doi:10.3788/gzxb20134205.0619

双向隐形传态方案及安全性分析

杨幼凤,叶志清

(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:提出了一种用 Bell 纠缠态作为量子信道,实现双向隐形传态的方案.通信双方 Alice、Bob 事先共享二对 Bell 纠缠态,通信开始后,Alice、Bob 分别对自己拥有的部分粒子作 Bell 基联合测量,并将测量结果通过经典信道告诉对方.Alice、Bob 根据对方提供的测量结果,做相应的幺正变换,即在己方的粒子上,再现对方要传的量子态信息,从而实现双向传态的目的.为了提高量子双向隐形传态的安全性,加入第三方控制,分析表明,通过增加控制方的粒子数可以增加系统的安全性,但增加到一定数量后,将无助于量子信道安全性的提高.

关键词:量子信息;隐形传态;双向通信;安全性

中图分类号:TN918 **文献标识码**:A **文章编号**:1004-4213(2013)05-0619-4

Scheme of Two-way Quantum Teleportation and Security

YANG You-feng, YE Zhi-qing

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

Abstract: A scheme of two-way teleportation is proposed, with Bell entangled state as Quantum Channel (QC). Firstly, two sides of communication(Alice and Bob), share two EPR entangled states. After communication, Alice and Bob perform Bell-state joint measurements to their own qubits respectively, and announce the measured results via Classical Channel (CC). Then according to the measured results, Alice and Bob make relevant unitary transformations, namely, its own party can reproduce the opposite quantum state information, and thus the two-way teleportation is realized. In order to enhance the security of two-way teleportation, and the analysis result indicates that the system's security will strengthen with the increase of the control particles, but the security will not strengthen when the control particles increase to a certain number.

Key words: Quantum information; Teleportation; Two-way communication; Security

0 引言

量子隐形传态是目前量子信息中最引人注目的课题之一,它是量子信息理论的重要组成部分,也是量子计算的基础[1-2].隐形传态的方案最早是由 Bennett 等[3]提出的.在此方案中用两粒子最大纠缠态作为量子信道,将未知量子态从一个地方隐形传送到另一个地方,从此人们对量子态的隐形传输产生了极大的兴趣.1997 年,奥地利的 Zeilinger 小组在实验上成功地实现了单光子态的隐形传输[2].近年来,人们提出许多在实验上可行的方案来传送未知量子态,如:单个 S 能级粒子态的隐形传输[4]、多粒子态的隐形传输[5-6]、受控的量子隐形传态[7-10]、相干态隐形传输[11]等.但对量子态的双向传递没有详细的讨论.本文提出以两对最大纠缠 Bell 态作为量子通道,实现双向隐形传态,由于经典信道传递测量结果时可能被窃听,因此加入第三方(Charlie)即控制方,通过改变第三方的粒子数,达到提高系统安

基金项目:国家自然科学基金(No. 60967002)、江西省自然科学基金(No. 20114BAB02003)和江西省教育厅科技项目(No. GJJ10401)资助

第一作者:杨幼凤(1988-),女,硕士研究生,主要研究方向为光量子通信. Email:yangyoufeng2007@126.com

导师(通讯作者):叶志清(1960-),男,教授,主要研究方向为光量子通信和光纤光栅传感器. Email:yezhiqing2008@163.com

收稿日期:2013-01-11;**录用日期**:2013-01-24

全性，并对本方案安全性进行了分析.

