doi:10.16055/j.issn.1672-058X.2015.0010.011

基于双向量子隐形传态上的双向量子安全直接通信*

孔令浩, 胡占宁
(天津工业大学 理学院,天津 300000)

摘　要:提出了一种利用 EPR 对和纠缠交换的双向量子隐形传态;在这个协议中,双方可同时发送一个未知的单一量子比特给对方,而且在实际操作中比以前的提出的协议更加简单;利用提出的双向量子隐形传态,建立了一种新的双向量子安全直接通信协议,协议在通信过程中不需要传递携带秘密信息的量子比特,大大提高了量子通信的安全信.

关键词:纠缠交换;双向量子隐形传态;双向量子安全直接通信
中图分类号:O402　　**文献标志码**:A　　**文章编号**:1672-058X(2015)10-0054-04

纠缠交换是量子通信的一个重要方面,它被广泛应用到量子的信息处理中,例如量子隐形传态、量子秘密共享等.量子隐形传态是在量子纠缠的帮助下,经由经典通道和 EPR 通道将甲地的某一个粒子的未知量子态在乙地的另一个粒子上还原出来[1].1984 年,Bennett 和 Brassard 提出了第一个量子密钥分配协议 BB84 协议,可以实现建立在量子力学原理上的安全通信,该协议也称 Bennett-Brassard 协议[2],标志着量子通信安全研究的开始.首先提出了一种利用 EPR 对和量子纠缠交换的双向量子隐形传态,然后在利用这个双向量子隐形传态提出一种双向量子安全直接通信协议,在这个协议中, Alice 和 Bob 就能同时读取双方已编码的信息,并且不需要在量子信道中传输携带秘密信息的量子比特.

1　双向量子隐形传态

1.1　量子纠缠交换方法

假设 4 个 EPR 形式可以写为

$$|\phi^+\rangle_{12}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{12},|\phi^-\rangle_{12}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{12}$$

$$|\psi^+\rangle_{12}=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{12},|\psi^-\rangle_{12}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{12}\quad(1)$$

假设信息发送者 Alice 和接收者 Bob 共享量子态 $|\psi^+\rangle_{12}$ 和 $|\psi^+\rangle_{34}$,其中量子比特 1 和 4 属于发送者 Alice,量子比特 2 和 3 属于接收者 Bob,对发送者 Alice 进行 Bell 基测量,则整个量子态塌缩,接收者的量子比特构成新的纠缠态,其形式如下:

收稿日期:2015-01-15;**修回日期**:2015-03-17.
* **基金项目**:国家自然科学理论物理专项基金(11447153).
作者简介:孔令浩(1990-),男,河北邢台人,硕士研究生,从事量子安全通信研究.

$$|\psi^+\rangle_{12}\otimes|\psi^+\rangle_{34}=\frac{1}{2}(|01\rangle+|10\rangle)_{12}\otimes(|01\rangle+|10\rangle)_{34}=$$

$$\frac{1}{2}(|01\rangle_{12}|01\rangle_{34}+|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}+|10\rangle_{12}|10\rangle_{34})=$$

$$\frac{1}{2}(|01\rangle_{14}|10\rangle_{23}+|00\rangle_{14}|11\rangle_{23}+|11\rangle_{14}|00\rangle_{23}+|10\rangle_{14}|01\rangle_{23})=$$

$$\frac{1}{2}(|\phi^+\rangle_{14}|\phi^+\rangle_{23}-|\phi^-\rangle_{14}|\phi^-\rangle_{23}+|\psi^+\rangle_{14}|\psi^+\rangle_{23}-|\psi^-\rangle_{14}|\psi^-\rangle_{23}) \tag{2}$$

如果发送者得到的结果是$|\phi^+\rangle_{14}$,那么接收者得到的结果必是$|\phi^+\rangle_{23}$.

