar{C}_2$ XOR $C \to M_1$.

3 Security Analysis

The security of the protocol is mainly guaranteed by the eavesdropping detection strategy based on

$$|\psi\rangle=\frac{1}{2\sqrt{2}}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123}$$

state and the identity string ID_B. If the receiver does not know ID_B (which means he is not a legitimate user), he can not recover C_3 in step 9 (which means he cannot decrypt the secret message), therefore, the protocol will not be threatened by man-in-the-middle attack. Next we analyze the eavesdropping detection rate of the protocol and how the protocol resists some common attacks in controlled protocols, such as attack from the receiver, attack

from the controller, and attack from the external eavesdropper. The security of ID_B is analyzed. The effect of noise is considered.

3.1 *Analysis of the Eavesdropping Detection Rate*

In the protocol, $|\psi\rangle$ states are used as decoy photons to detect eavesdropping. Because the positions of decoy photons are secret, Eve can not discriminate between decoy photons and information photons (photons in S_2 and in S_3). According to Stingspring dilation theorem, Eve's eavesdropping can be implemented by a unitary operation E acting on a bigger Hilbert space $H_{123} \otimes H_E$. The eavesdropping can be represented as:

$$\begin{aligned}
&E \otimes |+\rangle|x\rangle_E = a|+\rangle|x_0\rangle_E + b|-\rangle|x_1\rangle_E\,,\\
&E \otimes |-\rangle|x\rangle_E = m|+\rangle|y_0\rangle_E + n|-\rangle|y_1\rangle_E\,,\\
&E \otimes |0\rangle|x\rangle_E = c|0\rangle|z_0\rangle_E + d|1\rangle|z_1\rangle_E\,,\\
&E \otimes |1\rangle|x\rangle_E = e|0\rangle|v_0\rangle_E + f|1\rangle|v_1\rangle_E\,. \qquad (5)
\end{aligned}$$

Here $|x\rangle_E$ is the initial state of Eve's auxiliary particle and $a^2+b^2=1$, $m^2+n^2=1$, $c^2+d^2=1$, $e^2+f^2=1$. $|x_0\rangle_E$, $|x_1\rangle_E$, $|y_0\rangle_E$, $|y_1\rangle_E$, $|z_0\rangle_E$, $|z_1\rangle_E$, $|v_0\rangle_E$, $|v_1\rangle_E$ are pure states uniquely determined by unitary operation E.

The initial state

$$|\psi\rangle=\frac{1}{2\sqrt{2}}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123}$$

can be re-represented as:

$$\begin{aligned}
|\psi\rangle=&\frac{1}{2\sqrt{2}}(|+++\rangle+|+--\rangle+|-+-\rangle+|--+\rangle)_{123}\\
=&\frac{1}{2\sqrt{2}}\Big[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_2|+\rangle_3\\
&+\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_1\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_2|-\rangle_3\\
&+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_2|-\rangle_3\\
&+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_1\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_2|+\rangle_3\Big]\\
=&\frac{1}{2\sqrt{2}}(|00+\rangle+|11+\rangle+|00-\rangle+|11-\rangle)_{123}\,. \qquad (6)
\end{aligned}$$

After Eve's eavesdropping, the combined system changes to:

