International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.131-140
http://dx.doi.org/10.14257/ijsia.2015.9.9.12

Faithful Quantum Secure Communication with Authentication based on Bell States and Classical XOR Resisting Collective Noise

Tao Fang[1] and Min Li [2]

[1]*College of Fundamental Education Sichuan Normal University, Chengdu, China*
[2] *College of Computer Science, Sichuan Normal University, Chengdu, China*
**Corresponding author: lm_turnip@126.com*

Abstract

Two faithful quantum secure communication and authentication schemes based on Bell states and classical XOR operation are proposed, which withstand collective noises. The authentication and eavesdropping detection are completed by using logical decoy photons generating by previously shared identity string. The logical decoy photons are decoherence-free states over the two collective noisy channels respectively. The transmission of secret message is a one-time pad system, which guarantees the absolute security of secret message. Encoding secret message after particle transmission ensures the accuracy of secret message.

Keywords: *quantum secure direct communication; collective-dephasing noise; collective-rotation noise; authentication*

1. Introduction

Quantum key distribution (QKD) [1-3] and quantum secure direct communication (QSDC) [4-12] are the two most important fields of research in quantum communication. The first QKD scheme, also called the famous BB84 protocol, was proposed by Bennett *et al.* in 1984.[1] In 2000, the first QSDC protocol is developed by Long et al., which is essentially a QKD scheme too [4]. After that, many scholars focused on these two fields (QKD and QSDC). In 1992, Bennett proposed a simplified QKD scheme [2]. The scheme utilizes non-orthogonal polarization single photons as quantum carriers [2]. In 2003, another QKD protocol was put forward by Deng and Long. [3] The QKD protocol [3] utilizes order rearrangement of particles to ensure the security of information. In 2004, Deng proposed a QSDC protocol based on quantum one-time pad. [5] In this protocol [5], single photons are the carriers. In 2008, Gao analyzed the ping-pong protocol, he used Bell states as decoy photons which improved the security [6]. After that, Li Jian utilized respectively GHZ states[7] and other cluster states[8,9] as decoy photons to improve detection rate in QKD or QSDC protocols. In 2011, Wang T J developed a high-capacity QSDC protocol based on entanglement states in multiple degrees of freedom [10]. All there protocols are based on an assumption, that is, the quantum channel is noise free. However, in quantum channel, the noises are inevitable, because birefringence of photons fluctuate temporally. Photons transmitting in quantum channel will suffer from noise inevitably. Therefore, the study of QKD or QSDC protocols resisting noises appears particularly important.

In general, we suppose the noises in quantum channel are mainly the collective noises, which fluctuate slowly in time. The changes caused by collective noises on all qubits are the same, when several photons are sent at a time in a noisy channel, or they are as near as possible. The collective noises include noises with collective-dephasing characteristic or collective-rotation characteristic. Usually, when

ISSN: 1738-9976 IJSIA

transmitting through collective-dephasing noisy channel, a photon in state $|0\rangle$ will remain unchanged, while $|1\rangle$ will become $e^{i\theta}|1\rangle$; similarly, when transmitting through collective-rotation noisy channel, a photon in state $|0\rangle$ ($|1\rangle$) will become $\cos\theta|0\rangle+\sin\theta|1\rangle$ ($-\sin\theta|0\rangle+\cos\theta|1\rangle$). For these noises, the usual practice is to eliminate or decrease the noise effect. Decoherence free subspace (DFS) [13, 14] is one of the most effective techniques. Usually, several qubits meeting with the same noise can form DFS by making up the influence of channel noise. These qubits in the DFS remain unchanged even encountering with noises [17], which increases the robustness of quantum communication. [17]. In 2004, a robust QKD scheme was proposed by Boileau *et al.*, which resisted collective noise with random unitary [13-14]. Ge *et al.* put forward a fault tolerant QSDC schema against collective-dephasing noises, in which DFS unaffected by collective-dephasing noises is used.[15] After that, Li X H et al. respectively proposed robust QKD protocol [16] and fault tolerant dense-coding QKD protocol [17] over collective noisy channel. In 2011, YANG C W *et al.* developed two two-step QSDC schemes robust over collective-rotation noisy channel and collective-dephasing noisy channel respectively [18]. In 2012, Huang W et al. also put forward two fault tolerant QSDC schemes by using decoherence-free states over the two collective noisy channels respectively [19].

