doi:10.3788/gzxb20144301.0127001

基于五粒子团簇态的可控量子安全直接通信

聂义友,徐玮,章勤男,李渊华,桑明煌

(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:提出了一个利用五粒子团簇态实现的可控量子安全直接通信方案.在这一方案中,首先信息发送者 Alice、信息接收者 Bob 和控制者 Charlie 共享由 Alice 制备的一有序序列团簇态作为量子信道;在确定量子信道的安全性以后,Alice 制备编码量子态(Bell 态)序列,然后通过对自己手中的粒子进行 Bell 基测量,接着 Charlie 对自己手中的粒子进行单粒子的测量,就能把信息传送给接收者 Bob;最后,Bob 测量自己手中的粒子,并通过分析三人的测量结果,从而获得 Alice 要传送的信息.在我们提出的方案中,携带信息的粒子不需要在公共信道上传输.该文中,我们给出了方案的安全性分析,证明了我们的方案是决定性的和安全的.在未来,我们的方案在以目前的实验技术为基础条件下很可能得到实现.

关键词:量子信息; 量子安全直接通信; 团簇态; Bell 测量

中图分类号:O431.2 **文献标识码**:A **文章编号**:1004-4213(2014)01-0127001-5

Controlled Quantum Secure Direct Communication by Using Five-particle Cluster States

NIE Yi-you, XU Wei, ZHANG Qin-nan, LI Yuan-hua, SANG Ming-huang

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

Abstract: A novel controlled quantum secure direct communication scheme by using five-particle cluster states is proposed. In this scheme, the quantum channel between the sender Alice, the controller Charlie and the receiver Bob consists of an ordered sequence of five-particle cluster states which are prepared by Alice. After determine the security of quantum channel, Alice prepares the encoded Bell-state sequences, and Alice and Bob perform Bell-state measurements on the particles at hand, respectively, and then Charlie may make a single-particle measurement. Then Alice and Charlie tell their result to Bob, Bob can get the secret information through the analysis of their results. In our scheme, the information-carrying particles do not need to be transmitted over the public channel. Moreover, we analyze the security of the controlled quantum secure direct communication protocol, and demonstrate that our scheme is determinate and secure. In the future, our scheme might be realizable based on present experimental technology.

Key words: Quantum information; Quantum secure direct communication; Cluster state; Bell-state measurements

OCIS Codes: 270.0270; 270.5565

0 引言

量子安全直接通信是目前量子信息领域的研究热点之一.自从第一个无条件安全的量子密钥分发(Quantum Key Distribution, QKD)方案(即 BB84 协议)被提出以来,QKD 受到了人们广泛关注,并得到了迅速发展和不断改进[1-3].随后人们在 QKD 的基础上提出了量子安全直接通信(Quantum Secure Direct

基金项目:国家自然科学基金(No. 61265001)、江西省自然科学基金(No. 20122BAB202005)和江西省教育厅科研课题(No. GJJ13236)资助

第一作者:聂义友(1963—),男,教授,硕士,主要研究方向为量子光学、量子通信和量子信息. Email: nieyiyou@163.com

收稿日期:2013-04-27;**录用日期**:2013-07-03

Communication, QSDC)的方案,并吸引了众多研究者的关注. Bostrom 和 Felbinger 利用 EPR 对作为量子信道,提出了一个 QSDC 的乒乓协议[4],然而 Zhang 等人[5]证明了这个乒乓协议是不安全的. 后来,人们又利用各种量子态作为量子信道,提出了许多改进的 QSDC 的方案[6-14],这些量子信道包括 EPR 态[6]和 GHZ 态[8]态等.

团簇态[15](cluster states)是 H. J. Briegel 和 R. Raussendorf 于 2001 年提出的一种新的纠缠态,并证明团簇态在 $N>3$ 时有一些特殊的性质,例如最大联通性和持续纠缠性. 它的持续纠缠性比 GHZ 态更好,即团簇态包含了 GHZ 类[16-17]和 W 类[18-20]纠缠态的性质. 近些年来,人们利用团簇态为量子信道提出了一些 QSDC 方案[21-22]. 然而,在这些方案中,都是利用两步方法传送粒子,即除了要传送建立信道的粒子外,还要传送携带信息的粒子给信息接收者. 最近,文献[9]利用五粒子团簇态和经典 XOR 逻辑门提出了一个量子安全通信直接方案,该方案中的五粒子团簇态不是用于做量子信道,而是用于检测窃听. 本文提出一种利用五粒子团簇态为量子信道的新的可控量子安全直接通信方案,在该方案中,通信双方只在建立量子信道时传送一次粒子,而携带信息的粒子不需要在公共信道上传送,且只要进行局域的 Bell 测量和单粒子测量,就能实现可控的量子安全直接通信. 最后,对本方案的安全性进行了分析,证明了本文方案是决定性的和安全的.