1 双向隐形传态方案

1.1 量子态的双向传递原理

通信系统中，Alice 拥有三个粒子(A,A_1,A_2)，Bob 拥有三个粒子(B,B_1,B_2)，其中 A_1 与 B_1 纠缠，A_2 与 B_2 纠缠，通信双方 Alice 和 Bob 要把自己量子态信息传给对方，实现双向传态. 分别表示为 Alice 待传的量子态信息 $|\xi\rangle_A^I=(a_0|0\rangle+a_1|1\rangle)_A$，Bob 待传的量子态信息 $|\eta\rangle_B^I=(b_0|0\rangle+b_1|1\rangle)_B$. 量子信道由双粒子($A_1$,$B_1$)和($A_2$,$B_2$)Bell 纠缠态构成，表示为

$$|B^i\rangle_{A_1B_1}=|B^j\rangle_{A_2B_2}\{i,j=0,1,2,3\}=\{|\phi^\pm\rangle,|\Psi^\pm\rangle\}$$

式中

$$|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2},|\Psi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$$

量子信道表示为

$$|\psi\rangle_{A_1B_1A_2B_2}^E=|B^i\rangle_{A_1B_1}\otimes B^j\rangle_{A_2B_2}\tag{1}$$

整个量子系统的初态为

$$\begin{aligned}|\Psi_s\rangle&=|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1}\otimes|B^j\rangle_{A_2B_2}\otimes|\eta\rangle_B^I=\\&(|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1})\otimes(|\eta\rangle_B^I\otimes|B^j\rangle_{A_2B_2})\\&=\frac{1}{4}[\sum_{r=0}^{3}|B\rangle_{AA_1}^r\otimes(\sigma_{B_1}^i\sigma_{B_1}^r)|\xi\rangle_{B_1}^I]\otimes\\&[\sum_{s=0}^{3}|B\rangle_{BB_2}^s\otimes(\sigma_{A_2}^j\sigma_{A_2}^s)|\eta\rangle_{A_2}^I]\end{aligned}\tag{2}$$

式中

$$\sigma^{(i)}\{i=0,1,2,3\}=\{I,\sigma_z,\sigma_x,\sigma_x\sigma_z\}$$

是泡利矩阵.

通信开始后，Alice 和 Bob 分别对自己拥有的两个粒子(A,A_1)，(B,B_2)进行 Bell 基投影测量(Bell State Measurement，BSM)，测量后，系综态塌缩为

$$|\varphi\rangle=(\sigma_{B_1}^i\sigma_{B_1}^r)|\xi\rangle_{B_1}^I\otimes(\sigma_{A_2}^j\sigma_{A_2}^s)|\eta\rangle_{A_2}^I\tag{3}$$

式中，i，j，r，$s=0,1,2,3$.

由式(3)可见：Alice 处粒子 A 的量子态信息已出现在 Bob 处的粒子 B_1 上；且 Bob 处粒子 B 的量子态信息已出现在 Alice 处的粒子 A_2 上. 只要 Alice 和 Bob 根据对方通过经典信道告诉的测量结果，双方采取相应的幺正变换，就可以获得对方传递的量子态，完成量子态双向传递.

1.2 安全性分析

量子通信的安全性[10-12]一直以来受到人们的高度关注，在量子信道上传送的量子态，对任何人来说都是未知的. 根据量子力学的基本原理，未知量子态是不可克隆的. 另外，如果在量子信道上传送的量子态被攻击者改变，则结果将被改变，这表明攻击者的行为能被发现. 如果攻击者窃听量子信息，则纠缠态的纠缠性一定会被破坏，因此量子态不能传递到目的地. 由此可知，量子态在量子信道上的传递是保密的、安全的. 然而，要实现量子态的传递必须借助经典信道把各自的 Bell 基联合测量结果传送给对方. 各自测量的结果信息被窃听是有可能的，因此也存在部分量子信道信息以及幺正变换信息“泄露”的可能.

