doi:10.3788/gzxb20134211.1305

基于布朗态受控的安全量子对话方案

杨幼凤,叶志清,涂春雷
(江西师范大学 物理与通信电子学院;江西省光电子与通信重点实验室,南昌 330022)

摘 要:提出了一个基于布朗态受控安全量子对话方案.Alice、Bob 和 Charlie 共享一个五粒子布朗态,Alice 将自己要传递给 Bob 的秘密信息通过对其中两个粒子做幺正变换,实现待传的经典信息的编码;同理,Bob 对另外两个粒子做相应的幺正操作,实现待传的经典信息的编码;随后,Charlie 对布朗终态做布朗基的联合测量,并公布测量结果;Alice 和 Bob 根据 Charlie 公布的结果及自己编码时用的幺正变换,解码出对方传送的经典信息,完成安全量子对话.与以往的量子对话相比,该方案不仅增加了第三方控制,确保了通信双方对话安全,而且增加了参与通信过程的粒子数目,提高了编码效率.

关键词:量子对话;布朗态;安全;高编码效率
中图分类号:TN918 **文献标识码**:A **文章编号**:1004-4213(2013)11-1305-6

Controlled Secure Quantum Dialogue by Using Brown States

YANG You-feng, YE Zhi-qing, TU Chun-lei
(*College of Physics and Communication Electronic; Key Laboratory of Photoelectronics & Telecommunication of Jiangxi Province, Jiangxi Normal University, Nanchang* 330022, *China*)

Abstract: A novel scheme of controlled secure quantum dialogue by using Brown states was proposed in this paper. It this scheme, Alice, Bob and Charlie shared a five-particle Brown states. Alice made unitary operations on two particles of the Brown states to realize encoding her secret calssical message. Similarly, Bob performed corresponding unitary transformations to another two particles to encode the information that he wanted to send to Alice. Later, Charlie made Brown base states joint measurement on the Brown final state and announced the measured results. Alice and Bob deduced the opposite party′s information according to Charlie′s announced measurement results and her (his) unitary operation when encoding. They completed quantum dialogue successfully. Then the scheme′s security was discussed and a conclusion was drawn. Compared with the previous quantum dialogues, the secure quantum dialogue scheme adds the controlled party, ensures the communication security, and increases the particles number involving in the communication process and the coding efficiency.

Key words: Quantum dialogue; Brown states; Secure; High encoding efficiency

0 Introduction

Quantum key distribution protocol (QKD) was first proposed by Bennett and Brassard in 1984. Different from the QKD, quantum secure direct communication (QSDC) and deterministic secure quantum communication (DSQC) have shown that the secret information can be

Foundation item: The National Natural Science Foundation of China (No. 61368001), the Natural Science Foundation of Jiangxi Province (No. 20114BAB202003) and the Scientific Research Project of Jiangxi Province Education department(No. GJJ10401)

First author: YANG You-feng (1988 —), female, M. S. degree candidate, mainly focuses on quantum communication. Email: yangyoufeng2007@126.com

Supervisor(Corresponding author): YE Zhi-qing(1960—), male, professor, M. S. degree, mainly focuses on quantum communication, fiber grating sensor. Email: yezhiqing2008@163.com

Received: May. 27, 2013; **Accepted**: Jun. 28, 2013

transmitted directly from Alice to Bob, without creating a random key to encrypt the message beforehand. In another word, in these protocols, Alice and Bob (two legitimate users) cannot exchange their useful information simultaneously. Nguyen proposed the first quantum dialogue protocol[1] (QD) in 2004, overcoming the shortage. Since then, QD[2-4] has attracted the researchers' high attention. Later on, Xia *et al*. presented a quantum dialogue using GHZ states and Dong *et al*. proposed a quantum dialogue protocol using W states[2]. However GAO[5] *et al*. pointed out the transmitted information would be partly leaked out in some quantum dialogue[1,6]. So in order to solve the problem, the scholars focus on the controlled quantum dialogue[7-8]. It has become a hot spot. In the meantime, multi-particle entangled states quantum communication[9-14] draws some researchers' great interest, to acquire a better communication scheme. Different from the existed QDPs, it is using Brown states that the protocol of secure quantum dialogue is proposed in this paper. The protocol not only ensures the security of the communication process by means of adding the controlled party Charlie and inserting the decoy photons in the particles sequence which are used to carry secret information by making unitary operations, but also improves the coding efficiency via increasing the particles numbers used to communication one time.

A scheme of secure quantum dialogue by using Brown states is shown at length in Sec. 2. Then, in Sec. 3, we analyze the security of the scheme. Finally, we draw a conclusion in Sec. 4.

