doi:10.3788/gzxb20144308.0827001

基于四粒子 GHZ 态的可控量子双向隐形传态及安全性

胡钰安[1],叶志清[2]

(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:提出一个基于四粒子 GHZ 纠缠态实现未知单粒子态的可控量子双向传态方案.通信双方 Alice 和 Bob 以及控制方事先密享两对四粒子 GHZ 纠缠态以构建量子信道,根据纠缠粒子的不同分发方式,以及测量时所选择的不同测量基,可以分别实现三方和四方参与的可控量子双向传态.通信开始后,Alice 和 Bob 分别对自己拥有的部分粒子作量子投影测量,若控制方同意双方通信,则对自己拥有的粒子作测量并通过经典信道公布测量结果.通信双方根据控制方公布的测量结果对各自的某个粒子作相应的幺正变换,即可在己方的粒子上重建对方待传的量子态.由于第三方 Charlie 以及第四方 Dennis 的加入,整个双向传态的安全性大为提高.

关键词:量子通信;可控量子隐形传态;GHZ 纠缠态;Bell 基测量;安全性

中图分类号:TN911 **文献标识码**:A **文章编号**:1004-4213(2014)08-0827001-5

Controlled Two-way Quantum Teleportation via GHZ Quadripartite Entangled State and Security

HU Yu-an[1], YE Zhi-qing[2]

(*College of Physics and Communication Electronic; Key Laboratory of Photoelectronics & of Jiangxi Province, Jiangxi Normal University, Nanchang* 330022, *China*)

Abstract: A scheme for controlled two-way quantum teleportation of unknown one-qubit state via GHZ quadripartite entangled state was proposed. Two sides of communication (Alice and Bob) and the controller, secretly share two pairs of GHZ quadripartite entangled state in advance to construct quantum channel. According to the different ways of distribution along with different measuring vectors choosed to use, two-way quantum teleportation controlled by a third party and a fouth party were realized. After communication, Alice and Bob perform quantum projection measurement on parts of their qubits respectively. If the controller agrees to intercommunication, he should measure his qubits and announce the results via classical channel. Then the both sides of communication can make appropriate unitary transformations on their own certain qubit on the basis of the controller′s results, thus they are able to reconstruct each other′s unknown state on their own qubit. The security of the whole two-way communication is greatly impoved owing to the join of the third party Charlie and the fourth party Dennis.

Key words: Quantum communication; Controlled two-way quantum teleportation; GHZ entangled state; Bell-state measurement; Security

OCIS Codes: 270.0270; 270.5565; 270.5585

基金项目:国家自然科学基金(No. 61368001)资助

第一作者:胡钰安(1990—),男,硕士研究生,主要研究方向为光量子通信. Email:772315061@qq.com

导师(通讯作者):叶志清(1960—),男,博士,教授,主要研究方向为光量子通信. Email:yezhiqing2008@163.com

收稿日期:2013-12-02;**录用日期**:2014-01-27

0 引言

作为量子信息学的主要分支，量子通信[1]主要包括量子隐形传态、量子稠密编码、量子密钥分配[2]等. 量子隐形传态最早在1993年由Bennett[3]等提出，是经由经典通道和EPR通道传送未知量子态，此后量子隐形传态在理论[4-6]和实验[7]上都取得了重大进展，在实验上维也纳大学和奥地利科学院的物理学家于2012年实现了量子态隐形传态最远距离——143 km，创造了新的世界纪录. 而可控量子隐形传态则是在1998年由Karlsson[8]等以GHZ纠缠态作为量子信道而提出，是在控制方的帮助下重建待传的单粒子态. 邓[9]等介绍了一种对称性的多体可控量子隐形传态方案；周[10]等实现了通过一个纯纠缠量子信道传送一个任意量子比特态的可控量子隐形传态；洪[11]等利用四粒子团簇态实现可控量子隐形传态；邹[12]等基于Bell[13]态实现第三方控制的量子双向传态. 文献[5]提出了用六粒子纠缠态实现受控双向传态，但六粒子纠缠态在物理实现上比较困难，同时文献[11]提出了受控单向传态，但没有对双向传态进行讨论.

