doi:10.3788/gzxb20134211.1311

利用纠缠交换后的测量相关性和降低传输效率防止量子对话发生信息泄露

叶天语,蒋丽珍

(浙江工商大学 信息与电子工程学院,杭州 310018)

摘 要:针对量子对话协议信息泄露导致的安全威胁,提出一个无信息泄露的受控量子对话协议,使控制者 Alice 能够控制 Bob 和 Charlie 通信双方之间的双向通信.该协议充分利用两个最大纠缠的 GHZ 态纠缠交换后的测量相关性和降低传输效率来防止信息发生泄露;同时,不需要进行 GHZ 基测量而只需要进行 Bell 基测量.安全性分析表明,该协议能够检测到外部窃听者发起的截获-重发、测量-重发和纠缠-测量等主动攻击.

关键词:量子对话;双向量子安全直接通信;信息泄露;纠缠交换;测量相关;传输效率

中图分类号:O431.2 **文献标识码**:A **文章编号**:1004-4213(2013)11-1311-8

Information Leakage Prevention in Quantum Dialogue Using the Measurement Correlation after Entanglement Swapping and Decreasing the Transmission Efficiency

YE Tian-yu, JIANG Li-zhen

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

Abstract: In order to solve the security threat of information leakage in quantum dialogue protocols, a controlled quantum dialogue protocol without information leakage was proposed, where the controller Alice controlled the bidirectional communication between two communication parties, Bob and Charlie. The problem of information leakage was avoided by making full use of the measurement correlation property after entanglement swapping between two maximally entangled GHZ states and decreasing the transmission efficiency. Moreover, the Bell-basis measurement rather than the GHZ-basis measurement was needed. Security analysis shows that the active attacks from an outside eavesdropper can be detected, such as the intercept-resend attack, the measurement-resend attack and the entanglement-and-measurement attack.

Key words: Quantum dialogue; Bidirectional quantum secure direct communication; Information leakage; Entanglement swapping; Measurement correlation; Transmission efficiency

0 Introduction

Quantum key distribution (QKD), which was proposed by Bennett and Brassard first [1], is an ingenious application of quantum mechanics. It always uses the quantum mechanics principles rather than the difficulty of computation to guarantee the security of secret messages. The basic idea of QKD is that two remote authorized users can establish a shared secret key between them through the transmission of quantum signals. Since the first QKD was put forward, it has attracted a lot of attentions[2-4]. In the meanwhile, the concept of quantum secure direct

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: Apr. 16, 2013; **Accepted**: Jun. 1, 2013

communication (QSDC) has also been proposed, which offers confidential transmission of classic information over a quantum channel without prior key agreement. Since the pioneering QSDC was proposed by Beige *et al.*[5] in 2002, a lot of QSDC protocols[6-10] have been put forward. However, these protocols are one-way communication protocols, where the two parties can not exchange their secret messages simultaneously. Fortunately, the concept of quantum dialogue was proposed by Zhang *et al.*[11-13] and Nguyen[14] in 2004. Subsequently, Man *et al.*[15] pointed out that Nguyen′ protocol is unsafe towards the intercept-and-resend attack and gave a possible solution. In 2006, Jin *et al.*[16] presented a three-party simultaneous QSDC based on a maximally entangled GHZ state; Man and Xia[17] put forward a controlled bidirectional QSDC by using a maximally entangled GHZ state. In 2007, Man and Xia[18] firstly pointed out that Jin′s s protocol[16] has a problem of definite information leakage then proposed an improved version; Chen *et al.*[19] presented a bidirectional QSDC based on entanglement swapping of two maximally entangled Bell sates; Yang and Wen[20] proposed a quasi-secure quantum dialogue protocol based on a single photon; Xia *et al.*[21] put forward a controlled quantum dialogue using a pure entangled GHZ state. In 2008, Gao *et al.*[22] illustrated the information leakage problem in both Jin′ s protocol[16] and Man′s improved version[18] from the point of information theory and cryptography. In 2009, Shi *et al.*[23] put forward a quantum dialogue protocol without information leakage by using the auxiliary maximally entangled Bell state. In 2010, Shi *et al.*[24] put forward a quantum dialogue protocol without information leakage by using the auxiliary single photon; Shi[25] proposed a bidirectional QSDC without information leakage based on the auxiliary particle and the correlation extractability of maximally entangled Bell state. In 2013, Ye and Jiang[26] put forward two approaches to successfully solve the definite information leakage problem in Man′s protocol[17]. However, the two protocols in Ref. [26] still have the information leakage problem[27-28]. Moreover, in fact, all of the quantum dialogue protocols in Refs. [11-12,14-15,19-21] also still have the information leakage problem.

