Journal of Quantum Information Science, 2014, 4, 292-296
Published Online December 2014 in SciRes. http://www.scirp.org/journal/jqis
http://dx.doi.org/10.4236/jqis.2014.44024

Three-Party Simultaneous Quantum Secure Communication Based on Closed Transmission Loops

Xunru Yin[1,2]

[1]Department of Mathematics and Systems Science, Taishan University, Tai'an, China
[2]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China
Email: xryin@outlook.com

Received 12 October 2014; revised 7 November 2014; accepted 2 December 2014

Abstract

A kind of novel three-party quantum secure direct communication protocol is proposed with the correlation of two-particle entangled state. In this scheme the qubit transmission forms a closed loop and every one of the three participants is both a receiver and a sender of particle sequences in the bidirectional quantum channels. Each party implements the corresponding unitary operations according to its secret bit value over the quantum channels and then extracts the other two parties' unitary operations by performing Bell measurements on the encoded particles. Thus they can obtain the secret information simultaneously. Finally, the security analysis shows that the present three-party scheme is a secure protocol.

Keywords

Quantum Information, Quantum Cryptographic Protocol, Quantum Secure Direct Communication, Bell States

1. Introduction

Quantum key distribution (QKD) is based on quantum mechanics and has the unconditional security, in which all legitimate users can distribute a shared key beforehand to make secure communications. Different from QKD, quantum secure direct communication (QSDC), another important application of quantum cryptography, can allow the messages to be read out after qubit transmission and then exchange the secret information between all parties directly without distributing a shared secret key.

In 2002, Long *et al.* [1] presented the first QSDC protocol by using EPR entangled states. Then Beige *et al.* [2]

How to cite this paper: Yin, X.R. (2014) Three-Party Simultaneous Quantum Secure Communication Based on Closed Transmission Loops. *Journal of Quantum Information Science*, **4**, 292-296. http://dx.doi.org/10.4236/jqis.2014.44024

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

In this paper, we propose a novel three-party QSDC protocol by using the idea of quantum dense coding on the two-particle EPR pair. The three parties in our scheme are peer entities and they transmit the particle sequences each other synchronously in a closed loop of qubit transmission. One party can obtain the other two 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.

2. Description of the Present Protocol

The four Bell states can be written as $\left|\psi^{+}\right\rangle=1/\sqrt{2}\left(|01\rangle+|10\rangle\right)$, $\left|\psi^{-}\right\rangle=1/\sqrt{2}\left(|01\rangle-|10\rangle\right)$, $\left|\phi^{+}\right\rangle=1/\sqrt{2}\left(|00\rangle+|11\rangle\right)$, $\left|\phi^{-}\right\rangle=1/\sqrt{2}\left(|00\rangle-|11\rangle\right)$. Where $|0\rangle$, $|1\rangle$ are the up and down eigenstates of Pauli operator σ_z. Let $|+\rangle=1/\sqrt{2}\left(|0\rangle+|1\rangle\right)$, $|-\rangle=1/\sqrt{2}\left(|0\rangle-|1\rangle\right)$. Then $|+\rangle$ and $|-\rangle$ are the eigenstates of Pauli operator σ_x. Suppose U_0, U_1 and U_2 are three unitary operations, That is, $U_0=|0\rangle\langle 0|+|1\rangle\langle 1|$, $U_1=|0\rangle\langle 0|-|1\rangle\langle 1|$ and $U_2=|0\rangle\langle 1|+|1\rangle\langle 0|$. An EPR pair can be transformed to another EPR pair if we perform the unitary operation U_0 or U_1 on the first qubit and U_0 or U_2 on the second qubit. In this paper, we take $\left|\psi^{+}\right\rangle$ as the initial state and the transformation rule can be shown in **Table 1**.

Now, we suppose Alice, Bob, and Charlie as the three parties in our scheme. Let M_A, M_B and M_C denote their secret messages to be exchanged respectively. That is,

$$M_A=\{a_1a_2\cdots a_n\}$$
$$M_B=\{b_1b_2\cdots b_n\}$$
$$M_C=\{c_1c_2\cdots c_n\}$$

where $a_i,b_i,c_i\in\{0,1\}$, and $i=1,2,\cdots,n$. The three parties agree that they take the corresponding unitary operation according to their secret bit value. If the encoded particle is the first qubit of initial state $\left|\psi^{+}\right\rangle$, the rule is the following

$$\begin{cases} U_0,\ \text{if } a_i=0/b_i=0/c_i=0 \\ U_1,\ \text{if } a_i=1/b_i=1/c_i=1 \end{cases} \tag{1}$$

If the encoded particle is the second qubit, the rule is the following

Table 1. Encoding rule in the present protocol.