$$\begin{aligned}
|\psi\rangle_{\mathrm{Eve}} &= E\otimes E\otimes E\otimes\Big[\frac{1}{2\sqrt{2}}(|0x0x{+}x\rangle{+}|1x1x+x\rangle{+}|0x0x-x\rangle+|1x1x-x\rangle)_{123}\Big]\\
&=\frac{1}{2\sqrt{2}}[(c|0z_0\rangle+d|1z_1\rangle)\otimes(c|0z_0\rangle+d|1z_1\rangle)\otimes(a|{+}x_0\rangle+b|{-}x_1\rangle)\\
&\quad+(e|0v_0\rangle+f|1v_1\rangle)\otimes(e|0v_0\rangle+f|1v_1\rangle)\otimes(a|{+}x_0\rangle+b|{-}x_1\rangle)\\
&\quad+(c|0z_0\rangle+d|1z_1\rangle)\otimes(c|0z_0\rangle+d|1z_1\rangle)\otimes(m|{+}y_0\rangle+n|{-}y_1\rangle)\\
&\quad+(e|0v_0\rangle+f|1v_1\rangle)\otimes(e|0v_0\rangle+f|1v_1\rangle)\otimes(m|{+}y_0\rangle+n|{-}y_1\rangle)]\\
&=\frac{1}{2\sqrt{2}}(c^2a|0z_00z_0+x_0\rangle+dca|1z_10z_0+x_0\rangle+cda|0z_01z_1+x_0\rangle+d^2a|1z_11z_1+x_0\rangle\\
&\quad+c^2b|0z_00z_0-x_1\rangle+dcb|1z_10z_0-x_1\rangle+cdb|0z_01z_1-x_1\rangle+d^2b|1z_11z_1-x_1\rangle\\
&\quad+e^2a|0v_00v_0+x_0\rangle+fea|1v_10v_0+x_0\rangle+efa|0v_01v_1+x_0\rangle+f^2a|1v_11v_1+x_0\rangle\\
&\quad+e^2b|0v_00v_0-x_1\rangle+feb|1v_10v_0-x_1\rangle+efb|0v_01v_1-x_1\rangle+f^2b|1v_11v_1-x_1\rangle\\
&\quad+c^2m|0z_00z_0+y_0\rangle+dcm|1z_10z_0+y_0\rangle+cdm|0z_01z_1+y_0\rangle+d^2m|1z_11z_1+y_0\rangle\\
&\quad+c^2n|0z_00z_0-y_1\rangle+dcn|1z_10z_0-y_1\rangle+cdn|0z_01z_1-y_1\rangle+d^2n|1z_11z_1-y_1\rangle\\
&\quad+e^2m|0v_00v_0+y_0\rangle+fem|1v_10v_0+y_0\rangle+efm|0v_01v_1+y_0\rangle+f^2m|1v_11v_1+y_0\rangle\\
&\quad+e^2n|0v_00v_0-y_1\rangle+fen|1v_10v_0-y_1\rangle+efn|0v_01v_1-y_1\rangle+f^2n|1v_11v_1-y_1\rangle)\,. \qquad (7)
\end{aligned}$$

Obviously, after Bob (Charlie) receives S_2' (S_{3U}') (mixture of S_2 (S_{3U}) and S_T (S_T)), Bob (Charlie) extracts S_T and performs three single-qubit measurements $Z_1Z_2X_3$ on S_T. The probability without an eavesdropper is:

$$\begin{aligned}
p(|\psi_E\rangle) = \frac{1}{8}&(|c^2a|^2+|e^2a|^2+|c^2m|^2+|e^2m|^2+|d^2a|^2+|f^2a|^2+|d^2m|^2+|f^2m|^2\\
&+|c^2b|^2+|e^2b|^2+|c^2n|^2+|e^2n|^2+|d^2b|^2+|f^2b|^2+|d^2n|^2+|f^2n|^2)\,. \qquad (8)
\end{aligned}$$

Suppose $a^2=m^2=c^2=e^2=s$, $b^2=n^2=d^2=f^2=t$, then

$$p(|\psi_E\rangle)=\frac{1}{2}(s^3+t^2s+s^2t+t^3)\,. \qquad (9)$$

Because $a^2+b^2=1$, $m^2+n^2=1$, $c^2+d^2=1$, and $e^2+f^2=1$, $p(|\psi_E\rangle)=(1/2)\,(2s^2-2s+1)$ can be obtained. Therefore, the error rate of each qubit because of eavesdropping is:

$$\sigma = 1-p(|\psi_E\rangle) = 1-s^2+s-\frac{1}{2}\,, \qquad (10)$$

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

$$d_{\mathrm{low}} = 1-p(|\psi_E\rangle) = 1-s^2+s-\frac{1}{2}\,. \qquad (11)$$

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

$$I_1 = -s\log_2 s - (1-s)\log_2(1-s) = H(s)\,, \qquad (12)$$

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

$$I_2 = -t\log_2 t - (1-t)\log_2(1-t) = H(t)\,. \qquad (13)$$

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

$$I = \frac{1}{2}(I_1 + I_2) = \frac{1}{2}[H(s) + H(t)] = H(s)\,. \qquad (14)$$

According to formula (11) and formula (14), we calculate that, when $I = 1$, $d_{\rm low} = 0.75$ is obtained. Also $\sigma = 0.75$ can be obtained.

That is, the detection rate is more than 75 %, when Eve eavesdrops on the information contained in a qubit. Compared with Ref. [49], a novel detection strategy based on Bell states, in which the detection rate reaches 50 %, our detection rate has raised 25 %.

