doi:10.3788/gzxb20144305.0502701

基于 Bell 态和 Bell 测量的无信息泄露受控双向量子安全直接通信

叶天语

(浙江工商大学 信息与电子工程学院, 杭州 310018)

摘 要:提出一个无信息泄露的受控双向量子安全直接通信协议.协议中合法通信双方 Alice 和 Bob 在控制者 Charlie 的控制下实现彼此秘密信息的安全交换,利用 3 个 Bell 态纠缠交换后的测量相关性来克服信息泄露问题.由于该协议仅利用 Bell 态作为量子资源,而且仅需要进行 Bell 测量,所以方便实现.安全性分析表明,该协议不仅能检测到外部窃听者的主动攻击,而且还能检测到控制者 Charlie 的不诚实行为,因此,具备良好的安全性.

关键词:受控双向量子安全直接通信;信息泄露;纠缠交换;Bell 态;Bell 测量

中图分类号:O431.2 **文献标识码**:A **文章编号**:1004-4213(2014)05-0502701-6

Controlled Bidirectional Quantum Secure Direct Communication without Information Leakage Based on Bell States and Bell Measurements

YE Tian-yu

(*College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou* 310018, *China*)

Abstract: A controlled bidirectional quantum secure direct communication protocol without information leakage was proposed. In the proposed protocol, two authenticated communication parties, Alice and Bob, were able to securely exchange their secret messages simultaneously under the control of the controller, Charlie. The problem of information leakage was overcome by making full use of the measurement correlation property after entanglement swapping among three Bell states. Moreover, the proposed protocol merely took the Bell state as quantum resource and merely needed the Bell measurement so that it was convenient to implement. Security analysis shows that the proposed protocol can detect not only the active attacks from the outside eavesdropper, but also the dishonest behavior from the controller, Charlie. It can be concluded that the proposed protocol has good security.

Key words: Controlled bidirectional quantum secure direct communication; Information leakage; Entanglement swapping; Bell state; Bell measurement

OCIS Codes: 270.5568; 270.5565; 270.5585

0 Introduction

Quantum cryptography has been commonly regarded as one of the most attractive progress of quantum information processing. According to its function, quantum cryptography can be classified into several different types, such as Quantum Key Distribution (QKD)[1-4], Quantum Secure Direct Communication (QSDC)[5-9] and so on. Different from QKD, QSDC allows secret messages to be communicated directly without creating a key to encrypt them in advance. However, a lot previous

Foundation item: The National Natural Science Foundation of China (No. 11375152) and the Natural Science Foundation of Zhejiang Province (No. LQ12F02012)

First author: YE Tian-yu(1982—), male, associate professor, Ph. D. degree, mainly focuses on quantum cryptography and information hiding. Email: happyyty@aliyun.com.

Received: Jul. 22, 2013; **Accepted**: Nov. 18, 2013

QSDC protocols[5-9] can not exchange secret messages simultaneously between two authenticated communication parties, and belong to the kind of one-way communication protocol. Recently, the concept of bidirectional QSDC was put forward by Zhang *et al*.[10-12] and Nguyen[13]. Since then, bidirectional QSDC has been greatly pursued and quickly developed[14-34]. However, bidirectional QSDC may have the security loophole named as information leakage[22-24], i. e., partial of the secret messages are leaked out without any active attack. For example, the bidirectional QSDC protocols in Refs. [10-11, 13-21, 25, 31] always have the information leakage problem. Although the information leakage resistant bidirectional QSDC protocols[26-30,34] have emerged, how to solve the information leakage problem in bidirectional QSDC, especially in controlled bidirectional QSDC, still needs to be further studied at present.

In this paper, a controlled bidirectional QSDC without information leakage is proposed, which overcomes the information leakage problem by making full use of the measurement correlation property after entanglement swapping among three Bell states. Moreover, it merely takes the Bell state as quantum resource and merely needs the Bell measurement so that it is convenient to implement.

