物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于cluster态的信道容量可控的可控量子安全直接通信方案

郑晓毅　龙银香

Cluster state based controlled quantum secure direct communication protocol with controllable channel capacity

Zheng Xiao-Yi　Long Yin-Xiang

引用信息 Citation: Acta Physica Sinica, 66, 180303 (2017)　DOI: 10.7498/aps.66.180303
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.180303
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I18

基于cluster态的信道容量可控的可控量子安全直接通信方案*

郑晓毅† 龙银香

(广东水利电力职业技术学院自动化工程系, 广州 510635)

(2017年5月10日收到; 2017年6月2日收到修改稿)

提出了一种基于五粒子cluster态的信道容量可控的可控量子安全直接通信方案. 通信三方利用五粒子cluster态自身的粒子分布情况, 结合诱骗光子, 对粒子分别做Z基单粒子测量和Bell基测量, 便可完成信道的第一次安全性检测. 通信控制方Cindy通过对手中的粒子序列随机选用测量基(Z基或者X基)测量来决定信道容量, 并通过经典信道公布结果. 发送方Alice将要发送的信息以及校检信息用于对手中的粒子序列进行幺正操作编码, 并插入诱骗光子后将编码后的粒子序列发给接收方Bob并通过经典信道告知其诱骗光子的位置信息. Bob接收到粒子序列后, 按照经典信道Alice发送的信息, 结合Cindy公布的信息, 剔除诱骗光子后按照一定的规则对手中的两组粒子序列进行Bell基测量, 便可解码完成第二次安全性检测以及得到Alice发送的信息. 通过对五粒子cluster态的纠缠结构性质进行分析, 阐明了五粒子cluster态在该方案中所表现出的特点的物理缘由. 结果表明, 只需变化测量基的规则和用于编码的粒子, 可以将该方案推广成可控双向量子安全直接通信.

关键词: Bell基测量, 五粒子cluster态, 幺正操作, 可控量子安全直接通信

PACS: 03.67.Hk, 03.67.Ac, 03.65.Ud **DOI:** 10.7498/aps.66.180303

1 引 言

量子安全直接通信(quantum secure direct communication, QSDC)是在量子力学的基础上提出的一种拥有“赞歌”能力, 也就是在线探测窃听者[1]的能力, 以及“油床”能力, 也就是消除信息前泄露的安全信息技术[1,2]. 这种安全信息技术是一种物理原理上百分百保密信息技术, 因而成为量子信息技术的研究热点.

在2000年由Long和Liu[3]提出的被称为高效QSDC的方案是最早的QSDC方案. 该方案基于Einstein-Podolsky-Rosen (EPR)对生成共享密钥, 首次提出了量子数据块传输和分步传输的方法, 消除了信息的前泄露问题. 2003年, Deng等[4]基于量子密集编码提出了一个基于EPR对为信道的QSDC方案, 该方案被称之为“两步方案”. 同年, Deng和Long[5]提出了被称为DL-04的基于单光子量子态的一次一密QSDC方案. 这两个方案给出了QSDC方案的基本标准、构造原理以及安全判定条件, 有效地推动了QSDC的发展.

随后, 众多研究者依据数据块传输以及分步传输的原理, 利用不同的量子态作为量子信道, 研究设计出了多种具有实际应用意义的QSDC方案[6−11]. 这些量子信道包括了EPR态、Greenberger-Horne-Zeilinger (GHZ)态、cluster态等.

Cluster态是在2001年由Briegel和Raussendorf[12]报道的当粒子数$N > 3$时体现出特殊性质的一种量子态. Cluster态具有最大连通特性, 其持续纠缠比GHZ和W态更好, 并且比GHZ类纠缠态更难被局域操作破坏. Cluster态可以由多种方

* 广东省自然科学基金(批准号: 2016a030313736)资助的课题.

