Quantum dialogue without information leakage based on the entanglement swapping between any two Bell states and the shared secret Bell state

Tian-Yu Ye and Li-Zhen Jiang

College of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, People’s Republic of China
E-mail: happyty@aliyun.com

Received 8 July 2013, revised 11 November 2013
Accepted for publication 28 November 2013
Published 27 December 2013

Abstract
In order to avoid the risk of information leakage during the information mutual transmission between two authorized participants, i.e. Alice and Bob, a quantum dialogue protocol based on the entanglement swapping between any two Bell states and the shared secret Bell state is proposed. The proposed protocol integrates the ideas of block transmission, two-step transmission and unitary operation encoding together using the Bell states as the information carriers. Besides the entanglement swapping between any two Bell states, a shared secret Bell state is also used to overcome the information leakage problem, which not only makes Bob aware of the prepared initial state but also is used for Bob’s encoding and entanglement swapping. Security analysis shows that the proposed protocol can resist the general active attacks from an outside eavesdropper Eve. Moreover, the relation between the maximal amount of information Eve can gain and the detection probability is derived.

Keywords: quantum dialogue, information leakage, entanglement swapping, Bell state

1. Introduction

Different from classical cryptography, quantum cryptography is based on the physical laws of quantum mechanics rather than mathematical complexity. Quantum cryptography can be classified into several types, such as quantum key distribution (QKD), quantum secure direct communication (QSDC), quantum secret sharing (QSS) and so on. The aim of QKD is to establish a shared random key between two remote authorized users. Since Bennett and Brassard [1] put forward the first QKD protocol (BB84) in 1984, many other theoretical QKD protocols have been put forward [2–6]. Different from QKD, QSDC allows secret messages to be transmitted directly without creating a key to encrypt them in advance. In 2002, Long and Liu [4] proposed the first QSDC. In this protocol, two ordered particle sequences derived from the order Bell states are transmitted in blocks from Alice to Bob in two steps with two security checks. It should be emphasized that the Long and Liu protocol is also the first protocol employing the ideas of block transmission and two-step transmission. Since then, the block transmission technique has been widely adopted. For example, in 2003, Deng et al [7] also presented a two-step QSDC based on block transmission and two-step transmission. This protocol encodes information by applying unitary operations on Bell states. In other words, this protocol adopts the unitary operation encoding. Until now, a lot of other QSDC protocols have been proposed with different ways of implementation so that QSDC gained considerable development [8–17]. In 2002, Bostrom and Felbinger [8] proposed the famous ping-pong protocol using a Bell state. Later, Cai and Li [9] improved the capacity of the ping-pong protocol by introducing two additional unitary operations. In 2004, Deng and Long [10] put forward a one-time pad QSDC. In 2005, Wang et al [11] proposed a multi-step QSDC using the multi-particle Green–Horne–Zeilinger (GHZ) state. In 2007, Li et al [12] presented a QSDC with quantum encryption based on the pure entangled state. In 2008, Chen et al [13] presented a controlled QSDC protocol with quantum encryption using a partially entangled GHZ state; Chen et al [14] also presented a three-party controlled QSDC protocol based on the W state. In 2011, Yang et al [15] proposed two fault-tolerant two-step QSDC protocols which...
are robust against the collective-dephasing noises and the collective-rotation noises. In 2012, Li et al [16] improved the eavesdropping detection efficiency of the Deng et al [7] two-step QSDC by using the four-particle cluster state; Song and Wang [17] reviewed the recent development in quantum communication including QKD, QSDC, QSS, quantum teleportation and so on. They also pointed out that multi-step transmission, block transmission and order rearrangement are popularly used to construct quantum communication protocols, and that single photons and entangled photon pairs are often used as information carriers. With regard to the relation between QKD and QSDC, it should be emphasized that all QSDC protocols are QKD protocols at the same time, and that single photons and entangled photon pairs are popularly used to construct quantum communication between two Bell states [28, 29]. In addition, Ye and Jiang [30] analyzed the information leakage problem of Nguyen’s protocol [31] from the viewpoint of information theory and cryptography; Tan and Cai [32] analyzed the information leakage problem of Nguyen’s protocol [20] from the viewpoint of the Holevo bound. Afterwards, researchers began to concentrate on solving the information leakage problem in quantum dialogue. As a result, some information leakage resistant quantum dialogue protocols were derived, such as the protocols based on a shared private quantum state [33, 34], based on the correlation extractability of Bell state and the auxiliary particle [35] and based on the measurement correlation from entanglement swapping between two Bell states [36]. In addition, Ye and Jiang [37] suggested two methods to solve the information definite leakage problem in Man and Xia’s protocol [23] in 2013. However, their two protocols [37] still run the risk of information leakage [38, 39].

