Multiparty Bidirectional Quantum Secure Communication Based on Closed Qubit Transmission

Xunru Yin
Department of Mathematics and Systems Science, Taishan University, Tai'an 271000, China

***Abstract*—A multiparty bidirectional quantum secure communication protocol is proposed with two-photon entanglement and quantum dense coding, in which the qubit transmission forms a closed loop. In this scheme, each user performs the unitary operations according to his secret information to encode the exchanged messages into the particle sequences. Then, each participant can extract the other participants' secret messages by implementing Bell measurements on the encoded particles. Thus all the users realize the direct communication simultaneously. Finally, the security analysis shows that our scheme is secure.**

Keywords-quantum information; quantum cryptography; quantum secure direct communication; bell state.

I. Introduction

Quantum secure direct communication (QSDC) is an important branch of quantum cryptography. It is different from quantum key distribution in which two parties have to distribute a shared secret key before they make a secure session in the quantum channel [1]. However, QSDC can allow the messages to be read out directly when one user sends the encoded particle sequences which contain the secret messages to the other user. The receiver can read out directly the other user's messages without the secret key through the unitary operation.

In 2002, Long et al. [2] proposed a first quantum secret direct communication scheme with EPR pairs. Then Beige et al. [3] proposed a QSDC protocol based on the exchange of single photons. In the same year, Boström et al. [4] proposed a deterministic secure direct communication procotol named 'ping-pong' protocol based on EPR entangled states, which was improved by Li et al. [5]. In 2011, Deng et al. [6] proposed two-step quantum direct communication protocol using the EPR pair block. However, the transmission of secret messages is unidirectional in QSDC. Then Nguyen [7] proposed a kind of protocol called quantum dialogue. Later, Jin et al. [8] proposed a three-party quantum secure direct communication based on the GHZ states, which was improved by Man et al. [9]. Wang et al. [10] proposed a three-party QSDC scheme with EPR pairs, and their protocol was improved on the quantum channels and the efficiency by Chong et al. [11]. Unfortunately, in 2013, Yin et al. [12] pointed out that [10] and [11] can leak out the secret messages of the legitimate users with the classical correlation or information leakage [13, 14].

In this paper, we propose a multiparty QSDC protocol by using the correlation of two-particle EPR pair. All the parties in our scheme are peer entities. Every participant is both a sender and a receiver and forms a return qubit circuit. The transmission direction has the characteristics of unidirectional circulation. One party can obtain the other parties' secret messages through performing the joint measurement on the encoded particles. The rest of our scheme is structured as follows. Section 2 describes the whole protocol in detail. Section 3 analyzes the security of this protocol. Finally, Section 4 gives a conclusion briefly.

II. Description of the present protocol

Two assumptions are given the four Bell states can be written as

$$|\psi^+\rangle = 1/\sqrt{2}(|01\rangle+|10\rangle),$$

$$|\psi^-\rangle = 1/\sqrt{2}(|01\rangle-|10\rangle),$$

$$|\phi^+\rangle = 1/\sqrt{2}(|00\rangle+|11\rangle),$$

$$|\phi^-\rangle = 1/\sqrt{2}(|00\rangle-|11\rangle).$$

Let $|+\rangle = 1/\sqrt{2}(|0\rangle+|1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle-|1\rangle)$, then $|+\rangle$ and $|-\rangle$ are the up and down eigenstates of Pauli operator σ_x. Suppose U_0, U_1, and U_2 are three unitary operations, i.e., $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 \equiv \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, and $U_2 \equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. An EPR pair can been transformed to another EPR pair if we perform two unitary operations chosen from $\{U_0, U_1, U_2\}$ on the two particles. In this paper, we take $|\psi^+\rangle$ as the initial state and the transformation rule can be shown in Table 1. ("O1" denotes the operation on the particle 1; "O2" denotes the operation on the particle 2)

TABLE I. ENCODING RULE OF PERFORMING THE OPERATIONS ON THE PARTICLE 2

Initial state	O1	State	O2	Final state
$\|\psi^{+}\rangle_{12}$	U_0 →	$\|\psi^{+}\rangle_{12}$	U_0 →	$\|\psi^{+}\rangle_{12}$
			U_2 →	$\|\psi^{-}\rangle_{12}$
	U_1 →	$\|\phi^{+}\rangle_{12}$	U_0 →	$\|\phi^{+}\rangle_{12}$
			U_2 →	$\|\phi^{-}\rangle_{12}$

Suppose that $u_1,\dots,u_N$ are the N parties in our protocol and their secret messages denote as

$$M_i=\{\mathrm{m}_1^i\mathrm{m}_2^i\cdots\mathrm{m}_n^i\}$$

All the parties agree that the unitary operations on the particle 1 f an EPR pair is the following

$$\begin{cases}U_0,\text{ if the secret bit is 0}\\ U_1,\text{ if the secret bit is 1}\end{cases}\qquad(1)$$

The operation on the particle 2 is the following

$$\begin{cases}U_0,\text{ if the secret bit is 0}\\ U_2,\text{ if the secret bit is 1}\end{cases}\qquad(2)$$

Now we describe the protocol in detail.