† 通信作者. E-mail: kyle87@126.com

法制备得到, 如利用光学系统、腔量子电动力学系统和离子阱系统等. 其中较为简单的方法是利用线性系统制备, 有较强的可操作性[13−15]. 关于cluster态在量子通信中的各种应用研究[16−25]也得到了快速的发展, 研究者也利用cluster态的特殊性质设计了多种QSDC方案[26−32]. 2011年, Wang和Zha[26]基于四粒子cluster态提出了双向QSDC方案. 2012年, Sun等[27]提出了基于两光子四比特cluster态的QSDC方案. 同年, Li等[28]基于五粒子cluster态和经典异或门提出了一种QSDC方案, 将cluster态应用到检测窃听. 2014年, Chang等[29]基于五粒子cluster态和量子一次一密提出了一种可控量子安全直接通信(controlled quantum secure direct communication, CQSDC)方案, 并在方案中实现了身份的验证.

本文首先基于五粒子cluster态的特殊纠缠性质, 提出了一种信道容量可控的CQSDC方案. 在该方案中, 通信三方利用插入诱骗光子[33,34]的方法, 与Z基单粒子测量、Bell基测量、校验信息相结合的方式, 便可完成信道的安全性检测. 同时, 通信控制方可以通过采用不同的基测量来决定信道的容量, 并通过经典信道公布测量结果, 信息发送方和接收方在控制方的帮助下完成信息传送. 接着对五粒子cluster态的纠缠结构性质进行了分析, 阐明了五粒子cluster态在该CQSDC方案中所表现出的特点的物理缘由. 结果表明, 只需变化测量基的规则和用于编码的粒子, 可以将本文方案推广成可控双向量子安全直接通信. 最后, 对本方案进行安全性分析, 表明本文方案可以有效防止窃听者窃听到有用的信息并且可监测到窃听行为, 而且在理论上可在一定噪声环境中完成CQSDC.

2 基于cluster态的信道容量可控的CQSDC方案

方案使用五粒子cluster态作为量子信道, 该态可以表示为

$$|\Phi_{\rm cluster}\rangle_{12345} = \frac{1}{2}\left(|00000\rangle + |00111\rangle + |11101\rangle + |11010\rangle\right)_{12345}.$$

方案中三方参与者Alice为信息发送方, Bob为信息接收方, Cindy为半忠诚的控制方, 即Cindy在测量行为以及测量结果的公布上都是诚实以及配合的, 不发生作弊行为, 但不保证不发生窃听行为. 下面分步骤具体描述方案过程.

步骤1 准备阶段

通信中发送方Alice制备n组五粒子cluster态, 将这n组五粒子cluster态表示为

$$\begin{aligned}&[P_1(1),P_1(2),P_1(3),P_1(4),P_1(5);\\ &P_2(1),P_2(2),P_2(3),P_2(4),P_2(5);\cdots;\\ &P_i(1),P_i(2),P_i(3),P_i(4),P_i(5);\cdots;\\ &P_n(1),P_n(2),P_n(3),P_n(4),P_n(5)],\end{aligned}$$

其中$P_i(1),P_i(2),P_i(3),P_i(4),P_i(5)$ $(i=1,2,\cdots,n)$分别表示第i组团簇态中的第1, 2, 3, 4, 5个粒子. 制备出n组团簇态后, Alice从每组团簇态取出粒子, 组成三组粒子序列, 并制备数量为$m_{\rm b}$和$m_{\rm c}$的两组单光子态作为诱骗光子随机夹杂到其中的两组粒子序列$S_{\rm B}$和$S_{\rm C}$, Alice记录下诱骗光子的位置, 即

$$\begin{aligned}&S_{\rm A}\colon [P_1(2),P_1(3),P_2(2),P_2(3),\cdots,P_n(2),P_n(3)];\\ &S_{\rm B}\colon [P_1(1),P_1(5),P,P_2(1),P,P_2(5),\cdots,\\ &\quad P_n(1),P_n(5)]\\ &S_{\rm C}\colon [P_1(4),P,P_2(4),\cdots,P_n(4)],\end{aligned}$$

其中, $S_{\rm A}$序列的长度为$2n$, $S_{\rm B}$序列的长度为$2n+m_{\rm b}$, 而$S_{\rm C}$序列的长度为$n+m_{\rm c}$. Alice将制备好的三组粒子序列中的$S_{\rm B}$序列发给Bob, $S_{\rm C}$序列发给Cindy, 自己保留粒子序列$S_{\rm A}$.