Alice 和 Bob 通信双方秘密共享 2 个贝尔态，其中 $|B^i\rangle_{A_1B_1}(i=0,1,2,3)$ 有 4 种；$|B^j\rangle_{A_2B_2}(j=0,1,2,3)$ 有 4 种. 构成的量子信道 $|\psi\rangle_{A_1B_1A_2B_2}^E=|B^i\rangle_{A_1B_1}\otimes B^j\rangle_{A_2B_2}$ 有 16 种. 假设 Alice 的 Bell 基联合测量(BSM)的结果为 $i=0$，$r=1$，则表明

$$|B^i\rangle_{A_1B_1}=|B^0\rangle_{A_1B_1}=|\phi^+\rangle_{A_1B_1}=(|00\rangle+|11\rangle)_{A_1B_1}/\sqrt{2}\tag{4}$$

$$|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1}=\frac{1}{2}\sum_{r=0}^{3}|B^r\rangle_{AA_1}\otimes[(\sigma_{B_1}^i\sigma_{B_1}^r)|\xi\rangle_{B_1}^I]\tag{5}$$

$$|B^r\rangle_{AA_1}=|B^1\rangle_{AA_1}=|\phi^-\rangle_{AA_1}=(|00\rangle-|11\rangle)_{AA_1}/\sqrt{2}\tag{6}$$

又假设 Bob 的 Bell 基联合测量(BSM)的结果为 $j=2$，$s=3$，则表明

$$|B^j\rangle_{A_2B_2}=|B^2\rangle_{A_2B_2}=|\psi^+\rangle_{A_2B_2}=(|01\rangle+|10\rangle)_{A_2B_2}/\sqrt{2}\tag{7}$$

$$|\eta\rangle_B^I\otimes|B^j\rangle_{A_2B_2}=\frac{1}{2}\sum_{s=0}^{3}|B^s\rangle_{BB_2}\otimes[(\sigma_{A_2}^j\sigma_{A_2}^s)|\eta\rangle_{A_2}^I]\tag{8}$$

$$|B^s\rangle_{BB_2}=|B^3\rangle_{BB_2}=|\psi^-\rangle_{BB_2}=(|01\rangle-|10\rangle)_{BB_2}/\sqrt{2}\tag{9}$$

如果窃听者从经典信道上截获 $i=0$，$r=1$，$j=2$，$s=3$，则双向传递所用的量子信道及幺正变换信息被泄露.

2 加入第三方控制量子态双向传递

2.1 第三方为一个粒子的量子态双向传递

加入控制方 Charlie 后，量子信道则由两对 Bell 态和控制方的一个粒子构成，表示为

$$|\psi\rangle_{A_1B_1A_2B_2C_1}^E=\frac{1}{\sqrt{2}}(|B^i\rangle_{A_1B_1}\otimes|B^j\rangle_{A_2B_2}\otimes|0\rangle_{C_1})+(|B^{i'}\rangle_{A_1B_1}\otimes|B^{j'}\rangle_{A_2B_2}\otimes|1\rangle_{C_1})/\sqrt{2}\tag{10}$$

式中 $(i,j,i',j'\in(0,1,2,3))$，$i\neq i'$，$j\neq j'$.

量子通信系统的初态为

$$|\Psi_s\rangle=|\xi\rangle_A^I\otimes|\psi\rangle_{A_1B_1A_2B_2C_1}^E\otimes|\eta\rangle_B^I=\frac{1}{\sqrt{2}}\{(|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1})\otimes(|\eta\rangle_B^I\otimes|B^j\rangle_{A_2B_2})\otimes|0\rangle_{C_1}+(|\xi\rangle_A^I\otimes|B^{i'}\rangle_{A_1B_1})\otimes(|\eta\rangle_B^I\otimes|B^{j'}\rangle_{A_2B_2})\otimes$$

$$|1\rangle_{C_1}\}=\frac{1}{4\sqrt{2}}\{(\sum_{r=0}^{3}|B\rangle_{AA_1}^{r}\otimes(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I})\otimes$$
$$(\sum_{s=0}^{3}|B\rangle_{BB_2}^{s}\otimes(\sigma_{A_2}^{j}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I})\otimes|0\rangle_{C_1}+$$
$$(\sum_{r=0}^{3}|B\rangle_{AA_1}^{r}\otimes(\sigma_{B_1}^{i'}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I})\otimes$$
$$(\sum_{s=0}^{3}|B\rangle_{BB_2}^{s}\otimes(\sigma_{A_2}^{j'}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I})\otimes|1\rangle_{C_1}\}\quad(11)$$