In this paper, we propose a controlled quantum dialogue without information leakage, where the controller Alice controls the bidirectional communication between two communication parties, Bob and Charlie. It prevents the information leakage problem by making full use of the measurement correlation property after entanglement swapping between two GHZ states and decreasing the transmission efficiency. Moreover, it merely needs the Bell-basis measurement (BM) rather than the GHZ-basis measurement (GM). Furthermore, its security can be guaranteed.

1 Controlled bidirectional QSDC without information leakage

Consider the following scenario. The administrative personnel of the server named Alice, wants to control the secret mutual correspondence between two users, Bob and Charlie. We put forward a controlled quantum dialogue to accomplish this task. Without loss of generality, our protocol uses the maximally entangled GHZ state $|\Psi\rangle$ as quantum resource, which is defined as

$$|\Psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)=\frac{1}{2}[(|+\rangle|+\rangle+|-\rangle|-\rangle)|+\rangle+(|+\rangle|-\rangle+|-\rangle|+\rangle)|-\rangle] \quad (1)$$

where $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$. Suppose that two initial maximally entangled GHZ states are both in the state of $|\Psi\rangle$ (i. e., $|\Psi\rangle_{A_1B_1C_1}$ and $|\Psi\rangle_{A_2B_2C_2}$). Alice finally holds two particles A_1 and A_2, Bob holds two particles B_1 and B_2, and Charlie holds two particles C_1 and C_2. If Alice, Bob and Charlie perform BM on their own particles, two initial maximally entangled GHZ states will swap entanglement according to Eq. (2).

$$\begin{aligned}|\Psi\rangle_{A_1B_1C_1}\otimes|\Psi\rangle_{A_2B_2C_2}=&(\frac{1}{\sqrt{2}})^3[|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}\cdot\\&|\Phi^+\rangle_{C_1C_2}+|\Phi^+\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+\\&|\Phi^-\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2}|\Phi^-\rangle_{C_1C_2}+|\Phi^-\rangle_{A_1A_2}\cdot\\&|\Phi^-\rangle_{B_1B_2}|\Phi^+\rangle_{C_1C_2}+|\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}\cdot\\&|\Psi^+\rangle_{C_1C_2}+|\Psi^+\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+\\&|\Psi^-\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2}|\Psi^-\rangle_{C_1C_2}+|\Psi^-\rangle_{A_1A_2}\cdot\\&|\Psi^-\rangle_{B_1B_2}|\Psi^+\rangle_{C_1C_2}]\end{aligned} \quad (2)$$

where, $|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$ and $|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)$ are four maximally entangled Bell states. Note that one maximally entangled Bell state can be transformed into another after performed with unitary operations on its any particle. The transformation relations between any two maximally entangled Bell states are listed in

Table 1, 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 $\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$ are four unitary operations. According to Eq. (2), two initial maximally entangled GHZ states collapse to eight outcome combinations of 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 BM outcome of particles A_1 and A_2, Bob′s BM outcome of particles B_1 and B_2 and Charlie′s BM outcome of particles C_1 and C_2 are highly correlated. We call this character "the measurement correlation property after entanglement swapping between two maximally entangled GHZ states". It means that, if Alice publishes her BM outcome to Bob and Charlie, according to his (her) own BM outcome, Bob (Charlie) is able to infer the BM outcome of Charlie (Bob).

Table 1 The transformation relations between any two maximally entangled Bell states (The states in column denote the initial states, and the states in row denote the transformation outcomes)

	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\|\Phi^+\rangle$	I	σ_z	σ_x	$i\sigma_y$
$\|\Phi^-\rangle$	σ_z	I	$i\sigma_y$	σ_x
$\|\Psi^+\rangle$	σ_x	$i\sigma_y$	I	σ_z
$\|\Psi^-\rangle$	$i\sigma_y$	σ_x	σ_z	I

Suppose that Bob has N bits secret messages $\{i_1, i_2, \cdots, i_N\}$ and Charlie has N bits secret messages $\{k_1, k_2, \cdots, k_N\}$, where $i_n, k_n \in \{0,1\}$, $n \in \{1,2,\cdots,N\}$. As it is mentioned above, there are totally four unitary operations. However, in the proposed protocol, only two unitary operations, I and σ_z, are used for encoding secret messages by both Bob and Charlie. Let each unitary operation correspond to one-bit secret message. That is, $\{I \to 0, \sigma_z \to 1\}$. The controlled quantum dialogue is now illustrated in detail as follows.