步骤2 安全检测阶段

Bob和Cindy接收到粒子序列后, 进行第一步协议安全检测. Alice将记录下来的诱骗光子的位置通过经典信道告诉Bob和Cindy. Bob和Cindy根据收到的信息将诱骗光子从收到的序列中取出. 接着, Alice对自己拥有的$S_{\rm A}$粒子序列, 随机选取i组粒子2和粒子3做Bell基测量$(i<n)$, 并通过经典信道公布i组粒子在序列中的位置以及相对应的测量结果. Bob根据Alice公布的信息对自己手中摒弃诱骗光子后的$S_{\rm B}$序列的i组粒子1和粒子5做Bell基测量. 同样地, Cindy也根据Alice公布的信息对自己手中摒弃诱骗光子后的$S_{\rm C}$序列在Z基$\{|0\rangle, |1\rangle\}$上进行测量. 三方公布自己测量的结果并做对比, 测量结果应该满足表1中的关系. 其中$|B_{00}\rangle$, $|B_{01}\rangle$, $|B_{10}\rangle$, $|B_{11}\rangle$分别为4个Bell态,

具体为

$$|B_{00}\rangle=\frac{|00\rangle+|11\rangle}{\sqrt{2}},\quad |B_{01}\rangle=\frac{|01\rangle+|10\rangle}{\sqrt{2}},$$
$$|B_{10}\rangle=\frac{|00\rangle-|11\rangle}{\sqrt{2}},\quad |B_{11}\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}.$$

表 1 Alice, Bob, Cindy 的测量结果

Table 1. The outcome of the measurements preformed by Alice, Bob and Cindy.

Alice 测量结果	Bob 测量结果	Cindy 测量结果
$|B_{00}\rangle_{23}$	$|B_{00}\rangle_{15}$	$|0\rangle_4$
$|B_{01}\rangle_{23}$	$|B_{01}\rangle_{15}$	$|1\rangle_4$
$|B_{11}\rangle_{23}$	$|B_{11}\rangle_{15}$	$|1\rangle_4$
$|B_{10}\rangle_{23}$	$|B_{10}\rangle_{15}$	$|0\rangle_4$

Alice 统计 Bob 和 Cindy 测量结果的错误率, 当错误率低于某个特定的阈值, 可以认为协议安全, 通信继续. 否则表明存在窃听行为, 应该放弃此次通信, 防止信息泄露.

步骤 3 信道容量控制阶段

在通信三方确定了相互之间的通信安全的情况下, 通信三方弃除各自粒子序列中用于安全检测的 i 组粒子, 形成新的三组粒子序列 $S'_{\rm A}, S'_{\rm B}, S'_{\rm C}$. 通信控制方 Cindy 根据实际通信需求, 对手中的粒子序列 $S'_{\rm C}$ 随机选用 Z 基 $\{|0\rangle, |1\rangle\}$ 和 X 基 $\{|+\rangle, |-\rangle\}$ 中的一组基进行单粒子测量, 其中 $|\pm\rangle=\frac{\sqrt{2}}{2}(|0\rangle\pm|1\rangle)$. 并通过经典信道公布测量结果. 为方便讨论, 不失一般性, 假设弃除检测粒子后粒子序列 $S'_{\rm A}, S'_{\rm B}$ 的长度为 8, $S'_{\rm C}$ 长度为 4, Cindy 对 $S'_{\rm C}$ 序列中的粒子采用 $\{XZZX\}$ 基测量, 测量结果为 $\{+10-\}$.

步骤 4 信息编码阶段

得到 Cindy 公布的测量结果之后, 信息发送者 Alice 对自己所要发送的信息进行 Pauli 幺正操作编码, 编码的方式如下:

约定 $U_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|$, $U_1=\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$, $U_2=\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$, $U_3=\mathrm{i}\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$ 对应于经典信息 00, 01, 10, 11.

从 Cindy 公布的结果来看, Alice 可以通过对手中的 $S'_{\rm A}$ 粒子序列进行幺正操作编码达到传送 12 bit 的经典信息. 不失一般性, 假定要传送的经典信息为“10-11-00-11-01-10”, 则 Alice 对手中的 $S'_{\rm A}$ 粒子序列的 4 组粒子 $[P_1(2), P_1(3), \cdots, P_4(2), P_4(3)]$ 依序进行 $\{U_2, U_3;\ U_0, U_0;\ U_0, U_3;\ U_1, U_2\}$ 幺正操作, 其中对于以 Z 基测量的同组粒子 2 不进行操作, 同样以 U_0 表示.