In this paper, we integrate the ideas of block transmission [4, 7], two-step transmission [4, 7] and unitary operation encoding [7] together to construct a novel quantum dialogue protocol with the Bell states being the information carriers. Besides the entanglement swapping between any two Bell states, a shared secret Bell state is also used to overcome the information leakage problem. The shared secret Bell state has two functions in the dialogue process: firstly, it makes Bob aware of the prepared initial state; secondly, it is used for Bob’s encoding and entanglement swapping. Security analysis shows that the proposed protocol can resist the general active attacks from an outside eavesdropper Eve. Moreover, the relation between the maximal amount of information Eve can gain and the detection probability is derived.

2. Quantum dialogue protocol

The four Bell states can be expressed as follows:

\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|+\rangle |+\rangle - |\rangle |\rangle), \]  

(1)

\[ |\Phi^-\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}} (|+\rangle |\rangle + |\rangle |\rangle). \]  

(2)

\[ |\Psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}} (|\rangle |+\rangle + |+\rangle |\rangle), \]  

(3)

\[ |\Psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}} (|\rangle |\rangle - |+\rangle |\rangle). \]  

(4)

Here, \(|\pm\rangle = (|0\rangle \pm |1\rangle) / \sqrt{2}\). It is well known that \(I = |0\rangle|0\rangle + |1\rangle|1\rangle\), \(\sigma_x = |0\rangle \langle 1| + |1\rangle \langle 0|\), \(i\sigma_y = |0\rangle \langle 1| - |1\rangle \langle 0|\) and \(\sigma_z = |0\rangle \langle 0| - |1\rangle \langle 1|\) are four unitary operations. Here, both Alice and Bob agree in advance that each unitary operation corresponds to a two-bit secret message in a way like \(I \rightarrow 00\), \(\sigma_x \rightarrow 01\), \(i\sigma_y \rightarrow 10\) and \(\sigma_z \rightarrow 11\).

It is easy to verify that the entanglement swapping between \(|\Psi^-\rangle\) and an arbitrary one of the four Bell states can be described by formulas (5)–(8), where the subscripts \(A_i\) and \(B_i\) \((i = 1, 2)\) denote the two particles from a Bell state, respectively:

\[|\Psi^-\rangle_{A_1B_1} \otimes |\Psi^-\rangle_{A_2B_2} = \frac{1}{2} \left\{ |\Phi^+\rangle_{A_1A_2} |\Phi^+\rangle_{B_1B_2} - |\Phi^-\rangle_{A_1A_2} |\Phi^-\rangle_{B_1B_2} + |\Psi^-\rangle_{A_1A_2} |\Psi^-\rangle_{B_1B_2} \right\}, \]  

(5)

\[|\Psi^-\rangle_{A_1B_1} \otimes |\Psi^+\rangle_{A_2B_2} = \frac{1}{2} \left\{ |\Phi^-\rangle_{A_1A_2} |\Phi^+\rangle_{B_1B_2} - |\Phi^+\rangle_{A_1A_2} |\Phi^-\rangle_{B_1B_2} + |\Psi^-\rangle_{A_1A_2} |\Psi^+\rangle_{B_1B_2} \right\}, \]  

(6)
\[ |\psi^+\rangle_{A_1 B_2} \otimes |\psi^-\rangle_{A_2 B_2} = \frac{1}{2} \left( |\phi^+\rangle_{A_1 A_2} |\psi^+\rangle_{B_1 B_2} - |\phi^+\rangle_{A_1 A_2} |\psi^+\rangle_{B_1 B_2} + |\psi^-\rangle_{A_1 A_2} |\phi^-\rangle_{B_1 B_2} \right), \]  
\[ |\phi^-\rangle_{A_1 A_2} |\psi^-\rangle_{B_1 B_2} - |\phi^+\rangle_{A_1 A_2} |\psi^\rangle_{B_1 B_2} + |\psi^-\rangle_{A_1 A_2} |\phi^-\rangle_{B_1 B_2} \). \]  

According to formulas (5)–(8), if the Bell-basis measurements are performed on $A_1 A_2$ and $B_1 B_2$, respectively, each initial state group of $A_1 B_1$ and $A_2 B_2$ will collapse to four different outcome combinations of $A_1 A_2$ and $B_1 B_2$ with the same probability after entanglement swapping. Moreover, each outcome combination of $A_1 A_2$ and $B_1 B_2$ solely corresponds to one initial state group of $A_1 B_1$ and $A_2 B_2$. Corresponding to formulas (5)–(8), four collections composed by different outcome combinations of $A_1 A_2$ and $B_1 B_2$ are labeled as