In this study, two fault-tolerate quantum direct communication protocols with authentication respectively resisting collective-dephasing noise and collective-rotation noise are proposed. Two users verify their identities each other before they transmit secret message. The authentication is implemented by using previously shared reusable identity string. The identity string is encoded as decoherence-free states over the two collective noisy channels respectively, and is used as decoy photons. Bell state ϕ^+ in DFS is used as information carrier, based on which one-time pad system is implemented. After confirming successful transmission of particles, secret message is encoded on successfully transmitted particles, which ensures the accuracy of secret message. σ_Z and σ_X basis measurement in DFS is required, and logical Bell states measurement in DFS is not needed. Unitary operations in DFS are not used.

2. Description of Protocol

2.1. QSDC Scheme with Authentication against a Collective-dephasing Noise

Usually, when encountering with collective-dephasing noise, a photon will change its state according to the rule that $|0\rangle$ remains unchanged and $|1\rangle$ changes into $e^{i\phi}|1\rangle$, where $|\phi\rangle$ denotes a noise parameter fluctuating temporally. Thereby, we can represent a collective-dephasing noise as EQ. (1). This is like that in Ref [17].

$$P_{\mathrm{d}}|0\rangle=|0\rangle,\quad P_{\mathrm{d}}|1\rangle=e^{i\phi}|1\rangle \tag{1}$$

Because two physical qubits with anti-parallel parity obtain the same phase factor $\mathrm{i}\phi$, to defend against collective-dephasing noise, two anti-parallel qubits can form a logical qubit. The logical qubits are described as EQ. (2).

$$|0\rangle_L\equiv|0\rangle|1\rangle,\quad |1\rangle_L\equiv|1\rangle|0\rangle \tag{2}$$

Therefore, we can express an entangled logical state for Bell state $\phi^+=1/\sqrt{2}(|00\rangle+|11\rangle)$ as EQ. (3), which withstands a collective-dephasing noise.

$$\left|\phi_d^+\right\rangle_{XY} = \frac{1}{\sqrt{2}}(\left|0\right\rangle_X \left|01\right\rangle_{Y1Y2} + \left|1\right\rangle_X \left|10\right\rangle_{Y1Y2}) \quad (3)$$

Y_1 and Y_2 are physical qubits. Y is the logical qubit, which is made up of Y_1 and Y_2.

Now let us briefly describe our fault tolerate quantum direct communication with authentication against collective-dephasing noise. On assumption that, the sender, Alice transmits her secret message to Bob, the receiver. ID is a secret binary string, representing the identities of Alice and Bob, and being secret to others. Alice and Bob share ID in advance. If an orderly classical "0" or "1" numbers is used to denote the secret message, Alice can divide the secret into several parts. If each part includes *n*–bit binary-string, we can denote the first *n*–bit part as $M(m_1,m_2,\ldots,m_n)$.

(1) Alice prepares an orderly qubit sequence in state $\left|\phi_d^+\right\rangle_{XY}$. The sequence is divides into S_X and S_Y. All the qubits X in $\left|\phi_d^+\right\rangle_{XY}$ constitute S_X. And all the qubits Y (Y_1 and Y_2) consists of S_Y. This is very similar to Ref.[4].