为保证通信安全, Alice 在发送信息的同时可以通过添加校检信息的方式以及诱骗光子的方法进行第二次安全性检测, 譬如第七、八位的信息 11 为校检信息, 以及如第一次安全检测中一样随机插入适量的单光子态作为诱骗光子. 将操作过后的 $S''_{\rm A}$ 粒子序列发送给接受者 Bob, 并通过经典信道告知 Bob 校检信息以及诱骗光子的位置.

表 2 Bob, Cindy 的测量结果以及解码信息表

Table 2. The outcome of the measurements preformed by Bob and Cindy, and the corresponding decoding information.

Alice 发送的经典信息及对应的幺正操作	Bob 的测量结果其中 $mn\in\{1,2;3,5\}$		Cindy 的测量结果
(00) U_0	$|B_{00}\rangle_{mn}$		$|+\rangle$
(01) U_1	$|B_{01}\rangle_{mn}$		
(10) U_2	$|B_{10}\rangle_{mn}$		
(11) U_3	$|B_{11}\rangle_{mn}$		
(00) U_0	$|B_{10}\rangle_{mn}$		$|-\rangle$
(01) U_1	$|B_{11}\rangle_{mn}$		
(10) U_2	$|B_{00}\rangle_{mn}$		
(11) U_3	$|B_{01}\rangle_{mn}$		
(00) U_0	$|B_{01}\rangle_{13}$	$|B_{01}\rangle_{25}$	$|1\rangle$
(01) U_1	$|B_{00}\rangle_{13}$		
(10) U_2	$|B_{11}\rangle_{13}$		
(11) U_3	$|B_{10}\rangle_{13}$		
(00) U_0	$|B_{11}\rangle_{13}$	$|B_{11}\rangle_{25}$	
(01) U_1	$|B_{10}\rangle_{13}$		
(10) U_2	$|B_{01}\rangle_{13}$		
(11) U_3	$|B_{00}\rangle_{13}$		
(00) U_0	$|B_{00}\rangle_{13}$	$|B_{00}\rangle_{25}$	$|0\rangle$
(01) U_1	$|B_{01}\rangle_{13}$		
(10) U_2	$|B_{10}\rangle_{13}$		
(11) U_3	$|B_{11}\rangle_{13}$		
(00) U_0	$|B_{10}\rangle_{13}$	$|B_{10}\rangle_{25}$	
(01) U_1	$|B_{11}\rangle_{13}$		
(10) U_2	$|B_{00}\rangle_{13}$		
(11) U_3	$|B_{01}\rangle_{13}$		

步骤 5 信息解码阶段

信息接收者 Bob 接收到发送者 Alice 发送的粒子序列 $S''_{\rm A}$ 后, 首先根据经典信道的信息剔除诱骗光子, 然后进行测量解码校验. 根据 Cindy 公布的测量结果, 将粒子序列 $S''_{\rm A}$ 以及 $S'_{\rm B}$ 中的粒子配对做 Bell 基测量. 具体测量规则如下: 对于采用 X 基测量的, 将 $S'_{\rm B}$ 中的粒子 1 和 $S''_{\rm A}$ 中同组 cluster 态的粒子 2 配对, 而粒子 5 和对应的粒子 3 配对; 对于采用 Z 基测量的, 将 $S'_{\rm B}$ 中的粒子 1 和 $S''_{\rm A}$ 中同组 cluster 态的粒子 3 配对, 而粒子 5 和对应粒子 2 配对. 在该例中, Bob 先对 $S''_{\rm A}$ 和 $S'_{\rm B}$ 中第三组的粒子 1 和粒子 3, 粒子 2 和粒子 5 做 Bell 基测量, 按照表 2 所示进行解码, 如果解码结果为 11, 则表示信道安全有效. 一般情况下, Bob 可以统计解码错误的误码率, 当错误率低于某个特定的阈值, 可以认为协议安全, 通信结果有效, 否则应当放弃此次通信的结果. 假如信道安全, Bob 按照前述规则将粒子配对做 Bell 基测量, 将得到的测量结果按照表 2 所示进行解码, 可以精确得到 Alice 所传送的信息为 "10-11-00-(11)-01-10", 其中第七、八位为校检信息 11.