1 Controlled bidirectional QSDC without information leakage

The four Bell states are defined as

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|+\rangle+|-\rangle|-\rangle) \tag{1}$$

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|-\rangle+|-\rangle|+\rangle) \tag{2}$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|+\rangle-|-\rangle|-\rangle) \tag{3}$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)=\frac{1}{\sqrt{2}}(|+\rangle|-\rangle-|-\rangle|+\rangle) \tag{4}$$

where, $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$, $|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$. Without loss of generality, suppose that three initial Bell states are all in the state of $|\Phi^+\rangle$ (i. e., $|\Phi^+\rangle_{A_1B_1}$, $|\Phi^+\rangle_{B_2C_1}$ and $|\Phi^+\rangle_{C_2A_2}$). Alice finally holds two particles A_1 and A_2, Bob two particles B_1 and B_2, and Charlie two particles C_1 and C_2. If Alice, Bob and Charlie perform the Bell measurement on their particles, respectively, three initial Bell states will swap entanglement according to Eq. (5).

$$\begin{aligned}|\Phi^+\rangle_{A_1B_1}\otimes|\Phi^+\rangle_{B_2C_1}\otimes|\Phi^+\rangle_{C_2A_2}=\frac{1}{4}(&|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}+|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+\\
&|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}-|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+|\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+\\
&|\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}-|\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+|\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}+\\
&|\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}+|\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}-\\
&|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+|\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}-\\
&|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2})\end{aligned} \tag{5}$$

From Eq. (5), three initial Bell states collapse to sixteen different kinds of result combinations about particles A_1 and A_2, particles B_1 and B_2, and particles C_1 and C_2 with equal probability. Moreover, Alice′s measurement result of particles A_1 and A_2, Bob′s measurement result of particles B_1 and B_2 and Charlie′s measurement result of particles C_1 and C_2 are highly correlated. This character is called as the measurement correlation property after entanglement swapping among three Bell states. It is easy to know that if Charlie publishes her measurement result to Alice and Bob, according to her (his) measurement result, Alice (Bob) is able to infer the measurement result of Bob (Alice).

Alice and Bob agree on in advance that each unitary operation corresponds to two bit secret messages such as $I\rightarrow 00$, $\sigma_x\rightarrow 01$, $i\sigma_y\rightarrow 10$ and $\sigma_z\rightarrow 11$, where $I=|0\rangle\langle 0|+|1\rangle\langle 1|$, $\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$, $i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$ and $\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$. The proposed protocol is composed of the following steps.

Step 1: Preparation for the initial states. Alice produces $3N$ Bell states all in the state of $|\Phi^+\rangle$. She divides these Bell states into N groups, therefore each group has three Bell states all in the state of $|\Phi^+\rangle$ (i. e., $|\Phi^+\rangle_{A_1B_1}$, $|\Phi^+\rangle_{B_2C_1}$ and $|\Phi^+\rangle_{C_2A_2}$). Moreover, she divides the particles into six particle sequences. That is

$$S_{A_1}=\{P_1(A_1),P_2(A_1),\cdots,P_N(A_1)\},$$
$$S_{A_2}=\{P_1(A_2),P_2(A_2),\cdots,P_N(A_2)\},$$
$$S_{B_1}=\{P_1(B_1),P_2(B_1),\cdots,P_N(B_1)\},$$
$$S_{B_2}=\{P_1(B_2),P_2(B_2),\cdots,P_N(B_2)\},$$
$$S_{C_1}=\{P_1(C_1),P_2(C_1),\cdots,P_N(C_1)\},$$
$$S_{C_2}=\{P_1(C_2),P_2(C_2),\cdots,P_N(C_2)\}.$$