本文在实验上选取两对四粒子GHZ纠缠态[14]作为量子信道，实现了多方参与的受控双向隐形传态，增强了双向通信的安全性[15].

1 利用四粒子GHZ态实现三方参与的可控量子双向传态

1.1 控制方含两个粒子的量子态双向传递

通信系统中，Alice和Bob作为通信双方，Alice充当发送者要将自己拥有粒子的信息传送给接受者Bob，与此同时，Bob也充当发送者要将自身拥有粒子的信息传送给接受者Alice，为了保证通信的安全性，增加第三方参与者即控制者Charlie，三方事先密享两对四粒子GHZ纠缠态以构建量子信道. 假设Alice拥有粒子(A,A_1,A_2,A_3)，Bob拥有粒子(B,B_1,B_2,B_3)，而控制者Charlie拥有粒子(C_1,C_2)，Alice和Bob待传的粒子A和B的信息表示为

$$|\xi\rangle_A^I=(a_0|0\rangle+a_1|1\rangle)_A,|\eta\rangle_B^I=(b_0|0\rangle+b_1|1\rangle)_B \tag{1}$$

式中$a_0^2+a_1^2=1$. $b_0^2+b_1^2=1$. 量子信道为两对四粒子GHZ纠缠态，分别为(A_1,A_2,C_1,B_1)和(B_2,B_3,C_2,A_3)，四粒子GHZ态基本形式为$|\mathrm{GHZ}\rangle=\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)$，搭建好的八粒子量子信道表达式为

$$|\Psi\rangle_{A_1A_2C_1B_1B_2B_3C_2A_3}^E=|\mathrm{GHZ}\rangle_{A_1A_2C_1B_1}\otimes|\mathrm{GHZ}\rangle_{B_2B_3C_2A_3} \tag{2}$$

可以看出，这是一个三方共享的量子信道，信息的传送受第三方Charlie的控制，整个量子体系的复合波函数为直积态(张量积)形式，即

$$|\Psi\rangle_{AA_1A_2C_1B_1B_2B_3C_2A_3B}=|\xi\rangle_A^I\otimes|\Psi\rangle_{A_1A_2C_1B_1B_2B_3C_2A_3}^E\otimes|\eta\rangle_B^I=(|\xi\rangle_A^I\otimes|\mathrm{GHZ}\rangle_{A_1A_2C_1B_1})\otimes(|\mathrm{GHZ}\rangle_{B_2B_3C_2A_3}\otimes|\eta\rangle_B^I) \tag{3}$$

推导可得

$$\begin{aligned}|\xi\rangle_A^I|\otimes|\mathrm{GHZ}\rangle_{A_1A_2C_1B_1}&=\frac{1}{2\sqrt{2}}\sum_{i=0}^{3}\sum_{j=0}^{1}|3G\rangle_{AA_1A_2}^i\otimes|A\rangle_{C_1}^j\otimes(\sigma_{B_1}^j\sigma_{B_1}^i|\xi\rangle_{B_1}^I)|\eta\rangle_B^I\otimes\\|\mathrm{GHZ}\rangle_{B_2B_3C_2A_3}&=\frac{1}{2\sqrt{2}}\sum_{i'=0}^{3}\sum_{j'=0}^{1}|3G\rangle_{BB_2B_3}^{i'}\otimes|A\rangle_{C_2}^{j'}\otimes(\sigma_{A_3}^{j'}\sigma_{A_3}^{i'}|\eta\rangle_{A_3}^I)\end{aligned} \tag{4}$$