整个方案通信过程如图 1 中所示, 其中 [ ] 代表 Z 基测量, { } 表示 X 基测量, 两个例子间的连线表示 Bell 基测量, 幺正操作编码后的粒子用加了底色的粒子表示.

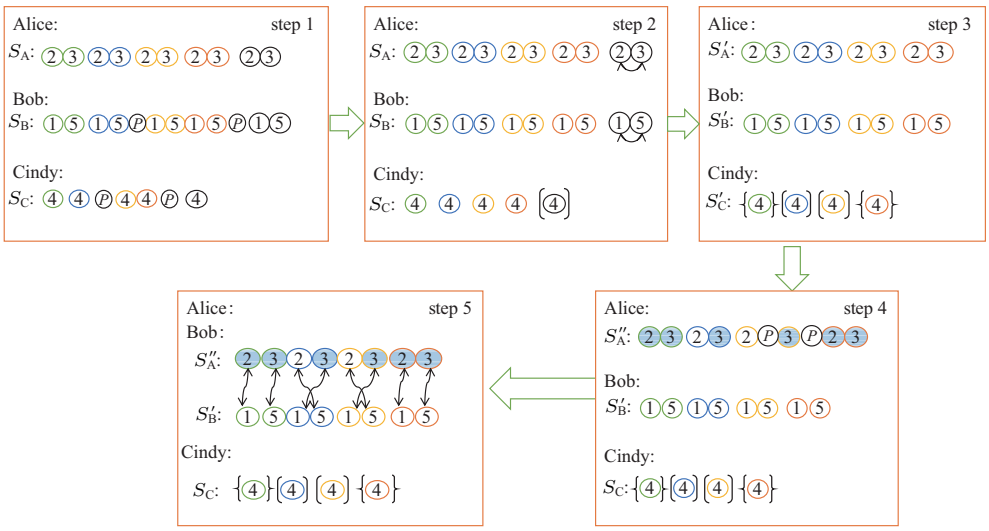

图 1 方案通信过程

Fig. 1. The process of protocol.

3 分析与讨论

3.1 五粒子 cluster 态三体纠缠结构分析

本方案是基于五粒子 cluster 态三体纠缠结构性质进行设计. 所谓的纠缠结构, 也就是一个既定量子态的量子比特的分布. 一旦确定了量子比特的分布, 那么纠缠结构也可以确定. 考虑进行可控通信的三个参与者, Alice 拥有两个粒子, Bob 拥有两个粒子, Cindy 拥有一个粒子的情形. 那么也就是只考虑三体纠缠结构中的 $S[(x,y);(z,v);w]$ 类, 其中 x,y,z,v 和 w 属于量子比特集 $\{1,2,3,4,5\}$, 且互不相等. 在此类纠缠结构中, 共包含 30 中纠缠结构. 按照量子比特的分布, 研究五粒子 cluster 态按照割 xy-zv-w 的 Schmidt 分解形式, 发现一部分纠缠结构适用于设计三方参与下的 QSDC. 具体情况如表 3 所列.

可以看出, 在表 3 中所显示的 6 种纠缠结构的分布下, 相应的五粒子 cluster 态 Schmidt 分解形式表示为两对 Bell 态以及单粒子态的不同纠缠形式. 由形式的相似性可以分为 A, B 两类. 本文所设计的通信容量可控的 CQSDC 方案, 便是结合了 A, B 两类纠缠结构的分布特点. 方案中在制备好 n 组 cluster 态后, 充分利用了五粒子 cluster 态不同粒子分布下的纠缠结构特性, 摒弃诱骗光子后, 随机挑选 i 组粒子进行 Bell 基测量即可完成第一次安全性检测. 这是本方案第一个特点. 控制方 Cindy 通过实际通信需求, 通过选用不同的测量基 Z 基和 X