Step 1. The first transmission loop. The user $u_i(i=1,2,...,N)$ prepares n state $|\psi^{+}\rangle_{12}$ and divides these states into two single particle sequences which can be denoted as S_{i1} and S_{i2}. In addition, u_i prepares enough decoy particles from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ randomly and inserts them into S_{i2}. After that, u_i sends the mixed sequences to u_{i+1} according to the transmission direction in Fig. 1. (Start from u_i, we denote u_{i+m} as the m-th user.)

Step 2. After confirming u_{i+1} has received the mixed sequence, u_i announces the positions and the measurement basis $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ of the decoy particles. Then they compare the measurement results to check the quantum channels. If the error rate exceeds the threshold, the protocol is discarded; otherwise, the two parties continue.

Step 3. The second transmission loop. After picking out the decoy particles, u_{i+1} performs the operations according to his secret message M_{i+1} and the rule (2) on the particles in S_{i2}, which forms a new sequence, i.e., $U_{i+1}:S_{i2}\to S'_{i2}$. Next, u_{i+1} inserts randomly enough decoy into S'_{i2} and send this mixed sequence to u_{i+2}.

Step 4. The user u_{i+1} announces the positions and the basis of the decoy particles after confirming u_{i+2} has received the mixed sequence. Then two parties begin to check the security of qubit transmission. If the error rate exceeds the threshold, they abort the protocol, otherwise, they continue.

Step 5. The third transmission loop. After picking out the decoy particles, u_{i+2} performs the operations on the particles in S'_{i2} according to M_{i+2} and the rule (2), which forms a new sequence, i.e.,

$$U_{i+2}\otimes U_{i+1}:S_{i2}\to S''_{i2}.$$

Moreover, u_{i+2} inserts enough decoy particles into S''_{i2} randomly and sends the mixed sequence to the next user according to the direction in Fig. 1. Similar to the previous steps, we can implement the protocol until the n-th loop if the security checking of quantum channels is passed.

Step 6. The n-th transmission loop. The user $u_{i+(\mathrm{n}-1)}$ performs the corresponding operation by his own message $M_{i+(\mathrm{n}-1)}$ and the rule (2). That is,

$$U_{i+(n-1)}\otimes U_{i+(n-2)}\otimes\cdots\otimes\pm U_{i+1}:S_{i2}\to S_{i2}^{(\mathrm{n}-1)}.$$

Then he inserts randomly decoy particles into $S_{i2}^{(\mathrm{n}-1)}$ and returns this mixed sequence to u_i

Step 7. Similar to the step 2, the users $u_{i+(\mathrm{n}-1)}$ and u_i check the security of quantum channel. If passed, this protocol is continued. According to the rule (1) and his message M_i, u_i performs the operation on S_{i1}, which can be written as S'_{i1}. Then u_i makes Bell measurements on the particles in S'_{i1} and $S_{i2}^{(\mathrm{n}-1)}$. Then u_i can extract the other parties' operations and obtain their respect secret bits. Thus all the parties can exchange their messages successfully.

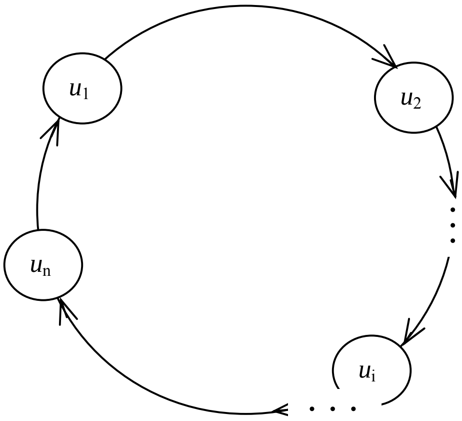

Figure 1. Transmission loop of our protocol

III. Security analysis

Now we analyze the security of our scheme. From the seven steps, we can see that there must be a security check over quantum channels when one party sends a particle sequence to another party. On the other hand, the decoy particles are chosen from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ randomly. Thus, if Eve is an evil eavesdropper who wants to obtain the secret messages to be exchanged between the three parties, one of attack strategies that she may takes is the intercept-resend attack. When Eve captures the particles in the quantum channel, she replaces her own particles and resends them. However, since the decoy photons are randomly inserted into the sequence, Eve cannot know the positions and the measurement basis of this particles. Suppose τ is the number of decoy particles, then Eve could not been detected is $1/4^{\tau}$. In fact, this kind of detection method is same with that in BB84 protocol. Another attack strategy is the entangle-measure attack. That is, Eve prepares an ancillary particle E and performs a unitary operation U on E and the intercepted particle. Thus we have