1 Scheme of SQD using Brown states

The whole communication system is composed of two legitimate users (Alice, Bob) and a controller(Charlie). Alice and Bob can exchange their useful secret information simultaneously and securely under the control of Charlie. First of all, Alice, Bob and Charlie share a Brown states $|B_0\rangle$, first proposed by Brown[15].

There are thirty-two mutually orthogonal Brown states in all, we show them as follows

$$|B_0\rangle=\frac{1}{2}(|001\rangle|\phi^-\rangle+|010\rangle|\varphi^-\rangle+|100\rangle|\phi^+\rangle+|111\rangle|\varphi^+\rangle)$$

$$|B_1\rangle=\frac{1}{2}(|001\rangle|\phi^-\rangle+|010\rangle|\varphi^-\rangle-|100\rangle|\phi^+\rangle-|111\rangle|\varphi^+\rangle)$$

$$|B_2\rangle=\frac{1}{2}(|001\rangle|\phi^-\rangle-|010\rangle|\varphi^-\rangle-|100\rangle|\phi^+\rangle+|111\rangle|\varphi^+\rangle)$$

$$|B_3\rangle=\frac{1}{2}(|001\rangle|\phi^-\rangle-|010\rangle|\varphi^-\rangle+|100\rangle|\phi^+\rangle-|111\rangle|\varphi^+\rangle)$$

$$|B_4\rangle=\frac{1}{2}(|001\rangle|\varphi^-\rangle+|010\rangle|\phi^-\rangle+|100\rangle|\varphi^+\rangle+|111\rangle|\phi^+\rangle)$$

$$|B_5\rangle=\frac{1}{2}(|001\rangle|\varphi^-\rangle+|010\rangle|\phi^-\rangle-|100\rangle|\varphi^+\rangle-|111\rangle|\phi^+\rangle)$$

$$|B_6\rangle=\frac{1}{2}(|001\rangle|\varphi^-\rangle-|010\rangle|\phi^-\rangle-|100\rangle|\varphi^+\rangle+|111\rangle|\phi^+\rangle)$$

$$|B_7\rangle=\frac{1}{2}(|001\rangle|\varphi^-\rangle-|010\rangle|\phi^-\rangle+|100\rangle|\varphi^+\rangle-|111\rangle|\phi^+\rangle)$$

$$|B_8\rangle=\frac{1}{2}(|001\rangle|\varphi^+\rangle+|010\rangle|\phi^+\rangle+|100\rangle|\varphi^-\rangle+|111\rangle|\phi^-\rangle)$$

$$|B_9\rangle=\frac{1}{2}(|001\rangle|\varphi^+\rangle+|010\rangle|\phi^+\rangle-|100\rangle|\varphi^-\rangle-|111\rangle|\phi^-\rangle)$$

$$|B_{10}\rangle=\frac{1}{2}(|001\rangle|\varphi^+\rangle-|010\rangle|\phi^+\rangle-|100\rangle|\varphi^-\rangle+|111\rangle|\phi^-\rangle)$$

$$|B_{11}\rangle=\frac{1}{2}(|001\rangle|\varphi^+\rangle-|010\rangle|\phi^+\rangle+|100\rangle|\varphi^-\rangle-|111\rangle|\phi^-\rangle)$$

$$|B_{12}\rangle=\frac{1}{2}(|001\rangle|\phi^+\rangle+|010\rangle|\varphi^+\rangle+|100\rangle|\phi^-\rangle+|111\rangle|\varphi^-\rangle)$$

$$|B_{13}\rangle=\frac{1}{2}(|001\rangle|\phi^+\rangle+|010\rangle|\varphi^+\rangle-|100\rangle|\phi^-\rangle-|111\rangle|\varphi^-\rangle)$$

$$|B_{14}\rangle=\frac{1}{2}(|001\rangle|\phi^+\rangle-|010\rangle|\varphi^+\rangle-|100\rangle|\phi^-\rangle+|111\rangle|\varphi^-\rangle)$$

$$|B_{15}\rangle=\frac{1}{2}(|001\rangle|\phi^+\rangle-|010\rangle|\varphi^+\rangle+|100\rangle|\phi^-\rangle-|111\rangle|\varphi^-\rangle)$$

$$|B_{16}\rangle=\frac{1}{2}(|011\rangle|\phi^-\rangle+|000\rangle|\varphi^-\rangle+|110\rangle|\phi^+\rangle+|101\rangle|\varphi^+\rangle)$$

$$|B_{17}\rangle=\frac{1}{2}(|011\rangle|\phi^-\rangle+|000\rangle|\varphi^-\rangle-|110\rangle|\phi^+\rangle-|101\rangle|\varphi^+\rangle)$$

