Efficient Three-Party Quantum Secure Direct Communication with EPR Pairs

Xunru Yin¹², Wenping Ma¹, Dongsu Shen¹, Chaoyang Hao³
¹State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an, China
²School of Mathematics and Systems Science, Taishan University, Tai’an, China
³Shandong 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.’s 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.’s 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
take $n = 1$ for example. If $X = 0, Y = 0$, then $M_4 = M_6 = M_8$. Thus, from the public classical channels, Eve can know the secret bits transmitted by three parties must be one of $\{0, 0, 0\}$, 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.,

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

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

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

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

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

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$

$$U_1 = \sigma_z = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$U_2 = i\sigma_x = |0\rangle\langle 1| - |1\rangle\langle 0|$$

$$U_3 = \sigma_x = |0\rangle\langle 0| - |1\rangle\langle 1|$$

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

$$M_4 = \{(i_s, j_s), (i_z, j_z), \ldots, (i_N, j_N)\}$$

$$M_6 = \{(k_s, l_s), (k_z, l_z), \ldots, (k_N, l_N)\}$$

$$M_8 = \{(p_s, q_s), (p_z, q_z), \ldots, (p_N, q_N)\}$$

where $i_s, j_s, k_s, l_s, p_s, q_s \in \{0, 1\}$.

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

$$U_0 \leftrightarrow 00, U_1 \leftrightarrow 01, U_2 \leftrightarrow 10, U_3 \leftrightarrow 11.$$ (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 $Q_r$, where $h(t)$ denotes the first (the second) particle in each pair. She encodes her message into $Q_r$ by performing the operation $U_i (i = 0, 1, 2, 3)$ according to Equation (9). Alice prepares five sets of decoy photons, $D_{B_1}, D_{B_2}, D_{C_1}, D_{D_1}$ and $D_{D_2}$, randomly chosen from $|0\rangle, |1\rangle, |+\rangle, |\rangle$, and $|\rangle$. Moreover, she generates single photon sequence $Q_s$, in which the particles is defined a one-to-one correspondence with the initial states prepared by herself, i.e.,

$$|0\rangle \leftrightarrow |\phi^\prime\rangle, |1\rangle \leftrightarrow |\phi^\prime\rangle, |+\rangle \leftrightarrow |\psi^\prime\rangle, |\rangle \leftrightarrow |\psi^\prime\rangle.$$ (9)

Then Alice randomly inserts all particles in $D_{B_1}$ and $D_{D_2}$ into $Q_h$. She randomly inserts all particles in $D_{B_2}, D_{C_1}, D_{D_2}$ and $Q_r$ into $Q_s$ to form $Q^\ast$. Finally, Alice sends $Q^\ast$ to Bob.

Step 2. After Bob receives $Q^\ast$, Alice announces the positions of $D_{B_2}, D_{C_1}, D_{D_2}, Q_s$ and the states of $D_{B_2}$. Then Bob measures the particles in $D_{B_2}$ by using basis $\sigma_z$ or $\sigma_x$. He can judge if the quantum channel is secure by analyzing the error rate. If no, Bob aborts the communication. Otherwise, after picking out $Q_h$, he encodes his message into $Q_r$ by performing the operation $U_i (i = 0, 1, 2, 3)$ according to Equation (9). After that, Bob asks Alice to send him $Q^\ast$.

Step 3. After Bob receives $Q^\ast$, Alice announces the positions of $D_{B_1}, D_{D_1}$ and the states of $D_{B_1}$. Then Bob measures $D_{B_1}$ and checks the quantum channel by analyzing the error rate. If the error rate exceeds the threshold.

<table>
<thead>
<tr>
<th>Table 1. Encoding of the present protocol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial state</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$</td>
</tr>
<tr>
<td>$</td>
</tr>
</tbody>
</table>

Copyright © 2013 SciRes.
old, this protocol is aborted. Otherwise, Bob picks out \( Q_a \) and performs Bell measurements on \( Q_a \) and \( Q \) (encoded sequence), which forms two new sequences \( Q'_b \) and \( Q'_c \). Let \( R_a = \{ r_1, r_2, \ldots, r_N \} (r_i \in \{ 0, 1, 2, 3 \}) \) be Bob’s measurement results, where 0, 1, 2, 3 denote \( \{ \phi^+, \phi^-, \psi^+, \psi^- \} \) respectively. Bob asks Alice to announce the measurement basis of \( Q_a \), then he measures \( Q_a \) with the same basis to form \( Q'_a \). Subsequently, Bob randomly inserts the particles in \( D_{a2} \) into \( Q'_a \) to form \( Q''_a \), and randomly inserts the particles in \( D_{c1}, D_{c2} \) and \( Q'_c \) into \( Q'_c \) to form \( Q''_c \). Finally, he sends \( Q''_c \) to Charlie.