(2) Alice prepares another orderly qubits sequence S_T in basis σ_Z or σ_X, where σ_Z basis is represented by EQ. (1), and σ_X can be described as EQ. (4):

$$\left|+\right\rangle_L = \frac{1}{\sqrt{2}}(\left|0\right\rangle_L + \left|1\right\rangle_L), \quad \left|-\right\rangle_L = \frac{1}{\sqrt{2}}(\left|0\right\rangle_L - \left|1\right\rangle_L) \quad (4)$$

Here, σ_Z and σ_X are two non-orthogonal bases. S_T is generated according to the rule: a qubit is randomly prepared by using the σ_Z basis, when a destination bit of ID is 0, that is, the qubit might be in $\left|0\right\rangle_L$ or $\left|1\right\rangle_L$; or else, in σ_X basis, in this case, the qubit in $\left|+\right\rangle_L$ or $\left|-\right\rangle_L$.Similar to Ref.[21], S_T will be used as a decoy sequence mixed into sequence S_Y according to the rule: when the *i*-th bit of ID is 0, the *i*-th photon of S_T is inserted before the ith photon of S_Y; or else, behind the *i*-th photon of S_Y. Then, Alice sends the sequence S_I (mixture of S_T and S_Y) to Bob.

(3) After Bob received S_I, he extracts S_T according to ID and measures photons in S_T with basis dominated by ID. After measurement, Bob will obtain two binary number sequences ID_1 and ID_2 on the basis of Rule 1 and Rule 2 respectively.

Rule 1: If the photon measured is in $\left|0\right\rangle_L$ or $\left|1\right\rangle_L$ state, the corresponding bit of ID_1 is denoted as 0; or else, the bit is denoted as 1.

Rule 2: If the photons measured is in state $\left|0\right\rangle_L$ or $\left|+\right\rangle_L$, the corresponding bit of ID_2 is denoted as 0; or else, the bit is denoted as 1.

Bob first compares ID_1 with ID; in the ideal cases, ID_1 should be equal to ID; however, in practical cases, ID_1 may not be completely identical with ID; therefore, if Bob obtains low error rate, Alice is accepted as authentic and eavesdroppers don't exist, then he publishes ID_2; otherwise, he stops the communication.

(4) After Bob publishes ID_2, Alice compares ID_2 with the initial state of S_T according to Rule 3.

Rule 3: If the photon in S_T is in state $\left|0\right\rangle_L$ or $\left|+\right\rangle_L$, the corresponding bit of ID_3 is denoted as 0; or else, the bit is denoted as 1.It is very similar with method in Ref.[22].

If ID_2 is equal to ID_3, Alice thinks Bob is legal. So far, the two users, Alice and Bob have finished the identity authentication. The communication goes on. If ID_2 is not equal to ID_3, Alice stops the communication.

(5)If Bob considers particle Y_1 as a controller of a controlled-NOT (CNOT) operation, and Y_2 as a target, after performing CNOT Y_1Y_2, he will obtain a new state:

$$\left|\gamma_d\right\rangle_{XY}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_X\left|01\right\rangle_{Y1Y2}+\left|1\right\rangle_X\left|11\right\rangle_{Y1Y2})=\frac{1}{\sqrt{2}}(\left|0\right\rangle_X\left|0\right\rangle_{Y1}+\left|1\right\rangle_X\left|1\right\rangle_{Y1})\left|1\right\rangle_{Y2} \quad (5).$$

This is very similar with method in Ref. [19].

(6)Bob obtains a random binary number C_{Y1} by measuring photons Y_1 in S_Y with the basis σ_Z. Alice discards the one-to-one matching photons in S_X, after Bob publishes the positions where he lost photons.

(7) Similar to the delayed measurement technique in Ref. [20], the remaining photons in S_X are measured with the σ_Z basis. After measurement, Alice will obtain a random binary number C_X, which is identical with C_{Y1} in theory. By performing M XOR C_X operation, Alice gets encrypted secret message C= M XOR C_X. Then, Alice publishes C. It is very similar with method in Refs. [7, 9, 11-12].