基来控制通信容量. 假若选用 Z 基测量, 则传送一组 cluster 态中两个粒子可以达到传送 2 个经典 bit 的信息. 假若选用 X 基测量, 则传送一组 cluster 态中两个粒子可以达到传送 4 个经典 bit 的信息. 同时, 信息的发送者 Alice 和 Bob 需要和控制方进行配合, 要得到 Cindy 的测量信息后才能做不同的幺正操作编码以及测量解码. 而测量结果虽经过经典信道公布, 但本身却不包含任何要传送的信息. 因而本方案是一个通信容量可控的 CQSDC 方案, 这是本方案的第二个特点. 实际上, 在该方案的基础上, 如果控制方 Cindy 只采用 X 基测量, 那么该方案将可以最大容量完成只传送两个粒子便传送 4 个经典 bit 的信息. 而且, 若 Alice 将要传送的信息利用幺正操作编码的方式编码到粒子 2 上, Bob 将要传送的信息编码到粒子 5 上, 并将编码后的粒子传送给对方. 对方收到粒子后, 与各自剩下的粒子做 Bell 基测量, 便可以得到对方发送的 2 bit 的经典信息, 这样便实现了可控双向量子安全直接通信.

表 3 五粒子 cluster 态按照割 xy-zv-w 的 Schmidt 分解

Table 3. The Schmidt decomposition of five-particle cluster state according to cut xy-zv-w.

分类	纠缠结构	对应的 Schmidt 分解形式
A	S[(1, 2); (3, 5); 4] S[(3, 5); (1, 2); 4]	$\|\Phi_{\rm cluster}\rangle = \frac{\sqrt{2}}{2}(\|B_{00}\rangle_{12}\|B_{00}\rangle_{35}\|+\rangle_4 + \|B_{10}\rangle_{12}\|B_{10}\rangle_{35}\|-\rangle_4)$
B	S[(1, 3); (2, 5); 4] S[(2, 5); (1, 3); 4]	$\|\Phi_{\rm cluster}\rangle = \frac{1}{2}(\|B_{00}\rangle_{13}\|B_{00}\rangle_{25}\|0\rangle_4 + \|B_{01}\rangle_{13}\|B_{01}\rangle_{25}\|1\rangle_4 + \|B_{11}\rangle_{13}\|B_{11}\rangle_{25}\|1\rangle_4 + \|B_{10}\rangle_{13}\|B_{10}\rangle_{25}\|0\rangle_4)$
B	S[(1, 5); (2, 3); 4] S[(2, 3); (1, 5); 4]	$\|\Phi_{\rm cluster}\rangle = \frac{1}{2}(\|B_{00}\rangle_{15}\|B_{00}\rangle_{23}\|0\rangle_4 + \|B_{01}\rangle_{15}\|B_{01}\rangle_{23}\|1\rangle_4 + \|B_{11}\rangle_{15}\|B_{11}\rangle_{23}\|1\rangle_4 + \|B_{10}\rangle_{15}\|B_{10}\rangle_{23}\|0\rangle_4)$

3.2 安全性分析

本方案采用基于两步 QSDC 方案的分步传输量子数据块的方式来保证信息的安全, 信道是否被窃听由两次安全性检测来判断 [35−38]. 两次安全性检测采用诱骗光子和 Bell 基测量、单粒子基测量、校验信息相结合的方式, 可以有效防止内部窃听者 Cindy* 和外部窃听者 Eve 的窃听行为.

内部窃听者 Cindy* 和外部窃听者 Eve 常见的窃听方法有截获-重发、测量-重发以及纠缠-测量攻击的方法. 窃听者要想正确获得通信的信息, 必须完整获得两次传输的粒子序列的状态. 在两次安全检测中, 由于传输的粒子序列中随机插入了诱骗光子. 内部窃听者 Cindy* 和外部窃听者 Eve 如果采用截获-重发、测量-重发方式, 由于在粒子序列传输的过程中无法知晓诱骗光子的具体信息, 因而得不到有用的信息, 而且肯定会在通信三方的 Bell 基测量和单粒子基测量的校对检验中被发现, 因而截获-重发、测量-重发对本方案无效.

