Journal of Quantum Information Science, 2013, 3, 1-5
http://dx.doi.org/10.4236/jqis.2013.31001 Published Online March 2013 (http://www.scirp.org/journal/jqis)

Efficient Three-Party Quantum Secure Direct Communication with EPR Pairs

Xunru Yin[1,2], Wenping Ma[1], Dongsu Shen[1], Chaoyang Hao[3]
[1]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China
[2]School of Mathematics and Systems Science, Taishan University, Tai'an, China
[3]Shandong Taikai Electric Automation Co., Ltd., Tai'an, China
Email: yxr03@yahoo.com.cn

Received January 30, 2013; revised March 2, 2013; accepted March 10, 2013

ABSTRACT

In order to get rid of the drawback of information leakage which existed in Chong *et al.*'s protocol (Opt. Commun., 284, 2011, 515-518), an efficient three-party quantum secure direct communication (3P-QSDC) based on some ideas of quantum dense coding with EPR pairs is proposed, in which each entangled pair can be used to exchange a longer length of secret message between three legal users. By improving the classical channels and the qubit transmissions, our scheme can avoid this kind of drawback. Thus, the secret messages are not leaked out to other people from the public information. Moreover, compared with Chong *et al.*'s protocol, our protocol can achieve higher efficiency.

Keywords: Quantum Secure Direct Communication; Quantum Dense Coding; Protocol Efficiency

1. Introduction

Quantum secure direct communication (QSDC) is an important branch of quantum cryptography, in which the secret messages are directly transmitted in a quantum channel between two legitimate parties, say Alice and Bob, without creating a private key to encode and decode the messages. Since QSDC has a great advantage of unconditional security based on quantum mechanics for the legal users to communicate, much attention has been focused on this research field and many schemes have been presented [1-12].

In 2002, Long and Liu [1] proposed the first QSDC scheme based on EPR pairs. Beige *et al.* [2] presented a QSDC protocol based on the exchange of single photons. Boström *et al.* [3] proposed a ping-pong QSDC scheme based on EPR pairs, which was improved by Li *et al.* [4] in 2011. Deng *et al.* [5] proposed an efficient QSDC scheme. However, the mode of message transmission in QSDC is one-way. Thus, in 2004, quantum dialogue or the so-called bidirectional QSDC was proposed [7]. Recently, many three-party QSDC schemes were proposed, in which a party can obtain the other two parties' messages simultaneously through a quantum channel. Jin *et al.* [10] presented a 3P-QSDC by using the GHZ states, and Man *et al.* [11] improved this scheme. Chamoli [12] also presented a 3P-QSDC with GHZ states. In 2007, Wang *et al.* [13] presented a 3P-QSDC by using EPR pairs. In 2011, Chong *et al.* [14] proposed an enhancement on Wang *et al.*' scheme [13]. They pointed out that the communication can be paralleled and thus the protocol efficiency is improved.

For simplicity, References [13,14] are shortened as CH protocol and WY protocol, respectively. From CH protocol, we can see that the main features of their work are the paralleled communication and the improved protocol efficiency. However, there are some questions in Chong *et al.*'s scheme, which can be summarized as follows:

1) The qubit transmissions in WY protocol are thought to be sequential by Chong *et al.*, *i.e.*, Alice → Bob → Charlie → Alice. That is, every party needs to wait for the other's response. So in CH scheme, the qubit transmissions are designed as Alice → (Bob and Charlie) and (Bob and Charlie) → Alice. However, the improvement has the following disadvantages: (a) The goal here is to save the response time throughout the process, but this new way can lead to double workload in Alice's site. Thus, this improvement would be of no great importance or value in practical application; (b) As will be described later, the qubit transmission mode of CH protocol can reduce 3P-QSDC protocol efficiency.

2) Chong *et al.* proposed an enhancement on Wang *et al.*'s scheme, but this work only compared with Men *et al.*'s scheme [11] in the qubit efficiency. However, Men *et al.*'s scheme is based on GHZ states, while Chong *et al.*' is based on EPR states. So it is more forceful if they can compare 3P-QSDC efficiency of their own scheme with that of Wang *et al.*'s scheme.