\[ \{ |\phi^+\rangle_{A_1 A_2} |\phi^+\rangle_{B_1 B_2}, |\phi^+\rangle_{A_1 A_2} |\psi^\rangle_{B_1 B_2}, |\psi^\rangle_{A_1 A_2} |\phi^+\rangle_{B_1 B_2}, \} \rightarrow C_0, \]  
\[ \{ |\phi^-\rangle_{A_1 A_2} |\phi^\rangle_{B_1 B_2}, |\phi^-\rangle_{A_1 A_2} |\psi^-\rangle_{B_1 B_2}, |\psi^-\rangle_{A_1 A_2} |\phi^-\rangle_{B_1 B_2} \} \rightarrow C_1, \]  
\[ \{ |\phi^+\rangle_{A_1 A_2} |\phi^\rangle_{B_1 B_2}, |\phi^+\rangle_{A_1 A_2} |\psi^-\rangle_{B_1 B_2}, |\psi^\rangle_{A_1 A_2} |\phi^\rangle_{B_1 B_2} \} \rightarrow C_2, \]  
\[ \{ |\phi^-\rangle_{A_1 A_2} |\phi^\rangle_{B_1 B_2}, |\phi^-\rangle_{A_1 A_2} |\psi^-\rangle_{B_1 B_2}, |\psi^-\rangle_{A_1 A_2} |\phi^-\rangle_{B_1 B_2} \} \rightarrow C_3. \]

Further extending the first Bell state in each initial state group from $|\psi^-\rangle$ to the other three Bell states, all the collections composed by different outcome combinations of $A_1 A_2$ and $B_1 B_2$ after entanglement swapping can be summarized as table 1.

| $|\phi^+\rangle_{A_1 B_2}$ | $|\phi^+\rangle_{A_2 B_2}$ | $|\psi^-\rangle_{A_1 B_2}$ | $|\psi^-\rangle_{A_2 B_2}$ |
|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| $|\phi^+\rangle_{A_1 B_2}$   | $|\phi^+\rangle_{A_1 B_2}$   | $|\phi^+\rangle_{A_1 B_2}$   | $|\phi^+\rangle_{A_1 B_2}$   |
| $|\phi^+\rangle_{A_2 B_2}$   | $|\phi^+\rangle_{A_2 B_2}$   | $|\phi^+\rangle_{A_2 B_2}$   | $|\phi^+\rangle_{A_2 B_2}$   |
| $|\psi^-\rangle_{A_1 B_2}$   | $|\psi^-\rangle_{A_1 B_2}$   | $|\psi^-\rangle_{A_1 B_2}$   | $|\psi^-\rangle_{A_1 B_2}$   |
| $|\psi^-\rangle_{A_2 B_2}$   | $|\psi^-\rangle_{A_2 B_2}$   | $|\psi^-\rangle_{A_2 B_2}$   | $|\psi^-\rangle_{A_2 B_2}$   |

Carriers. That is to say, the two ordered particle sequences from the order Bell states are transmitted from Alice to Bob in two steps here. In the meanwhile, the secret is encoded with unitary operations performed on the ordered particle sequences.

**Step 1: preparation.** Alice prepares $2N$ Bell states \{$(A_1, B_1), (A_2, B_2), \ldots, (A_{2N}, B_{2N})$\} in order with each adjacent Bell states \{$(A_{2n-1}, B_{2n-1}), (A_{2n}, B_{2n})$, $n = 1, 2, \ldots, N$\} in the same state. Here, the subscript denotes the order of each Bell state. She extracts all the particles $A$ from these Bell states in order to form the sequence $S_A$. Likewise, the remaining particles $B$ form the sequence $S_B$. That is, $S_A = \{A_1, A_2, \ldots, A_{2N}\}$ and $S_B = \{B_1, B_2, \ldots, B_{2N}\}$. For the first security check, Alice prepares another batch of sample Bell states, and randomly inserts the sample particles $A$ and $B$ into the sequences $S_A$ and $S_B$, respectively. As a result, $S_A$ and $S_B$ turn into two new sequences $S'_A$ and $S'_B$, respectively. Then, Alice sends $S'_B$ to Bob, and keeps $S'_A$ in her hand. After Bob confirms with Alice that he has received $S'_B$, they start the first security check to test whether $S'_B$ was eavesdropped during the transmission.

**Step 2: Alice’s encoding.** After dropping out the sample particles, $S'_A$ and $S'_B$ turn back into $S_A$ and $S_B$, respectively. Both Alice and Bob divide their own sequences into groups (a group contains two adjacent particles). That is, $(A_{2n-1}, A_{2n})$ forms the group $n$ in $S_A$, while $(B_{2n-1}, B_{2n})$ forms the group $n$ in $S_B$. They agree that the particle $A$ performed with Alice’s unitary operation in each group should have a different position to the particle $B$ performed with Bob’s unitary operation in the corresponding group. Concretely speaking, in group $n$, once Alice performs her unitary operation $U_{i_{A_{2n}}}$ on the particle $A_{2n-1}$ (A_{2n}), Bob should perform his unitary operation $U_{i_{B_{2n}}}$ on the particle $B_{2n-1}$. Without loss of generality, assume that Alice performs $U_{i_{A_{2n}}}$ on $A_{2n-1}$ for encoding her two-bit secret $(i_{a}, i_{b})$ here. For the second security check, Alice prepares a large number of single sample particles, which are randomly in one of the four states \{$(0), (1), (+), (-)$\}, and randomly inserts them into $S_A$. As a result, $S_A$ turns into a new sequence $S''_A$. Then, Alice sends $S''_A$ to Bob. After Bob confirms with Alice that he has received $S''_A$, they start the second security check to test whether $S''_A$ was eavesdropped during the transmission.