Step 2: Preparation for the first round security check. Alice produces four particle sets randomly in one of the four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ as the sample sets used for security check. These four particle

sets are denoted as D_{B_1}, D_{B_2}, D_{C_1} and D_{C_2}, respectively. Here, D_{B_1} (D_{B_2}) is used for security check when S_{B_1} (S_{B_2}) is transmitted from Alice to Bob, and D_{C_1} (D_{C_2}) is used for security check when S_{C_1} (S_{C_2}) is transmitted from Alice to Charlie. Alice randomly inserts D_{B_1}, D_{B_2}, D_{C_1} and D_{C_2} into S_{B_1}, S_{B_2}, S_{C_1} and S_{C_2}, respectively. Consequently, S_{B_1}, S_{B_2}, S_{C_1} and S_{C_2} turn into four new sequences S'_{B_1}, S'_{B_2}, S'_{C_1} and S'_{C_2}. Alice always makes a record of the preparation basis of the sample particles and their positions in new sequences.

Step 3: The first round transmission and security check. Alice sends two sequences S'_{B_1} and S'_{B_2} to the other communication participant Bob and two sequences S'_{C_1} and S'_{C_2} to the controller Charlie, and keeps S_{A_1} and S_{A_2} by herself. After Bob (Charlie) confirms Alice that he (she) has received the two sequenceS'_{B_1} and S'_{B_2} (S'_{C_1} and S'_{C_2}), Alice firstly publishes the positions and the corresponding preparation basis of the sample particles. Then, Bob (Charlie) measures the sample particles in the same basis as the preparation basis of Alice and tells Alice his (her) measurement results. Alice can judge whether there is an eavesdropping by comparing the initial states of the sample particles with Bob′s (Charlie′s) measurement results. If there is an eavesdropping, Alice halts the communication; otherwise, the communication goes on.

Step 4: Bell measurements after entanglement swapping and Alice′s encoding. After getting rid of the sample particles, S'_{B_1}, S'_{B_2}, S'_{C_1} and S'_{C_2} turn back into S_{B_1}, S_{B_2}, S_{C_1} and S_{C_2}, respectively. Alice picks up one particle from S_{A_1} and the corresponding particle from S_{A_2} to make up a two-particle pair. $(P_n(A_1), P_n(A_2))$ ($n=1,2,\cdots,N$) is the nth two-particle pair from S_{A_1} and S_{A_2}. Bob (Charlie) does the same thing on S_{B_1} andS_{B_2} (S_{C_1} and S_{C_2}). Then, all of them perform Bell measurements on their own two-particle pairs. In other words, Alice/Bob/Charlie measures $(P_n(A_1), P_n(A_2))$/ $(P_n(B_1), P_n(B_2))$/ $(P_n(C_1), P_n(C_2))$ with Bell basis. Consequently, after entanglement swapping, $(P_n(A_1), P_n(A_2))$/ $(P_n(B_1), P_n(B_2))$/ $(P_n(C_1), P_n(C_2))$ collapses to a new Bell state. According to her Bell-basis measurement outcome, Alice reproduces a new $(P_n(A_1), P_n(A_2))$ with no state measurement performed. Afterward, Alice performs the unitary operation $U^A_{i_n,j_n}$ on the new $(P_n(A_1), P_n(A_2))$, where (i_n, j_n) $(i_n, j_n \in \{0,1\}$, $n=1,2,\cdots,N)$ are her two bits secret messages. Consequently, $(P_n(A_1), P_n(A_2))$ turns into $U^A_{i_n,j_n}$ $(P_n(A_1), P_n(A_2))$.