3) From step 11 in CH protocol, we can see that there exists a message correlation between three parties. Let us

Copyright © 2013 SciRes.

take $n=1$ for example. If $X=0, Y=0$, then $M_A = M_B = M_C$. Thus, from the public classical channels, Eve can know the secret bits transmitted by three parties must be one of $\{(0,0,0),(1,1,1)\}$ randomly, which contains $-2\times(1/2)\log_2(1/2)=1$ bit of information. This insecurity is called information leakage or classical correlation [15,16]. In fact, WY protocol also has this kind of drawback.

In this paper, we present an efficient 3P-QSDC scheme based on some ideas in quantum dense coding with EPR pairs. Each photon pair can be used to exchange a longer length of secret message and the drawback of information leakage does not exist in our scheme. Moreover, in an ideal quantum channel, the efficiency of CH protocol is 50%, but our 3P-QSDC efficiency can be increased to 60%. Finally, the security of our scheme is analyzed.

2. Description of the Protocol

Firstly, let us introduce two-qubit entangled states. An EPR pair is one of the four Bell states, *i.e.*,

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) = \frac{1}{\sqrt{2}}\left(|++\rangle+|--\rangle\right) \quad (1)$$

$$\left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle-|11\rangle\right) = \frac{1}{\sqrt{2}}\left(|+-\rangle+|-+\rangle\right) \quad (2)$$

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right) = \frac{1}{\sqrt{2}}\left(|++\rangle-|--\rangle\right) \quad (3)$$

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right) = \frac{1}{\sqrt{2}}\left(|-+\rangle-|+-\rangle\right) \quad (4)$$

where $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of Pauli operator σ_z. $|+\rangle=\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ and $|-\rangle=\left(|0\rangle-|1\rangle\right)/\sqrt{2}$ are the up and down eigenstates of Pauli operator σ_x. Let U_0, U_1, U_2 and U_3 be four local unitary operations. That is

$$U_0 \equiv I = |0\rangle\langle 0|+|1\rangle\langle 1|, \quad (5)$$

$$U_1 \equiv \sigma_x = |0\rangle\langle 1|+|1\rangle\langle 0|, \quad (6)$$

$$U_2 \equiv i\sigma_y = |0\rangle\langle 1|-|1\rangle\langle 0|, \quad (7)$$

$$U_3 \equiv \sigma_z = |0\rangle\langle 0|-|1\rangle\langle 1|. \quad (8)$$

Suppose that Alice, Bob, and Charlie have a secret message to exchange respectively. Their messages can be assumed as the following in sequence:

$$M_A = \{(i_1, j_1),(i_2, j_2), \quad ,(i_N, j_N)\},$$
$$M_B = \{(k_1, l_1),(k_2, l_2), \quad ,(k_N, l_N)\},$$
$$M_C = \{(p_1, q_1),(p_2, q_2), \quad ,(p_N, q_N)\},$$

where $i_n, j_n, k_n, l_n, p_n, q_n \in \{0,1\}$.

Three parties agree that the four Pauli operations represent two-bit classical information, respectively, *i.e.*,

$$U_0 \leftrightarrow 00, U_1 \leftrightarrow 01, U_2 \leftrightarrow 10, U_3 \leftrightarrow 11. \quad (9)$$

An EPR pair can be transformed into another EPR pair by performing the unitary operation $U_i\,(i=0,1,2,3)$. Then the encoding of our 3P-QSDC can be summarized as **Table 1**.

Now, let us describe the present protocol in detail by the following steps.