1.2　双向量子隐形状态的实现

$$|\phi\rangle_A=\alpha_0|0\rangle+\alpha_1|1\rangle,|\phi\rangle_B=\beta_0|0\rangle+\beta_1|1\rangle \tag{3}$$

在 Alice 和 Bob 之间建立一条量子信道,假定这条量子信道是由两个 EPR 纠缠对构成,其形式为

$$|\phi\rangle_{a_1b_1a_2b_2}=\frac{1}{2}(|00\rangle+|11\rangle)_{a_1b_1}\otimes(|00\rangle+|11\rangle)_{a_2b_2}=$$

$$\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle)_{a_1b_1a_2b_2} \tag{4}$$

其中量子比特 a_1 和 a_2 属于 Alice,b_1 和 b_2 属于 Bob.整个量子体系的总量子态为

$$|\Psi\rangle_{a_1b_1a_2b_2AB}=|\phi\rangle_{a_1b_1a_2b_2}\otimes|\phi\rangle_A\otimes|\phi\rangle_B \tag{5}$$

将 A 和 B 当做控制位,a_1 和 b_2 当做靶位,进行受控非门操作,得到的结果为[3]

$$\begin{aligned}|\Psi'\rangle_{a_1b_1a_2b_2AB}=\frac{1}{2}[&(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle)_{a_1b_1a_2b_2}\alpha_0\beta_0|00\rangle_{AB}+\\&(|0001\rangle+|0010\rangle+|1101\rangle+|1110\rangle)_{a_1b_1a_2b_2}\alpha_0\beta_1|10\rangle_{AB}+\\&(|1000\rangle+|1011\rangle+|0100\rangle+|0111\rangle)_{a_1b_1a_2b_2}\alpha_1\beta_0|10\rangle_{AB}+\\&(|1001\rangle+|1010\rangle+|0101\rangle+|0110)_{a_1b_1a_2b_2}\alpha_1\beta_1|11\rangle_{AB}]\end{aligned} \tag{6}$$

Alice 和 Bob 各自将量子比特 a_1 和 b_2 在 Z 基上进行测量,量子比特 A 和 B 在 X 基上进行测量,然后将测量的结果告诉对方,其测量结果见表 2.根据得到的结果应用一位门操作(表 1),即可还原出另一方的单一量子比特态,举例说明:假设 Alice 的测量结果是$|0\rangle_{a_1}|+\rangle_A$,Bob 的测量结果是$|0\rangle_{b_2}|-\rangle_B$,则其他粒子状态塌缩成[4,5]

$$\begin{aligned}|\Omega\rangle_{b_1a_2}=&(\alpha_0\beta_0|00\rangle-\alpha_0\beta_1|01\rangle+\alpha_1\beta_0|10\rangle-\alpha_1\beta_1|11\rangle)_{b_1a_2}\\&\xrightarrow{\sigma_z}(\alpha_0|0\rangle+\alpha_1|1\rangle)_{b_1}(\beta_0|0\rangle+\beta_1|1\rangle)_{a_2}\end{aligned} \tag{7}$$

即双向量子隐形传态能够成功实现.