三粒子正交测量基为

$$|3G\rangle^{0,1}=\frac{1}{\sqrt{2}}(|000\rangle\pm|111\rangle),$$

$$|3G\rangle^{2,3}=\frac{1}{\sqrt{2}}(|011\rangle\pm|100\rangle),$$

单粒子测量基为

$$|A\rangle^{0,1}=|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle),$$

幺正变换所用到的矩阵$\sigma^0,\sigma^1,\sigma^2,\sigma^3$分别对应泡利矩阵$\sigma_I,\sigma_z,\sigma_x,\sigma\times\sigma_z$，结合式(3)、(4)，系统的初态改写为

$$|\Psi\rangle_{AA_1A_2C_1B_1B_2B_3C_2A_3B}=\frac{1}{8}\sum_{i,i'=0}^{3}\sum_{j,j'=0}^{1}\{[|3G\rangle_{AA_1A_2}^i\otimes|A\rangle_{C_1}^j\otimes(\sigma_{B_1}^j\sigma_{B_1}^i|\xi\rangle_{B_1}^I)]\otimes[|3G\rangle_{BB_2B_3}^{i'}\otimes|A\rangle_{C_2}^{j'}\otimes(\sigma_{A_3}^{j'}\sigma_{A_3}^{i'}|\eta\rangle_{A_3}^I)]\} \tag{5}$$

通信开始后，Alice和Bob分别对粒子(A,A_1,A_2)和(B,B_2,B_3)作三粒子正交基联合测量，共有16种测量结果组合，记为：$|3G\rangle_{AA_1A_2}^i\otimes|3G\rangle_{BB_2B_3}^{i'}(i,i'=0,1,2,3)$且概率都为1/16，此后系统塌缩为相应塌缩态

$$|\Psi\rangle_{C_1B_1C_2A_3}^{i,i'}=\sum_{j,j'=0}^{1}[|A\rangle_{C_1}^j\otimes(\sigma_{B_1}^j\sigma_{B_1}^i|\xi\rangle_{B_1}^I)]\otimes[|A\rangle_{C_2}^{j'}\otimes(\sigma_{A_3}^{j'}\sigma_{A_3}^{i'}|\eta\rangle_{A_3}^I)](i,i'=0,1,2,3) \tag{6}$$

即Bob-Charlie系统及Alice-Charlie系统的联合系统，也有十六种可能，并记为子系统. 接下来，Alice和Bob通过经典信道公开自己的测量结果，如果没有Charlie的允许或者Charlie只对其中一个纠缠粒子进行测量，都无法完成双向传态. 若Charlie同意对自己拥有的两个粒子(C_1,C_2)分别作单粒子正交基投影测量，测量结

果有四种可能：$|A\rangle_{C_1}^{j}\otimes|A\rangle_{C_2}^{j'}(j,j'=0,1)$，并将测量结果通过经典信道分别告知 Bob 和 Alice，子系统塌缩为终态：

$$|\Psi\rangle_{B_1A_3}^{S}=(\sigma_{B_1}^{j}\sigma_{B_1}^{i}|\xi\rangle_{B_1}^{I})\otimes(\sigma_{A_3}^{j'}\sigma_{A_3}^{i'}|\eta\rangle_{A_2}^{I})(i,i'=0,1,2,3;j,j'=0,1),$$

不同的可能态为十六种. 随之 *Bob* 和 *Alice* 根据对方公布的测量结果以及控制方告知的测量结果分别对粒子 B_1、A_3 做相应的幺正变换：$\sigma_{B_1}^{j}\sigma_{B_1}^{i}$、$\sigma_{A_3}^{j'}\sigma_{A_3}^{i'}$ $(i,i'=0,1,2,3;j,j'=0,1)$即可得到对方待传的未知量子态，从而整个受控量子双向传态得到实现.

1.2 控制方含四个粒子的量子态双向传递

与 1.1 节中方案类似，Alice 和 Bob 要实现相互且安全的通信，加入第三方控制者 Charlie，量子信道仍然为两对四粒子 GHZ 团簇态，共八个粒子，唯一不同的是纠缠粒子的分配，即控制方拥有四个粒子，假设 Alice 拥有粒子(A,A_1,A_2)，Bob 拥有粒子(B,B_1,B_2)，控制方 Charlie 拥有粒子(C_1,C_2,C_3,C_4)，待传的粒子 A 和 B 的信息表达形式同式(1)，量子信道则表示为

$$|\Psi\rangle_{A_1C_1C_2B_1B_2C_3C_4A_2}^{E}=|\mathrm{GHZ}\rangle_{A_1C_1C_2B_1}\otimes|\mathrm{GHZ}\rangle_{B_2C_3C_4A_2} \tag{7}$$