Step 1. Alice prepares N EPR pairs and each EPR pair is one of the four Bell states randomly. Alice takes one particle from each EPR pair to form two single photon sequences Q_h and Q_t, where $h(t)$ denotes the first (the second) particle in each pair. She encodes her message into Q_t by performing the operation $U_i\,(i=0,1,2,3)$ according to Equation (9). Alice prepares five sets of decoy photons, $D_{B1}, D_{B2}, D_C, D_{A1}$ and D_{A2}, randomly chosen from $|0\rangle, |1\rangle, |+\rangle$, and $|-\rangle$. Moreover, she generates single photon sequence Q_r, in which the particles is defined a one-to-one correspondence with the initial states prepared by herself, *i.e.*, $|0\rangle \leftrightarrow \left|\phi^+\right\rangle, |1\rangle \leftrightarrow \left|\phi^-\right\rangle, |+\rangle \leftrightarrow \left|\psi^+\right\rangle$, and $|-\rangle \leftrightarrow \left|\psi^-\right\rangle$.

Then Alice randomly inserts all particles in D_{B1} and D_{A1} into Q_h to form Q_h^a. She randomly inserts all particles in D_{B2}, D_C, D_{A2} and Q_r into Q_t to form Q_t^a. Finally, Alice sends Q_t^a to Bob.

Step 2. After Bob receives Q_t^a, Alice announces the positions of D_{B2}, D_C, D_{A2}, Q_r and the states of D_{B2}. Then Bob measures the particles in D_{B2} by using basis σ_z or σ_x. He can judge if the quantum channel is secure by analyzing the error rate. If no, Bob aborts the communication. Otherwise, after picking out Q_t, he encodes his message into Q_t by performing the operation $U_i\,(i=0,1,2,3)$ according to Equation (9). After that, Bob asks Alice to send him Q_h^a.

Step 3. After Bob receives Q_h^a, Alice announces the positions of D_{B1}, D_{A1} and the states of D_{B1}. Then Bob measures D_{B1} and checks the quantum channel by analyzing the error rate. If the error rate exceeds the thresh

Table 1. Encoding of the present protocol.

initial state	operation	final state
$\left\|\phi^\pm\right\rangle$	$I\otimes U_0$	$\left\|\phi^\pm\right\rangle$
	$I\otimes U_1$	$\left\|\psi^\pm\right\rangle$
	$I\otimes U_2$	$\left\|\psi\ \right\rangle$
	$I\otimes U_3$	$\left\|\phi\ \right\rangle$
$\left\|\psi^\pm\right\rangle$	$I\otimes U_0$	$\left\|\psi^\pm\right\rangle$
	$I\otimes U_1$	$\left\|\phi^\pm\right\rangle$
	$I\otimes U_2$	$\left\|\phi\ \right\rangle$
	$I\otimes U_3$	$\left\|\psi\ \right\rangle$

Copyright © 2013 SciRes.

old, this protocol is aborted. Otherwise, Bob picks out Q_h and performs Bell measurements on Q_h and Q_t (encoded sequence), which forms two new sequences Q_h' and Q_t'. Let $R_B = \{r_1, r_2, \ldots, r_N\} (r_i \in \{0,1,2,3\})$ be Bob's measurement results, where 0, 1, 2, 3 denote $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ respectively. Bob asks Alice to announce the measurement basis of Q_r, then he measures Q_r with the same basis to form Q_r'. Subsequently, Bob randomly inserts the particles in D_{A1} into Q_h' to form Q_h^b, and randomly inserts the particles in D_C, D_{A2} and Q_r' into Q_t' to form Q_t^b. Finally, he sends Q_t^b to Charlie.

Step 4. After Charlie receives Q_t^b, Bob announces the positions of D_C, D_{A2}, Q_r' and the states of D_C. Then Charlie measures D_C and checks the quantum channel by analyzing the error rate. If the error rate exceeds the threshold, this protocol is aborted. Otherwise, Charlie encodes his message into Q_t' by performing the unitary operations according to Equation (9). After picking out Q_r', Charlie measures this sequence with the basis announced by Alice. Next, Charlie randomly inserts the particles in D_{A2} into Q_t' (encoded sequence) to form Q_t^c. Then Charlie sends Q_t^c to Alice.