通信开始后，Alice 对自己拥有的粒子(A,A_1)作 BSM 联合测量，Bob 对自己拥有的粒子(B,B_2)作 BSM 联合测量. 则量子系统最终态塌缩为

$$|\varphi\rangle=(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes(\sigma_{A_2}^{j}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I}\otimes|0\rangle_{C_1}+$$
$$(\sigma_{B_1}^{i'}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes(\sigma_{A_2}^{j'}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I}\otimes|1\rangle_{C_1}\quad(12)$$

如果没有 Charlie 的允许，Alice 和 Bob 只能猜对一半的信息. 如果 Charlie 允许，Charlie 对 C_1 粒子作基矢测量，把测量结果通过经典信道告诉 Alice，Bob，则 Alice 和 Bob 根据各自对方以及 Charlie 的测量结果，作相应的幺正变换，就可以分别在 A_2 和 B_1 粒子上再现对方传递的量子态信息.

该方案与前一种方案相比，由于 Charlie 控制方参与，使安全性有了提高，而 Charlie 不知道 Alice 和 Bob 要传送的量子态. 如果窃听者截获 Alice 和 Bob 通过经典信道传递的各自的 BSM 测量结果. 则有 50%的量子信息可以猜对，即有 50%的量子信道和幺正变换信息泄露.

2.2　第三方为两个粒子控制量子态双向传递

量子信道由两对 Bell 态和控制方的两粒子构成，表示为

$$|\psi\rangle_{A_1B_1A_2B_2C_1C_2}^{E}=\frac{1}{2}[\sum_{i=0}^{3}|B^i\rangle_{A_1B_1}\otimes|B^i\rangle_{A_2B_2}\otimes$$
$$|\phi^i\rangle_{C_1C_2}]=\frac{1}{2}[|B^0\rangle_{A_1B_1}\otimes|B^0\rangle_{A_2B_2}\otimes|00\rangle_{C_1C_2}+$$
$$|B^1\rangle_{A_1B_1}\otimes|B^1\rangle_{A_2B_2}\otimes|01\rangle_{C_1C_2}+|B^2\rangle_{A_1B_1}\otimes$$
$$|B^2\rangle_{A_2B_2}\otimes|10\rangle_{C_1C_2}+|B^3\rangle_{A_1B_1}\otimes|B^3\rangle_{A_2B_2}\otimes$$
$$|11\rangle_{C_1C_2}]\quad(13)$$

量子系统的初态为

$$|\Psi_s\rangle=|\xi\rangle_A^I\otimes|\psi\rangle_{A_1B_1A_2B_2C_1C_2}^{E}\otimes|\eta\rangle_B^I=$$
$$\frac{1}{2}[\sum_{i=0}^{3}(|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1})\otimes(|\eta\rangle_B^I\otimes|B^i\rangle_{A_2B_2})\otimes$$
$$|\phi^i\rangle_{C_1C_2}]=\frac{1}{8}[\sum_{i,r,s=0}^{3}|B\rangle_{AA_1}^{r}\otimes(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes$$
$$(|B\rangle_{BB_2}^{s}\otimes(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I})\otimes|\varphi^i\rangle_{C_1C_2}]\quad(14)$$

通信开始后，Alice 对自己拥有的粒子(A,A_1)作 BSM 联合测量，Bob 对自己拥有的粒子(B,B_2)作 BSM 联合测量. 则量子系统最终态塌缩为

$$|\varphi\rangle=\frac{1}{2}\sum_{i=0}^{3}(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I}\otimes$$
$$|\phi^i\rangle_{C_1C_2}\quad(15)$$