3.2 *Receiver Attack*

As a receiver, Bob cannot read out secret message without Charlie's permission. If Charlie does not allow Bob to obtain secret message, he will not publish C_{3U}. Without C_{3U}, Bob can not recover C_3. Then, he does not know what he should do to decrypt C (performing XOR with C_2 or with $\bar{C}_2$). Therefore, he cannot get secret message.

3.3 *Controller Attack*

As a controller, Charlie cannot get any secret message. Before Alice sends S_3 sequence to Charlie, Alice performs operations I or U on photon 3 according to ID_B. Because Charlie does not know ID_B, he cannot get the right C_3 by performing X-basis measurement on photons in S_{3U}. Therefore, he cannot deduce the right relationship between the one-to-one bits of C_1 and C_2. When Alice publishes C (M_1 XOR C_1), he cannot get M_1 through C and C_2.

3.4 *External Eavesdropper Attack*

As an external eavesdropper, Eve cannot get secret message. In the process of information transmission, Alice measures photons in S_1 with X-basis in order and constructs an ordered classical numbers sequence C_1. According to the uncertainty principle of quantum, C_1 is a real random number, which is used as a one-time-pad to encrypt secret message by using XOR operation. C_1 is not known by anybody except Alice, and it also cannot be deduced by using any classical information already published without the cooperation of Bob and Charlie, which ensures the security of the protocol.

In intercept-resend attack, when Alice sends particles to Bob, Eve intercepts some particles; Eve measures these particles and resends them to Bob. Eve intents to obtain some information by performing intercept-resend attack. In this protocol, if Eve has intercepted some particles, Eve has a 25% chance to guess right the intercepted particle is not decoy particle and a 75 % chance to guess wrong. If Eve guesses wrong, she cannot obtain any secret message contained in one 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. However, because Eve does not know ID_B, when Charlie publishes C_{3U}, Eve can not recover C_3. Therefore, Eve does not know what he should do to decrypt C. Eve has a 50% chance to guess right the bit value of C_3, therefore, in this case, Eve has a 6.3 % (25 % ×50 %×50 %) chance to know the secret.

3.5 *The Security of ID_B*

ID_B is shared by Alice and Bob previously. They can be shared by executing QKD protocol; therefore the QKD protocol can guarantee the security of ID_B in the process of quantum key distribution. In the process of secret transmission in our protocol, ID_B will not be delivered in classical channel in any form; they will be transmitted unconditional secure in quantum form under the protection of quantum mechanics. Therefore, in the process of secret transmission, ID_B will be safe. The only unsafe factor is the improper storage of Alice and Bob. Thus, without considering the unsafe factor of improper storage, ID_B can be reused unconditional safe.

3.6 *The Influence of Noise*

Obviously, our protocol is secure in ideal cases. However, noises might appear in all of quantum preparation setups, quantum channel and measurement equipments. Therefore, to protect our protocol from noise, we can add the process of error-correcting code (ECC) in our protocol. Alice and Bob can select an $[s, n]$ error-correcting code[50] which uses s bits codeword to encode n bits word using generator matrix $G(x^n)$ and can correct t codeword error bits with the error-correcting function $D(y^s)$.

4 Conclusion

In summary, the different CDSQC protocol based on three-particle GHZ state and quantum one-time-pad is secure in both ideal cases and noisy cases. Charlie, as the controller, decides whether Bob, the receiver, can read out the secret message by using photon 3 in each three-particle GHZ state in X-basis as his permission. But Charlie cannot get the secret message under any circumstances, because before Alice sends photon 3 to Charlie, she performs the unitary operation $I(U)$ on photon 3 according to ID_B, while ID_B is secret to Charlie. The classical XOR operation serving as a one-time-pad is used to forbid external eavesdroppers and Charlie to eavesdrop. The three-particle GHZ state in X-basis is used as decoy photons

to detect eavesdropping. The detection rate reaches 75% under the condition of full information in one qubit leaked out. If the eavesdropper performs intercept-resend attack, he only has 6.3 % chances to know the secret.

References

[1] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York (1984) 175.

[2] A.K. Ekert, Phys. Rev. Lett. **67** (1991) 661.

[3] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68** (1992) 557.

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

[5] F.G. Deng and G.L. Long, Phys. Rev. A **70** (2004) 012311.

[6] W.Y. Hwang, Phys. Rev. Lett. **91** (2003) 057901.

[7] X.H. Li, F.G. Deng, and H.Y. Zhou, Phys. Rev. A **78** (2008) 022321.