整个系统的初态为直积态的形式

$$|\Psi\rangle_{AA_1C_1C_2B_1B_2C_3C_4A_2B}=|\xi\rangle_{A}^{I}\otimes|\Psi\rangle_{A_1C_1C_2B_1B_2C_3C_4A_2}^{E}\otimes|\eta\rangle_{B}^{I}=(|\xi\rangle_{A}^{I}\otimes|\mathrm{GHZ}\rangle_{A_1C_1C_2B_1})\otimes(|\mathrm{GHZ}\rangle_{B_2C_3C_4A_2}\otimes|\eta\rangle_{B}^{I}) \tag{8}$$

同式(4)推导类似，可得

$$\begin{aligned}|\xi\rangle_{A}^{I}\otimes|\mathrm{GHZ}\rangle_{A_1C_1C_2B_1}&=\frac{1}{2\sqrt{2}}\sum_{k=0}^{3}\sum_{l=0}^{1}|B\rangle_{AA_1}^{k}\otimes|B\rangle_{C_1C_2}^{l}\otimes(\sigma_{B_1}^{l}\sigma_{B_1}^{k}|\xi\rangle_{B_1}^{I})\\|\eta\rangle_{B}^{I}\otimes|\mathrm{GHZ}\rangle_{B_2C_3C_4A_2}&=\frac{1}{2\sqrt{2}}\sum_{k'=0}^{3}\sum_{l'=0}^{1}|B\rangle_{BB_2}^{k'}\otimes|B\rangle_{C_3C_4}^{l'}\otimes(\sigma_{A_2}^{l'}\sigma_{A_2}^{k'}|\eta\rangle_{A_2}^{I})\end{aligned} \tag{9}$$

式中$|B\rangle$代表 Bell 基，$|B\rangle^{0,1}=|\varphi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle)$，$|B\rangle^{2,3}=|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|01\rangle)$，且幺正变换用到的矩阵 $\sigma^0,\sigma^1,\sigma^2,\sigma^3$ 分别对应泡利矩 $\sigma_I,\sigma_z,\sigma_x,\sigma_x\sigma_z$，结合式(8)、(9)，此系统的初态可以写为

$$|\Psi\rangle_{AA_1C_1C_2B_1B_2C_3C_4A_2B}=\frac{1}{8}\sum_{k,k'=0}^{3}\sum_{l,l'=0}^{1}\{[|B\rangle_{AA_1}^{k}\otimes|B\rangle_{C_1C_2}^{l}\otimes(\sigma_{B_1}^{l}\sigma_{B_1}^{k}|\xi\rangle_{B_1}^{I})]\otimes[|B\rangle_{BB_2}^{k'}\otimes|B\rangle_{C_3C_2}^{l'}\otimes(\sigma_{A_2}^{l'}\sigma_{A_2}^{k'}|\eta\rangle_{A_2}^{I})]\} \tag{10}$$

相比于 1.1 节中方案，使用 Bell 测量基更易在物理实验上实现测量. 通信开始后 Alice 和 Bob 分别对粒子(A,A_1)和(B,B_2)作 Bell 基投影测量(Bell State Mesurement，BSM)，系统塌缩为：$|\Psi\rangle_{C_1C_2B_1C_3C_4A_2}^{k,k'}(k,k'=0,1,2,3)$，共有 16 种测量结果组合，概率都一样. 接下来，Alice 和 Bob 都通过经典信道将各自的测量结果公开，类似的，如果 Charlie 同意双方通信继续，那么 Charlie 对两个粒子对(C_1,C_2)和(C_3,C_4)分别作两次 Bell 基投影测量，系统最终塌缩态$|\Psi\rangle_{B_1A_2}^{s}$，共有 16 种不同可能，并将测量结果通过经典信道分别告知 Bob 和 Alice，随后 Bob 和 Alice 结合对方公开的测量结果和控制方的测量结果分别对粒子 B_1、A_2 作相应的幺正变换，即可得到对方待传的未知量子态，从而实现整个受控量子双向传态方案.