Step 5: The second round transmission and security check. Alice produces two particle sets randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ as the sample sets used for security check, which are denoted as D_{A_1} and D_{A_2}, respectively. Here, D_{A_1} (D_{A_2}) is used for security check when S_{A_1} (S_{A_2}) is transmitted from Alice to Bob. Alice randomly inserts D_{A_1} and D_{A_2} into S_{A_1} and S_{A_2}, respectively. Consequently, S_{A_1} and S_{A_2} turn into two new sequences S'_{A_1} and S'_{A_2}. Alice always makes a record of the preparation basis of the sample particles and their positions in new sequences. Then, Alice sends two sequences S'_{A_1} and S'_{A_2} to Bob. After Bob confirms Alice that he has received the two sequences S'_{A_1} and S'_{A_2}, Alice firstly publishes the positions and the corresponding preparation basis of the sample particles. Then, Bob measures the sample particles in the same basis as the preparation basis of Alice and tells Alice his measurement results. Alice can judge whether there is an eavesdropping by comparing the initial states of the sample particles with Bob′s measurement results. If there is an eavesdropping, Alice halts the communication; otherwise, the communication goes on.

Step 6: Quantum dialogue. After getting rid of checking particles, two sequence S'_{A_1} and S'_{A_2} turn back into S_{A_1} and S_{A_2} again, respectively. Now, Bob has four sequences S_{A_1}, S_{A_2}, S_{B_1} and S_{B_2} in his hand. Bob performs the unitary operation $U^B_{k_n,l_n}$ on $U^A_{i_n,j_n}$ $(P_n(A_1), P_n(A_2))$, where $(k_n, l_n)(k_n, l_n \in \{0,1\}$, $n=1,2,\cdots,N)$ are his two bits secret messages. Consequently, $U^A_{i_n,j_n}(P_n(A_1), P_n(A_2))$ turns into $U^B_{k_n,l_n}$ $U^A_{i_n,j_n}(P_n(A_1), P_n(A_2))$. Then, Bob measures $U^B_{k_n,l_n}$ $U^A_{i_n,j_n}(P_n(A_1), P_n(A_2))$ with Bell basis. If Charlie permits the dialogue between Alice and Bob, she will publish her measurement result of $(P_n(C_1), P_n(C_2))$ to Bob. Therefore, according to Charlie′s announcement and his own measurement result of $(P_n(B_1), P_n(B_2))$, Bob is able to infer Alice′s measurement result of $(P_n(A_1), P_n(A_2))$. Moreover, according to his own unitary operation $U^B_{k_n,l_n}$ and his own measurement result of $U^B_{k_n,l_n}$ $U^A_{i_n,j_n}$ $(P_n(A_1), P_n(A_2))$, Bob is able to know Alice′s two bits. On the other hand, Bob does not publish his measurement result of $U^B_{k_n,l_n}U^A_{i_n,j_n}(P_n(A_1), P_n(A_2))$ to Alice until he has heard from Charlie′s announcement of $(P_n(C_1), P_n(C_2))$. According to her own measurement result of $(P_n(A_1), P_n(A_2))$, her own unitary operation $U^A_{i_n,j_n}$ and the announcement of measurement result on $U^B_{k_n,l_n}U^A_{i_n,j_n}(P_n(A_1), P_n(A_2))$ from Bob, Alice is able to infer Bob′s two bits. If Charlie does not permit the dialogue between Alice and Bob, she will not publish her measurement result of $(P_n(C_1), P_n(C_2))$ to Bob. Consequently, Bob is unable to know Alice′s measurement result of

$(P_n(A_1),P_n(A_2))$. Moreover, Bob does not publish his measurement result of $U^{B}_{k_n l_n}U^{A}_{i_n j_n}(P_n(A_1),P_n(A_2))$ to Alice. Therefore, the dialogue between Alice and Bob is halted.