$$|B_{18}\rangle=\frac{1}{2}(|011\rangle|\phi^-\rangle-|000\rangle|\varphi^-\rangle-|110\rangle|\phi^+\rangle+|101\rangle|\varphi^+\rangle)$$

$$|B_{19}\rangle=\frac{1}{2}(|011\rangle|\phi^-\rangle-|000\rangle|\varphi^-\rangle+|110\rangle|\phi^+\rangle-|101\rangle|\varphi^+\rangle)$$

$$|B_{20}\rangle=\frac{1}{2}(|011\rangle|\varphi^-\rangle+|000\rangle|\phi^-\rangle+|110\rangle|\varphi^+\rangle+|101\rangle|\phi^+\rangle)$$

$$|B_{21}\rangle=\frac{1}{2}(|011\rangle|\varphi^-\rangle+|000\rangle|\phi^-\rangle-|110\rangle|\varphi^+\rangle-|101\rangle|\phi^+\rangle)$$

$$|B_{22}\rangle=\frac{1}{2}(|011\rangle|\varphi^-\rangle-|000\rangle|\phi^-\rangle-|110\rangle|\varphi^+\rangle+|101\rangle|\phi^+\rangle)$$

$$|B_{23}\rangle=\frac{1}{2}(|011\rangle|\varphi^-\rangle-|000\rangle|\phi^-\rangle+|110\rangle|\varphi^+\rangle-|101\rangle|\phi^+\rangle)$$

$$|B_{24}\rangle=\frac{1}{2}(|011\rangle|\varphi^+\rangle+|000\rangle|\phi^+\rangle+|110\rangle|\varphi^-\rangle+|101\rangle|\phi^-\rangle)$$

$$|B_{25}\rangle=\frac{1}{2}(|011\rangle|\varphi^+\rangle+|000\rangle|\phi^+\rangle-|110\rangle|\varphi^-\rangle-|101\rangle|\phi^-\rangle)$$

$$|B_{26}\rangle=\frac{1}{2}(|011\rangle|\varphi^+\rangle-|000\rangle|\phi^+\rangle-|110\rangle|\varphi^-\rangle+|101\rangle|\phi^-\rangle)$$

$$|B_{27}\rangle=\frac{1}{2}(|011\rangle|\varphi^+\rangle-|000\rangle|\phi^+\rangle+|110\rangle|\varphi^-\rangle-|101\rangle|\phi^-\rangle)$$

$$|B_{28}\rangle=\frac{1}{2}(|011\rangle|\phi^+\rangle+|000\rangle|\varphi^+\rangle+|110\rangle|\phi^-\rangle+|101\rangle|\varphi^-\rangle)$$

$$|B_{29}\rangle=\frac{1}{2}(|011\rangle|\phi^+\rangle+|000\rangle|\varphi^+\rangle-|110\rangle|\phi^-\rangle-|101|\varphi^-\rangle)$$

$$|B_{30}\rangle=\frac{1}{2}(|011\rangle|\phi^+\rangle-|000\rangle|\varphi^+\rangle-|110\rangle|\phi^-\rangle+|101\rangle|\varphi^-\rangle)$$

$$|B_{31}\rangle=\frac{1}{2}(|011\rangle|\phi^+\rangle-|000\rangle|\varphi^+\rangle+|110\rangle|\phi^-\rangle-|101\rangle|\varphi^-\rangle) \quad (1)$$

where

$$|\phi^\pm\rangle=\frac{\sqrt{2}}{2}(|00\rangle\pm|11\rangle)$$

$$|\varphi^\pm\rangle=\frac{\sqrt{2}}{2}(|01\rangle\pm|10\rangle) \quad (2)$$

are four Bell states.

Before they start to communication, two communication parties Alice and Bob make a deal that every pauli matrix denotes a kind of classical information. The deal can be given by

$$\sigma^0=I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \sigma^1=\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$\sigma^2=\sigma_y=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \sigma^3=\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

$I\rightarrow 00$, $\sigma_x\rightarrow 01$, $\sigma_y\rightarrow 10$, $\sigma_z\rightarrow 11$

After the preparation, the whole communication program can be realized according to the following detailed steps.

Step 1: Preparation of Brown states and checking qubits.