表 1　对应的一位门操作

测量结果	对应操作
0+	I
1+	σ_x
0−	σ_z
1−	$i\sigma_y$

表 2 测量结果和其余粒子塌缩的量子态

Alice 的测量结果	Bob 的测量结果	b_1 和 a_2 塌缩后的状态
$\|0\rangle_{a_1}\|+\rangle_A$	$\|0\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|00\rangle+\alpha_0\beta_1\|01\rangle+\alpha_1\beta_0\|10\rangle+\alpha_1\beta_1\|11\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|+\rangle_A$	$\|0\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|00\rangle-\alpha_0\beta_1\|01\rangle+\alpha_1\beta_0\|10\rangle-\alpha_1\beta_1\|11\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|-\rangle_A$	$\|0\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|00\rangle+\alpha_0\beta_1\|01\rangle-\alpha_1\beta_0\|10\rangle-\alpha_1\beta_1\|11)_{b_1a_2}$
$\|0\rangle_{a_1}\|-\rangle_A$	$\|0\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|00\rangle-\alpha_0\beta_1\|01\rangle-\alpha_1\beta_0\|10\rangle+\alpha_1\beta_1\|11\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|+\rangle_A$	$\|1\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|01\rangle+\alpha_0\beta_1\|00\rangle+\alpha_1\beta_0\|11\rangle+\alpha_1\beta_1\|10\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|+\rangle_A$	$\|1\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|01\rangle-\alpha_0\beta_1\|00\rangle+\alpha_1\beta_0\|11\rangle-\alpha_1\beta_1\|10\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|-\rangle_A$	$\|1\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|01\rangle+\alpha_0\beta_1\|00\rangle-\alpha_1\beta_0\|11\rangle-\alpha_1\beta_1\|10\rangle)_{b_1a_2}$
$\|0\rangle_{a_1}\|-\rangle_A$	$\|1\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|01\rangle-\alpha_0\beta_1\|00\rangle-\alpha_1\beta_0\|11\rangle+\alpha_1\beta_1\|10\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|+\rangle_A$	$\|0\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|10\rangle+\alpha_0\beta_1\|11\rangle+\alpha_1\beta_0\|00\rangle+\alpha_1\beta_1\|01\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|+\rangle_A$	$\|0\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|10\rangle-\alpha_0\beta_1\|11\rangle+\alpha_1\beta_0\|00\rangle-\alpha_1\beta_1\|01\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|-\rangle_A$	$\|0\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|10\rangle+\alpha_0\beta_1\|11\rangle-\alpha_1\beta_0\|00\rangle-\alpha_1\beta_1\|01\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|-\rangle_A$	$\|0\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|10\rangle-\alpha_0\beta_1\|11\rangle-\alpha_1\beta_0\|00\rangle+\alpha_1\beta_1\|01\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|+\rangle_A$	$\|1\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|11\rangle+\alpha_0\beta_1\|10\rangle+\alpha_1\beta_0\|01\rangle+\alpha_1\beta_1\|00\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|+\rangle_A$	$\|1\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|11\rangle-\alpha_0\beta_1\|10\rangle+\alpha_1\beta_0\|01\rangle-\alpha_1\beta_1\|00\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|-\rangle_A$	$\|1\rangle_{b_2}\|+\rangle_B$	$(\alpha_0\beta_0\|11\rangle+\alpha_0\beta_1\|10\rangle-\alpha_1\beta_0\|01\rangle-\alpha_1\beta_1\|00\rangle)_{b_1a_2}$
$\|1\rangle_{a_1}\|-\rangle_A$	$\|1\rangle_{b_2}\|-\rangle_B$	$(\alpha_0\beta_0\|11\rangle-\alpha_0\beta_1\|10\rangle-\alpha_1\beta_0\|01\rangle+\alpha_1\beta_1\|00)_{b_1a_2}$

对比已经提出的双向量子隐形传态协议[6].首先,在式(4)中把两个 EPR 对作为量子信道,这就使实验在准备阶段更加简单,其次,利用纠缠交换的特性,进行单一量子比特测量比进行 Bell 基测量的准确度更高.

2 双向量子安全直接通信协议

在准备阶段,Alice 准备大量排序相同的两粒子 EPR 对(式(8)),其中 Alice 自己保留第一个粒子,并将第 2 个粒子发送给 Bob.

$$|\phi^+\rangle_{ab}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_{ab} \tag{8}$$

进行窃听检测,在被告知 Bob 收到所有第 2 个粒子以后,Alice 从自己持有的粒子中任意选取足够多的粒子作为检测粒子,任意选取 Z 基或者 X 基进行测量,然后 Alice 将测量的粒子序列以及测量基告诉 Bob,Bob 在同一测量基下测量相同的粒子,并将测量结果告诉 Alice,如果测量结果完全一致,说明量子信道中没有 Eve 存在,通信就可以继续.