2 利用四粒子 GHZ 态实现四方参与的可控量子双向传态

为了尽可能的实现安全高效的双向通信，提出四方参与的方案，通信双方仍为 Alice 和 Bob，控制方则为 Charlie 和 Dennis. 假设 Alice 拥有粒子(A,A_1)，Bob 拥有粒子(B,B_1)，控制方 Charlie 和 Dennis 分别拥有粒子(C_1,C_2)、(D_1,D_2)，这四方各自拥有事先处于两对四粒子 GHZ 纠缠态中的各一个粒子，记为(A_1,C_1,D_1,B_1)和(B_2,D_2,C_2,A_2)，并以此作为量子信道，这八个粒子所处的纠缠态的表达式为

$$|\Psi\rangle_{A_1C_1D_1B_1B_2D_2C_2A_2}^{E}=|\mathrm{GHZ}\rangle_{A_1C_1D_1B_1}\otimes|\mathrm{GHZ}\rangle_{B_2D_2C_2A_2} \tag{11}$$

不难看出，这是一个四方共享的量子信道. Alice 要把粒子 A 所处的一个未知态的信息传送给远方的 Bob，同时 Bob 也要把自己拥有的粒子 B 上的信息态传给 Alice 时，是一个双向传态，待传的信息表示为

$$\begin{aligned}&|\xi\rangle_{A}^{I}=(a_0|0\rangle+a_1|1\rangle)_A\text{且}\,a_0^2+a_1^2=1\\&|\eta\rangle_{B}^{I}=(b_0|0\rangle+b_1|1\rangle)_B\text{且}\,b_0^2+b_1^2=1\end{aligned} \tag{12}$$

$$\begin{aligned}|\Psi\rangle_{AA_1C_1D_1B_1B_2D_2C_2A_2B}=&|\xi\rangle_{A}^{I}\otimes|\Psi\rangle_{A_1C_1D_1B_1B_2D_2C_2A_2}^{E}\otimes|\eta\rangle_{B}^{I}=\\&(|\xi\rangle_{A}^{I}\otimes|\mathrm{GHZ}\rangle_{A_1C_1D_1B_1})\otimes\\&(|\mathrm{GHZ}\rangle_{B_2D_2C_2A_2}\otimes|\eta\rangle_{B}^{I})\end{aligned} \tag{13}$$

那么量子体系的总量子态表示为

经过推导有

$$\begin{aligned}|\xi\rangle_{A}^{I}\otimes|\mathrm{GHZ}\rangle_{A_1C_1D_1B_1}&=\frac{1}{4}\sum_{r=0}^{3}\sum_{s=0}^{1}\sum_{t=0}^{1}|B\rangle_{AA_1}^{r}\otimes|A\rangle_{C_1}^{s}\otimes|A\rangle_{D_1}^{t}\otimes(\sigma_{B_1}^{t}\sigma_{B_1}^{s}\sigma_{B_1}^{r}|\xi\rangle_{B_1}^{I})\\|\eta\rangle_{B}^{I}\otimes|\mathrm{GHZ}\rangle_{B_2D_2C_2A_2}&=\frac{1}{4}\sum_{r'=0}^{3}\sum_{s'=0}^{1}\sum_{t'=0}^{1}|B\rangle_{BB_2}^{r'}\otimes|A\rangle_{D_2}^{s'}\otimes|A\rangle_{C_2}^{t'}\otimes(\sigma_{A_2}^{t'}\sigma_{A_2}^{s'}\sigma_{A_2}^{r'}|\eta\rangle_{A_2}^{I})\end{aligned} \tag{14}$$

式中$|B\rangle$代表 Bell 基，

$$|B\rangle^{0,1}=|\varphi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle),$$

$$|B\rangle^{2,3}=|\Psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|01\rangle),$$

$$|A\rangle^{0,1}=|\pm\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|01\rangle),$$