**Step 3: quantum dialogue.** After dropping out the single sample particles, $S''_A$ turns back into $S_A$ again. Having both $S_A$ and $S_B$ in his hand, Bob picks up one particle from each sequence in order, and stores each two adjacent Bell states as a group. That is, group $n$ contains two adjacent Bell states \{(U_{i_{A_{2n-1}}}, A_{2n-1}), (A_{2n}, B_{2n})\}. For simplicity, we just deal with group 1 to illustrate the dialogue process (other groups are similar). In group 1, \{(U_{i_{A_{2n-1}}}, A_{2n}), (A_{2n-1}, B_{2n})\}, Bob first performs the Bell-basis
measurement on \((A_2, B_2)\). Consequently, Bob can know the initial state of group 1 prepared by Alice in step 1. According to his Bell-basis measurement outcome, Bob reproduces a new \((A_2, B_2)\) with no state measurement performed. Then Bob encodes his two-bit secret \((k_1, l_1)\) by performing \(U^{B}_{k_1, l_1}\) on the new particle \(B_2\). As a result, group 1 turns into \([(U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)]\). Afterward, Bob performs the Bell-basis measurements on \((U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)\) respectively. According to formulas (9)–(12), Bob can know which outcome collection \([(U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)]\) belongs to. Then, Bob announces this outcome collection to Alice through a classical channel. After hearing Bob’s announcement, Alice can infer the four possible kinds of states for \([(U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)]\) from table 1. Furthermore, since Alice prepares the initial state herself, according to her own unitary operation \(U^{A}_{i_1, j_1}\), Alice is able to read out Bob’s two-bit secret \((k_1, l_1)\) from table 1. Similarly, according to the outcome collection \([(U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)]\) belongs to, Bob can also infer the four possible kinds of states of \([(U^{A}_{i_1, j_1}, A_1), (A_2, U^{B}_{k_1, l_1}, B_2)]\) from table 1. Since Bob knows the prepared initial state from the Bell-basis measurement on \((A_2, B_2)\), according to his own unitary operation \(U^{B}_{k_1, l_1}\), Bob is able to read Alice’s two-bit secret \((i_1, j_1)\) from table 1. Therefore, Alice and Bob have accomplished the dialogue process successfully.

Here we also use the first two Bell states \((A_1, B_1)\) and \((A_2, B_2)\) to further explain the dialogue process. Suppose that Alice’s first two-bit secret \((i_1, j_1)\) is 01 and Bob’s first two-bit secret \((k_1, l_1)\) is 11. Moreover, assume that the first two Bell states \((A_1, B_1)\) and \((A_2, B_2)\) are prepared by Alice in the states of \(|\Psi^+\rangle_{A_1, B_1}\) and \(|\Psi^-\rangle_{A_2, B_2}\), respectively. Consequently, \((A_1, B_1)\) and \((A_2, B_2)\) will change in the following manner:

\[
\begin{align*}
|\Psi^-\rangle_{A_1, B_1} &\Rightarrow \sigma^A_{i_1, j_1} \otimes |\Psi^-\rangle_{A_1, B_1} = |\Phi^-\rangle_{A_1, B_1}, \\
|\Psi^-\rangle_{A_2, B_2} &\Rightarrow \sigma^B_{k_1, l_1} \otimes |\Psi^-\rangle_{A_2, B_2} = |\Psi^-\rangle_{A_2, B_2}, \\
|\Phi^-\rangle_{A_1, A_2} &\otimes |\Psi^-\rangle_{B_1, B_2} = |\Phi^-\rangle_{A_1, A_2}, \\
|\Phi^+\rangle_{A_1, A_2} &\otimes |\Psi^-\rangle_{B_1, B_2} = |\Phi^-\rangle_{A_1, A_2}, \\
|\Psi^-\rangle_{A_1, A_2} &\otimes |\Phi^+\rangle_{B_1, B_2} = |\Psi^-\rangle_{A_1, A_2}, \\
|\Psi^+\rangle_{A_1, A_2} &\otimes |\Phi^+\rangle_{B_1, B_2} = |\Phi^-\rangle_{A_1, A_2}, \\
\end{align*}
\]

C\(_2\) is published by Bob through a classical channel. According to three known pieces of information: the outcome collection C\(_2\), the prepared initial state \(|\Psi^-\rangle\) and her own unitary operation \(\sigma^A_{i_1, j_1}\). Alice can read from table 1 that Bob’s two-bit secret \((k_1, l_1)\) is 11. Likewise, according to the outcome collection C\(_3\), the initial state \(|\Phi^-\rangle\) known from his Bell-basis measurement on \((A_2, B_2)\) and his own unitary operation \(\sigma^B_{k_1, l_1}\). Bob can read from table 1 that Alice’s two-bit secret \((i_1, j_1)\) is 01. Apparently, during the dialogue process, \((A_2, B_2)\) acts as a shared secret Bell state between Alice and Bob. It has two functions: firstly, it makes Bob aware of the prepared initial state; secondly, it is used for Bob’s encoding and entanglement swapping.