In order to realize a controlled quantum dialogue, Charlie prepares large numbers (N) of Brown states, which are in the state $|B_0\rangle_n$, first, where $n\in\{1,N\}$. We divide the ordered N five-qubit states into three groups and denote them with three ordered sequence: P_A- sequence: $\{P_1(A), P_1(A'), P_2(A), P_2(A'), \cdots, P_N(A), P_N(A')\}$; P_B- sequence: $\{P_1(B), P_1(B'), P_2(B), P_2(B'), \cdots, P_N(B), P_N(B')\}$; P_c- sequence: $\{P_1(C), P_2(C), \cdots, P_N(C)\}$, where the subscripts indicates the order of each particle in each sequence.

Then, Charlie produces a series of ($2Nm$) decoy photons which are in the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ randomly as checking qubits. Charlie inserts Nm decoy photons into these sequences P_A and P_B randomly, respectively and forms two new sequences named P_A', P_B'. At last, Charlie sends the reordered sequences P_A' to Alice, P_B' to Bob. The sequence P_c is kept to herself. The actual order of two sequences P_A, P_B are just known to Charlie.

$$|+\rangle=(\frac{1}{\sqrt{2}})(|0\rangle+|1\rangle)$$

$$|-\rangle=(\frac{1}{\sqrt{2}})(|0\rangle-|1\rangle) \quad (3)$$

Step 2: First process of security checking

After confirming Alice and Bob have already received sequences P_A', P_B' sent by himself, Charlie publicly announces the position of the decoy photons in different sequences. Alice performs projective measurements on the corresponding decoy photons particles in her sequence P_A' by using X basis or Z basis at random, here, ($X=\{|+\rangle,|-\rangle\}$, $Z=\{|0\rangle, |1\rangle\}$). After the measurements, Alice publicly tells her measurement outcomes and the basis she has used. The initial state of the decoy photon is known to Charlie. In principle, the measurement results of Alice should coincide with the basis which Charlie has used to prepare the decoy photon. Charlie can compute the error rate by comparing with the results told by Alice and check whether it exceeds the predeclared threshold or not. If it doesn't exceed the threshold, that means there is no eavesdropping i. e. our communication is secure, then go to the next step, or we will abort this communication to turn to step 1. The same to

Bob.

Step 3: Encoding process of Alice and Bob

Alice and Bob wipe out the decoy photons from Charlie in the sequence P_A', P_B', then encode their classical information on the true particles by performing the corresponding unitary operations. After completing the process of encoding, Alice and Bob randomly insert Nm new decoy states created by themselves in the true particles having been encoded secret message, to form two brand new sequences P_A'', P_B'', then send them back to Charlie.

Step 4: Second security checking process

After confirming Charlie have received the sequences P_A'', P_B'', Alice publicizes her decoy photons position. Charlie performs projective measurement to decoy photons and announces the measured results and the basis she has used. In principle, Charlie′s measured results should coincide with the basis Alice has used to prepare the decoy photons. Compared with the results announced by Charlie, Alice can compute the error rate and check if it exceeds the predeclared threshold. If it exceeds the threshold, that means there is Eves on the line, i. e. our communication is not safe, then they will abandon this communication, or they will go to the next step. Charlie will do something to Bob in the same way, too.

Step 5: Decoding process of Alice and Bob

Charlie makes five-particle Brown states $|B_0\rangle$ joint measurement to the final state and publicizes the measured outcomes by using classical channel. Alice and Bob can deduce the counterpart′s secret message according to Charlie′s measurement results and themselves operators, as shown in Table 1.

Table 1 Corresponding relations between Alice′s and Bob′s unitary operations with the final state measured in base $|B_0\rangle$. Alice′s (Bob′s) unitary operations listed in the first line(column)