Step1: Preparation for the initial states. Alice prepares $2N+P+Q$ maximally entangled GHZ states all in the state of $|\Psi\rangle$. Each maximally entangled GHZ state is denoted as $[A_n, B_n, C_n]$ $(n=1,2,\cdots,2N+P+Q)$. She classifies all particles into three ordered particle sequences. That is, $S_A=\{A_1, A_2, \cdots, A_{2N+P+Q}\}$, $S_B=\{B_1, B_2, \cdots, B_{2N+P+Q}\}$ and $S_C=\{C_1, C_2, \cdots, C_{2N+P+Q}\}$. Then she sends S_C to Charlie and keeps S_A and S_B by herself.

Step2: The first security checking. Charlie confirms Alice that she has received S_C at first. Then Charlie randomly selects Q particles from S_C and measures them randomly with Z-basis ($\{|0\rangle, |1\rangle\}$) or X-basis ($\{|+\rangle, |-\rangle\}$). Charlie publishes the positions and the measurement basis of these particles to Alice. Alice uses the same measurement basis as Charlie to measure the corresponding particles in S_A and S_B, respectively. Charlie makes Alice publish her measurement outcomes at first. Then, Charlie publishes her own measurement outcomes. If there is no eavesdropping, their measurement outcomes should be highly correlated, according to Eq. (1). If the channel is unsafe, the communication is halted. Otherwise, the communication goes on.

Step3: The second security checking. Alice sends S_B to Bob. Bob confirms Alice that he has received S_B at first. Then Bob randomly selects P particles from S_B, which are different from the Q particles used in the first security checking, and measures them randomly with Z-basis or X-basis. Bob publishes the positions and the measurement basis of these particles to Alice and Charlie. Alice and Charlie use the same measurement basis as Bob to measure the corresponding particles in S_A and S_C, respectively. Bob makes Alice publish her measurement outcomes at first. Then, Bob and Charlie publish their own measurement outcomes. If there is no eavesdropping, the measurement outcomes from all of them should be highly correlated, according to Eq. (1). If the channel is unsafe, the communication is halted. Otherwise, the communication goes on.

Step4: Bob′s encoding. After getting rid of the $P+Q$ checking particles, S_A, S_B and S_C turn into three new sequences S_A', S_B' and S_C', respectively, where $S_A'=\{A_1, A_2, \cdots, A_{2N}\}$, $S_B'=\{B_1, B_2, \cdots, B_{2N}\}$ and $S_C'=\{C_1, C_2, \cdots, C_{2N}\}$. All of them divide their own sequence into groups (a group contains two adjacent particles). That is, (A_{2n-1}, A_{2n}), (B_{2n-1}, B_{2n}) and (C_{2n-1}, C_{2n}) $(n=1,2,\cdots,N)$ form a group in S_A', S_B' and S_C', respectively. Then, Alice/Bob/Charlie measures (A_{2n-1}, A_{2n})/ (B_{2n-1}, B_{2n})/ (C_{2n-1}, C_{2n}) with Bell-basis. Consequently, as described in Eq. (2), (A_{2n-1}, A_{2n})/ (B_{2n-1}, B_{2n})/ (C_{2n-1}, C_{2n}) collapses to a Bell state after entanglement swapping. According to his Bell-basis measurement outcome, Bob reproduces a new (B_{2n-1}, B_{2n}) with no state measurement performed. Afterward, Bob performs the unitary operation $U_{i_n}^B$ on the first particle in the new (B_{2n-1}, B_{2n}) to encode his one-bit secret message. Accordingly, (B_{2n-1}, B_{2n})

turns into $(U_{i_n}^B B_{2n-1}, B_{2n})$. Then, Bob prepares enough sample particles randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ for security checking and randomly inserts them into S_B'. Accordingly, S_B' turns into a new sequence S_B''. Bob always makes a record of the preparation basis of the sample particles and their positions in S_B''. Finally, Bob sends S_B'' to Charlie.