3. Security checks and security analysis

As well known to all, a quantum secure communication protocol should possess good security. Otherwise, it will be meaningless. In the literature of quantum secure communication, the security check is always adopted to guarantee its security.

In the proposed protocol, since Alice sends two particle sequences composed by Bell states to Bob in two steps, two security checks are needed in total. The first is used to check the transmission security of \(S'_E\), while the second is used to check the transmission security of \(S'\). The first security check is implemented in the following way: (a) Alice first tells Bob the positions of the sample particles \(B\) in \(S'\); (b) Bob chooses randomly one of the two sets of measuring basis, i.e. Z-basis \(((0), (1))\) and X-basis \(((|+\rangle), (|-\rangle))\), to measure the sample particles \(B\), and tells Alice his measurement basis and measurement outcomes; (c) Alice chooses the same measurement basis as Bob’s to measure the sample particles \(A\) in \(S'_A\); and (d) Alice judges whether there is eavesdropping by comparing their measurement outcomes. If there is no eavesdropping, their measurement outcomes should be highly correlated, according to formulas (1)–(4), and they continue the communication. Otherwise, they halt the communication.

The second security check is implemented as follows: (a) Alice first tells Bob the positions and the preparation basis of the single sample particles in \(S'_A\); (b) Bob measures the single sample particles in the same basis as the preparation basis of Alice and tells Alice his measurement outcomes; and (c) Alice judges whether there is eavesdropping by comparing the initial states of the single sample particles with Bob’s measurement outcomes. If there is no eavesdropping, they continue the communication. Otherwise, they halt the communication.

In fact, during the second transmission, an outside eavesdropper Eve can only disturb the transmission of \(S'_E\) and cannot steal any secret, since no one can distinguish a Bell state by only obtaining one particle. The reason lies in that particle \(A\) is a complete mixed state, since its reduced density matrix is \(\rho_A = \tr_B [\rho_A^{\beta^+} \Phi^+] = \tr_B [\rho_A^{\beta^+} \Phi^+] = \frac{1}{2} I\). Therefore, the security of the proposed protocol mainly depends on the transmission of \(S'_E\). In essence, the first security check uses the entanglement correlation between two particles from a Bell state for eavesdropping detection. This security check method has been popularly used in some previous protocols [7, 9, 21, 33, 35, 36, 37], and its effectiveness has been widely accepted. Detailed analysis of its effectiveness against general active attacks like the intercept–resend attack, the measure–resend attack and the entangle–measure attack has been made in [33, 35–37].

Now let us turn to analyze how much information Eve can maximally gain. First suppose that Alice sends \(0\) to Bob. Then the state of the system composed of Bob’s particle and Eve’s probe can be expressed as [7]

\[
|\psi'\rangle = \hat{E} |0, 0\rangle \equiv \hat{E} |0, 0\rangle |\epsilon\rangle = \alpha |0, 0\rangle |0, 0\rangle + \beta |1, 0\rangle |0, 0\rangle = \alpha |0, 0\rangle + \beta |1, 0\rangle ,
\]

\[
\rho' = \langle \alpha^2 |0, 0\rangle \langle 0, 0| + |\beta|^2 |1, 0\rangle \langle 1, 0| + \alpha \beta^* |1, 0\rangle \langle 0, 0| + \alpha \beta |0, 0\rangle \langle 1, 0| ,
\]

where \(\hat{E}\) is an attack unitary operation, \(|\epsilon\rangle\) is the state of an ancilla, \(|\epsilon_{a, b}\rangle\) (a, b \(\in (0, 1)\)) are pure ancillary states uniquely determined by \(\hat{E}\) and \(|\alpha|^2 + |\beta|^2 = 1\). After encoding of the
unitary operations \( I, \sigma_x, \sigma_y \) and \( \sigma_z \) with the probabilities \( p_0, p_1, p_2 \) and \( p_3 \), respectively, the state reads \(^7\)

\[
\rho'' = (p_0 + p_1) |\alpha|^2 |0, \epsilon_00\rangle \langle 0, \epsilon_00| + (p_0 + p_3) |\beta|^2 |1, \epsilon_{01}\rangle \langle 1, \epsilon_{01}| + (p_0 - p_3) \alpha \beta^* |0, \epsilon_{00}\rangle \langle 1, \epsilon_{01}| + (p_0 - p_2) \alpha^* \beta |1, \epsilon_{01}\rangle \langle 0, \epsilon_{00}| + (p_1 + p_2) |\alpha|^2 |1, \epsilon_{00}\rangle \langle 1, \epsilon_{00}| + (p_1 - p_2) \alpha \beta^* |1, \epsilon_{00}\rangle \langle 0, \epsilon_{01}| + (p_1 - p_3) \alpha^* \beta |0, \epsilon_{00}\rangle \langle 1, \epsilon_{00}| \tag{16}
\]

which can be rewritten in the orthogonal basis \([0, \epsilon_{00}), [1, \epsilon_{01}), [1, \epsilon_{00}), [0, \epsilon_{01})\].