Initial state	Operation on particle 1	Operation on particle 2	Final state
$\left|\psi^{+}\right\rangle_{12}$	U_0	U_0	$\left|\psi^{+}\right\rangle_{12}$
	U_0	U_2	$\left|\phi^{+}\right\rangle_{12}$
	U_1	U_0	$\left|\psi^{-}\right\rangle_{12}$
	U_1	U_2	$\left|\phi^{-}\right\rangle_{12}$

$$\begin{cases} U_0, \text{ if } a_i = 0/b_i = 0/c_i = 0 \\ U_2, \text{ if } a_i = 1/b_i = 1/c_i = 1 \end{cases} \tag{2}$$

Next, we describe this protocol in detail.

Step 1. Alice/Bob/Charlie prepares n states $|\psi^+\rangle_{12}$ and takes two particles 1 and 2 from each entangled state to form two single particle sequences which can be denoted as $(S_{A1}, S_{A2})/(S_{B1}, S_{B2})/(S_{C1}, S_{C2})$. Moreover, each party chooses enough decoy photons from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ randomly and inserts them into their own two sequences. After that, Alice sends the mixed sequences S_{A1} and S_{A2} to Bob and Charlie respectively; Bob sends the mixed S_{B1} and S_{B2} to Charlie and Alice respectively; Charlie sends the mixed S_{C1} and S_{C2} to Alice and Bob respectively.

Step 2. After confirming (Bob, Charlie)/(Charlie, Alice)/(Alice, Bob) has received the mixed sequences, Alice/Bob/Charlie publishes the positions and the measurement basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ of the decoy particles. Then they check the quantum channels by presenting the measurement results. If the error rate exceeds the threshold, the protocol is discarded; otherwise, it will go to the next step.

Step 3. After picking out the decoy particles, Bob/Charlie/Alice performs the unitary operations on $S_{A1}/S_{B1}/S_{C1}$ according to the rule (1). Charlie/Alice/Bob performs the unitary operations on $S_{A2}/S_{B2}/S_{C2}$ according to the rule (2). The encoded sequences can be written as $S'_{A1}/S'_{B1}/S'_{C1}$ and $S'_{A2}/S'_{B2}/S'_{C2}$, respectively. For the next security check of quantum channels, they insert randomly enough into their own sequences. Next, (Bob, Charlie) return (S'_{A1}, S'_{A2}) which contain decoy particles to Alice respectively; (Charlie, Alice) return (S'_{B1}, S'_{B2}) which contain decoy particles to Bob respectively; (Alice, Bob) return (S'_{C1}, S'_{C2}) which contain decoy particles to Charlie respectively.

Step 4. After confirming that Alice/Bob/Charlie has received the mixed two sequences, the other two parties announce the positions and the corresponding measurement basis of the decoy particles. Then they check the security of quantum channels by comparing the measurement results of the decoy particles. If the error rate does not meet the requirement, the three parties abort the protocol; otherwise, they continue it.

Step 5. Alice/Bob/Charlie first picks out the decoy particles. Now, each party has two encoded sequences and performs Bell measurement orderly on the corresponding photon pairs in this two sequences, for instance, Alice performs Bell measurement on the EPR pairs in S'_{A1} and S'_{A2}. According to **Table 1**, each party can obtain the other two parties' operation and then extract the secret messages from rules (1) and (2). Thus, three parties realize the information exchange.

From the above steps, we can see the qubit transmission forms a closed loop and every party sends or receives particles simultaneously. For conciseness, we take $n = 1$ for example and only consider Alice obtains M_B and M_C. Suppose $M_B = M_C = 1$, Alice first prepares $|\psi^+\rangle_{12}$. She sends particles 1 and 2 to Bob and Charlie respectively. Bob performs U_1 on particle 1 from rule (1). Charlie performs U_2 on particle 2 from rule (2). Then Bob and Charlie return particles 1, 2 to Alice. Alice performs Bell measurement on the two particles and the measurement results must be $|\phi^-\rangle_{12}$. According to **Table 1**, Alice can know Bob's and Charlie's operation are U_1 and U_2 respectively. Thus she obtains $M_B = 1, M_C = 1$.