	U_0	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9	U_{10}	U_{11}	U_{12}	U_{13}	U_{14}	U_{15}
U_0	$\|B_0\rangle$	$\|B_{16}\rangle$	$\|B_{19}\rangle$	$\|B_3\rangle$	$\|B_{24}\rangle$	$\|B_8\rangle$	$\|B_{11}\rangle$	$\|B_{27}\rangle$	$\|B_{25}\rangle$	$\|B_9\rangle$	$\|B_{10}\rangle$	$\|B_{26}\rangle$	$\|B_1\rangle$	$\|B_{17}\rangle$	$\|B_{18}\rangle$	$\|B_2\rangle$
U_1	$\|B_4\rangle$	$\|B_{20}\rangle$	$\|B_{23}\rangle$	$\|B_7\rangle$	$\|B_{28}\rangle$	$\|B_{12}\rangle$	$\|B_{15}\rangle$	$\|B_{31}\rangle$	$\|B_{29}\rangle$	$\|B_{13}\rangle$	$\|B_{14}\rangle$	$\|B_{30}\rangle$	$\|B_5\rangle$	$\|B_{21}\rangle$	$\|B_{22}\rangle$	$\|B_6\rangle$
U_2	$\|B_{11}\rangle$	$\|B_{27}\rangle$	$\|B_{24}\rangle$	$\|B_8\rangle$	$\|B_{19}\rangle$	$\|B_3\rangle$	$\|B_0\rangle$	$\|B_{16}\rangle$	$\|B_{18}\rangle$	$\|B_2\rangle$	$\|B_1\rangle$	$\|B_{17}\rangle$	$\|B_{10}\rangle$	$\|B_{26}\rangle$	$\|B_{25}\rangle$	$\|B_9\rangle$
U_3	$\|B_{15}\rangle$	$\|B_{31}\rangle$	$\|B_{28}\rangle$	$\|B_{12}\rangle$	$\|B_{23}\rangle$	$\|B_7\rangle$	$\|B_4\rangle$	$\|B_{20}\rangle$	$\|B_{22}\rangle$	$\|B_6\rangle$	$\|B_5\rangle$	$\|B_{21}\rangle$	$\|B_{14}\rangle$	$\|B_{30}\rangle$	$\|B_{29}\rangle$	$\|B_{13}\rangle$
U_4	$\|B_5\rangle$	$\|B_{21}\rangle$	$\|B_{22}\rangle$	$\|B_6\rangle$	$\|B_{29}\rangle$	$\|B_{13}\rangle$	$\|B_{14}\rangle$	$\|B_{30}\rangle$	$\|B_{28}\rangle$	$\|B_{12}\rangle$	$\|B_{12}\rangle$	$\|B_{31}\rangle$	$\|B_4\rangle$	$\|B_{20}\rangle$	$\|B_{23}\rangle$	$\|B_7\rangle$
U_5	$\|B_1\rangle$	$\|B_{17}\rangle$	$\|B_{18}\rangle$	$\|B_2\rangle$	$\|B_{25}\rangle$	$\|B_9\rangle$	$\|B_{10}\rangle$	$\|B_{26}\rangle$	$\|B_{24}\rangle$	$\|B_8\rangle$	$\|B_{11}\rangle$	$\|B_{27}\rangle$	$\|B_0\rangle$	$\|B_{16}\rangle$	$\|B_{19}\rangle$	$\|B_3\rangle$
U_6	$\|B_{14}\rangle$	$\|B_{30}\rangle$	$\|B_{29}\rangle$	$\|B_{13}\rangle$	$\|B_{22}\rangle$	$\|B_6\rangle$	$\|B_5\rangle$	$\|B_{21}\rangle$	$\|B_{23}\rangle$	$\|B_7\rangle$	$\|B_4\rangle$	$\|B_{20}\rangle$	$\|B_{15}\rangle$	$\|B_{31}\rangle$	$\|B_{28}\rangle$	$\|B_{12}\rangle$
U_7	$\|B_{10}\rangle$	$\|B_{26}\rangle$	$\|B_{25}\rangle$	$\|B_9\rangle$	$\|B_{18}\rangle$	$\|B_2\rangle$	$\|B_1\rangle$	$\|B_{17}\rangle$	$\|B_{19}\rangle$	$\|B_3\rangle$	$\|B_0\rangle$	$\|B_{16}\rangle$	$\|B_{11}\rangle$	$\|B_{27}\rangle$	$\|B_{24}\rangle$	$\|B_8\rangle$
U_8	$\|B_8\rangle$	$\|B_{25}\rangle$	$\|B_{26}\rangle$	$\|B_{11}\rangle$	$\|B_{17}\rangle$	$\|B_1\rangle$	$\|B_2\rangle$	$\|B_{18}\rangle$	$\|B_{16}\rangle$	$\|B_0\rangle$	$\|B_3\rangle$	$\|B_{19}\rangle$	$\|B_9\rangle$	$\|B_{24}\rangle$	$\|B_{27}\rangle$	$\|B_{10}\rangle$
U_9	$\|B_{13}\rangle$	$\|B_{29}\rangle$	$\|B_{30}\rangle$	$\|B_{14}\rangle$	$\|B_{21}\rangle$	$\|B_5\rangle$	$\|B_6\rangle$	$\|B_{22}\rangle$	$\|B_{20}\rangle$	$\|B_4\rangle$	$\|B_7\rangle$	$\|B_{23}\rangle$	$\|B_{12}\rangle$	$\|B_{28}\rangle$	$\|B_{31}\rangle$	$\|B_{15}\rangle$
U_{10}	$\|B_2\rangle$	$\|B_{18}\rangle$	$\|B_{17}\rangle$	$\|B_1\rangle$	$\|B_{26}\rangle$	$\|B_{10}\rangle$	$\|B_9\rangle$	$\|B_{25}\rangle$	$\|B_{27}\rangle$	$\|B_{11}\rangle$	$\|B_8\rangle$	$\|B_{24}\rangle$	$\|B_3\rangle$	$\|B_{19}\rangle$	$\|B_{16}\rangle$	$\|B_0\rangle$
U_{11}	$\|B_6\rangle$	$\|B_{22}\rangle$	$\|B_{21}\rangle$	$\|B_5\rangle$	$\|B_{30}\rangle$	$\|B_{14}\rangle$	$\|B_{13}\rangle$	$\|B_{29}\rangle$	$\|B_{31}\rangle$	$\|B_{15}\rangle$	$\|B_{15}\rangle$	$\|B_{28}\rangle$	$\|B_7\rangle$	$\|B_{23}\rangle$	$\|B_{20}\rangle$	$\|B_4\rangle$
U_{12}	$\|B_{12}\rangle$	$\|B_{28}\rangle$	$\|B_{31}\rangle$	$\|B_{15}\rangle$	$\|B_{20}\rangle$	$\|B_4\rangle$	$\|B_7\rangle$	$\|B_{23}\rangle$	$\|B_{21}\rangle$	$\|B_5\rangle$	$\|B_6\rangle$	$\|B_{22}\rangle$	$\|B_{13}\rangle$	$\|B_{29}\rangle$	$\|B_{30}\rangle$	$\|B_{14}\rangle$
U_{13}	$\|B_9\rangle$	$\|B_{24}\rangle$	$\|B_{27}\rangle$	$\|B_{10}\rangle$	$\|B_{16}\rangle$	$\|B_0\rangle$	$\|B_3\rangle$	$\|B_{19}\rangle$	$\|B_{17}\rangle$	$\|B_1\rangle$	$\|B_2\rangle$	$\|B_{18}\rangle$	$\|B_8\rangle$	$\|B_{25}\rangle$	$\|B_{26}\rangle$	$\|B_{11}\rangle$
U_{14}	$\|B_7\rangle$	$\|B_{23}\rangle$	$\|B_{20}\rangle$	$\|B_4\rangle$	$\|B_{31}\rangle$	$\|B_{15}\rangle$	$\|B_{12}\rangle$	$\|B_{28}\rangle$	$\|B_{30}\rangle$	$\|B_{14}\rangle$	$\|B_{13}\rangle$	$\|B_{29}\rangle$	$\|B_6\rangle$	$\|B_{22}\rangle$	$\|B_{21}\rangle$	$\|B_5\rangle$
U_{15}	$\|B_3\rangle$	$\|B_{19}\rangle$	$\|B_{16}\rangle$	$\|B_0\rangle$	$\|B_{27}\rangle$	$\|B_{11}\rangle$	$\|B_8\rangle$	$\|B_{24}\rangle$	$\|B_{26}\rangle$	$\|B_{10}\rangle$	$\|B_9\rangle$	$\|B_{25}\rangle$	$\|B_2\rangle$	$\|B_{18}\rangle$	$\|B_{17}\rangle$	$\|B_1\rangle$