\[
\rho'' = \begin{pmatrix}
(p_0 + p_1) |\alpha|^2 & (p_0 - p_3) \alpha \beta^* & 0 & 0 \\
(p_0 - p_3) \alpha^* \beta & (p_0 + p_3) |\beta|^2 & 0 & 0 \\
0 & 0 & (p_1 + p_3) |\alpha|^2 & (p_1 - p_2) \alpha \beta^* \\
0 & 0 & (p_1 - p_2) \alpha^* \beta & (p_1 + p_2) |\beta|^2
\end{pmatrix}.
\tag{17}
\]

where \( p_0 + p_1 + p_2 + p_3 = 1 \).

The information \( I_0 \) Eve can gain is equal to the Von Neumann entropy \(^7\)

\[
I_0 = \sum_{i=0}^{3} -\lambda_i \log_2 \lambda_i, \tag{18}
\]

where \( \lambda_i \) \((i = 0, 1, 2, 3)\) are the eigenvalues of \( \rho'' \), and can be expressed as

\[
\begin{align*}
\lambda_{0,1} &= \frac{1}{2} (p_0 + p_1) + \frac{1}{2} \sqrt{(p_0 + p_3)^2 - 16 p_0 p_3 |\alpha|^2 |\beta|^2} \\
&= \frac{1}{2} (p_0 + p_1) + \frac{1}{2} \sqrt{(p_0 + p_3)^2 - 16 p_0 p_3 (d - d^2)}, \tag{19}
\end{align*}
\]

\[
\begin{align*}
\lambda_{2,3} &= \frac{1}{2} (p_1 + p_2) + \frac{1}{2} \sqrt{(p_1 + p_3)^2 - 16 p_1 p_3 |\alpha|^2 |\beta|^2} \\
&= \frac{1}{2} (p_1 + p_2) + \frac{1}{2} \sqrt{(p_1 + p_3)^2 - 16 p_1 p_3 (d - d^2)}, \tag{20}
\end{align*}
\]

where \( d \) is the detection probability. In the case of \( p_0 = p_1 = p_2 = p_3 = \frac{1}{4} \), where Alice encodes two bits, we have \( \lambda_0 = \frac{1}{2} d, \lambda_1 = \frac{1}{2} (1 - d), \lambda_2 = \frac{1}{4} d \) and \( \lambda_3 = \frac{1}{4} (1 - d) \). As a result, the maximal amount of information Eve can gain in this case is equal to the Shannon entropy of a binary channel

\[
I_0(d) = -d \log_2 \left( \frac{1}{2}^d \right) - (1 - d) \log_2 \left( \frac{1}{2}^{1 - d} \right). \tag{21}
\]

Then suppose that Alice sends \(|1\rangle\) to Bob. After the above security analysis is done in full analogy, the same crucial relations can be obtained. The maximal amount of information Eve can gain in this case is also equal to the Shannon entropy of a binary channel

\[
I_1(d) = -d \log_2 \left( \frac{1}{2}^d \right) - (1 - d) \log_2 \left( \frac{1}{2}^{1 - d} \right) \tag{22}
\]

Therefore, the maximal amount of information Eve can gain is

\[
I(d) = \frac{1}{2} (I_0(d) + I_1(d)) = 1 - d \log_2 d - (1 - d) \log_2 (1 - d). \tag{23}
\]

The function \( I(d) \) is plotted in Figure 1. Obviously, \( I(d) \) reaches its maximum at \( d = 1/2 \), and can be inversed on the interval \([0, 1/2]\), resulting in a monotonic function, \( 0 \leq d(I) \leq 1/2, I \in [1, 2] \). In order to gain desired information \( I > 1 \) per attack, Eve has to encounter a detection probability \( d(I) > 0 \). If Eve wants to gain the full information \( I = 2 \), the detection probability will be \( d(I = 2) = \frac{1}{2} \).