[8] G.L. Long and X.S. Liu, Phys. Rev. A **65** (2002) 032302.

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

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

[11] C. Wang, *et al.*, Phys. Rev. A **71** (2005) 044305.

[12] C. Wang, *et al.*, Opt. Commun. **253** (2005) 15.

[13] X.H. Li, *et al.*, Chin. Phys. **16** (2007) 2149.

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

[15] B. Gu, *et al.*, Sci. China Phys. Mech. Astron. **54** (2011) 942.

[16] B. Gu, *et al.*, Chin. Phys. B **20** (2011) 100309.

[17] D. Liu, J.L. Chen, and W. Jiang, Int. J. Theor. Phys. **51** (2012) 2923.

[18] Z.W. Sun, R.G. Du, and D.Y. Long, Int. J. Theor. Phys. **51** (2012) 1946.

[19] B.C. Ren, *et al.*, Eur. Phys. J. D **67** (2013) 30.

[20] B. Gu, *et al.*, Int. J. Theor. Phys. **52** (2013) 4461.

[21] Q.N. Zhang, C.C. Li, Y.H. Li, and Y.Y. Nie, Int. J. Theor. Phys. **52** (2013) 22.

[22] Y. Chang, C.X. Xu, S.B. Zhang, and L.L. Yan, Chin. Sci. Bull. **58** (2013) 4571.

[23] Y. Chang, C.X. Xu, S.B. Zhang, *et al.*, Chin. Phys. B **23** (2014) 010305.

[24] Y. Chang, S.B. Zhang, L.L. Yan, *et al.*, Chin. Sci. Bull. **59** (2014) 2835.

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

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

[27] J.S. Shaari, M. Lucamarini, and M.R.B. Wahiddin, Phys. Lett. A **358** (2006) 85.

[28] X.H. Li, F.G. Deng, and C.Y. Li, J. Korean Phys. Soc. **49** (2006) 1354.

[29] Z.X. Man, Y.J. Xia, and Z.J. Zhang, Int. J. Quantum Inf. **4** (2006) 739.

[30] W. Huang, Q.Y. Wen, B. Liu, F. Gao, and H. Chen, Int. J. Theor. Phys. **51** (2012) 2787.

[31] Z.X. Man and Y.J. Xia, Chin. Phys. Lett. **23** (2006) 1680.

[32] Z.H. Liu and H.W. Chen, Chin. Phys. Lett. **30** (2013) 079901.

[33] T.Y. Ye and L.Z. Jiang, Chin. Phys. Lett. **30** (2013) 040305.

[34] J. Wang, Q. Zhang, and C.J. Tang, Opt. Commun. **266** (2006) 732.

[35] F. Gao, S.J. Qin, Q.Y. Wen, and F.C. Zhu, Opt. Commun. **283** (2010) 192.

[36] S.H. Kao, C.W. Tsai, and T. Hwang, Commun. Theor. Phys. **55** (2011) 1007.

[37] J. Dong, J.F. Teng, and S.Y. Wang, Int. Inf. Tech. Appl. **3** (2008) 551.

[38] L. Dong, X.M. Xiu, Y.J. Gao, Y.P. Ren, and H.W. Liu, Opt. Commun. **284** (2011) 905.

[39] Y.H. Li, X.L. Li and Y.Y. Nie, Int. J. Theor. Phys. **52** (2013) 2395.

[40] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390** (1997) 575.

[41] G. Vernam, J. Am. Inst. Electr. Eng. **55** (1926) 109.

[42] C.E. Shannon, Bell Syst. Tech. J. **28** (1949) 656.

[43] D.W. Leung, Quantum. Inf. Comput. **2** (2002) 14.

[44] G.H. Zeng, Quantum Private Communication, Higher Education Press, Beijing (2009) 139.

[45] G.L. Long and X.S. Liu, Phys. Rev. A **65** (2002) 032302.

[46] C.Y. Li, *et al.*, Chin. Phys. Lett. **22** (2005) 1049.

[47] C.Y. Li, *et al.*, Chin. Phys. Lett. **23** (2006) 2896.

[48] F.G. Deng, G.L. Long, Y. Wang, *et al.*, Chin. Phys. Lett. **21** (2004) 2097

[49] F. Gao, F.Z. Guo, Q.Y. Wen, *et al.*, Sci. China. Ser. G-Phys. Mech. Astron. **39** (2009) 161.

[50] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Lib, New York (1977).