纠缠-测量攻击也称为辅助粒子攻击方法, 通过截获粒子, 和自身提前准备好的粒子进行纠缠, 也就是对两个粒子进行幺正操作, 常见的方法是对两个粒子进行 CNOT 操作. 根据海森伯测不准定理以及不可克隆定理, Cindy* 或者 Eve 不可能在不引起任何错误的情况下来获取有用的信息. 也就是说, 所执行的幺正操作使得通过辅助粒子和截获粒子产生一定的纠缠从而获得截获粒子的信息, 必定也会对粒子原先的纠缠性质产生一定的影响. 那么肯定也会在两次安全校验检测中导致错误率过高而被发现.

实际上, 在第一次安全检测成功的情况下, 外部窃听者 Eve 就已不可能再窃听到信息. 因为 Eve 已经无法同时得到两列粒子序列的信息, 即使后面获得其他信息她也无法对纠缠系统做 Bell 基测量, 机密信息也就无法获得.

而第二次安全性检测主要是防范半诚实的控制者 Cindy 利用其合法得到的信息来窃听 Alice 发送的机密信息而成为内部窃听者 Cindy*. Cindy* 根据自己的合法信息, 可以得到 Alice 和 Bob 用于通信的通道的全部信息或者部分信息, 譬如, 当用 X 基测量时, Cindy* 可以轻易根据自己的测量结果得到通道的全部信息, 制备出相应的 Bell 态, 从而通过截获 Alice 的粒子与制备出的 Bell 态做联合 Bell 基测量来获得 Alice 发送的信息. 而通过插入诱骗光子以及校验信息的方法, 同样可以及时监测到 Cindy* 的窃听行为以及有效地防止 Cindy* 窃听

到有用的信息.

在控制方 Cindy 忠诚的前提下, 那么第二次安全性检测更主要的作用便是判断在实际有噪声的情况下, $S''_{\rm A}$ 粒子序列是否被破坏, 是否失去了与 $S'_{\rm B}$ 粒子序列的纠缠性, 并依此来判断是否需要做数据纠错或者增加冗余编码处理来保证传输数据的有效性.

4 结 论

本文基于五粒子 cluster 态为量子信道, 设计出了三方参与下的信道容量可控的 CQSDC 方案. 方案在量子密集编码思想以及两步传输的基础上, 充分利用了五粒子 cluster 态在三方分布下的特殊纠缠结构性质. 通信三方利用 cluster 态自身的粒子分布情况, 结合诱骗光子以及校验信息, 对粒子分别做 Z 基单粒子测量和 Bell 基测量, 便可完成信道的安全性检测. 相比其他利用 cluster 态做信道的 CQSDC 方案, 该方案最显著的特点是通信控制方 Cindy 可以通过对粒子序列选用不同的基 (Z 基或者 X 基) 做测量来决定信道容量. 通信双方根据 Cindy 公布的测量结果按照一定规则进行编码和解码, 来实现信道可控的 CQSDC.

该方案是一个确定性和安全的方案, 理论上可在一定噪声环境中完成 CQSDC. 而且, 通过变化测量基的规则和用于编码的粒子, 可以将本方案推广成可控双向量子安全直接通信. 该方案中所采用的测量只涉及最常见的 Bell 基测量、单粒子基测量, 操作方便, 相应的幺正操作也是最简单的 Pauli 幺正操作. 这表明, 一旦实验技术条件成熟, 五粒子 cluster 态是实现信道容量可控的 CQSDC 的优异信道.

参考文献

[1] Long G L, Wang C, Li Y S, Deng F G 2011 *Sci. China: Phys. Mech. Astron.* **41** 332 (in Chinese) [龙桂鲁, 王川, 李岩松, 邓富国 2011 中国科学: 物理 力学 天文学 **41** 332]

[2] Long G L, Qin G Q 2014 *Phys. Eng.* **24** 3 (in Chinese) [龙桂鲁, 秦国卿 2014 物理与工程 **24** 3]

[3] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302

[4] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317

[5] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319

[6] Wang C, Deng F G, Li Y S, Liu X S, Long G L 2005 *Phys. Rev. A* **71** 044305

[7] Gu B, Zhang C Y, Cheng G S, Huang Y G 2011 *Sci. China: Phys. Mech. Astron.* **54** 942