如果没有控制方 Charlie 的允许，Alice 和 Bob 只能猜对 25%的正确信息. 如果 Charlie 允许 Alice 和 Bob 可以双向传态，则 Charlie 对(C_1,C_2)两个粒子作基矢测量，把测量结果告诉 Alice 和 Bob，那么 Alice 和 Bob 根据 Charlie 的测量结果，作相应的幺正变换，得到对方传送的量子态. 该方案的安全性比 2.1 中的方案的安全性有了提高，即使窃听者截获 Alice 和 Bob 的测量结果也只能有 25%的概率猜对量子信道和幺正变换信息.

2.3　第三方为三个粒子控制量子态双向传递

量子信道由两对 Bell 态和控制方的三个粒子构成，表示为

$$|\psi\rangle_{A_1B_1A_2B_2C_1C_2C_3}^{E}=\frac{1}{2\sqrt{2}}[|B^0\rangle_{A_1B_1}\otimes|B^0\rangle_{A_2B_2}\otimes$$
$$|000\rangle_{C_1C_2C_3}+|B^1\rangle_{A_1B_1}\otimes|B^1\rangle_{A_2B_2}\otimes|001\rangle_{C_1C_2C_3}+$$
$$|B^2\rangle_{A_1B_1}\otimes|B^2\rangle_{A_2B_2}\otimes|010\rangle_{C_1C_2C_3}+|B^3\rangle_{A_1B_1}\otimes$$
$$|B^3\rangle_{A_2B_2}\otimes|011\rangle_{C_1C_2C_3}+|B^0\rangle_{A_1B_1}\otimes|B^1\rangle_{A_2B_2}\otimes$$
$$|100\rangle_{C_1C_2C_3}+|B^1\rangle_{A_1B_1}\otimes|B^0\rangle_{A_2B_2}\otimes|101\rangle_{C_1C_2C_3}+$$
$$|B^2\rangle_{A_1B_1}\otimes|B^3\rangle_{A_2B_2}\otimes|110\rangle_{C_1C_2C_3}+|B^3\rangle_{A_1B_1}\otimes$$
$$|B^2\rangle_{A_2B_2}\otimes|111\rangle_{C_1C_2C_3}]\quad(16)$$

量子系统的初态为

$$|\Psi_s\rangle=|\xi\rangle_A^I\otimes|\psi\rangle_{A_1B_1A_2B_2C_1C_2C_3}^{E}\otimes|\eta\rangle_B^I=$$
$$\frac{1}{2\sqrt{2}}[\sum_{i=0}^{3}(|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1})\otimes(|\eta\rangle_B^I\otimes|B^i\rangle_{A_2B_2})\otimes$$
$$|\phi^i\rangle_{C_1C_2}\otimes|0\rangle_{C_3}]+\frac{1}{2\sqrt{2}}[\sum_{i=0}^{3}(|\xi\rangle_A^I\otimes|B^i\rangle_{A_1B_1})\otimes$$
$$(|\eta\rangle_B^I\otimes|B^i\rangle_{A_2B_2})\otimes|\phi^i\rangle_{C_1C_2}\otimes|1\rangle_{C_3}]=$$
$$\frac{1}{8\sqrt{2}}[\sum_{i,r,s=0}^{3}(|B\rangle_{AA_1}^{r}\otimes(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I})\otimes(|B\rangle_{BB_2}^{s}\otimes$$
$$(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I})\otimes|\phi^i\rangle_{C_1C_2}\otimes|0\rangle_{C_3}]+$$
$$\frac{1}{8\sqrt{2}}[\sum_{i,r,s=0}^{3}(|B\rangle_{AA_1}^{r}\otimes(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I})\otimes(|B\rangle_{BB_2}^{s}\otimes$$
$$(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I})\otimes|\phi^i\rangle_{C_1C_2}\otimes|1\rangle_{C_3}]\quad(17)$$