Suppose that Alice′s two bits are 11, and Bob′s two bits are 10. Take the first two-particle pair for example to explicitly explain the dialogue process. Alice/Bob/Charlie measures $(P_1(A_1),P_1(A_2))$/ $(P_1(B_1),P_1(B_2))$/ $(P_1(C_1),P_1(C_2))$ with Bell basis. Consequently, after entanglement swapping, $(P_1(A_1),P_1(A_2))$, $(P_1(B_1),P_1(B_2))$ and $(P_1(C_1),P_1(C_2))$ collapse to $|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}$, $|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}$, $|\Phi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}$, $|\Phi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}$, $|\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}$, $|\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}$, $|\Phi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}$, $|\Phi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}$, $|\Psi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}$, $|\Psi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}$, $|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}$, $|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}$, $|\Psi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}$, $|\Psi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}$, $|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}$ or $|\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}$, each with probability 1/16. Without loss of generality, suppose that $(P_1(A_1),P_1(A_2))$, $(P_1(B_1),P_1(B_2))$ and $(P_1(C_1),P_1(C_2))$ collapse to $|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}$ after entanglement swapping. According to her Bell-basis measurement outcome, Alice reproduces a new $|\Phi^+\rangle_{A_1A_2}$ with no state measurement performed. Afterward, Alice performs the unitary operation σ_z on the new $|\Phi^+\rangle_{A_1A_2}$ to encode her two bits. Consequently, $|\Phi^+\rangle_{A_1A_2}$ turns into $|\Phi^-\rangle_{A_1A_2}$. After Bob has four sequences S_{A_1}, S_{A_2}, S_{B_1} and S_{B_2} in his hand, he performs the unitary operation $i\sigma_y$ on $|\Phi^-\rangle_{A_1A_2}$ to encode his two bits. Consequently, $|\Phi^-\rangle_{A_1A_2}$ turns into $|\Psi^+\rangle_{A_1A_2}$. Then, Bob measures $|\Psi^+\rangle_{A_1A_2}$ with Bell basis. If Charlie permits the dialogue between Alice and Bob, Charlie publishes Bob that her measurement result of $(P_1(C_1),P_1(C_2))$ is $|\Phi^-\rangle_{C_1C_2}$. Since his own measurement result of $(P_1(B_1),P_1(B_2))$ is $|\Phi^-\rangle_{B_1B_2}$, Bob can know that Alice′s measurement result of $(P_1(A_1),P_1(A_2))$ is $|\Phi^+\rangle_{A_1A_2}$. Moreover, since his own measurement result of $i\sigma_y\otimes\sigma_z$ $(P_1(A_1),P_1(A_2))$ is $|\Psi^+\rangle_{A_1A_2}$, according to his own unitary operation $i\sigma_y$, Bob is able to know that Alice′s two bits are 11. On the other hand, Bob publishes Alice that his measurement result of $i\sigma_y\otimes\sigma_z$ $(P_1(A_1),P_1(A_2))$ is $|\Psi^+\rangle_{A_1A_2}$, after he has heard from Charlie′s announcement of $(P_1(C_1),P_1(C_2))$. Since her own measurement result of $(P_1(A_1),P_1(A_2))$ is $|\Phi^+\rangle_{A_1A_2}$, according to her own unitary operation σ_z, Alice is able to infer that Bob′s two bits are 10.

2 Security analysis

It is well known that the security of a quantum secret communication protocol highly depends on the security check process. An effective security check process should have two criterions[35]: 1) if there is no eavesdropping, the false alarm probability will be 0; 2) if there is an eavesdropping, it can discover the eavesdropping behavior with enough high detection probability. In the proposed protocol, both the first round and the second round security check use particles randomly prepared in one of the four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ as sample particles, which is derived from the idea of the BB84 QKD protocol[1]. Without loss of generality, take S'_{B_1} sent from Alice to Bob for example to analyze the effectiveness of the security check processes. Obviously, its false alarm probability is equal to 0 when there is no eavesdropping. Then, the detection probability towards general attacks, such as the intercept-resend attack, the measure-resend attack and the entangle-and- measure attack, should be analyzed. Just as pointed out in Refs. [20, 31], all of these general attacks can be discovered with enough high detection probability by using sample particles randomly prepared in one of the four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. It can be concluded that the security check processes of the proposed protocol are effective, according to the two criterions suggested in Ref. [35].