Note: $U_0=\sigma_M^0\sigma_N^0$, $U_1=\sigma_M^0\sigma_N^1$, $U_2=\sigma_M^0\sigma_N^2$, $U_3=\sigma_M^0\sigma_N^3$; $U_4=\sigma_M^1\sigma_N^0$, $U_5=\sigma_M^1\sigma_N^1$, $U_6=\sigma_M^1\sigma_N^2$, $U_7=\sigma_M^1\sigma_N^3$, $U_8=\sigma_M^2\sigma_N^0$, $U_9=\sigma_M^2\sigma_N^1$, $U_{10}=\sigma_M^2\sigma_N^2$, $U_{11}=\sigma_M^2\sigma_N^3$; $U_{12}=\sigma_M^3\sigma_N^0$, $U_{13}=\sigma_M^3\sigma_N^1$, $U_{14}=\sigma_M^3\sigma_N^2$, $U_{15}=\sigma_M^3\sigma_N^3$, $\sigma_M^i\sigma_N^j$ $(i,j=0,1,2,3)$ represents making unitary operation on two different particles M and N

To sum up, the controlled secure quantum dialogue has been realized successfully.

During one time communication, both Alice and Bob can get four-bit information only by her (his) two particles, thus this scheme increase encoding efficiency, i. e. improving the channel capacity.