1 基于五粒子团簇态的可控量子安全直接通信方案

为了实现直接通信,选择五粒子团簇态为量子信道. 五粒子团簇态为[9]

$$|\psi\rangle_{12345}=\frac{1}{2}(|00000\rangle+|00111\rangle+|11101\rangle+|11010\rangle)_{12345} \tag{1}$$

这个量子态又可以表示为

$$|\psi\rangle_{12345}=\frac{1}{2}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{25}|0\rangle_4+|\Phi^-\rangle_{13}|\Phi^-\rangle_{25}|0\rangle_4+|\Psi^+\rangle_{13}|\Psi^+\rangle_{25}|1\rangle_4+|\Psi^-\rangle_{13}|\Psi^-\rangle_{25}|1\rangle_4) \tag{2}$$

式中:$|\Phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$,$|\Psi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$,为 Bell 态. 下面详细描述本文的方案:

1) Alice 想与 Bob 进行直接通信. 在通信之前,Alice 和 Bob 事先约定用 4 个 Bell 态按如下方式进行编码:

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\longrightarrow 00$$

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)\longrightarrow 11$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)\longrightarrow 01$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)\longrightarrow 10$$

2) 信息发送者 Alice 制备一有序序列团簇态 $|\psi^i\rangle_{12345}$ 和足够多的单粒子态. 团簇态用来建立通信信道,而单粒子态用于产生干扰. 接着,Alice 把有序序列团簇态 $|\psi^i\rangle_{12345}$ 中的粒子分成三组有序粒子对序列,每个团簇态中的粒子 1 和 3 为一组有序粒子对序列,用 P_{13}^i 表示,粒子 2 和 5 为另一组,用 P_{25}^i 表示,粒子 4 为第三组,用 P_4^i. 然后,Alice 把 P_{13}^i 序列保留在自己手中,依次把 P_4^i 粒子发送给 Charlie 和 P_{25}^i 序列粒子对发送给 Bob. 为了防止窃听者 Eve 的窃听,Alice 在发送 P_{25}^i 序列粒子对时,把干扰的单粒子按自己知道的方式随意夹杂在由粒子 2 和 5 组成的序列中,并记录下所有干扰粒子所在的位置. 夹杂粒子序列的示意图如图 1(a). 用同样的方法给 Charlie 发送 P_4^i 粒子,夹杂粒子序列的示意图如图 1(b).

②⑤②⑤②⑤②⑤……②⑤——→②⊙⑤②⑤⊙②⑤⊙②⑤②⊙⑤②……⑤⊙②⑤

(a) The sketch of mixing single-qubit in P_{25}^i sequence, where ⊙ represents a mixed single qubit

④④④④④④④④……④④——→④⊙④④④⊙④④⊙④④④⊙④④……④⊙④④

(b) The sketch of mixing single-qubit in P_4^i sequence, where ⊙ represents a mixed single qubit

图 1 Alice 夹杂粒子序列的示意图

Fig. 1 The sketch of mixing single-qubit for Alice

3) 接收者 Bob 和控制者 Charlie 分别接到 P_{25}^i 粒子对和 P_4^i 粒子序列后,通过经典信道告诉发送者 Alice 自己经收到了粒子对序列. 接着,Alice 告诉 Bob 和 Charlie 干扰粒子所在的位置,并且 Bob 和 Charlie 把干扰粒子从收到的粒子序列中取出并抛弃.

4) Bob 在剩下的粒子对序列中随机地取出足够多的检验粒子对进行 Bell 基测量,并把随机取出的检验粒子对的位置和 Bell 基测量结果告诉 Alice 和 Charlie. 接着,Charlie 在剩下的 P_4^i 序列中相对应的位置取出粒子在基$\{|0\rangle,|1\rangle\}$下进行单粒子测量,Alice 在 P_{13}^i 序列中相应的位置取出粒子对也进行 Bell 基测量. 然后,检验三人的测量结果是否相关联,如果三人的测量结果是按式(2)中的形式相配对,说明信道是安全的,没有被窃听者 Eve 窃听,可以进行下一步通信;如果不是,说明信道不安全,被 Eve 窃听,应抛弃这一信道,并重新开始建立信道.