3. Security Analysis

Now we analyze the security of our scheme. From the five 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. For example, Eve can intercept the particles which are sent from Alice to Bob and resend them to Bob after she has some useful information by means of measurement method. 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 corresponding measurement basis of these particles before the sender publishes the relevant information in the classical channels. Suppose τ is the number of decoy particles, then the probability that Eve could not been detected is $1/4^{\tau}$. In fact, this kind of detection method is same with that in BB84 protocol. Therefore, Eve cannot steal any valuable information of shared secret key by this kind of attack strategies. Another attack strategy Eve may take is the entangle-measure attack. That is, Eve prepares an ancillary particle E in the initial state $|E\rangle$. When she intercepts the qubits which are propagated from one party to another party, Eve makes the ancilla E interact unitarily with these qubits. After that she sends them to the receiver and captures them again when the encoded particles are gone back. In this way Eve may obtain some information about the secret messages of the participants. Next, we will show that she cannot gain any secret information if Eve want to avoid that no errors are to occur. She adds the particle E in the eavesdropping phase and performs a unitary operation U on E and the intercepted particle. Thus we have

$$\begin{aligned} U: \left|0,e\right\rangle &\to \left|0,e_{00}\right\rangle + \left|1,e_{01}\right\rangle \\ \left|1,e\right\rangle &\to \left|0,e_{10}\right\rangle + \left|1,e_{11}\right\rangle \end{aligned}$$

Then the whole system is in the state

$$\begin{aligned} U\left|\psi^{+}\right\rangle_{12}\left|E\right\rangle_{E} &= U\left(\frac{1}{\sqrt{2}}\left(\left|10\right\rangle_{21} + \left|01\right\rangle_{21}\right)\right)\left|E\right\rangle_{E} \\ &\to 1\big/\sqrt{2}\left(\left|1\right\rangle_{2}\left|x\right\rangle_{1E} + \left|0\right\rangle_{2}\left|y\right\rangle_{1E}\right) \end{aligned}$$

where

$$\begin{aligned} \left|x\right\rangle &\to \left|0\right\rangle\left|e_{00}\right\rangle + \left|1\right\rangle\left|e_{01}\right\rangle \\ \left|y\right\rangle &\to \left|0\right\rangle\left|e_{10}\right\rangle + \left|1\right\rangle\left|e_{11}\right\rangle \end{aligned}$$

If Eve wants to avoid any error, the following conditions should be satisfied

$$\begin{aligned} \left\langle 1 | x\right\rangle &= 0 \\ \left\langle 0 | y\right\rangle &= 0 \end{aligned}$$

According to the above equations, we can have

$$e_{01} = e_{10} = 0.$$

On the other hand, in the security check step, the measurement basis are chosen from $\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$ and $\left\{\left|+\right\rangle,\left|-\right\rangle\right\}$ randomly. So we also have the following for the basis $\left\{\left|+\right\rangle,\left|-\right\rangle\right\}$

$$\begin{aligned} U: \left|+\right\rangle\left|E\right\rangle &\to \frac{1}{2}\left(\left|+\right\rangle\left(\left|e_{00}\right\rangle + \left|e_{11}\right\rangle\right) + \left|-\right\rangle\left(\left|e_{00}\right\rangle - \left|e_{11}\right\rangle\right)\right) \\ \left|-\right\rangle\left|E\right\rangle &\to \frac{1}{2}\left(\left|+\right\rangle\left(\left|e_{00}\right\rangle - \left|e_{11}\right\rangle\right) + \left|-\right\rangle\left(\left|e_{00}\right\rangle + \left|e_{11}\right\rangle\right)\right) \end{aligned}$$

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

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

Then the whole quantum system is in the following state

$$\begin{aligned} U\left|\psi^{+}\right\rangle_{12}\left|E\right\rangle_{E} &= U\left(\frac{1}{\sqrt{2}}\left(\left|++\right\rangle_{21} - \left|--\right\rangle_{21}\right)\right)\left|E\right\rangle_{E} \\ &\to \frac{1}{2\sqrt{2}}\Big(\left|+\right\rangle_{2}\left(\left|+\right\rangle_{1}\left(\left|e_{00}\right\rangle + \left|e_{11}\right\rangle\right)_{E} + \left|-\right\rangle_{2}\left(\left|e_{00}\right\rangle - \left|e_{11}\right\rangle\right)_{E}\right) \\ &\quad - \left|-\right\rangle_{2}\left(\left|+\right\rangle_{1}\left(\left|e_{00}\right\rangle - \left|e_{11}\right\rangle\right)_{E} + \left|-\right\rangle_{2}\left(\left|e_{00}\right\rangle + \left|e_{11}\right\rangle\right)_{E}\right)\Big) \end{aligned}$$