Step 5. After Alice receives Q_t^c, Charlie announces the positions and the states of D_{A2}. Alice measures D_{A2} and verifies if the transmission of Q_t^c is secure by analyzing the error rate. If no, the protocol is aborted. Otherwise, Alice picks out Q_t' which has been encoded by herself, Bob, and Charlie. Finally, Alice asks Bob to send her Q_h^b.

Step 6. After Alice receives Q_h^b, Bob announces the positions and the states of D_{A1}. Then Alice checks the quantum channel by measuring D_{A1}. If the transmission of Q_h^b is insecure, the protocol is aborted. Otherwise, after picking out D_{A1}, Alice performs Bell measurement on Q_h' and Q_t' (encoded sequence), and she records the measurement results as R_A. Alice encodes 00, 01,10,11 into $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ respectively, thus she can generate a corresponding bit string $R = \{(x_1, y_1), \ldots, (x_N, y_N)\}$ according to the initial states prepared randomly by herself in Step 1, where $x_1, y_1 \in \{0,1\}$.

Step 7. Bob announces R_B.

Step 8. Alice can obtain M_B and M_C from R_A and R_B. Then Alice announces $M = M_B \oplus M_C \oplus R$.

According to all above steps, Bob and Charlie can get the other two users' messages. Thus three parties can exchange their secret messages successfully. The simple steps can be seen in **Figure 1**. Decoding rules can be described as: 1) According to **Table 1**, Alice can know the final states in her site, which are also the initial states in Bob's site, from the initial states prepared by herself and her own operations in Step 1. Combining the final-

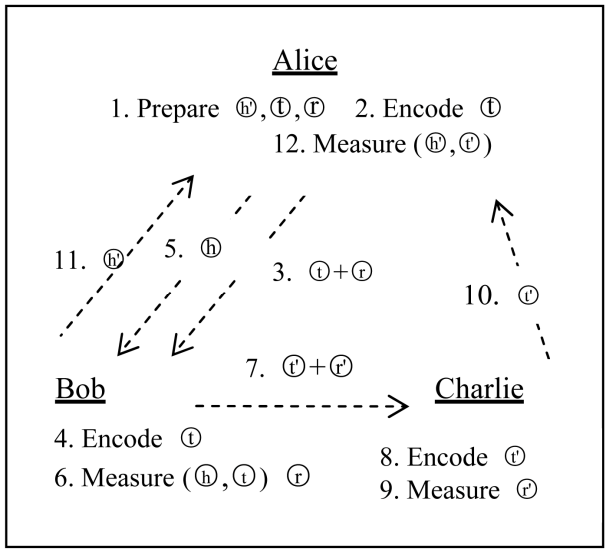

Figure 1. Qubit transmissions.

states in Bob' site (R_B), Alice can deduce Bob's operations. Thus she obtains M_B. From the initial states (R_B) and the final states (R_A) in Charlie's site, Alice deduces Charlie's operations. Thus she gets M_C; 2) Bob can deduce the final states in Alice's site from his operations and R_B, thus he can know Alice's operations from the initial states prepared by Alice (the measurement result of Q_r). Then Bob gets M_A. Bob can know R from the measurement result of Q_r and obtains $M_C = M_B \oplus M \oplus R$; 3) From the measurement result of Q_r', which is equal to that of Q_r, Charlie can know R. Then he obtains $M_B = M \oplus R \oplus M_C$. From R, Charlie gets the initial states prepared by Alice. By M_B and R_B, Charlie can deduce the initial states in Bob's site, which are also the final states in Alice's site. Thus Charlie gets M_A.