$$U:|0,e\rangle \rightarrow |0,e_{00}\rangle + |1,e_{01}\rangle,$$

$$|1,e\rangle \rightarrow |0,e_{10}\rangle + |1,e_{11}\rangle$$

The whole system is in the state

$$1/\sqrt{2}(|1\rangle_2 |x\rangle_{1E} + |0\rangle_2 |y\rangle_{1E}),$$

where $|x\rangle \rightarrow |0\rangle |e_{00}\rangle + |1\rangle |e_{01}\rangle$, $|y\rangle \rightarrow |0\rangle |e_{10}\rangle + |1\rangle |e_{11}\rangle$. If Eve wants to avoid any error, then $\langle 1|x\rangle = 0, \langle 0|y\rangle = 0$. So $e_{01} = e_{10} = \mathbf{0}$. In the security check step, the measurement basis are chosen from $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ randomly. So we also have the following for the basis $\{|+\rangle,|-\rangle\}$

$$U:|+\rangle|E\rangle \rightarrow \frac{1}{2}(|+\rangle(|e_{00}\rangle + |e_{11}\rangle) + |-\rangle(|e_{00}\rangle - |e_{11}\rangle))$$

$$|-\rangle|E\rangle \rightarrow \frac{1}{2}(|+\rangle(|e_{00}\rangle - |e_{11}\rangle) + |-\rangle(|e_{00}\rangle + |e_{11}\rangle))$$

From the correlations of Bell states, the state $|\psi^+\rangle$ can been written as

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

Then the whole quantum system is in the following state

$$U|\psi^+\rangle_{12}|E\rangle_E = U\left(\frac{1}{\sqrt{2}}(|{++}\rangle_{21} - |{--}\rangle_{21})\right)|E\rangle_E$$

$$\rightarrow \frac{1}{2\sqrt{2}}(|+\rangle_2(|+\rangle_1(|e_{00}\rangle + |e_{11}\rangle)_E$$

$$+|-\rangle_2(|e_{00}\rangle - |e_{11}\rangle)_E)$$

$$-|-\rangle_2(|+\rangle_1(|e_{00}\rangle - |e_{11}\rangle)_E$$

$$+|-\rangle_2(|e_{00}\rangle + |e_{11}\rangle)_E))$$

Similarly, from the above formula and the correlations of $|\psi^+\rangle$, we can know that the measurement results $|+\rangle_2|-\rangle_1$ and $|-\rangle_2|+\rangle_1$ must not exist under the condition that no errors are to occur. Thus the following equation can been obtained $e_{00} = e_{11}$. Therefore the quantum system is in $|\psi^+\rangle_{12}|e_{00}\rangle_E$ and Eve cannot gain any information from the ancilla. According to the above analysis our protocol is secure.

IV. Conclusion

In this paper, we propose a multiparty quantum secure communication protocol with the qubit transmission loop. Every participant is both a sender and a receiver and forms a return qubit circuit. The transmission direction has the characteristics of unidirectional circulation. By performing the joint measurement on the encoded particles and unitary operations, the N parties can exchange their own secret messages over the quantum channels. Our scheme is easy to implement and has a novel characteristic for the member equivalence.

Acknowledgements

This work was supported by the Shandong Provincial Natural Science oundation (No. ZR2013FQ011), the Project of Shandong Province higher Educational Science and Technology Program (No. J13LN60), Technology Development Projects of Tai'an (No.20140629-2) and Project of Taishan University Doctoral Fund (Y-01-2014020).

References

[1] C. Kollmitzer and M. Pivk: Applied Quantum Cryptography (Springer, Berlin Heidelberg, 2010).

[2] G.L. Long and X.S. Liu: Phys. Rev. A, Vol. 65 (2002), p.032-302

[3] A. Beige, B.G. Englert, C. Kurtsiefer, et. al.: Acta Physics Polonica A, Vol.101 (2002), p.357-368

[4] K. Boström and T. Felbinger: Phys. Rev. Lett., vol.89 (2002), p.187902-187905

[5] J. Li, H. Jin and B. Jing: Science in China Series G, Vol. 54 (2011), p. 1612-1618

[6] F. G. Deng, G. L. Long and X. S. Liu: Phys. Rev. A, Vol. 68 (2003), p.042317

[7] B.A. Nguyen: Physics Letters A, Vol.328 (2004) p.6-10

[8] X.R. Jin, X. Ji, and S. Zhang, et al.: Physics Letters A, Vol.354 (2006), p.67-70

[9] Z. X. Man and Y. J. Xia: Chinese Physics Letters, Vol. 24 (2007), p.15-18

[10] M. Y. Wang and F. L. Yan: Chinese Physics Letters, Vol. 24 (2007), p.2486-2488

[11] S. K. Chong and T. Hwang: Optics Communication, Vol. 284 (2011), p. 515-518

[12] X.R. Yin, W.P. Ma, D.S. Shen and C. Hao: Journal of Quantum Information Science, Vol. 3 (2013), p. 1-5.

[13] F. Gao, F. Z. Guo, Q. Y. Wen, et al.: Science in China Series G, Vol.51 (2008), p.559-566

[14] Y. G. Tan and Q. Y. Cai: Int J Quantum Inf, Vol. 6 (2008), p. 325-329