Step5: The third security checking. After Charlie confirms Bob that she has received S_B'', Bob firstly publishes the positions and the corresponding preparation basis of the sample particles. Then, Charlie measures the sample particles in the same basis as the preparation basis of Bob and tells Bob her measurement outcomes. Bob judges whether there is an eavesdropping by comparing the initial states of the sample particles with Charlie′s measurement outcomes. If the channel is unsafe, they halt the communication. Otherwise, they continue to implement the next step.

Step6: Quantum dialogue. After getting rid of the sample particles, S_B'' turns back into S_B'. Now Charlie has two sequences S_B' and S_C' in her hand. Charlie performs the unitary operation $U_{k_n}^C$ on the second particle of $(U_{i_n}^B B_{2n-1}, B_{2n})$ to encode her one-bit secret message. Accordingly, $(U_{i_n}^B B_{2n-1}, B_{2n})$ turns into $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$. Then, Charlie measures $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$ with Bell-basis. If Alice permits the dialogue between Bob and Charlie, she publishes her BM outcome of (A_{2n-1}, A_{2n}) to Charlie. According to Alice′s announcement and her own BM outcome of (C_{2n-1}, C_{2n}), Charlie can infer Bob′s BM outcome of (B_{2n-1}, B_{2n}). Moreover, according to her own unitary operation $U_{k_n}^C$ and her own BM outcome of $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$, Charlie can infer Bob′s one-bit secret message. On the other hand, Charlie does not publish her BM outcome of $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$ to Bob until she has heard of Alice′s announcement of (A_{2n-1}, A_{2n}). According to his own BM outcome of (B_{2n-1}, B_{2n}), his own unitary operation $U_{i_n}^B$ and Charlie′s announcement of $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$, Bob can infer Charlie′s one-bit secret message. If Alice does not permit the dialogue between Bob and Charlie, she will not publish her BM outcome of (A_{2n-1}, A_{2n}) to Charlie. Consequently, Charlie can not infer Bob′s BM outcome of (B_{2n-1}, B_{2n}). Moreover, Charlie does not publish her BM outcome of $(U_{i_n}^B B_{2n-1}, U_{k_n}^C B_{2n})$ to Bob. Therefore, the dialogue between Bob and Charlie is halted.

This concludes the description of our protocol. An example will be given to explain the dialogue process. Suppose that Bob′s one-bit secret message is 1, and Charlie′s one-bit secret message is 0. We take the nth particle group for example. Alice/Bob/Charlie measures $(A_{2n-1}, A_{2n})/(B_{2n-1}, B_{2n})/(C_{2n-1}, C_{2n})$ with Bell-basis. Consequently, after entanglement swapping, (A_{2n-1}, A_{2n}), (B_{2n-1}, B_{2n}) and (C_{2n-1}, C_{2n}) collapse to $|\Phi^+\rangle_{A_{2n-1}A_{2n}} \cdot |\Phi^+\rangle_{B_{2n-1}B_{2n}} |\Phi^+\rangle_{C_{2n-1}C_{2n}}$, $|\Phi^+\rangle_{A_{2n-1}A_{2n}} |\Phi^-\rangle_{B_{2n-1}B_{2n}} \cdot |\Phi^-\rangle_{C_{2n-1}C_{2n}}$, $|\Phi^-\rangle_{A_{2n-1}A_{2n}} |\Phi^+\rangle_{B_{2n-1}B_{2n}} |\Phi^-\rangle_{C_{2n-1}C_{2n}}$, $|\Phi^-\rangle_{A_{2n-1}A_{2n}} |\Phi^-\rangle_{B_{2n-1}B_{2n}} |\Phi^+\rangle_{C_{2n-1}C_{2n}}$, $|\Psi^+\rangle_{A_{2n-1}A_{2n}} \cdot |\Psi^+\rangle_{B_{2n-1}B_{2n}} |\Psi^+\rangle_{C_{2n-1}C_{2n}}$, $|\Psi^+\rangle_{A_{2n-1}A_{2n}} |\Psi^-\rangle_{B_{2n-1}B_{2n}} \cdot |\Psi^-\rangle_{C_{2n-1}C_{2n}}$, $|\Psi^-\rangle_{A_{2n-1}A_{2n}} |\Psi^+\rangle_{B_{2n-1}B_{2n}} |\Psi^-\rangle_{C_{2n-1}C_{2n}}$ or $|\Psi^-\rangle_{A_{2n-1}A_{2n}} |\Psi^-\rangle_{B_{2n-1}B_{2n}} |\Psi^+\rangle_{C_{2n-1}C_{2n}}$ each with probability 1/8. Without loss of generality, suppose that (A_{2n-1}, A_{2n}), (B_{2n-1}, B_{2n}) and (C_{2n-1}, C_{2n}) collapse to $|\Phi^+\rangle_{A_{2n-1}A_{2n}} |\Phi^+\rangle_{B_{2n-1}B_{2n}} |\Phi^+\rangle_{C_{2n-1}C_{2n}}$. According to his Bell-basis measurement outcome, Bob reproduces a new $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$ with no state measurement performed. Afterward, Bob performs the unitary operation σ_z on the first particle of the new $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$ to encode his one-bit secret message. Accordingly, $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$ turns into $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$. After having both S'_B and S'_C in her hand, Charlie performs the unitary operation I on the second particle of $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$ to encode her one-bit secret message. Accordingly, $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$ keeps unchanged. Then, Charlie measures $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$ with Bell-basis. If Alice permits the dialogue between Bob and Charlie, Alice publishes Charlie that her BM outcome of (A_{2n-1}, A_{2n}) is $|\Phi^+\rangle_{A_{2n-1}A_{2n}}$. Since her own BM outcome of (C_{2n-1}, C_{2n}) is $|\Phi^+\rangle_{C_{2n-1}C_{2n}}$, Charlie can infer that Bob′s BM outcome of (B_{2n-1}, B_{2n}) is $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$. Moreover, since her own BM outcome of $(\sigma_z \otimes B_{2n-1}, I \otimes B_{2n})$ is $|\Phi^-\rangle_{B_{2n-1}B_{2n}}$, according to her own unitary operation I, Charlie can know that Bob′s one-bit secret message is 1. On the other hand, after having heard of Alice′s announcement of (A_{2n-1}, A_{2n}), Charlie publishes Bob her BM outcome of $(\sigma_z \otimes B_{2n-1}, I \otimes B_{2n})$. Since his own BM outcome of (B_{2n-1}, B_{2n}) is $|\Phi^+\rangle_{B_{2n-1}B_{2n}}$, according to his own unitary operation σ_z, Bob can infer that Charlie′s one-bit secret message is 0.