$\sigma^0,\sigma^1,\sigma^2,\sigma^3$ 对应矩阵 $\sigma_I,\sigma_z,\sigma_x,\sigma_x\sigma_z$，结合式(13)、(14)，此系统的初态可以改写为

$$|\Psi\rangle_{AA_1C_1D_1B_1B_2D_2C_2A_2B}=\frac{1}{16}\sum_{r,r'=0s,s'=0t,t'=0}^{3}\sum^{1}\sum^{1}\{[|B\rangle^{r}_{AA_1}\otimes|A\rangle^{s}_{C_1}\otimes|A\rangle^{t}_{D_1}\otimes(\sigma^{t}_{B_1}\sigma^{s}_{B_1}\sigma^{r}_{B_1}|\xi\rangle^{I}_{B_1})]\otimes[|B\rangle^{r'}_{BB_2}\otimes|A\rangle^{s'}_{D_2}\otimes|A\rangle^{t'}_{C_2}\otimes(\sigma^{t'}_{A_2}\sigma^{s'}_{A_2}\sigma^{r'}_{A_2}|\eta\rangle^{I}_{A_2})]\} \tag{15}$$

首先，Alice 对自己拥有的粒子(A,A_1)作 BSM，并公布测量结果，与此同时，Bob 也对自己拥有的粒子(B,B_1)作 BSM，并将测量结果通过经典信道公布，他们各自有四种测量结果，记为$(B\rangle^{r}_{AA_1}$、$|B\rangle^{r'}_{BB_2}(r,r'=0,1,2,3)$，系统塌缩为相应的态

$$|\Psi\rangle^{r,r'}_{C_1D_1B_1B_2D_2C_2A_2}=\sum_{s,s'=0t,t'=0}^{1}\sum^{1}[|A\rangle^{s}_{C_1}\otimes|A\rangle^{t}_{D_1}\otimes(\sigma^{t}_{B_1}\sigma^{s}_{B_1}\sigma^{r}_{B_1}|\xi\rangle^{I}_{B_1})]\otimes[|A\rangle^{s'}_{D_2}\otimes|A\rangle^{t'}_{C_2}\otimes(\sigma^{t'}_{A_2}\sigma^{s'}_{A_2}\sigma^{r'}_{A_2}|\eta\rangle^{I}_{A_2})](r,r'=0,1,2,3) \tag{16}$$

易知有 16 种可能，此时若 Charlie 和 Dennis 同意并合作分别对(C_1,D_1)和(C_2,D_2)进行 BSM，则为 1.2 节中的方案. 假设 Charlie 和 Dennis 不同意或者只有一方同意，都无法完成双向传态，若 Charlie 和 Dennis 同意帮助双方通信，则同时分别对自己拥有的粒子 C_1,D_2 作单粒子正交基量子投影测量，各有两种测量结果：$|A\rangle^{s}_{C_1}$、$|A\rangle^{s'}_{D_2}(s,s'=0,1)$，将测量结果公开，系统此时进一步塌缩为相应的态

$$|\Psi\rangle^{r,r',s,s'}_{D_1B_1C_2A_2}=\sum_{t,t'=0}^{1}[|A\rangle^{t}_{D_1}\otimes(\sigma^{t}_{B_1}\sigma^{s}_{B_1}\sigma^{r}_{B_1}|\xi\rangle^{I}_{B_1})]\otimes[|A\rangle^{t'}_{C_2}\otimes(\sigma^{t'}_{A_2}\sigma^{s'}_{A_2}\sigma^{r'}_{A_2}|\eta\rangle^{I}_{A_2})](r,r'=0,1,2,3;s,s'=0,1),$$