5) 在确定信道是安全的以后,Alice 根据通信内容按事先约定的编码方式制备编码态序列 $|\Phi^\pm\rangle_{ab}^i$ 和 $|\Psi^\pm\rangle_{ab}^i$,然后按顺序对自己拥有的粒子 (a,1) 和 (b,3) 分别做 Bell 基测量,并把测量结果通过经典信道发送给 Bob. Charlie 对自己拥有的粒子 4 在基$\{|0\rangle,|1\rangle\}$下进行单粒子测量,并把测量结果通过经典信道发送

给 Bob.

6) 最后,Bob 对自己手中的粒子 2 和 5 进行 Bell 基测量,并把自己测得的结果和 Alice、Charlie 发送来的测量结果进行分析解码,从而能得到 Alice 要发送的信息.

为了使编码和解码过程更加明了,我们举一个例子加以说明:假设 Alice 要发送经典信息 00,则她制备 $|\Phi^+\rangle_{ab}$ 态;然后把处于 Bell 态的粒子 a、b 和处于团簇态的粒子 1、3 按 (a,1) 和 (b,3) 分别进行 Bell 基测量,并且 Charlie 对粒子 4 在基 $\{|0\rangle,|1\rangle\}$ 下进行单粒子测量,两人都把测量结果告诉 Bob;最后,Bob 对自己手中的粒子 2 和 5 进行 Bell 基测量,并把自己的测量结果和 Alice 对 (a,1) 和 (b,3) 的测量结果以及 Charlie 对粒子 4 的测量结果进行分析解码,便知 Alice 要传送的信息是 00. 其原理和相应的测量结果如下:

$$
\begin{aligned}
&|\Phi^+\rangle_{ab}\otimes|\psi\rangle_{12345}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{ab}\otimes\frac{1}{2}(|00000\rangle+|00111\rangle+|11101\rangle+|11010\rangle)_{12345}=\\
&\frac{1}{2}|\Phi^+\rangle_{ab}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{25}|0\rangle_4+|\Phi^-\rangle_{13}|\Phi^-\rangle_{25}|0\rangle_4+|\Psi^+\rangle_{13}|\Psi^+\rangle_{25}|1\rangle_4+|\Psi^-\rangle_{13}|\Psi^-\rangle_{25}|1\rangle_4)=\\
&\frac{1}{4}[(|\Phi^+\rangle_{a1}|\Phi^+\rangle_{b3}+|\Phi^-\rangle_{a1}|\Phi^-\rangle_{b3}+|\Psi^+\rangle_{a1}|\Psi^+\rangle_{b3}+|\Psi^-\rangle_{a1}|\Psi^-\rangle_{b3})|\Phi^+\rangle_{25}|0\rangle_4+\frac{1}{4}(|\Phi^+\rangle_{a1}|\Phi^-\rangle_{b3}+\\
&|\Phi^-\rangle_{a1}|\Phi^+\rangle_{b3}-|\Psi^+\rangle_{a1}|\Psi^-\rangle_{b3}-|\Psi^-\rangle_{a1}|\Psi^+\rangle_{b3})|\Phi^-\rangle_{25}|0\rangle_4+\frac{1}{4}(|\Phi^+\rangle_{a1}|\Psi^+\rangle_{b3}+|\Phi^-\rangle_{a1}|\Psi^-\rangle_{b3}+\\
&|\Psi^+\rangle_{a1}|\Phi^+\rangle_{b3}+|\Psi^-\rangle_{a1}|\Phi^-\rangle_{b3})|\Psi^+\rangle_{25}|1\rangle_4+\frac{1}{4}(|\Phi^+\rangle_{a1}|\Psi^-\rangle_{b3}+|\Phi^-\rangle_{a1}|\Psi^+\rangle_{b3}-|\Psi^+\rangle_{a1}|\Phi^-\rangle_{b3}-\\
&|\Psi^-\rangle_{a1}|\Phi^+\rangle_{b3})|\Psi^-\rangle_{25}|1\rangle_4]
\end{aligned}
\tag{3}
$$

若 Alice 要发送的经典信息是 01、10 和 11,则她分别制备 $|\Psi^+\rangle_{ab}$、$|\Psi^-\rangle_{ab}$ 和 $|\Phi^-\rangle_{ab}$ 态;然后分别对 (a,1) 和 (b,3) 进行 Bell 基测量并把测量结果告诉 Bob. 其次,在控制者 Charlie 对粒子 4 进行单粒子测量,最后,Bob 对粒子 2、5 进行 Bell 基测量,并分析三人的测量结果进行解码. Alice、Charlie 和 Bob 的测量结果和相应的解码表如表 1.