4. Discussions

(1) The information leakage problem. Here we consider the passive attack named information leakage. We also use the first two Bell states \((A_1, B_1)\) and \((A_2, B_2)\) to analyze it. Although Eve hears from Bob the outcome collection \([U_{1i}^A, A_1, A_2], (B_1, U_{2i}^B, B_2)\) belongs to, she still cannot read out any information about the secret, due to no knowledge about the initial state of the shared secret quantum state \((A_2, B_2)\). Consequently, no information leaks to Eve. On the other hand, the information leakage problem can also be analyzed via the perspective of information theory. Since Eve is not aware of \((A_2, B_2)\), with respect to the unitary operation combinations performed by Alice and Bob, there are 16 different possibilities for the outcome collection \([U_{1i}^A, A_1, A_2], (B_1, U_{2i}^B, B_2)\), corresponding to \(-\sum_{i=1}^{16} p_i \log_2 p_i = -16 \times \frac{1}{16} \log_2 \frac{1}{16} = 4\) bits for Eve. Fortunately, this amount of information for Eve is equal to the total amount of secret transmitted between Alice and Bob. Hence, no information leakage
happens in the proposed protocol. Obviously, besides the entanglement swapping between any two Bell states, the shared secret quantum state \((A_2, B_2)\) also plays a key role in avoiding the information leakage problem.

(2) Information-theoretical efficiency. The information-theoretical efficiency defined by Cabello [3] is \(\eta = b_3/(q_1 + b_1)\), where \(b_1, q_1, \) and \(b_3\) are the expected secret bits received, the qubits used and the classical bits exchanged between Alice and Bob. In the proposed protocol, the first two adjacent Bell states \((A_1, B_1)\) and \((A_2, B_2)\) can be used for exchanging four bits in total, i.e. two bits from Alice and two bits from Bob. In addition, two classical bits are needed by Bob to announce to Alice the outcome collection \([(U_{11}^A, A_1, A_2), (B_1, U_{12}^B, B_2)]\) belongs to through a classical channel. Therefore, the information-theoretical efficiency of the proposed protocol is \(\eta = (2 + 2)/(4 + 2) = 66.7\%\).

(3) Comparisons with Gao’s protocols [36]. Here we compare the proposed protocol with Gao’s protocols [36] in detail, since both of them belong to the kind of information leakage resistant quantum dialogue protocols using the entanglement swapping between Bell states. (a) Quantum resource: in every round communication, both the proposed protocol and Gao’s protocols only need two Bell states, thus the same quantum resource is needed. (b) Quantum measurement: in every round communication, both the proposed protocol and Gao’s protocols only need three Bell-basis measurements, thus the same number of quantum measurements is needed. (c) The information-theoretical efficiency: in Gao’s protocols, Alice and Bob exchange their individual two bits per round communication by using four qubits and two bits of classical information, thus their information-theoretical efficiency is \(\eta = (2 + 2)/(4 + 2) = 66.7\%\). As a result, the information-theoretical efficiency of the proposed protocol is equal to its counterpart of Gao’s protocols. Therefore, it can be concluded that the proposed protocol has the same performance as Gao’s protocols in quantum resource, quantum measurement and information-theoretical efficiency.

However, there are still big differences between them. We also take the first two Bell states \((A_1, B_1)\) and \((A_2, B_2)\) for an example. (a) The encoded Bell states are different. In the proposed protocol, the initial Bell states are encoded by Alice and Bob, respectively. Concretely speaking, \(A_1\) from \((A_1, B_1)\) is encoded by Alice with \(U_{11}^A\), while \(B_2\) from \((A_2, B_2)\) is encoded by Bob with \(U_{21}^B\). However, in Gao’s protocols, the same Bell state, derived from the entanglement swapping between two initial Bell states, is encoded by both Alice and Bob. Concretely speaking, \((B_1, B_2)\) (or \((A_1, A_2)\)) is encoded by both Alice and Bob. (b) The key parameters needed for decoding are different. The proposed protocol needs two key parameters for decoding, i.e. the Bell-basis measurement of the initial shared secret Bell state and the corresponding relation between the two encoded initial Bell states and their entanglement swapping outcome. Concretely speaking, in order to know the prepared initial state of group 1, \((A_2, B_2)\) needs to be measured with Bell-basis by Bob. Moreover, the Bell-basis measurement outcomes of \((U_{11}^A, A_1, A_2)\) and \((B_1, U_{12}^B, B_2)\) are needed to infer the four possible kinds of initial states for \([(U_{11}^A, A_1, B_1), (A_2, U_{12}^B, B_2)]\) by both Alice and Bob. However, Gao’s protocols only need one key parameter for decoding, i.e. the measurement correlation of two Bell states derived from the entanglement swapping between two initial Bell states. That is to say, in Gao’s first protocol, in order to decode Bob’s secret, Alice needs to use the Bell-basis measurement outcome of \((A_1, A_2)\) to infer its counterpart of \((B_1, B_2)\); in Gao’s second protocol, in order to decode Alice’s secret, Bob needs to use the Bell-basis measurement outcome of \((B_1, B_2)\) to infer its counterpart of \((A_1, A_2)\). (c) The methods for avoiding the information leakage problem are different. As analyzed above, in the proposed protocol, besides the entanglement swapping between any two Bell states, the shared secret Bell state also plays a key role in avoiding the information leakage problem. However, in Gao’s protocols, the measurement correlation of two Bell states derived from the entanglement swapping between two initial Bell states helps overcome the information leakage problem.