系统此时可区分的态只有 16 种可能，将测量结果通过经典信道公开，随后 Dennis 和 Charlie 再同时分别对自己拥有的粒子 D_1,C_2 作单粒子正交基测量，也是各有两种测量结果，记为：$|A\rangle^{t}_{D_1}$、$|A\rangle^{t'}_{C2}(t,t'=0,1)$，最终系统塌缩为对应的终态：

$$|\Psi\rangle^{s}_{B_1A_2}=(\sigma^{t}_{B_1}\sigma^{s}_{B_1}\sigma^{r}_{B_1}|\xi\rangle^{I}_{B_1})\otimes(\sigma^{t'}_{A_2}\sigma^{s'}_{A_2}\sigma^{r'}_{A_2}|\eta\rangle^{I}_{A_2})(r,r'=0,1,2,3;s,s',t,t'=0,1),$$

共 16 种不同的态. 将测量结果通过经典信道告诉 Bob 和 Alice，只要 Bob 和 Alice 结合对方和控制方 Charlie 和 Dennis 公开的测量结果分别对粒子 B_1、A_2 做相应的幺正变换即：$\sigma^{t}_{B_1}\sigma^{s}_{B_1}\sigma^{r}_{B_1}$、$\sigma^{t'}_{A_2}\sigma^{s'}_{A_2}\sigma^{r'}_{A_2}(r,r'=0,1,2,3;s,s',t,t'=0,1)$就可以重建对方待传的量子态，从而完成整个四方参与的受控量子双向通信.

3 安全性分析

实验中使用两对四粒子 GHZ 团簇态作为量子信道比一般的纠缠态纠缠特性强、可靠性高，且传送成功的总概率原则上为 100%. 基于量子力学的基本原理如测不准原理和量子不可克隆，量子态不可精确复制，窃听者无法通过窃听量子信道获得有效的信息，纠缠信道会因此受到破坏，并且窃听者的窃听操作必然会对量子态带来干扰，从而引入错误. 一旦通信者在窃听检测过程中发现错误率过高，则认为有窃听者的存在，便会丢弃这次通信所得数据而重新执行该协议. 可见量子态在量子信道上的传输是安全的，至于经典信道，窃听者只能窃听经典信息而无法篡改它们. 其次，本文相对于文献[12]一个重要的不同点在于控制方控制的是纠缠信道中的粒子，这使得如果第三方或者第四方中的任意一方不对自己拥有的粒子进行测量并公布结果，接受者或窃听者显然无法猜出或者重建发送者待传的未知量子态. 如果窃听者获得了双方公开的信息，也无法准确推算出他们所作的幺正变换，具体来讲，在三方参与的方案中系统共有 64 种组合测量结果，对应 64 种幺正变换信息，而在四方参与的方案中系统共有 256 种测量结果，对应 256 种幺正变换信息，可见窃听者推算出幺正变换的概率大为降低. 由分析可知，多方参与的可控量子双向传态相对于文献[15]提到的直接双向通信协议(存在部分信息泄露)，安全性提高，且控制方的增加，有助于安全性的增加，使得方案更具有实用性.

4 结论

本文提出了一种多方参与的受控量子双向隐形传态方案，通信双方和控制方事先共享两对四粒子 GHZ 纠缠态作为量子信道，利用 GHZ 纠缠态关联度好，顽固性强的特点高效地实现通信. 通信开始后，通信双方 Alice 和 Bob 分别对自己拥有的粒子作正交基量子投影测量，并分别将测量结果公开，若控制者 Charlie 或者 Charlie-Dennis 联合控制同意双方继续通信，则对自己拥有的粒子作量子投影测量，并将测量结果通过经典信道最终分别告诉 Bob 和 Alice，接受者对自己拥有的某个粒子结合公开测量结果作相应的幺正变换，即可重建对方待传的未知单粒子量子态. 只要纠缠粒子采用不同的分配方式，并选择不同测量基测量，即可分别实现三方参与和四方参与的受控双向通信，由于其安全性逐层提高，因此具有广泛的实用性和较高的研

究价值.

参考文献

[1] SU Xiao-qin, GUO Guang-can. Quantum communication and quantum computation [J]. *Chinese Journal of Quantum Electronics*, 2004, **21**(6): 706-718.

[2] CHEN Pan. Theoretical study on quantum key distribution and quantum secret sharing [D]. Beijing: Tsinghua University, 2006: 1-122.
陈攀. 量子密钥分配及量子机密共享的理论研究[D]. 北京:清华大学, 2006: 1-122.