2 Security analysis

In the proposed protocol, there are totally three security checking processes. The first security checking is to check the transmission of S_C

from Alice to Charlie, while the second security checking is to check the transmission of S_B from Alice to Bob. Both of them use the entanglement correlation formed by three particles in the maximally entangled GHZ state of $|\Psi\rangle$ to check eavesdropping. Therefore, the security of the transmission of S_C is similar to that of S_B. Without loss of generality, we take the transmission of S_C for example to analyze the active attacks an outside eavesdropper Eve may employ. It should be pointed out that both the transmission mode of S_C and its security checking method have been also used in Refs. [9, 29]. (I) The intercept-resend attack. Eve firstly intercepts S_C then sends his fake sequence prepared in advance instead of it to Charlie. Since the original entanglement correlations between particle A, particle B and particle C have been destroyed, Eve can be discovered. If there is not any eavesdropping, the measurement outcome of Alice and Charlie will be $|000\rangle$ or $|111\rangle$ ($|+\rangle|+\rangle|+\rangle$, $|-\rangle|-\rangle|+\rangle$, $|+\rangle|-\rangle|-\rangle$ or $|-\rangle|+\rangle|-\rangle$). If there is an eavesdropping from Eve, he will intercept particle C and send particle c instead of it to Charlie. If particle c is prepared in the state of $|0\rangle_c$ by Eve, given that Charlie and Alice select Z-basis (X-basis), their measurement outcome will be $|000\rangle_{ABc}$ or $|110\rangle_{ABc}$ ($|opq\rangle_{ABc}$, $o, p, q = +, -$). According to Eq. (1), the error rate introduced by Eve will be 1/2(1/2). If particle c is prepared in the state of $|1\rangle_c$ by Eve, the error rate introduced by Eve will also be 1/2 (1/2). If particle c is prepared in the state of $|+\rangle_c$ by Eve, the error rate introduced by Eve will be 3/4 (1/2). If particle c is prepared in the state of $|-\rangle_c$ by Eve, the error rate introduced by Eve will also be 3/4 (1/2). (II) The measurement-resend attack. After intercepting S_C, Eve firstly measures it then resends it to Charlie. Since the measuring basis that Charlie and Alice select are not always consistent with that of Eve, this eavesdropping attack can be discovered. Eve intercepts particle C, measures it in Z-basis or X-basis and resends his measurement outcome to Charlie. In the first case, Eve measures it with Z-basis. The state of the whole system will collapse to $|000\rangle$ or $|111\rangle$ each with probability 1/2. Take the state to be $|000\rangle_{ABC}$ for example. Accordingly, Eve resends $|0\rangle_C$ to Charlie. Consequently, if Charlie and Alice select Z-basis, no error will be introduced by Eve. If Charlie and Alice select X-basis, the state will collapse to $|opq\rangle_{ABC}$ ($o, p, q = +, -$) each with probability 1/8. According to Eq. (1), the error rate introduced by Eve will be 1/2. Therefore, the total error rate introduced by Eve in this case is 1/4. In the second case, Eve measures it with X-basis. The state of the whole system will collapse to $|+\rangle_A|+\rangle_B|+\rangle_C$, $|+\rangle_A|-\rangle_B|-\rangle_C$, $|-\rangle_A \cdot |+\rangle_B|-\rangle_C$ or $|-\rangle_A|-\rangle_B|+\rangle_C$ each with probability 1/4. Take the state to be $|+\rangle_A|+\rangle_B \cdot |+\rangle_C$ for example. Accordingly, Eve resends $|+\rangle_C$ to Charlie. Consequently, if Charlie and Alice select Z-basis, the state will collapse to $|opq\rangle_{ABC}$ ($o, p, q = 0, 1$) each with probability 1/8. According to Eq. (1), the error rate introduced by Eve will be 3/4. If Charlie and Alice select X-basis, no error will be introduced by Eve. Therefore, the total error rate introduced by Eve in this case is 3/8[29]. (III) The entanglement-and-measurement attack. According to the Stinespring dilation theorem, Eve′s eavesdropping can be realized by a unitary operation $\hat{E}$ on a larger Hilbert space, $|x, E\rangle \equiv |x\rangle|E\rangle$. Therefore, the state of the composite system will be