Similarly, from the above formula and the correlations of $\left|\psi^{+}\right\rangle$, we can know that the measurement results $\left|+\right\rangle_{2}\left|-\right\rangle_{1}$ and $\left|-\right\rangle_{2}\left|+\right\rangle_{1}$ 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 the state

$$\left|\psi^{+}\right\rangle_{12}\left|e_{00}\right\rangle_{E}$$

That is, regardless of what the legitimate users take the measurement basis, the eavesdropper Eve cannot extract any useful information of the secret messages by observing the ancillary particle. Then our scheme is secure according to the above analysis and discussion.

4. Conclusion

In this paper, we propose a three-party quantum secret direct communication protocol with the bidirectional qubit transmission. In the whole process, we can see that all the parties form a return qubit circuit and they are peer entities. The three parties can exchange their own secret messages by using Bell measurement and unitary operations over the quantum channels. This scheme has a novel characteristic for the quantum return circuit and the member equivalence. However, the security discussion is based on the condition of ideal quantum channels. We have not considered the actual physical environment. In the quantum channel, noise and loss cannot be ignored with the particle transmission because they reduce the efficiency of quantum communication and increase the risk of information leakage. With the existing technologies, it has become more difficult to study such quantum communication protocols. We hope this problem can be solved in future research.

Acknowledgements

This work was supported by the Shandong Provincial Natural Science Foundation (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] Long, G.L. and Liu, X.S. (2002) Theoretically Efficient High-Capacity Quantum Key Distribution Scheme. *Physical Review A*, **65**, Article ID: 032302. http://dx.doi.org/10.1103/PhysRevA.65.032302

[2] Beige, A., Englert, B.G., Kurtsiefer, C., *et al*. (2002) Secure Communication with a Publicly Known Key. *Acta Physics Polonica A*, **101**, 357-368.

[3] Boström, K. and Felbinger, T. (2002) Deterministic Secure Direct Communication Using Entanglement. *Physical Review Letters*, **89**, Article ID: 187902. http://dx.doi.org/10.1103/PhysRevLett.89.187902

[4] Li, J., Jin, H. and Jing, B. (2011) Improved Quantum "Ping-Pong" Protocol Based on GHZ State Operation. *Science in China Series G*, **54**, 1612-1618. http://dx.doi.org/10.1007/s11433-011-4448-0

[5] Deng, F.G., Long, G.L. and Liu, X.S. (2003) Two-Step Quantum Direct Communication Protocol Using the Einstein-Podolsky-Rosen Pair Block. *Physical Review A*, **68**, Article ID: 042317. http://dx.doi.org/10.1007/s11433-011-4448-0

[6] Nguyen, B.A. (2004) Quantum Dialogue. *Physics Letters A*, **328**, 6-10. http://dx.doi.org/10.1016/j.physleta.2004.06.009

[7] Jin, X.R., Ji, X., Zhang, S., *et al*. (2006) Three-Party Quantum Secure Direct Communication Based on GHZ States. *Physics Letters A*, **354**, 67-70. http://dx.doi.org/10.1016/j.physleta.2006.01.035

[8] Man, Z.X. and Xia, Y.J. (2007) Improvement of Security of Three-Party Quantum Secure Direct Communication Based on GHZ States. *Chinese Physics Letters*, **24**, 15-18. http://dx.doi.org/10.1088/0256-307X/24/1/005

[9] Wang, M.Y. and Yan, F.L. (2007) Three-Party Simultaneous Quantum Secure Direct Communication Scheme with EPR Pair. *Chinese Physics Letters*, **24**, 2486-2488. http://dx.doi.org/10.1088/0256-307X/24/9/007

[10] Chong, S.K. and Hwang, T. (2011) The Enhancement of Three-Party Simultaneous Quantum Secure Direct Communication Scheme with EPR Pairs. *Optics Communication*, **284**, 515-518. http://dx.doi.org/10.1016/j.optcom.2010.08.037

[11] Yin, X.R., Ma, W.P., Shen, D.S. and Hao, C. (2013) Efficient Three-Party Quantum Secure Direct Communication with EPR Pairs. *Journal of Quantum Information Science*, **3**, 1-5. http://dx.doi.org/10.4236/jqis.2013.31001