通信开始后，Alice 对自己拥有的粒子(A,A_1)作 BSM 联合测量，Bob 对自己拥有的粒子(B,B_2)作 BSM 联合测量. 则量子系统最终态塌缩为

$$|\varphi\rangle=\frac{1}{2\sqrt{2}}[\sum_{i=0}^{3}(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I}\otimes$$
$$|\phi^i\rangle_{C_1C_2}\otimes|0\rangle_{C_3}]+\frac{1}{2\sqrt{2}}[\sum_{i=0}^{3}(\sigma_{B_1}^{i}\sigma_{B_1}^{r})|\xi\rangle_{B_1}^{I}\otimes$$
$$(\sigma_{A_2}^{i}\sigma_{A_2}^{s})|\eta\rangle_{A_2}^{I}\otimes|\phi^i\rangle_{C_1C_2}\otimes|1\rangle_{C_3}]\quad(18)$$

如果没有控制方 Charlie 的允许，Alice 和 Bob 根据对方告诉的测量结果，只能猜对，即 12.5%. 如果 Charlie 允许，Charlie 对(C_1,C_2,C_3)三个粒子作基矢测量，把测量结果告诉 Alice 和 Bob，那么 Alice 和 Bob 就可以作相应的幺正变换，得到对方传送的正确量子态. 同理，窃听者截获 Alice 和 Bob 的测量结果也

只能猜对，即有12.5%的量子信道信息被泄露.

2.4 第三方为四个粒子控制量子态双向传递

量子信道由两对Bell态和控制方的四个粒子构成，表示为

$$|\psi\rangle^{E}_{A_1B_1A_2B_2C_1C_2C_3C_4}=\frac{1}{4}\Big[\sum_{i,j=0}^{3}|B^i\rangle_{A_1B_1}\otimes|B^j\rangle_{A_2B_2}\otimes |\phi^i\rangle_{C_1C_2}\otimes|\phi^j\rangle_{C_3C_4}\Big] \tag{19}$$

式中：$|\phi^i\rangle,|\phi^j\rangle\in(|00\rangle,|01\rangle,|10\rangle,|11\rangle)$

量子系统的初态为

$$\begin{aligned}|\Psi_s\rangle&=|\xi\rangle^{I}_{A}\otimes|\psi\rangle^{E}_{A_1B_1A_2B_2C_1C_2C_3C_4}\otimes|\eta\rangle^{I}_{B}\\&=\frac{1}{4}\Big[\sum_{i,j=0}^{3}(|\xi\rangle^{I}_{A}\otimes|B^i\rangle_{A_1B_1})\otimes(|\eta\rangle^{I}_{B}\otimes|B^j\rangle_{A_2B_2})\otimes|\phi^i\rangle_{C_1C_2}\otimes|\phi^j\rangle_{C_3C_4}\Big]=\\&\frac{1}{16}\Big[\sum_{i,j,r,s=0}^{3}(|B^r\rangle_{AA_1}\otimes(\sigma^i_{B_1}\sigma^r_{B_1})|\xi\rangle^{I}_{B_1})\otimes|\phi^i\rangle_{C_1C_2}\otimes(|B^s\rangle_{BB_2}\otimes(\sigma^j_{A_2}\sigma^s_{A_2})|\eta\rangle^{I}_{A_2})\otimes|\phi^j\rangle_{C_3C_4}\Big]\end{aligned} \tag{20}$$

通信开始后，Alice对自己拥有的粒子(A,A_1)作BSM联合测量，Bob对自己拥有的粒子(B,B_2)作BSM联合测量.则整个量子系统塌缩为

$$|\varphi\rangle=\frac{1}{4}\Big[\sum_{i,j=0}^{3}(\sigma^i_{B_1}\sigma^r_{B_1})|\xi\rangle^{I}_{B_1}\otimes(\sigma^j_{A_2}\sigma^s_{A_2})|\eta\rangle^{I}_{A_2}\otimes|\phi^i\rangle_{C_1C_2}\otimes|\phi^j\rangle_{C_3C_4}\Big] \tag{21}$$