3. Security Analysis

Now, we analyze the security of our protocol in detail below. The transmission security of the particle sequences in the present 3P-QSDC scheme is similar to that of Chong *et al.*'s scheme which is based on security of Wang *et al.*'s scheme. In addition, we can see that the entangled photon pairs act as a quantum channel based on the idea of two-step transmission in our protocol. If the sequence Q_t^a is securely transmitted, Eve can not obtain any encoded information because one can not gain the secret messages from one particle of an EPR pair. On the other hand, although Q_t^a contains a sub-sequence Q_r which directly corresponds to the initial states prepared by Alice, Eve can not get any useful information about Alice's message or Bob's. This is because the decoy photons in D_{B2} are used for detecting the existence

Copyright © 2013 SciRes.

of eavesdroppers, and the communication will be aborted by Alice and Bob if the eavesdropping checks fail. In the same way, Eve can not obtain Charlie's message through Steps 4 and 5.

In our protocol, Eve can see the public information R_B and M in the classical channels. Eve wants to get some secret messages from R_B and M. Next, we first consider R_B. We take $N=1$ for example and suppose that R_B denotes $\left|\phi^+\right\rangle$. From **Table 1**, Eve can infer the final state in Alice's site and Bob's operation must be one of $\left\{\left(\left|\phi^+\right\rangle,U_0\right),\left(\left|\phi^-\right\rangle,U_3\right),\left(\left|\psi^+\right\rangle,U_1\right),\left(\left|\psi^-\right\rangle,U_2\right)\right\}$.

However, the initial states prepared by Alice in Step 1 are randomly generated. Thus, if Eve guesses $\left(\left|\phi^-\right\rangle,U_3\right)$ (similar for the other three cases), the initial states and Alice's operations must be one of $\left\{\left(\left|\phi^-\right\rangle,U_0\right),\left(\left|\phi^+\right\rangle,U_3\right),\left(\left|\psi^-\right\rangle,U_1\right),\left(\left|\psi^+\right\rangle,U_2\right)\right\}$. So there are totally sixteen possibilities, which contains $-16\times\left(1/16\right)\times\log_2\left(1/16\right)=4$ bits for Eve. On the other hand, R_B contains nothing about M_C, Eve can only explore 4 bits of secret information exchanged between Alice and Bob (each user has 2 bits). Thus Eve cannot get any information from R_B. Next, Eve may get a message correlation between three parties by combining with M. However, because R has the nature of randomness, Eve also cannot get any secret information. So all the secret bits exchanged between three parties are not leaked out from the classical channels.

4. Discussion and Conclusion

In the following, let us discuss the efficiency of the present protocol. The efficiency of a quantum communication scheme is defined as $\eta=b_s/\left(q_t+b_t\right)$ [17], where b_s denotes the expected number of secret bits received by the users, q_t is the number of transmitted qubits, and b_t is the number of needed classical bits. In CH protocol, we can see that $\eta=3N/\left(4N+2N\right)$, thus the efficiency is 50%. In our scheme, 3P-QSDC protocol can achieve higher efficiency with $\eta=6N/\left(7N+3N\right)=60\%$. For clarity, we make a comparison between CH protocol and our protocol, which can be seen in **Table 2**.

In this paper, we point out that CH protocol has a drawback of information leakage and propose a new protocol to get rid of this kind of drawback. Moreover, our scheme has higher efficiency. In summary, our protocol is efficient and secure in theory.

Table 2. Comparisons of two protocols.

CH protocol		Our protocol
Quantum resource	EPR pair	EPR pair
Message length	N	$2N$
3P-QSDC efficiency	50%	60%
Information leakage	Yes	No

5. Acknowledgements

This work was supported by the National Science Foundation of China under grant No. 61072140; the 111 Project under grant No. B08038; and the Specialized Research Fund for the Doctoral Program of Higher Education under grant No. 20100203110003.

REFERENCES

[1] G. L. Long and X. S. Liu, "Theoretically Efficient High-Capacity Quantum Key Distribution Scheme," *Physics Review A*, Vol. 65, No. 3, 2002, Article ID: 032302. doi:10.1103/PhysRevA.65.032302

[2] A Beige, B. G. Englert, C. Kurtsiefer, *et al.*, "Secure Communication with a Publicly Known Key," *Acta Physics Polonica A*, Vol. 101, No. 3, 2002, pp. 357-368.