(8) Because C_X is equal to C_{Y1}, Bob can get secret message M by decrypting C with C_{Y1} (M =C XOR C_{Y1}).

2.2. QSDC Scheme with Authentication against a Collective-rotation Noise

Usually, when suffering from collective-rotation noise, a photon will change its state according to the rule that $\left|0\right\rangle$ ($\left|1\right\rangle$) changes into $f\left|0\right\rangle+g\left|1\right\rangle$ ($-g\theta\left|0\right\rangle+f\left|1\right\rangle$), where $f=\cos\theta$, $g=\sin\theta$, and θ is a parameter fluctuating with time and relying on the noise. Therefore a collective- rotation noise is represented as EQ. (6). It is very similar to that in Ref [17].

$$P_r\left|0\right\rangle=f\left|0\right\rangle+g\left|1\right\rangle$$
$$P_r\left|1\right\rangle=-g\left|0\right\rangle+f\left|1\right\rangle$$
$$f=\cos\theta,\ g=\sin\theta \quad (6)$$

Here, for collective-rotation noise, $\left|\phi^+\right\rangle$ and $\left|\psi^-\right\rangle$ are invariant. Therefore, logical qubits are described as:

$$\left|0\right\rangle_L\equiv\left|\phi^+\right\rangle,\quad \left|1\right\rangle_L\equiv\left|\psi^-\right\rangle \quad (7)$$

Then, we can denote an entangled logical state for Bell state $\phi^+=1/\sqrt{2}(\left|00\right\rangle+\left|11\right\rangle)$ as EQ. (8), which withstands a collective-rotation noise.

$$\left|\phi_r^+\right\rangle_{XY}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_X\left|\phi^+\right\rangle_{Y1Y2}+\left|1\right\rangle_X\left|\psi^-\right\rangle_{Y1Y2})$$

$$=\frac{1}{2}[\left|0\right\rangle_X(\left|00\right\rangle_{Y1Y2}+\left|11\right\rangle_{Y1Y2})+\left|1\right\rangle_X(\left|01\right\rangle_{Y1Y2}-\left|10\right\rangle_{Y1Y2})] \quad (8)$$

The fault tolerate schema with authentication against collective-rotation noise is very similar with the schema against collective-dephasing noise.

(1) Alice prepares an orderly qubit sequence in $\left|\phi_r^+\right\rangle_{XY}$ state. The sequence is divides into S_X and S_Y. Here, all the qubits Y (Y_1 and Y_2) consists of S_Y.

(2) Alice prepares another orderly qubits sequence S_T in basis σ_Z or σ_X, where σ_Z basis is represented as ($\left|0\right\rangle_L,\left|1\right\rangle_L$) = ($\left|\phi^+\right\rangle,\left|\psi^-\right\rangle$), and σ_X as ($\left|+\right\rangle_L,\left|-\right\rangle_L$) = ($\frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle+\left|\psi^-\right\rangle)$, $\frac{1}{\sqrt{2}}(\left|\phi^+\right\rangle-\left|\psi^-\right\rangle)$). σ_Z and σ_X are two non-orthogonal bases. S_T is generated according to the rule: a qubit is randomly prepared by using the σ_Z basis, when a destination bit of ID is 0; or else, in σ_X basis. S_T will be used as a

decoy sequence mixed into sequence S_Y, the rule is similar with that in step (2) in scheme against collective-dephasing noise. Then, Alice sends the sequence S_I (mixture of S_T and S_Y) to Bob.

(3) After Bob received S_I, he extracts S_T according to ID and measures photons in S_T with basis dominated by ID. After measurement, Bob will obtain two binary number sequences ID_1 and ID_2 according to Rule 1 and Rule 2 respectively.

Bob first compares ID_1 with ID; if Bob obtains low error rate, Alice is accepted as authentic and eavesdroppers don't exist, then he publishes ID_2; otherwise, he stops the communication.