In addition, with regard to the security of the proposed protocol, besides considering an outside eavesdropper Eve, it is necessary to consider the dishonesty of the controller Charlie. There are two round security checks in the proposed protocol. However, Charlie only joins in the first one. During the first round security check, Alice always makes a record of the preparation basis of the sample particles in D_{C_1} and D_{C_2} and their positions in S'_{C_1} and S'_{C_2}, and publishes the positions and the corresponding preparation basis of the sample particles to Charlie at first. Then, Charlie measures the sample particles in the same basis as the preparation basis of Alice and tells Alice her measurement results. Alice judges whether there is an eavesdropping by comparing the initial states of the sample particles with Charlie′s measurement results. Obviously, any dishonest behavior from Charlie will result in the inconsistency between the measurement results of sample particles and their initial states, thus it can be easily discovered by Alice.

3 Discussions

3.1 The information leakage problem

Due to the measurement correlation property after entanglement swapping among three Bell states, Bob will be able to deduce the state of $(P_n(A_1),P_n(A_2))$

if Charlie publishes her measurement result of $(P_n(C_1), P_n(C_2))$. Therefore, it is not necessary for Alice to publish her measurement result of $(P_n(A_1), P_n(A_2))$ to Bob, which makes Eve have no access to $(P_n(A_1), P_n(A_2))$. As a result, as to Eve, Bob′s announcement of measurement result on $U^B_{k_n l_n} U^A_{i_n j_n}$ $(P_n(A_1), P_n(A_2))$ means totally 4×4 kinds of unitary operation combinations performed by Alice and Bob. It means that the quantum channel contains $-\sum_{i=1}^{16} p_i \log_2 p_i = -16 \times \frac{1}{16} \log_2 \frac{1}{16} = 4$ bits for Eve, which are equal to the total amount of secret messages from Alice and Bob. Therefore, no information leakage happens in the proposed protocol. Apparently, the reason why it can avoid the information leakage problem lies in making full use of the measurement correlation property after entanglement swapping among three Bell states.

3.2 Comparison with those previous controlled quantum dialogue protocols

Since all of the protocols in Refs. [16,31] and the proposed protocol belong to the kind of controlled bidirectional QSDC, a comparison among them is drawn here.

As analyzed above, the proposed protocol can avoid the information leakage problem. However, all of the protocols in Ref. [16] and Ref. [31] have the information leakage problem. In Ref. [16], each GHZ state can be used for the transmission of 4 bits (2 for Alice and 2 for Bob), where 3 bits are leaked out to Eve. In the first protocol of Ref. [31], each GHZ state can be also used for the transmission of 4 bits (2 for Alice and 2 for Bob), where 3 bits are leaked out to Eve. In the second protocol of Ref. [31], each Bell state can be used for the transmission of 4 bits (2 for Alice and 2 for Bob), where 2 bits are leaked out to Eve.

On the other hand, the protocol in Ref. [16] and the first protocol in Ref. [31] take the GHZ state as quantum resource. Moreover, both the protocol in Ref. [16] and the first protocol in Ref. [31] need the GHZ measurement. It is well known that the generation of GHZ state and the implementation of GHZ measurement are much more complicated than those of Bell state and Bell measurement, respectively. Therefore, it can be concluded that, generally speaking, compared with the protocols in Refs. [16, 31], the advantage of the proposed protocol lies in having the following two characters simultaneously: 1) no information leakage happens in the proposed protocol; 2) the proposed protocol merely takes the Bell state as quantum resource and merely needs the Bell measurement, thus it is more convenient to implement.