[3] K. Boström and T. Felbinger, "Deterministic Secure Direct Communication Using Entanglement," *Physics Review Letters*, Vol. 89, No. 18, 2002, pp. 187902-187905. doi:10.1103/PhysRevLett.89.187902

[4] J. Li, H. Jin and B. Jing, "Improved Quantum 'Ping-pong' Protocol Based on GHZ State and Classical XOR Operation," *Science in China Series G*, Vol. 54, No. 9, 2011, pp. 1612-1618.

[5] F. G. Deng, G. L. Long and X. S. Liu, "Two-Step Quantum Direct Communication Protocol Using the Einstein-Podolsky-Rosen Pair Block," *Physics Review A*, Vol. 68, No. 4, 2003, Article ID: 042317. doi:10.1103/PhysRevA.68.042317

[6] F. L. Yan and X. Q. Zhang, "A Scheme for Secure Direct Communication Using EPR Pairs and Teleportation," *European Physical Journal B*, Vol. 41, No. 1, 2004, pp. 75-78. doi:10.1140/epjb/e2004-00296-4

[7] B. A. Nguyen, "Quantum Dialogue," *Physics Letters A*, Vol. 328, No. 1, 2004, pp. 6-10. doi:10.1016/j.physleta.2004.06.009

[8] X. Ji and S. Zhang, "Secure Quantum Dialogue Based on Single-Photon," *Chinese Physics*, Vol. 15, No. 7, 2006, pp. 1418-1420. doi:10.1088/1009-1963/15/7/005

[9] Y. G. Yang and Q. Y. Wen, "Quasi-Secure Quantum Dialogue Using Single Photons," *Science in China Series G*, Vol. 50, No. 5, 2007, pp. 558-562. doi:10.1007/s11433-007-0057-3

[10] X. R. Jin, X. Ji, S. Zhang, *et al.*, "Three-Party Quantum Secure Direct Communication Based on GHZ States," *Physics Letters A*, Vol. 354, No. 1-2, 2006, pp. 67-70. doi:10.1016/j.physleta.2006.01.035

[11] Z. X. Man and Y. J. Xia, "Improvement of Security of Three-Party Quantum Secure Direct Communication Based on GHZ States," *Chinese Physics Letters*, Vol. 24, No. 1, 2007, pp. 15-18. doi:10.1088/0256-307X/24/1/005

[12] A. Chamoli and C. M. Bhandari, "Secure Direct Commu-

Copyright © 2013 SciRes.

nication Based on Ping-pong Protocol," *Quantum Information Processing*, Vol. 8, No. 4, 2009, pp. 347-356. doi:10.1007/s11128-009-0112-2

[13] M. Y. Wang and F. L. Yan, "Three-Party Simultaneous Quantum Secure Direct Communication Scheme with EPR Pairs," *Chinese Physics Letters*, Vol. 24, No. 9, 2007, pp. 2486-2488. doi:10.1088/0256-307X/24/9/007

[14] S. K. Chong and T. Hwang, "The Enhancement of Three-party Simultaneous Quantum Secure Direct Communication Scheme with EPR Pairs," *Optics Communication*, Vol. 284, No. 1, 2011, pp. 515-518. doi:10.1016/j.optcom.2010.08.037

[15] F. Gao, F. Z. Guo, Q. Y. Wen, *et al.*, "Revisiting The Security of Quantum Dialogue and Bidirectional Quantum Secure Direct Communication," *Science in China Series G*, Vol. 51, No. 5, 2008, pp. 559-566. doi:10.1007/s11433-008-0065-y

[16] Y. G. Tan and Q. Y. Cai, "Classical Correlation in Quantum Dialogue," *International Journal of Quantum Information*, Vol. 6, No. 2, 2008, pp. 325-329. doi:10.1142/S021974990800344X

[17] A. Cabello, "Quantum Key Distribution in the Holevo Limit," *Physics Review Letters*, Vol. 85, No. 26, 2000, pp. 5635-5638. doi:10.1103/PhysRevLett.85.5635

Copyright © 2013 SciRes.