在确定量子信道是安全以后,Alice 和 Bob 将其余的 EPR 对分成几组,每组包含两个 EPR 对以保证 Alice 和 Bob 能够交换他们的秘密信息,Alice 和 Bob 依照自己的秘密信息创建一个单一的量子比特态(式(9)),并且将这个单一比特态传输给对方.

$$|\phi\rangle_A=\frac{1}{\sqrt{2}}(|0\rangle+\alpha|1\rangle)_A,\ |\phi\rangle_B=\frac{1}{\sqrt{2}}(|0\rangle+\beta|1\rangle)_B \tag{9}$$

在式(9)上进行操作(式(4)(5)(6)),同样 Alice 和 Bob 各自将量子比特 a_1 和 b_2 在 Z 基上进行测量,量子比特 A 和 B 在 X 基上进行测量,然后将各自测量的结果通过经典通道告诉对方.由于经典通道中的信息传播速度比光速慢,所以并不违背光速不可超越理论.根据得到的结果应用一位门操作(表 1),Alice 和 Bob 就能成功还原出另一方的单一比特态,从而得知对方的秘密信息.举例:Alice 和 Bob 测量的结果是 $|0\rangle_{a_1}|+\rangle_A$ 和 $|0\rangle_{b_2}|+\rangle_B$,则其他粒子状态塌缩成:

$$|\Omega\rangle_{b_1a_2}=\frac{1}{8}(|00\rangle+\beta|01\rangle+\alpha|10\rangle+\alpha\beta|11\rangle)_{b_1a_2}=$$

$$\frac{1}{4}\left[\frac{1}{\sqrt{2}}(|0\rangle+\alpha|1\rangle)_{b_1}\otimes\frac{1}{\sqrt{2}}(|0\rangle+\beta|1\rangle_{a_2})\right] \tag{10}$$

即双向量子安全直接通信也能成功实现.

3　双向量子安全直接通信的安全分析

在传输秘密信息过程中是用双向隐形传输,在量子信道中没有携带秘密信息的量子比特通过.因此 Eve 只能在准备阶段对通信进行攻击,Eve 用测量基 X 或者 Z 测量 Bob 的量子比特,再将她测量的信息代替 Alice 的信息发送给 Bob.举例:假设 Alice 用的测量基是 X 基,当 Eve 用的测量基是 X 基时,攻击不会被发现;当 Eve 用的测量基是 Z 基时,有 1/2 的概率被发现(式(11)):

$$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{2}(|0+\rangle+|0-\rangle+|1+\rangle+|1-\rangle) \tag{11}$$

Eve 运用一种一元运算在 Bob 的量子比特上[7],然后在将结果作为替代者发送给 Bob.

$$U=\begin{bmatrix}u_{00}u_{01}\\u_{10}u_{11}\end{bmatrix}$$

$$(I\otimes U)\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}=\frac{1}{\sqrt{2}}[|0\rangle(u_{00}|0\rangle+u_{10}|1\rangle)+|1\rangle(u_{01}|0\rangle+u_{11}|1\rangle)]=$$

$$\frac{1}{2\sqrt{2}}[|+\rangle(u_{00}+u_{01}+u_{10}+u_{11})|+\rangle+|+\rangle(u_{00}+u_{01}-u_{10}-u_{11})|-\rangle+$$

$$|-\rangle(u_{00}-u_{01}+u_{10}-u_{11})|-\rangle+|-\rangle(u_{00}-u_{01}-u_{10}+u_{11})|-\rangle \tag{12}$$

由式(12)可知,Alice 运用的测量基是 X 基时,Eve 被发现的概率是 $\frac{1}{2}(|u_{01}|^2+|u_{10}|^2)$.当 Alice 运用的测量基是 Z 基时,那么 Eve 被发现的概率就是 $\frac{1}{8}(|u_{00}+u_{01}+u_{10}+u_{11}|^2+|u_{00}+u_{01}-u_{10}-u_{11}|^2+|u_{00}-u_{01}+u_{10}-u_{11}|^2+|u_{00}-u_{01}+u_{10}-u_{11}|^2)$.

4　结　论

首先提出来一种理想的双向量子隐形传态,这个协议仅需要单一量子比特测量、受控非门操作、以及一位门操作,比现有的协议更加方便.又利用双向量子隐形传态提出双向量子安全直接通信,运用了纠缠交换和隐形传输技巧,没有携带秘密信息的量子比特从量子信道中传输,因此量子信道是理想的,双向量子安全通信肯定是安全的.

(下转第 67 页)