Step 4. After Charlie receives \( Q''_c \), Bob announces the positions of \( D_{c1}, D_{c2}, Q'_c \) and the states of \( D_{c1} \). Then Charlie measures \( D_{c1} \) 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 \( Q'_c \) by performing the unitary operations according to Equation (9). After picking out \( Q'_c \), Charlie measures this sequence with the basis announced by Alice. Next, Charlie randomly inserts the particles in \( D_{c2} \) into \( Q''_c \) (encoded sequence) to form \( Q''_c \). Then Charlie sends \( Q''_c \) to Alice.

Step 5. After Alice receives \( Q''_c \), Charlie announces the positions and the states of \( D_{a2} \). Alice measures \( D_{a2} \) and verifies if the transmission of \( Q''_c \) is secure by analyzing the error rate. If no, the protocol is aborted. Otherwise, Alice picks out \( Q'_c \) which has been encoded by herself, Bob, and Charlie. Finally, Alice asks Bob to send her \( Q'_b \).

Step 6. After Alice receives \( Q'_b \), Bob announces the positions and the states of \( D_{a1} \). Then Alice checks the quantum channel by measuring \( D_{a1} \). If the transmission of \( Q'_b \) is insecure, the protocol is aborted. Otherwise, after picking out \( D_{a1} \), Alice performs Bell measurement on \( Q'_b \) and \( Q'_c \) (encoded sequence), and she records the measurement results as \( R_a \). Alice encodes 00, 01, 10, 11 into \( \{ \phi^+, \phi^-, \psi^+, \psi^- \} \) respectively, thus she can generate a corresponding bit string \( R = \{(x_1, y_1), (x_2, y_2)\} \) according to the initial states prepared randomly by herself in Step 1, where \( x_1, y_1 \in \{0, 1\} \).

Step 7. Bob announces \( R_a \).

Step 8. Alice can obtain \( M_B \) and \( M_C \) from \( R_a \) and \( R_a \). 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-states in Bob’s site \( R_B \), Alice can deduce Bob’s operations. Thus she obtains \( M_B \). From the initial states \( R_B \) and the final states \( R_B \) 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 \( Q_a \)). Then Bob gets \( M_A \). Bob can know \( R \) from the measurement result of \( Q_B \) and obtains \( M_C = M_B \oplus M \oplus R \); 3) From the measurement result of \( Q'_c \), which is equal to that of \( Q_a \), 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 \( Q''_c \) 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 \( Q''_c \) contains a sub-sequence \( Q \), 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.

---

**Figure 1. Qubit transmissions.**

1. Prepare \( \odot, \odot, \odot \)
2. Encode \( \odot \)
3. \( \odot \)
4. Encode \( \odot \)
5. \( \odot \)
6. Measure \( \odot, \odot \)
7. \( \odot \)
8. Encode \( \odot \)
9. Measure \( \odot \)
10. \( \odot \)
11. \( \odot \)
12. Measure \( \odot, \odot \)

---

**Table 1**

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \odot )</td>
<td>( \odot )</td>
</tr>
<tr>
<td>( \odot )</td>
<td>( \odot )</td>
</tr>
<tr>
<td>( \odot )</td>
<td>( \odot )</td>
</tr>
<tr>
<td>( \odot )</td>
<td>( \odot )</td>
</tr>
</tbody>
</table>

**Figure 1.** Qubit transmissions.
of eavesdroppers, and the communication will be aborted by Alice and Bob if the eavesdropping checks fail. In the same way, Eve cannot obtain Charlie’s message through Steps 4 and 5.

In our protocol, Eve can see the public information $R_q$ and $M$ in the classical channels. Eve wants to get some secret messages from $R_q$ and $M$. Next, we first consider $R_q$. We take $N = 1$ for example and suppose that $R_q$ denotes $\{\phi^+\}$. From Table 1, Eve can infer the final state in Alice’s site and Bob’s operation must be one of $\{(|\phi^+\rangle, U_0), (|\phi^+\rangle, U_1), (|\phi^-\rangle, U_0), (|\phi^-\rangle, U_1)\}$. However, the initial states prepared by Alice in Step 1 are totally sixteen possibilities, which contains $-16 \times (1/16) \times \log_2 (1/16) = 4$ bits for Eve. On the other hand, $R_q$ 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 $R_q$. 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 $\eta = \frac{b_1}{(q_e + b_1)}$ [17], where $b_1$ denotes the expected number of secret bits received by the users, $q_e$ is the number of transmitted qubits, and $b_1$ is the number of needed classical bits. In CH protocol, we can see that $\eta = 3N/(4N + 2N)$, thus the efficiency is 50%. In our scheme, 3P-QSDC protocol can achieve higher efficiency with $\eta = 6N/(7N + 3N) = 60\%$. 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.

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


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