$$\hat{E}|\Psi\rangle|\varepsilon\rangle = \frac{1}{\sqrt{2}}[|00\rangle(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle) + |11\rangle(\beta'|0\rangle|\varepsilon_{10}\rangle + \alpha'|1\rangle|\varepsilon_{11}\rangle)] \quad (3)$$

where $\varepsilon_{00}, \varepsilon_{01}, \varepsilon_{10}, \varepsilon_{11}$ are Eve′s probe states and $\hat{E} = \begin{pmatrix} \alpha & \beta' \\ \beta & \alpha' \end{pmatrix}$ is Eve′s probe operator. Since $\hat{E}$ is a unitary operator, the error rate introduced by Eve will be $\tau_1 = |\beta|^2 = |\beta'|^2 = 1 - |\alpha|^2 = 1 - |\alpha'|^2$ when the security checking is implemented under Z-basis[9]. The third security checking is to check the transmission of S_B'' from Bob to Charlie. It uses sample particles randomly prepared in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to check eavesdropping, which is derived from the idea of the BB84 QKD protocol[1]. This checking method has also been used in Refs. [17, 19, 20, 23, 26]. An eavesdropper Eve may employ the active attacks to steal useful information. (I) The intercept-resend attack. Eve firstly intercepts S_B'' then sends his fake sequence prepared in advance instead of it to Charlie. Since Charlie′s measurement outcomes on the fake sequence are not always identical with the genuine ones, the error rate introduced by Eve will be 1/2[19, 26]. (II) The measurement-resend attack. After intercepting S_B'', Eve firstly measures it then resends it to Charlie. Since Eve′s measurement basis is not always consistent with Bob′s preparation basis, the error rate introduced by Eve

will be 1/4[19,26]. (III) The entanglement-and-measurement attack. Eve may steal partial information by entangling his auxiliary particle $|\varepsilon\rangle$ with the particles in S''_B. Then it follows that

$$\hat{E}|0\rangle|\varepsilon\rangle=\alpha|0\rangle|\varepsilon_{00}\rangle+\beta|1\rangle|\varepsilon_{01}\rangle,\hat{E}|1\rangle|\varepsilon\rangle=\beta'|0\rangle|\varepsilon_{10}\rangle+\alpha'|1\rangle|\varepsilon_{11}\rangle \quad (4)$$

Apparently, the error rate introduced by Eve will be $\tau_2=|\beta|^2=|\beta'|^2=1-|\alpha|^2=1-|\alpha'|^2$ when the security checking is implemented under Z-basis[19,26]. In addition, with regard to the security of our protocol, besides considering an outside eavesdropper Eve, it is necessary to consider the dishonesty of the controller Alice. During the first (second) security checking, it is Charlie (Bob) rather than Alice that selects the positions and the measurement basis of the checking particles. Moreover, it is Alice that firstly publishes the measurement outcomes of the checking particles in both security checking processes. In the meanwhile, Alice has no chance to implement the third security checking. Therefore, the dishonest behavior of Alice can always be discovered.