(4) After Bob publishes ID_2, Alice compares ID_2 with the initial state of S_T according to Rule 3.If ID_2 is equal to ID_3, Alice thinks Bob is legal. So far, the two users, Alice and Bob have finished the identity authentication. The communication goes on. If ID_2 is not equal to ID_3, Alice stops the communication.

(5) For each $\left|\phi_r^+\right\rangle_{XY}$ state, Bob performs operation $S \otimes S \otimes S$ first, and then $H \otimes H \otimes H$. He will obtain a new state:

$$\left|\vartheta_r\right\rangle_{XY} = \frac{1}{\sqrt{2}}(\left|1\right\rangle_X \left|10\right\rangle_{Y1Y2} + \left|0\right\rangle_X \left|01\right\rangle_{Y1Y2}) \tag{9}$$

The phase gate S and Hadamard gate H are represented as EQ. (10)

$$\mathrm{S}=\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad \mathrm{H}=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{10}$$

If Bob considers particle Y_1 as a controller of a controlled-NOT (CNOT) operation, and Y_2 as a target, after performing CNOT Y_1Y_2, he will obtain another new state:

$$\left|\xi_r\right\rangle_{XY} = \frac{1}{\sqrt{2}}(\left|0\right\rangle_X \left|0\right\rangle_{Y1} + \left|1\right\rangle_X \left|1\right\rangle_{Y1})\left|1\right\rangle_{Y2} \tag{11}$$

It is very similar with method in Ref. [19].

(6) Bob obtains a random binary number C_{Y1} by measuring photons Y_1 in S_Y with basis σ_Z. Alice discards the one-to-one matching photons in S_X, after Bob publishes the positions where he lost photons.

(7)Alice measures photons in S_X with basis σ_Z. After measurement, she will obtain a random binary number C_X. By performing M XOR C_X operation, Alice gets encrypted secret message C= M XOR C_X. Then, Alice publishes C.

(8) Because C_X is equal to C_{Y1}, Bob can get secret message M by decrypting C with C_{Y1} (M =C XOR C_{Y1}).

3. Analysis

3.1. Correct Analysis

A. Protocol against Collective-dephasing Noise

Prerequisites: Alice and Bob share ID. Alice's secret message is a series of classical 0 or 1 numbers in order, called M. M is divided into several parts called M_i.

In step 2, Alice prepares decoy sequence S_T according to ID:

Alice: Prepare (S_T, ID)

Alice: S_I= Z (S_Y, S_T, ID)

, where Z denotes inserts S_T to S_Y according to ID.

Then Alice sends S_B' to Bob.

Alice→ Bob: S_I

Bob: $S_Y = Z^{-1}(S_I, S_T, ID)$

, where Z^{-1} denotes extracting S_T from S_I according to ID.

Bob: ID_1=M (S_T, Rule1)

Bob: ID_2=M (S_T, Rule2)

, where M (S_T, Rule1) and M (S_T, Rule2) denote measuring S_T with bases Z= $\{|0\rangle, |1\rangle\}$according to Rule1 and Rule2 respectively.

Bob: R_1=COMP(ID, ID_1)

If the result R_1 is true, Alice is accepted as authentic and eavesdroppers don't exist.

Bob: Publish (ID_2)

Because ID_2 doesn't contain basis information of ID, the publishing of ID_2 will not lead to the leakage of ID.

Alice acts Rule3 on S_T and obtains ID_3:

Alice: ID_3= Rule3 (S_T)

Alice: R_2=COMP (ID_2, ID_3)

If the result $R_2$is true, Bob is accepted as authentic and eavesdroppers don't exist.

Here, the mutually authenticate between Alice and Bob is finished.

Bob: *CNOT* (Y_1,Y_2)

Bob: C_{Y1} = Ms(S_{Y1})

Alice: C_X = Ms(S_X)

, where Ms(S_{Y1}) denotes measuring photon Y_1 in S_{Y1} with *Z*-basis $\{|0\rangle, |1\rangle\}$ in order.