In addition, since the proposed protocol has no information leakage problem, a comparison between it and the previous ordinary information leakage resistant bidirectional QSDC protocols may be needed. Without loss of generality, take the protocol in Ref. [28] for example. Obviously, there are some major differences between the proposed protocol and the protocol in Ref. [28]. 1) They belong to different kinds of bidirectional QSDC. The former one is a controlled bidirectional QSDC, while the latter one is an ordinary bidirectional QSDC. 2) The number of participants is different. The former one has three participants, while the latter one only has two participants. 3) The method for avoiding the information leakage problem is different. The former one uses the measurement correlation property after entanglement swapping among three Bell states to resist it, while the latter one uses the correlation extractability of Bell state and the auxiliary particle to avoid it. 4) The total number of secret messages transmitted in each round is different. The former one transmits four bits each round, while the latter one only transmits three bits each round. 5) The encoding method for secret is different. The former encodes both Alice′s and Bob′s secret by performing unitary operation on Bell state, while the latter encodes Bob′s secret by performing unitary operation on Bell state and transmits Alice′s secret by means of deterministic secure quantum communication. 6) The former one merely needs the Bell measurement, while the latter one needs both the Bell measurement and the single-particle measurement. 7) The security check method used is different. The former one uses sample particles randomly prepared in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to check eavesdropping in both the first round and the second round security check, while the latter one uses the entanglement correlation between two particles from Bell states in the first and the third round, the measurement of Bell states in the second round and the checking message authentication in the forth round. Therefore, it can be concluded that compared with the protocol in Ref. [28], the proposed protocol is a brand new controlled bidirectional QSDC protocol.

4 Conclusions

To sum up, a controlled bidirectional QSDC without information leakage based on Bell states and Bell measurements is proposed in this paper. Two authenticated communication parties, Alice and Bob, can securely exchange their secret messages simultaneously under the control of the controller named Charlie. The problem of information leakage is

overcome by making full use of the measurement correlation property after entanglement swapping among three Bell states. Moreover, it merely takes the Bell state as quantum resource and merely needs the Bell measurement. Therefore, it is convenient to implement.

References

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public-key distribution and coin tossing[C]. Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 1984, 11: 175-179.

[2] BENNETT C H, BRASSARD G, MERMIN N D. Quantum cryptography without Bell theorem [J]. *Physical Review Letters*, 1992, **68**: 557.

[3] CABELLO A. Quantum key distribution in the Holevo limit [J]. *Physical Review Letters*, 2000, **85**: 5635.

[4] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. *Physical Review A*, 2002, **65**: 032302.

[5] BEIGE A, ENGLERT B G, KURTSIEFER C, *et al*. Secure communication with a publicly known key[J]. *Acta Physica Polonica A*, 2002, **101**: 357.

[6] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. *Physical Review A*, 2003, **68**: 042317.

[7] CAI Q Y, LI B W. Improving the capacity of the Bostrom-Felbinger protocol [J]. *Physical Review A*, 2004, **69**: 054301.

[8] CHEN X B, WANG T Y, DU J Z, *et al*. Controlled quantum secure direct communication with quantum encryption [J]. *International Journal of Quantum Information*, 2008, **6**(3): 543-551.

[9] CHEN X B, WEN Q Y, GUO F Z, *et al*. Controlled quantum secure direct communication with W state[J]. *International Journal of Quantum Information*, 2008, **6**(4): 899-906.

[10] ZHANG Z J, MAN Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block[EB/OL]. [2013-07-22]. http://arxiv. org/pdf/quant-ph/0403215. pdf.

[11] ZHANG Z J, MAN Z X. Secure bidirectional quantum communication protocol without quantum channel [EB/OL]. [2013-07-22]. http://arvix. org/pdf/quant-ph/0403217. pdf.

[12] ZHANG Z J, MAN Z X, LI Y. Economically improving message-unilaterally-transmitted quantum secure direct communication to realize two-way communication [EB/OL]. [2013-07-22]. http://arvix. org/pdf/quant-ph/0406181. pdf.

[13] NGUYEN B A. Quantum dialogue[J]. *Physics Letters A*, 2004, **328**(1): 6-10.