3 Discussions

3.1 The information leakage problem

Here, we analyze whether the proposed protocol has the information leakage problem. Charlie can infer the state of (B_{2n-1},B_{2n}) if Alice publishes her BM outcome of (A_{2n-1},A_{2n}) through the measurement correlation property after entanglement swapping between two maximally entangled GHZ states. This means that there is no need for Bob to publish his BM outcome of (B_{2n-1},B_{2n}) to Charlie, which makes Eve have no chance to know the state of (B_{2n-1},B_{2n}). Therefore, the only thing Eve can do is a pure guess. Although Eve knows the state of $(U^B_{i_n}B_{2n-1},U^C_{k_n}B_{2n})$ from Charlie's announcement, he still obtains nothing useful about the secret messages of Bob and Charlie. Therefore, the proposed protocol avoids the information leakage problem successfully. In addition, we consider "information leakage" from the perspective of information theory. Since Eve has no chance to know the state of (B_{2n-1},B_{2n}), according to Eq. (2) and Table 1, Charlie's announcement of $(U^B_{i_n}B_{2n-1},U^C_{k_n}B_{2n})$ means totally 2×2 unitary operation combinations from Bob and Charlie for Eve. This means that the quantum channel contains $-\sum_{i=1}^{4}p_i\log_2 p_i=-4\times\frac{1}{4}\log_2\frac{1}{4}=2$ bits information for Eve, which is equal to the quantity of secret messages from Bob and Charlie. Therefore, no information leakage happens in our protocol. Apparently, the measurement correlation property after entanglement swapping between two maximally entangled GHZ states helps the proposed protocol overcome the information leakage problem.

3.2 The choice of encoding rule

Someone may doubt why only two unitary operations are used for encoding one bit secret message by both Bob and Charlie, since there are four unitary operations. It is straightforward that the more unitary operations are used, the more secret messages are transmitted. Imagine the first case where all the four unitary operations are used for encoding by both Bob and Charlie. That is to say, both Bob and Charlie send two bits to each other. However, in this case, according to Eq. (2) and Table 1, Charlie's announcement means totally 2×4 unitary operation combinations from Bob and Charlie for Eve. This means that the quantum channel contains $-\sum_{i=1}^{8}p_i\log_2 p_i=-8\times\frac{1}{8}\log_2\frac{1}{8}=3$ bits information for Eve, which is smaller than the quantity of secret messages. That is to say, one bit is leaked out in this case. Imagine the second case where all the four unitary operations are used for encoding by Bob and only two unitary operations by Charlie. That is to say, Bob sends two bits to Charlie while Charlie sends one bit to Bob. However, in this case, according to Eq. (2) and Table 1, Charlie's announcement means totally 2×2 unitary operation combinations from Bob and Charlie for Eve. This means that the quantum channel contains $-\sum_{i=1}^{4}p_i\log_2 p_i=-4\times\frac{1}{4}\log_2\frac{1}{4}=2$ bits information for Eve, which is smaller than the quantity of secret messages. That is to say, one bit is also leaked out in the second case. Therefore, it can be concluded that decreasing the transmission efficiency helps the proposed protocol prevent the information leakage problem, since two unitary operations can only be used to encode one bit by any party in our protocol. On the other hand, besides the encoding rule described as above, three alternative ones can also be used to prevent the information leakage problem, i.e., $\{I\to1,\sigma_z\to0\}$, $\{\sigma_x\to0,i\sigma_y\to1\}$ and $\{\sigma_x\to1,i\sigma_y\to0\}$.