表 1 Alice、Charlie 和 Bob 的测量结果以及解码信息表

Table 1 The outcome of measurements performed by Alice, Charlie and Bob, the corresponding decoding information

Alice's result	Charlie's result	Bob's result	Decoding information
$\|\Phi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^+\rangle_{25}$	00
$\|\Phi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle 4$		
$\|\Psi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle 4$		
$\|\Psi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^-\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^+\rangle_{25}$	
$\|\Psi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^-\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^+\rangle_{25}$	11
$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^-\rangle_{25}$	
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^+\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^-\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^+\rangle_{25}$	10
$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^-\rangle_{25}$	
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^+\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^-\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^+\rangle_{25}$	01
$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^-\rangle_{25}$	
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^+\rangle_{25}$	
$\|\Phi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		

$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^-\rangle_{25}$	
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^+\rangle_{25}$	10
$\|\Phi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|0\rangle_4$	$\|\Phi^-\rangle_{25}$	
$\|\Psi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|0\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|0\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^+\rangle_{25}$	
$\|\Psi^+\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^+\rangle_{a1}\|\Phi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Phi^-\rangle_{a1}\|\Phi^-\rangle_{b3}$	$\|1\rangle_4$	$\|\Psi^-\rangle_{25}$	
$\|\Psi^+\rangle_{a1}\|\Psi^+\rangle_{b3}$	$\|1\rangle_4$		
$\|\Psi^-\rangle_{a1}\|\Psi^-\rangle_{b3}$	$\|1\rangle_4$		

由分析可知，本文提出的通信方案有二个优点，一是携带秘密信息的粒子不需要在公共信道上传输，第二是该方案可控. 因此，在整个信息传送过程中，潜在的窃听者 Eve 不可能获得任何秘密信息.

2 安全性分析

该方案的安全性要求是：Alice 在发送 P_{25}^i 有序序列粒子对和 P_4^i 有序序列粒子分别给 Bob 和 Charlie 的过程中，建立的通信信道是安全的. 只要通信信道安全，则秘密信息就不可能被泄露，因为携带信息的粒子始终在 Alice 手中，而没有在公共信道上传输. 因此，本文仅对建立信道的安全性进行分析.

第一，假设窃听者 Eve 对传送 P_{25}^i 有序序列粒子对实行拦截——重发攻击. 即 Eve 在截获 Alice 发送给 Bob 的 P_{25}^i 有序序列粒子对后，制备数量相等的处于团簇态的粒子对发送给 Bob. 由于 Alice 在发送 P_{25}^i 有序序列粒子对时，夹杂了足够多的干扰单粒子在其中，而这些粒子所在的位置只有 Alice 知道，Eve 并不知道. 当 Bob 接到 Eve 发送的序列粒子对后，告诉 Alice 自己已经收到粒子序列. 然后 Alice 告诉 Bob 夹杂干扰单粒子所在的位置，接着 Bob 把夹杂的干扰单粒子取出并抛弃. 这样就会破坏团簇态原有的关联性，在随后检测中就会被发现. 所以，实施拦截——重发攻击是无效的.