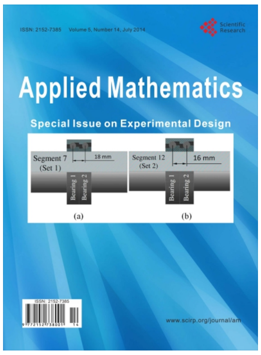
[12] Gao, F., Guo, F.Z., Wen, Q.Y., *et al*. (2008) Revisiting the Security of Quantum Dialogue and Bidirectional Quantum Secure Direct Communication. *Science in China Series G*, **51**, 559-566. http://dx.doi.org/10.1007/s11433-008-0065-y

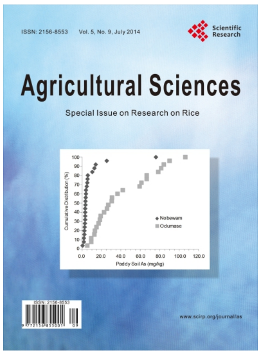
[13] Yin, X.R., Ma, W.P., Liu, W.Y. and Shen, D.S. (2013) Efficient Bidirectional Quantum Secure Communication with Two-Photon Entanglement. *Quantum Information Processing*, **12**, 3093-3102. http://dx.doi.org/10.1007/s11128-013-0584-y

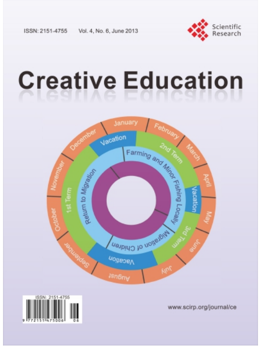
Advances in Bioscience and Biotechnology

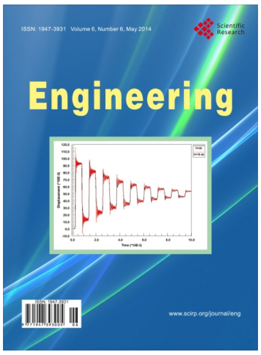
American Journal of Analytical Chemistry

American Journal of Plant Sciences
Special Issue on Photosynthesis

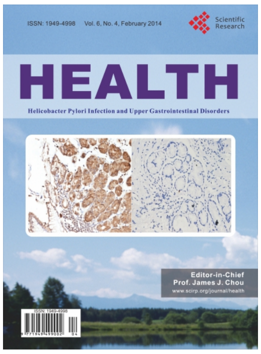

Applied Mathematics
Special Issue on Experimental Design


Agricultural Sciences
Special Issue on Research on Rice


Creative Education

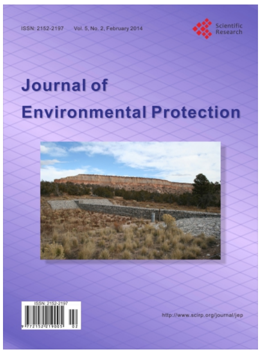

Engineering

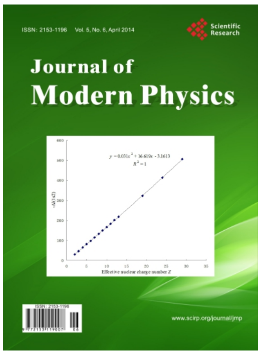
Food and Nutrition Sciences


HEALTH
Helicobacter Pylori Infection and Upper Gastrointestinal Disorders
Editor-in-Chief
Prof. James J. Chou

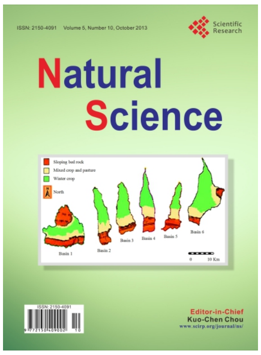
Journal of Computer and Communications

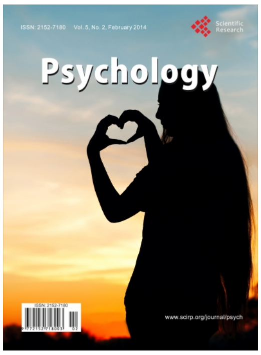
Journal of Cancer Therapy
Special Issue on Bone Tumor Research


Journal of Environmental Protection


Journal of Modern Physics

Modern Economy


Natural Science
Editor-in-Chief
Kuo-Chen Chou


Psychology