Therefore, it can be concluded that compared with Gao’s protocols, the proposed protocol provides another novel alternative idea for constructing an information leakage resistant quantum dialogue protocol using the entanglement swapping between Bell states.

5. Conclusions

To sum up, we have put forward a quantum dialogue protocol, which is based on the entanglement swapping between any two Bell states and the shared secret Bell state. The proposed protocol integrates the ideas of block transmission [4, 7], two-step transmission [4, 7] and unitary operation encoding [7] together using the Bell states as the information carriers. Besides the entanglement swapping between any two Bell states, a shared secret Bell state is also used to overcome the information leakage problem. The shared secret Bell state has two functions in the dialogue process: firstly, it makes Bob aware of the prepared initial state; secondly, it is used for Bob’s encoding and entanglement swapping. Security analysis shows that the proposed protocol can resist general active attacks from an outside eavesdropper Eve. Moreover, the relation between the maximal amount of information Eve can gain and the detection probability is derived.

Acknowledgments

The authors thank the anonymous reviewers for valuable comments and suggestions on the improvement of this paper. Funding by the National Natural Science Foundation of China (grant number 11375152) and the Natural Science Foundation of Zhejiang Province (grant number LQ12F02012) is also gratefully acknowledged.

References

[1] Bennett C H and Brassard G 1984 Proc. Int. Conf. on Computers, Systems & Signal Processing (Bangalore, India) (New York: IEEE) p. 175
[2] Bennett C H, Brassard G and Mermin N D 1992 Phys. Rev. Lett. 68 557
[3] Cabell A 2000 Phys. Rev. Lett. 85 5635
[4] Long G L and Liu X S 2002 Phys. Rev. A 65 032302
[5] Xue P, Li C F and Guo G C 2002 Phys. Rev. A 65 022317
[6] Yan T and Yan F L 2011 Chin. Sci. Bull. 56 24
[7] Deng F G, Long G L and Liu X S 2003 Phys. Rev. A 68 042317
[8] Bostrom K and Felbinger T 2002 Phys. Rev. Lett. 89 187902
[9] Cai Q Y and Li B W 2004 Phys. Rev. A 69 054301
[10] Deng F G and Long G L 2004 Phys. Rev. A 69 052319
[11] Wang C, Deng F G and Long G L 2005 Opt. Commun. 253 15
[12] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 Chin. Phys. 16 2149
[13] Chen X B, Wang T Y, Du J Z, Wen Q Y and Zhu F C 2008 Int. J. Quantum Inform. 6 543
[14] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 Int. J. Quantum Inform. 6 899
[15] Yang C W, Tsai C W and Hwang T 2011 Sci. China G 54 496
[16] Li J, Jin H F and Jing B 2012 Chin. Sci. Bull. 57 4434
[17] Song S Y and Wang C 2012 Chin. Sci. Bull. 57 4694
[18] Zhang Z J and Man Z X 2004 arXiv:quant-ph/0403215v1
[19] Zhang Z J and Man Z X 2004 arXiv:quant-ph/0403217v4
[20] Nguyen B A 2004 Phys. Lett. A 326 6
[21] Man Z X, Zhang Z J and Li Y 2005 Chin. Phys. Lett. 22 22
[22] Jin X R et al 2006 Phys. Lett. A 354 67
[23] Man Z X and Xia Y J 2006 Chin. Phys. Lett. 23 1680
[24] Man Z X, Xia Y J and Nguyen B A 2006 J. Phys. B: At. Mol. Opt. Phys. 39 3855
[25] Ji X and Zhang S 2006 Chin. Phys. 15 1418
[26] Yang Y G and Wen Q Y 2007 Sci. China Ser. G 50 558
[27] Chen Y, Man Z X and Xia Y J 2007 Chin. Phys. Lett. 24 19
[28] Shan C J, Liu J B, Cheng W W, Liu T K, Huang Y X and Li H 2009 Mod. Phys. Lett. B 23 3225
[29] Man Z X and Xia Y J 2007 Chin. Phys. Lett. 24 15
[30] Gao F, Qin S J, Wen Q Y and Zhu F C 2008 Phys. Lett. A 372 3333
[31] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 Sci. China G 51 559
[32] Tan Y G and Cai Q Y 2008 Int. J. Quantum Inform. 6 325
[33] Shi G F, Xi X Q, Tian X L and Yue R H 2009 Opt. Commun. 282 2460
[34] Shi G F, Xi X Q, Hu M L and Yue R H 2010 Opt. Commun. 283 1984
[35] Shi G F, Xi X Q, Tian X L and Yue R H 2010 Opt. Commun. 283 1984
[36] Gao F 2010 Opt. Commun. 283 5275
[37] Ye T Y and Jiang L Z 2013 Chin. Phys. Lett. 30 040305
[38] Liu Z H and Chen H W 2013 Chin. Phys. Lett. 30 079901
[39] Ye T Y and Jiang L Z 2013 Chin. Phys. Lett. 30 079902