[14] MAN Z X, ZHANG Z J, LI Y. Quantum dialogue revisited [J]. *Chinese Physics Letters*, 2005, **22**(1): 22-24.

[15] JIN X R, JI X, ZHANG Y Q, ZHANG S, *et al*. Three-party quantum secure direct communication based on GHZ states [J]. *Physics Letters A*, 2006, **354**(1-2): 67-70.

[16] MAN Z X, XIA Y J. Controlled bidirectional quantum direct communication by using a GHZ state[J]. *Chinese Physics Letters*, 2006, **23**(7): 1680-1682.

[17] MAN Z X, XIA Y J, NGUYEN B A. Quantum secure direct communication by using GHZ states and entanglement swapping[J]. *Journal of Physics B*, 2006, **39**: 3855-3863.

[18] JI X, ZHANG S. Secure quantum dialogue based on single-photon[J]. *Chinese Physics*, 2006, **15**(7): 1418-1420.

[19] MAN Z X, XIA Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states [J]. *Chinese Physics Letters*, 2007, **24**(1): 15-18.

[20] CHEN Y, MAN Z X, XIA Y J. Quantum bidirectional secure direct communication via entanglement swapping[J]. *Chinese Physics Letters*, 2007, **24**(1): 19-22.

[21] YANG Y G, WEN Q Y. Quasi-secure quantum dialogue using single photons[J]. *Science in China Series G*, 2007, **50**(5): 558-562.

[22] GAO F, QIN S J, WEN Q Y, *et al*. Comment on: "Three-party quantum secure direct communication based on GHZ states"[J]. *Physics Letters A*, 2008, **372**(18): 3333-3336.

[23] GAO F, GUO F Z, WEN Q Y, *et al*. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication[J]. *Science in China Series G*, 2008, **51**(5): 559-566.

[24] TAN Y G, CAI Q Y. Classical correlation in quantum dialogue [J]. *International Journal of Quantum Information*, 2008, **6**(2): 325-329.

[25] SHAN C J, LIU J B, CHENG W W, *et al*. Bidirectional quantum secure direct communication in driven cavity QED [J]. *Modern Physics Letters B*, 2009, **23**(27): 3225-3234.

[26] SHI G F, XI X Q, TIAN X L, *et al*. Bidirectional quantum secure communication based on a shared private Bell state[J]. *Optics Communications*, 2009, **282**(12): 2460-2463.

[27] SHI G F, XI X Q, HU M L, *et al*. Quantum secure dialogue by using single photons[J]. *Optics Communications*, 2010, **283**(9): 1984-1986.

[28] SHI G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles[J]. *Optics Communications*, 2010, **283**(24): 5275-5278.

[29] GAO G. Two quantum dialogue protocols without information leakage[J]. *Optics Communications*, 2010, **283**(10): 2288-2293.

[30] WANG H, ZHANG Y Q, HU Y P, *et al*. Two quantum dialogue schemes based on Bell states and two-qutrit entangled states without information leakage [J]. *Journal of National University of Defense Technology*, 2012, **34**(2): 10-13.

[31] YE T Y, JIANG L Z. Improvement of controlled bidirectional quantum direct communication using a GHZ state[J]. *Chinese Physics Letters*, 2013, **30**(4): 040305.

[32] LIU Z H, CHEN H W. Comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state"[J]. *Chinese Physics Letters*, 2013, **30**(7): 079901.

[33] YE T Y, JIANG L Z. Reply to the comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state" [J]. *Chinese Physics Letters*, 2013, **30**(7): 079902.

[34] YE T Y. Large payload bidirectional quantum secure direct communication without information leakage[J]. *International Journal of Quantum Information*, 2013, **11**(5): 1350051.

[35] YE T Y, JIANG L Z. False alarm probability of eavesdropping checks for controllable quantum secret sharing [J]. *Acta Photonica Sinica*, 2012, **41**(9): 1113-1117.