In all, the whole communication plan can be expressed with the following formula

$$|B_n\rangle_{A_nA_n'C_nB_nB_n'}=|B\rangle_{\text{final}}=U_pU_q|B_0\rangle_{A_nA_n'C_nB_nB_n'}=\sigma_{A_n}^i\sigma_{A_n'}^j\sigma_B^{i'}\sigma_{B_n'}^{j'}|B_0\rangle_{A_nA_n'C_nB_nB_n'} \quad (4)$$

Here, $p,q=0,1,2,\cdots,15$, $i,j,i',j'=0,1,2,3$.

Take an example, Charlie prepares the following state as quantum channel

$$|\psi\rangle=|B_0\rangle_{A_1A_1'C_1B_1B_1'}|B_0\rangle_{A_2A_2'C_2B_2B_2'} \quad (5)$$

Supposing Alice wants to send classical secret information 01001100 to Bob, she performs unitary operations $(\sigma_{A_1}^1\sigma_{A_1}^{0'},\sigma_{A_2}^3\sigma_{A_2}^{0'})$ on $|\psi\rangle$. Bob wants to transmit classical secret message 11101000 to Alice, he encodes his secret message on $|\psi\rangle$ by making the unitary operations $(\sigma_{B_1}^3\sigma_{B_1}^{2'},\sigma_{B_2}^2\sigma_{B_2}^{0'})$.

$$|\psi'\rangle=\sigma_{A_1}^1\sigma_{A_1}^{0'}\sigma_{A_2}^3\sigma_{A_2}^{0'}\sigma_{B_1}^3\sigma_{B_1}^{2'}\sigma_{B_2}^2\sigma_{B_2}^{0'}|\psi\rangle \quad (6)$$

Charlie measures the final state $|\psi'\rangle$ in the Brown base states $|B_0\rangle_n$. She tells her measurement results publicly. After knowing Charlie′s Brown base measurement results, the initial state $|B_0\rangle_n$ and her unitary operations, Alice can conclude the exact unitary operators performed by Bob on B_1, B_1', B_2, B_2'. She can deduce eight-bit message 11101000 from Bob. Similarly, Bob can get information 01001100 from Alice. From the Table 1, we can get the results fast and conveniently.

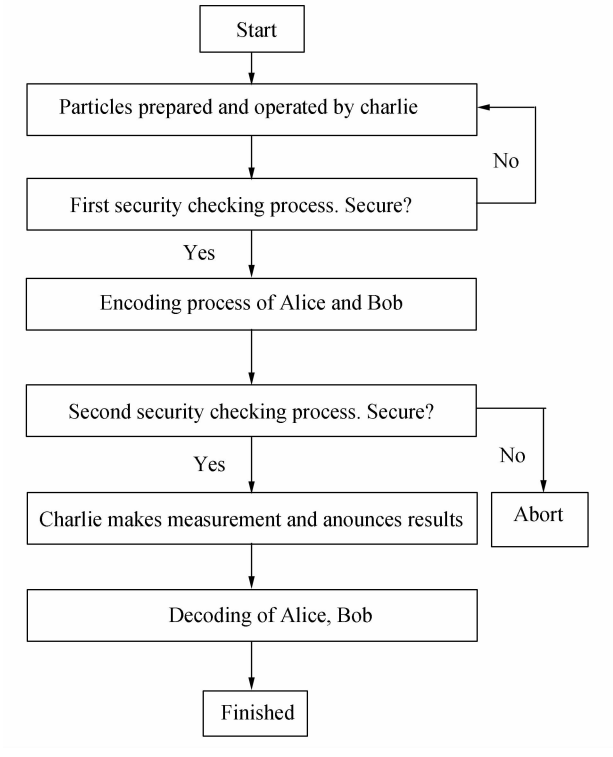

Fig. 1　The flow chart of the controlled secure quantum dialogue′s working process

2　Security

In our scheme, c_n, one particle of the Brown states, has always been kept in the controller Charlie′s hand securely, which is similar to BBM92 QKD protocol[16]. Eve cannot makes Brown base states joint measurement just getting part particles of the entangled states, because the secret message is encoded in the whole Brown states. So Eve cannot get any meaningful information.