3.3 Comparison with those previous controlled quantum dialogue protocols

Since all of our protocol and the protocols in Refs. [17,21,26] belong to the kind of controlled

quantum dialogue, we draw a comparison among them on the transmission efficiency, the security and the quantum measurement. We compare their transmission efficiency and security at first. The Cabello's definition of transmission efficiency[3] is $\eta=b_s/(q_t+b_t)$, where b_s, q_t and b_t are the expected secret bits received, the qubit used and the classical bits exchanged between two communication parties. In Ref. [17], each maximally entangled GHZ state is used to transmit two bits from Alice and two bits from Bob by consuming three bits classical information. Accordingly, its transmission efficiency is $\eta=4/(3+3)=66.7\%$. However, among the 4 bits, 3 bits are leaked out to Eve unintentionally. Consequently, information leakage happens in the protocol of Ref. [17]. It also can be found out that both the transmission efficiency and the information leakage situation in the protocol of Ref. [21] and the first protocol of Ref. [26] are the same as those in the protocol of Ref. [17]. In the second protocol of Ref. [26], each maximally entangled Bell state is used to transmit two bits from Alice and two bits from Bob by consuming two bits classical information. Accordingly, the transmission efficiency in this case is $\eta=4/(2+2)=100\%$. However, among the 4 bits, 2 bits are leaked out to Eve unintentionally. Therefore, both the two protocols of Ref. [26] still have the information leakage problem, although they have successfully solved the definite information leakage problem in the protocol of Ref. [17]. In our protocol, each two maximally entangled GHZ state is used to transmit one bit from Bob and one bit from Charlie by consuming four bits classical information. Accordingly, the transmission efficiency in this case is $\eta=2/(6+4)=20\%$. Moreover, no information leakage has happened in our protocol. As we all know, high security is indispensable to a quantum communication protocol, since a quantum communication protocol will be meaningless if it is not secure. Therefore, compared with the protocols in Refs. [17,21,26], it is worthy for the proposed protocol to avoid the information leakage problem at the cost of transmission efficiency. On the other hand, both the protocols of Refs. [17, 21] and the first protocol of Ref. [26] need GM, which is more complicated than BM. Therefore, generally speaking, compared with the protocols of Refs. [17, 21, 26], the proposed protocol has two advantages: 1) information leakage happens in the protocols of Refs. [17, 21, 26] rather than the proposed protocol; 2) the proposed protocol merely needs BM rather than GM.

4 Conclusion

To sum up, we propose a controlled quantum dialogue without information leakage in this paper, where the controller Alice controls the bidirectional communication between two communication parties, Bob and Charlie. It prevents the information leakage problem by making full use of the measurement correlation property after entanglement swapping between two maximally entangled GHZ states and decreasing the transmission efficiency. Moreover, it merely needs BM rather than GM. Security analysis shows that its security can be guaranteed.

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**(5): 557-559.

[3] CABELLO A. Quantum key distribution in the Holevo limit [J]. *Physical Review Letters*, 2000, **85**(26): 5635-5638.

[4] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. *Physical Review A*, 2002, **65**(3): 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**(3): 357-368.

[6] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. *Physical Review Letters*, 2002, **89**(18): 187902.

[7] 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**(4): 042317.

[8] CAI Q Y, LI B W. Improving the capacity of the Bostrom-Felbinger protocol[J]. *Physical Review A*, 2004, **69**(5): 054301.

[9] WANG C, DENG F G, LONG G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state[J]. *Optics Communications*, 2005, **253**(1-3): 15-20.

[10] 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.

[11] ZHANG Z J, MAN Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. arXiv: quant-ph/0403215v1, 2004.

[12] ZHANG Z J, MAN Z X. Secure bidirectional quantum communication protocol without quantum channel. arXiv: quant-ph/0403217v4, 2004.

[13] ZHANG Z J, MAN Z X, LI Y. Economically improving message-unilaterally-transmitted quantum secure direct communication to realize two-way communication. arXiv:

quant-ph/0406181v1, 2004.

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

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] XIA Y, SONG J, NIE J, *et al*. Controlled secure quantum dialogue using a pure entangled GHZ states [J]. *Communications in Theoretical Physics*, 2007, **48**(5): 841-846.

[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] 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.

[24] 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.

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

[26] 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.

[27] LIU Z H, CHEN H W. Comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state"[Chin Phys Lett 30 (2013) 040305][J]. *Chinese Physics Letters*, 2013, **30**(7): 079901.

[28] YE T Y, JIANG L Z. Reply to comment on"Improvement of controlled bidirectional quantum direct communication using a GHZ state"[Chin Phys Lett 30 (2013) 040305][J]. *Chinese Physics Letters*, 2013, **30**(7): 079902.

[29] YE T Y, JIANG L Z. Quantum steganography with a large payload based on dense coding and entanglement swapping of Greenberger-Horne-Zeilinger states[J]. *Chinese Physics B*, 2013, **22**(5): 050309.