Alice: C= C_X XOR M_1

Alice publishes C. Because C_A is a random number, the publishing of C is safe. According to the state:

$$|\gamma_d\rangle_{XY} = \frac{1}{\sqrt{2}}(|0\rangle_X |0\rangle_{Y1} + |1\rangle_X |1\rangle_{Y1})|1\rangle_{Y2}$$

, we know:

C_X= C_{Y1}

Bob: M_1= *C* XOR C_{Y1}

Here, M_1 is transmitted securely. The transmission of M_2 and M_i is similar to the transmission of M_1. In the whole process, ID is reused. However the reuse of ID will not lead to message leak out, the reason will be analyzed in security analysis.

Obviously, the protocol is correct in ideal scenario.

B. Protocol against Collective-rotation Noise

Prerequisites: Alice and Bob share ID. Alice's secret message is a series of classical 0 or 1 numbers in order, called *M*. *M* is divided into several parts called M_i.

In step 2, Alice prepares decoy sequence S_T according to ID:

Alice: Prepare (S_T, ID)

Alice: S_I= Z (S_Y, S_T, ID)

, where Z denotes inserts S_T to S_Y according to ID.

Then Alice sends S_B' to Bob.

Alice→ Bob: S_I

Bob: $S_Y = Z^{-1}(S_I, S_T, ID)$

, where Z^{-1} denotes extracting S_T from S_I according to ID.

Bob: ID_1=M (S_T, Rule1)

Bob: ID_2=M (S_T, Rule2)

, where M (S_T, Rule1) and M (S_T, Rule2) denote measuring S_T with bases Z= $\{|0\rangle, |1\rangle\}$according to Rule1 and Rule2 respectively.

Bob: R_1=COMP(ID, ID_1)

If the result R_1 is true, Alice is accepted as authentic and eavesdroppers don't exist.

Bob: Publish (ID_2)

Because ID_2 doesn't contain basis information of ID, the publishing of ID_2 will not lead to the leakage of ID.

Alice acts Rule3 on S_T and obtains ID_3:

Alice: ID_3= Rule3 (S_T)

Alice: R_2=COMP (ID_2, ID_3)

If the result $R_2$is true, Bob is accepted as authentic and eavesdroppers don't exist.

Here, the mutually authenticate between Alice and Bob is finished.

Alice: H(S (X))

Bob: H(S (Y_1,Y_2))

Bob: *CNOT* (Y_1,Y_2)

Bob: C_{Y1} = Ms(S_{Y1})

Alice: C_X = Ms(S_X)

, where H(S (X)) denotes Alice performs operation S first and then H operation on particle X in S_X; H(S (Y_1,Y_2)) denotes Bob performs operation S first and then H operation on particle Y_1 and Y_2 in S_Y. Here, S=$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, H=$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Ms($S_{Y1}$) denotes measuring photon Y_1 in S_{Y1} with Z-basis $\{|0\rangle, |1\rangle\}$ in order.

Alice: C= C_X XOR M_1

Alice publishes C. Because C_A is a random number, the publishing of C is safe.

According to the state:

$$|\xi_r\rangle_{XY} = \frac{1}{\sqrt{2}}(|0\rangle_X |0\rangle_{Y1} + |1\rangle_X |1\rangle_{Y1})|1\rangle_{Y2}$$

, we know:

C_X= C_{Y1}

Bob: M_1= C XOR C_{Y1}

Obviously, the protocol is correct in ideal scenario.