From the entire communication process, we can find out there are two eavesdropping checking test. One is implemented after Alice and Bob receive the particles (i. e. Step 2), the other is done after Charlie gets encoding particles from Alice and Bob (i. e. Step 4). The two checking processes are similar. Eves′ attack can be detected by making the measurements on the decoy photons inserted in the sequence and comparing the measured results. If their measurement results coincide when they use the same basis to measure, then there not exist Eves. The steps of security checking process make the Eves on the line impossible to get any useful secret information successfully. Suppose Eve can make measurements on the intercepted particles, Eve only can obtain a random result of the secret message on the quantum channel. She cannot distinguish the true particles from the whole sequence. However, considering the decoherence effect and possible network eavesdropping in the real communication system, we analysis the communication efficiency and security. In the Cabello′s definition[17], the efficiency is $\eta = b_s/(q_t + b_t)$, where η denotes a quantum communication scheme efficiency, b_s is the total number of transmitted secret message, q_t and b_t denote the total number of qubits and the number of classical bits exchanged for decoding the message respectively. Here $b_s = 8N$, $q_t = 5N + 10Nm$, $b_t = 5N$, our efficiency is $\eta = 8N/(5N + 10Nm + 5N) = 4/(5 + 2m)$. If $m = 1$, then $\eta = 57.2\%$, which is higher than the QKD′s efficiency. Supposing Eve guesses that the initial state is $|B_0\rangle$, however, the final state has 32 kinds of results, and every final state owns 8 corresponding possible unitary operations, then there are total 256 possibilities, containing $-\sum_i p_i \log_2 p_i = -256 \times \frac{1}{256} \log_2 \frac{1}{256} = 7$ bit secret information for Eve. That′s mean only 1 bit information is possible to leak out, i. e. it′s very difficult to get useful information. To sum up, our proposed scheme is secure.

3　Conclusion

In summary, we proposed a novel scheme of controlled secure quantum dialogue based on Brown states for two authorized parties to exchange their secret message securely and simultaneously under the control of Charlie. Compared with the existed quantum dialogues, there are several advantages. In the whole process of communication, we add the controller and insert decoy photons twice to ensure security of the whole communication system, and improve the encoding efficiency by increasing the particle numbers joining in the communication process. To some extent, the idea has reference value in practical quantum communication in the near future.

References

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

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

[3] ZHAN You-bang, ZHANG Ling-ling, WANG Yu-wu. Quantum dialogue by using non-symmetric quantum channel [J]. *Communications in Theoretical Physics*, 2010, **53**(4): 2288-2293.

[4] LI Dong, XIU Xiao-ming, GAO Ya-jun, *et al*. Quantum dialogue protocol using a class of three-photon w states[J]. *Communications in Theoretical Physics*, 2009, **52**(5): 853-856.

[5] GAO Fei, GUO Fen-zhuo, WEN Qiao-yan, *et al*. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication[J]. *Science in China Series G: Physics, Mechanics & Astronomy*, 2008, **51**(5): 559-566.

[6] MAN Zhong-xiao, ZHANG Zhan-jun, LI Yong. Quantum dialogue revisited[J]. *Chinese Physics Letters*, 2005, **22**(1): 22-24.

[7] ZOU Xin, YE Zhi-qing. Controlled by a third party to realize quantum secure dialogue[J]. *Acta Photonica Sinica*, 2012, **41**(4): 501-504.

[8] XIA Yan, SONG Jie, SONG He-shan. Controlled secure quantun dialogue using a pure entangled GHZ states[J]. *Communications in Theoretical Physics*, 2007, **48**(5): 841-846.

[9] XIU Xiao-ming. LI Dong, GAO Ya-jun, *et al*. Controlled deterministic secure quantum communication using five-qubit entangled states and two-step security test [J]. *Optics Communications*, 2009, **282**(2): 333-337.

[10] WANG Dong, ZHA Xin-wei. Quantum communication based on cluster state [J]. *Chinese Journal of Quantum Electronics*, 2011, **28**(6): 687-692.

[11] LIU Jun-chang, LI Yuan-hua, NIE Yi-you. Controlled teleportation of two an arbitrary two-particle state by using a four-qubit cluster state and entanglement swapping[J]. *Acta Photonica Sinica*, 2010, **39**(11): 2078-2083.

[12] LI Yuan-hua, LIU Jun-chang, NIE Yi-you. Quantum information splitting by using a genuinely entangled six-qubit and Bell-state measurements[J]. *Acta Photonica Sinica*, 2011, **40**(2): 307-310.

[13] SHUKLA C, KOTHARI V, BANER J, *et al*. On the group-theotetic struvture of a class of quantum dialogue protocols [J]. *Physics Letters A*, 2013, **377**(7): 518-527.

[14] YANG You-feng, YE Zhi-qing. Scheme of two-way quantum teleportation and security[J]. *Acta Photonica Sinica*, 2013, **42**(5): 619-622.

[15] BROWN I D K, STEPNEY S, SUDBERY A. Searching for highly entangled multi-qubit states[J]. *Journal of physcis A: Mathematical and General*, 2005, **38**(5): 1119-1131.

[16] BENNETT C H, BRASSARD G, MERMIN N D. Quantum cryptography without Bells theorem[J]. *Physical Review Letters*, 1992, **68**(5): 557-559.

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