[3] BENNETT C H, BRASSARD G, CREPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Poldolsky-Rosen channels [J]. *Physical Review Letters*, 1993, **70**(13): 1895-1899.

[4] YANG You-feng, YE Zhi-qing. Scheme of two-way quantum teleportation and security[J]. *Acta Photonica Sinica*, 2013, **42**(5): 619-622.
杨幼凤,叶志清. 双向隐形传态方案及安全性分析[J]. 光子学报, 2013, **42**(5): 619-622.

[5] SUN Xin-mei, ZHA Xin-wei. A scheme of bidirectional quantum controlled teleportation via six-qubit maximally entangled state[J]. *Acta Photonica Sinica*, 2013, **42**(9): 1052-1056.
孙新梅,查新未. 基于六粒子最大纠缠态的双向控制隐形传态方案[J]. 光子学报, 2013, **42**(9): 1052-1056.

[6] LU Hong, CHEN Li-bing, HUANG Chun-qing, *et al*. Teleportation of an entangled state via the W states [J]. *Chinese Journal of Quantum Electronics*, 2004, **21**(6): 730-733.
路洪,陈立冰,黄纯青,等. 用 W 态作量子信道实现纠缠态的隐形传送[J]. 量子电子学报, 2004, **21**(6): 730-733.

[7] YE Liu, YAO Chun-mei, GUO Guang-can. Teleportation of two-particle entangled state [J]. *Chinese Physics*, 2001, **10**(11): 1001-1003.

[8] KARLSSON A, BOURENNANE M. Quantum teleportation using three-particle entanglement [J]. *Physical Review A*, 1998, **58**: 4394-4400.

[9] DENG F G, LI C Y, LI Y S, *et al*. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement [J]. *Physical Review A*, 2005, **72**: 022338-022345.

[10] ZHOU P, LI X H, DENG F G, *et al*. Multiparty-controlled teleportation of an arbitrary m-qubit state with pure entangled quantum channel[OL]. arXiv: quant-ph/0705.2660v1.

[11] HONG Zhi-hui, NIE Yi-you, HUANG Yi-bin, *et al*. Controlled quantum teleportation via four particle cluster state[J]. *Chinese Journal of Quantum Electronic*, 2008, **25**(4): 458-461.
洪智慧,聂义友,黄亦斌,等. 基于四粒子团簇态的可控量子隐形传态[J]. 量子电子学报, 2008, **25**(4): 458-461.

[12] ZOU Xin, YE Zhi-qing. Two-way quantum teleportation controlled by a third party[J]. *Chineses Journal of Quantum Electronics*, 2012, **29**(6): 683-687.
邹昕,叶志清. 基于第三方控制的量子双向传态[J]. 量子电子学报, 2012, **29**(6): 683-687.

[13] HE Min, GONG Jing, YAO Ze-qing, *et al*. Realization of quantum teleportation based on bell state[J]. *Communications Technology*, 2007, **40**(12): 244-246
何敏,龚晶,姚泽清,等. 利用 Bell 态实现量子隐形传态[J]. 通信技术, 2007, **40**(12): 244-246.

[14] HUANG Hong-mei. Teleportation of N-particle entangled GHZ state via two-particle entangled quantum channel[J]. *Chinese Journal of Quantum Electronics*, 2012, **29**(6): 695-700.
黄红梅. 利用一个两粒子纠缠态实现 N 粒子 GHZ 纠缠态的隐形传态[J]. 量子电子学报, 2012, **29**(6): 695-700.

[15] GAO Fei, GUO Feng-zhuo, WEN Qiao-yan, *et al*. Reexamine the security of quantum dialogue and bidirectional quantum direct communication[J]. *Science in China Series G: Physics, Mechanics&Astronomy*, 2008, **38**(5): 477-484.
高飞,郭奋卓,温巧燕,等. 重新审视量子对话和双向量子安全直接通信的安全性[J]. 中国科学 G 辑:物理学 力学 天文学, 2008, **38**(5): 477-484.