第二，在量子密码中，纠缠攻击是一种可能的技巧. 假设窃听者 Eve 在 Alice 和 Bob 建立量子信道时，通过执行 CNOT 操作，把自己的分别处于 $|0\rangle_6$ 和 $|0\rangle_7$ 态的粒子 6 和 7 纠缠到处于团簇态的粒子 2 和 5 上，执行 CNOT 操作时，分别把粒子 2 和 5 作为控制比特，把粒子 6 和 7 作为目标比特，则量子信道就处于七粒子纠缠态

$$
\begin{aligned}
|\psi\rangle_{1234567}&=\frac{1}{2}(|0000000\rangle+|0011101\rangle+|1110111\rangle+|1101010\rangle)_{1234567}=\frac{1}{2\sqrt{2}}\{|\Phi^+\rangle_{13}(|00000\rangle+|10111\rangle)_{24567}+\\
&|\Phi^-\rangle_{13}(|000000\rangle-|10111\rangle)_{24567}+|\Psi^+\rangle_{13}(|01101\rangle+|11010\rangle)_{24567}+|\Psi^-\rangle_{13}(|01101\rangle-|11010\rangle)_{24567}\}=\\
&\frac{1}{2\sqrt{2}}\{|\Phi^+\rangle_{13}(|\Phi^+\rangle_{25}|\Phi^+\rangle_{67}+|\Phi^-\rangle_{25}|\Phi^-\rangle_{67})|0\rangle_4+|\Phi^-\rangle_{13}(|\Phi^+\rangle_{25}|\Phi^-\rangle_{67}+|\Phi^-\rangle_{25}|\Phi^+\rangle_{67})|0\rangle_4+\\
&|\Psi^+\rangle_{13}(|\Psi^+\rangle_{25}|\Psi^+\rangle_{67}+|\Psi^-\rangle_{25}|\Psi^-\rangle_{67})|1\rangle_4+|\Psi^-\rangle_{13}(|\Psi^+\rangle_{25}|\Psi^-\rangle_{67}+|\Psi^-\rangle_{25}|\Psi^+\rangle_{67})|1\rangle_4\}
\end{aligned}
\tag{4}
$$

从式(4)可见，Eve 和 Bob 是处于同等的地位. 但是，这种情况是可以排除的. 因为，当 Alice 和 Bob 以及 Charlie 在随机选择一些相对应的粒子对进行 Bell 基测量和单粒子测量后，通过分析两人的测量结果，就会发现此时有 50% 的测量结果是不相关联的，从而得出通信信道是不安全的结论. 因此，实施纠缠攻击也是无效的.

综合上述分析，可见本文提出的量子安全直接通信方案是可行的、决定性的和安全的.

3 效率分析

方案中，为了建立安全的通信信道，使用了诱骗粒子(掺杂粒子). 可是，诱骗粒子的比例是很小的，在理论上是可以忽略的. 可就是说，在控制者能够合作的情况下，所有的量子资源(除了少量用于检测窃听的粒子外)都能被使用来承载量子信息，因此量子比特的内禀效率接近 100%. 另外，按照文献[23]的方法，该方案的总效率为

$$\eta_t=q_u/(q_t+b_t) \tag{5}$$

式中 q_u 表示有效的量子比特数，q_t 表示被传输的量子比特数，b_t 表示通过经典信道传送的经典比特数. 根据公式(5)可计算出我们方案的总效率为 50%.

4 结论

本文提出了一个基于五粒子团簇态的可控量子安全直接通信方案. 在这个方案中，首先信息发送者 Alice、控制者 Charlie 和信息接收者 Bob 共享由 Alice 制备的一有序序列团簇态作为量子信道. 在确定量子信道的安全性以后，Alice 制备编码量子态(Bell 态)序列，然后通过对自己手中的粒子进行 Bell 基测量，以及

控制者对自己手中的粒子进行单粒子测量后,就能把信息传送给接收者 Bob,每次能传送 2 比特的经典信息.最后,Bob 测量自己手中的粒子,并通过分析三人的测量结果,从而获得 Alice 要传送的信息.这一方案是决定性的和安全的,而且在现有的技术条件下是可以实现的.

参考文献

[1] DENG F G, LONG G L. Controlled order rearrangement encryption for quantum key distribution[J]. *Physical Review A*, 2003, **68**(4): 042315.

[2] DENG F G, LONG G L. Bidirectional quantum key distribution protocol with practical faint laser pulses [J]. *Physical Review A*, 2004, **70**(1): 012311.

[3] ZHANG Z J, MAN Z X, SHI S H. An efficient multiparty quantum key distribution scheme[J]. *International Journal of Quantum Information*, 2005, **3**(3): 555-559.

[4] BOSTROM K, FELBINGER T. Deterministic secure direct communication using entanglement [J]. *Physical Review Letters*, 2002, **89**(18): 187902.

[5] ZHANG Z J, MAN Z X, LI Y. Improving Wójcik′s eavesdropping attack on the ping - pong protocol[J]. *Physics Letters A*, 2004, **333**(1): 46-50.