3.2. Security Analysis

In Ref. [17], sequence S_Y is first transmitted to Bob, and then Bob encodes on it and sends it to Alice. During this process, to ensure the security of data, two eavesdropping detections are needed. Furthermore, if some photons in encoded S_Y are missing when they are sent to Alice, the secret message Alice received will be inaccurate. In our study, S_Y is first transmitted to Bob. Then, Bob performs controlled-NOT operation on photons Y_1 and Y_2, the state of ϕ^+ will be reconstructed on physical qubits X and Y_1. If Alice performs σ_Z basis measurement over collective-dephasing noise environment or collective-rotation noise environment on particle X, she will obtain a random binary sequence. Using this random binary sequence as a random key to encrypt secret message, the protocol can be regarded as a one-time pad system. If Bob performs σ_Z basis measurement over collective-dephasing noise environment or collective-rotation noise environment on particle Y_1, he will obtain an identical random binary sequence with Alice in ideal cases, so that he can decrypt the secret message. During this process, particles are transmitted once, and the secret message is encoded after particles transmission, and then is published. Therefore, the secret message received in this protocol might be more accurate theoretically.

In this study, the secret message is transmitted by using initially Bell state $\phi^+ = 1/\sqrt{2}(|00\rangle + |11\rangle)$. To send particle Y to Bob unaffected by noise, logical qubits composed of Y_1 and Y_2 against collective noise with dephasing or rotation characteristics are transmitted in quantum channel. After successful transmission, performing controlled-NOT operation on particles Y_1 and Y_2 will recover ϕ^+ on particles X and Y_1. In theory, particle Y in $\phi^+ = 1/\sqrt{2}(|00\rangle + |11\rangle)$ state is distributed successfully without being affected by noise, which ensures the accuracy of the information transmitted.

Eavesdropping detection with identity authentication and one-time-pad guarantees the security of the protocol. In the process of eavesdropping detection, decoy photons are produced based on the previously shared identity string and inserted into sequence S_Y, the positions inserted are agreed in advance, however dominated by identity string. Without the identity string, even if the eavesdroppers have found the agreement, they can not get the positions of decoy photons; therefore they cannot implement specific attacks. By comparing ID and ID_1, Bob confirms the legality of Alice, if Eve impersonates Alice, then Bob cannot get the same or approximately the same ID and ID_1. By comparing ID_2 (Bob published) and ID3 (the initial state of S_T), Alice confirms the legality of Bob. However, the publication of ID_2 will not cause leakage of ID, because ID_2 doesn't include basis information of S_T. The final key used to encrypt secret message is a random binary sequence, by using XOR operation, the protocol implements one-time-pad system, which implements absolute security.

4. Conclusion

In summary, two fault tolerant QSDC schemes with authentication resisting two kinds of collective noise respectively are put forward. Identity string is encoded as decoherence-free states over the two collective noisy channels respectively, which is used as decoy photons, not only verifies the identities of two users, but also implements eavesdropping detection. The transmission of secret message is a one-time pad system, which guarantees the absolute security of secret message. Encoding secret message after particle transmission ensures the accuracy of secret message.

Acknowledgements

This work was supported by Sichuan Department of Education (Grant No.13ZB0152).

References

[1] C H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: IEEE, (**1984**), pp. 175-179.
[2] C H. Bennett, "Quantum cryptography using any two nonorthgonal states", Phys Rev Lett, vol. 68, (**1992**), pp. 3121–3124.
[3] F G. Deng and G L. Long, "Controlled order rearrangement encryption for quantum key distribution", Phys. Rev. A, vol. 68, (**2003**), 042315.
[4] G L. Long and X S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme", Phys. Rev. A, vol. 65, (**2002**), pp. 032302.
[5] F G. Deng and G L. Long, "Secure direct communication with a quantum one-time pad", Phys Rev A, vol. 69, no. 5, (**2004**), 052319.
[6] F. Gao, F Z. Guo, Q Y. Wen and F C. Zhu, "Comparing the efficiencies of different detect strategies in the ping-pong protocol", Sci. Chin.Ser. G-Phys. Mech. Astron., vol. 51, (**2008**), pp. 1853-1860.
[7] J. Li, H F. Jin and B. Jing, "Improved quantum "Ping-pong" protocol based on GHZ state and classical XOR operation", Sci. Chin. Phys. Mech. Astron, vol. 54, (**2011**), pp. 1612-1618.
[8] J. Li, H F. Jin and B. Jing, "Improved eavesdropping detection strategy based on four-particle cluster state in quantum direct communication protocol", Chin. Sci. Bull., vol. 57, (**2012**), pp. 4434-4441.