如果Charlie不允许，则Alice和Bob根据对方告诉的测量结果，只能猜对6.25%.如果Charlie允许Alice和Bob双向传态，Charlie对(C_1,C_2,C_3,C_4)四个粒子作计算基矢测量，并把测量结果告诉Alice和Bob，那么Alice和Bob就可以选择相应的幺正变换，得到对方传送的量子态.实现双向传态的目的.如果有窃听者截获Alice和Bob的测量结果也只能猜对6.25%的概率.这是该双向传递量子态方案的最高安全性.如果再增加Charlie控制粒子数，由于采用标准双粒子Bell态为纠缠态，$|B^i\rangle_{A_1B}\otimes B^j\rangle_{A_2B}$总共只有16种组合.如果Charlie启用5个粒子作为控制粒子，最多可组合32种态，其中由双粒子标准Bell态构成的量子信道会出现两次，无助于量子信道安全性提高.

3 结论

本文提出一种双向传态方案，通信双方Alice、Bob和控制方Charlie事先共享一个多粒子团簇态来构建量子信道，利用团簇态关联度好、纠缠顽固度高的特点，能够更安全、高效地实现双向通信.通信开始后，Alice、Bob分别对自己拥有的部分粒子作Bell基联合测量(BSM)，若控制方Charlie同意双方通信，则对自己拥有的粒子作测量，将粒子所处的态公布；通信双方根据控制方公布的测量结果，对各自的某些粒子作适当的幺正变换，即可在这些粒子上重建对方要传的态，从而实现双向传态的目的.方案的安全性分析表明，通过增加控制方的粒子数可以增加系统的安全性，但增加到一定数量后，再增加控制方的粒子数也无助于量子信道安全性提高.

参考文献

[1] BOUWMEESTER D, PAN J W, MATTLE K, *et al*. Experimental quantum teleportation[J]. *Nature*, 1997, **390**(6660): 575-579.

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

[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] ZHOU J D, ZHANG Y D, HOU G. Teleportation scheme of S- level quantum pure states by two-level EPRs[J]. *Physical Review A*, 2001, **64**(1): 4095-4101.

[5] YAO Chun-mei. Multi-atom teleportation through GHZ States [J]. *Acta Photonica Sinica*, 2002, **31**(6): 647-649.

[6] XU Jian-gang, ZHA Xin-wei. A theoretical analysis of teleportation of n particle quantum state [J]. *Acta Sinica Quantum Optica*, 2009, **15**(4): 325-328.
徐建刚，查新未. N粒子量子态的隐形传送的理论分析[J]. 量子光学学报，2009，**15**(4)：325-328.

[7] XIONG Xue-shi, FU Jie, SHEN Ke. Controlled teleportation of an unknown two-particle partly entangled state[J]. *Acta Photonica Sinica*, 2006, **35**(5): 780-782.
熊学士，付洁，沈柯. 二粒子部分纠缠未知态的量子受控传递[J]. 光子学报，2006，**35**(5)：780-782.

[8] 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.

[9] YANG C P, CHU S J, HAN S Y. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement[J]. *Physical Review A*, 2004, **70**(2): 022329.

[10] ZOU Xin, YE Zhi-qing. Controlled by a third party to realize quantum secure dialogue[J]. *Acta Photonica Sinica*, 2012, **41**(4): 501-504.
邹昕，叶志清. 受第三方控制的量子安全对话方案[J]. 光子学报，2012，**41**(4)：501-504.

[11] WANG Xiao-guang. Quantum teleportation of entangled coherent states[J]. *Physical Review A*, 2001, **64**(2): 022302.

[12] 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 Ser 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.