[6] YI X J, NIE Y Y, ZHOU N R, *et al*. Quantum secure direct communication using entangled photon pairs and local measurement[J]. *Communications in Theoretical Physics*, 2008, **50**(1): 81-84.

[7] JIN X R, JI X, ZHANG YQ, *et al*. Three-party quantum secure direct communication based on GHZ states[J]. *Physics Letters A*, 2006, **354**(1): 67-70.

[8] WANG J, ZHANG Q, TANG C J. Multiparty controlled quantum secure direct communication using Greenberger - Horne - Zeilinger state[J]. *Optics Communications*, 2006, **266**(2): 732-737.

[9] LI J, SONG D J, GUO X J, *et al*. A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation[J]. *Chinese Physics C*, 2012, **36**(1): 31-36.

[10] SUN Z W, DU R G, LONG DY. Quantum secure direct communication with two-photon four-qubit cluster states[J]. *International Journal of Theoretical Physics*, 2012, **51**(6): 1946-1952.

[11] QIN S J. Reexamining the security of controlled quantum secure direct communication by using four particle cluster states[J]. *International Journal of Theoretical Physics*, 2012, **51**(9): 2714-2718.

[12] SUN Z W, DU R G, LONG D Y. Quantum secure direct communication with two-photon four-qubit cluster states[J]. *International Journal of Theoretical Physics*, 2012, **51**(6): 1946-1952.

[13] LIU Z H, CHEN H W, LIU W J, *et al*. Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states [J]. *Quantum Information Processing*, 2013, **12**(1): 587-599.

[14] QUAN Dong-xiao, PEI Chang-xing, LIU Dan, *et al*. Scheme for wide-area quantum secure direct communication network based on decoy states[J]. *Acta Photonica Sinica*, 2009, **38**(12): 3283-3287.
权东晓,裴昌幸,刘丹,等. 一种基于诱骗态的广域量子安全直接通信网络方案[J]. 光子学报, 2009, **38**(12): 3283-3287.

[15] BRIEGEL H J, RAUSSENDORF R. Persistent Entanglement in Arrays of Interacting Particles[J]. *Physical Review Letters*, 2001, **86**(5): 910-913.

[16] NIE Y Y, LI Y H, WANG Z S. Semi-quantum information splitting using GHZ-type states[J]. *Quantum Information Processing*, 2013, **12**(1): 437-448.

[17] YE Tian-yu, JIANG Li-zhen. False alarm probability of eavesdropping checks for controllable quantum secret sharing [J]. *Acta Photonica Sinica*, 2012, **41**(9): 1113-1117.
叶天语,蒋丽珍. 可控量子秘密共享协议窃听检测虚警概率分析[J]. 光子学报, 2012, **41**(9): 1113-1117.

[18] SHENG Y B, ZHOU L, ZHAO S M. Efficient two-step entanglement concentration for arbitrary W states [J]. *Physics Letters A*, 2012, **85**(4): 042302.

[19] LI Yuan-hua, LIU Jun-chang, NIE Yi-you. Quantum identification scheme of cross-center based on W-state[J]. *Acta Photonica Sinica*, 2010, **39**(9): 1616-1620.
李渊华,刘俊昌,聂义友. 基于 W 态的跨中心量子网络身份认证方案[J]. 光子学报, 2010, **39**(9): 1616-1620.

[20] ZHOU Xiao-qing, WU Yun-wen. Token-bus network fidelity of quantum teleportation by three-photon entangled W state [J]. *Acta Photonica Sinica*, 2010, **39**(9): 1616-1620.
周小清, 邬云文. 三光子纠缠 W 态隐形传输令牌总线网的保真度计算[J]. 光子学报, 2010, **39**(11): 2093-2096.

[21] GAO F, GUO F Z, WEN Q Y, *et al*. Forcible-measurement attack on quantum secure direct communication protocol with cluster state [J]. *Chinese Physics Letters*, 2008, **25**(8): 2766-2769.

[22] CAO W F, YANG Y G, WEN Q Y. Quantum secure direct communication with cluster states [J]. *Science China Physics, Mechanics & Astronomy*, 2010, **53**(7): 1271-1275.

[23] LI X H, ZHOU P, LI C Y, *et al*. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state [J]. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 2006, **39**(8): 1975-1983.