[9] J. Li, D J. Song, X J. Guo and B. Jing, "A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation", Chin. Phys. C, vol. 36, (**2012**), pp. 31-36.
[10] T J. Wang, T. Li, F F. Du and F G. Deng, "High-Capacity Quantum Secure Direct Communication Based on Quantum Hyperdense Coding with Hyperentanglement", Chin. Phys. Lett., vol. 28, (**2011**), pp. 040305.
[11] Y. Chang, S.-B. Zhang and L.-L. Yan, «A Multiparty Controlled Bidirectional Quantum Secure Direct Communication and Authentication Protocol Based on EPR Pairs", Chin. Phys. Lett., vol. 30, (**2013**), 060301.
[12] Y. Chang, S.-B. Zhang and L.-L. Yan, «A Bidirectional Quantum Secure Direct Communication Protocol Based on Five-Particle Cluster State", Chin. Phys. Lett., vol. 30, (**2013**), pp. 090301.
[13] Z D. Walton, A F. Abouraddy and A V. Sergienko, "Decoherence-free subspaces in quantum key distribution", Phys Rev Lett, vol. 91, (**2003**), pp. 087901.
[14] J C. Boileau, D. Gottesman and R. Laflamme, «Robust polarization-based quantum key distribution over a collective-noise channel", Phys Rev Lett, vol. 92, (**2004**), pp. 017901.
[15] H. Ge and W Y. Liu, "A new quantum secure direct communication protocol using decoherence-free subspace", Chin Phys Lett, vol. 24, (**2007**), pp. 2727–2729.
[16] X H. Li, F G. Deng and H Y. Zhou, "Efficient quantum key distribution over a collective noise channel", Phys Rev A, vol. 78, (**2008**), pp. 022321.
[17] X H. Li, B K. Zhao and Y B. Sheng, «Fault tolerant quantum key distribution based on quantum dense coding with collective noise", Int J Quant Inform, vol. 7, no. 8, (**2009**), pp. 1479–1489.
[18] C W. Yang, C W. Tsai and T. Hwang, "Fault tolerant two-step quantum secure direct communication protocol against collective noises", SCIENCE CHINA Physics, Mechanics & Astronomy, vol. 54, (**2011**), pp. 496-501.
[19] W. Huang, Q Y. Wen, H Y. Jia, S J. Qin and F. Gao, "Fault tolerant quantum secure direct communication ith quantum encryption against collective noise", Chin. Phys. B, vol. 21, (**2012**), pp. 100308.
[20] F G. Deng, G L. Long and Y. Wang, "Increasing the Efficiencies of Random-Choice-Based Quantum Communication Protocols with Delayed Measurement", Chin. Phys. Lett., vol. 21, (**2004**), pp. 2097-2100.
[21] C Y. Li, H Y. Zhou and Y. Wang, "Secure Quantum Key Distribution Network with Bell States and Local Unitary Operations", Chin. Phys. Lett., vol. 22, (**2005**), pp. 1049-1052.
[22] F. Gao, S J. Qin, F Z. Guo and Q Y. Wen, "Cryptanalysis of Quantum Secure Direct Communication and Authentication Scheme via Bell States", Chin. Phys. Lett., vol. 28, (**2011**), pp. 020303.

Authors

Tao Fang, received the M.S. degree from the Sichuan Normal University. Her main research interests include the network secur ity protocol, privacy protection.

Min Li, she received the M.S. degree from the University of Electronic Science and Technology of China (UESTC). Currently she has got Ph.D. degree in computer science at UESTC. Her main research interests include the network security protocol, privacy protection, specifically the location privacy in LBS.