[8] Wang C, Deng F G, Long G L 2005 *Opt. Commun.* **253** 15

[9] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J, Zhou H Y 2007 *Chin. Phys.* **16** 2149

[10] Shi J, Gong Y X, Xu P, Zhu S N, Zhan Y B 2011 *Commun. Theor. Phys.* **56** 831

[11] Wang T J, Li T, Du F F, Deng F G 2011 *Chin. Phys. Lett.* **28** 040305

[12] Briegel H J, Raussendorf R 2001 *Phys. Rev. Lett.* **86** 910

[13] Borhani M, Loss D 2005 *Phys. Rev. A* **71** 032308

[14] Browne D E, Rudolph T 2005 *Phys. Rev. Lett.* **95** 010501

[15] Zou X B, Mathis W 2005 *Phys. Rev. A* **72** 013809

[16] Yu L Z, Wu T 2013 *Acta Photon. Sin.* **42** 623 (in Chinese) [于立志, 吴韬 2013 光子学报 **42** 623]

[17] Li Y H, Liu J C, Nie Y Y 2010 *Acta Photon. Sin.* **39** 2073 (in Chinese) [李渊华, 刘俊昌, 聂义友 2010 光子学报 **39** 2073]

[18] Tian D Y, Tao Y J, Qin M 2008 *Sci. China G: Phys. Mech. Astron.* **38** 1128 (in Chinese) [田东平, 陶应娟, 秦猛 2008 中国科学 G 辑: 物理 力学 天文学 **38** 1128]

[19] Li Y P, Wang T Y, Yi B Y 2014 *Acta Photon. Sin.* **43** 0927002 (in Chinese) [李艳平, 王天银, 易宝银 2014 光子学报 **43** 0927002]

[20] Sun X M, Zha X W, Qi J X 2013 *Acta Phys. Sin.* **62** 230302 (in Chinese) [孙新梅, 查新末, 祁建霞 2013 物理学报 **62** 230302]

[21] Nie Y Y, Hong Z H, Huang Y B, Yi X J, Li S S 2009 *Int. J. Theor. Phys.* **48** 1485

[22] An Y 2013 *Int. J. Theor. Phys.* **52** 3870

[23] Li Y H, Liu J C, Nie Y Y 2011 *Acta Photon. Sin.* **40** 307 (in Chinese) [李渊华, 刘俊昌, 聂义友 2011 光子学报 **40** 307]

[24] Wu L W, Ye Z Q 2014 *Chin. J. Quantum Electron.* **31** 291 (in Chinese) [吴柳雯, 叶志清 2014 量子电子学报 **31** 291]

[25] Zheng X Y 2016 *Chin. J. Quantum Electron.* **33** 177 (in Chinese) [郑晓毅 2016 量子电子学报 **33** 177]

[26] Wang D, Zha X W 2011 *Chin. J. Quantum Electron.* **28** 687

[27] Sun Z W, Du R G, Long D Y 2012 *Int. J. Theor. Phys.* **51** 1946

[28] Li J, Song D J, Guo X J, Jing B 2012 *Chin. Phys. C* **36** 31

[29] Chang Y, Xu C X, Zhang S B, Yan L L 2014 *Chin. Sci. Bull.* **59** 2541

[30] Gao F, Guo F Z, Wen Q Y 2008 *Chin. Phys. Lett.* **25** 2766

[31] Cao W F, Yang Y G, Wen Q Y 2010 *Sci. China: Phys. Mech. Astron.* **53** 1271

[32] Chang Y, Zhang W B, Zhang S B, Wang H C, Yan L L, Han G H, Sheng Z W, Huang Y Y, Suo W, Xiong J X 2016 *Commun. Theor. Phys.* **66** 621

[33] Li C Y, Zhou H Y, Wang Y, Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[34] Li C Y, Li X H, Deng F G 2006 *Chin. Phys. Lett.* **23** 2896

[35] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Phys. Lett. A* **359** 359

[36] Lucamarini M, Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

[37] Li X H 2015 *Acta Phys. Sin.* **64** 160307 (in Chinese) [李熙涵 2015 物理学报 **64** 160307]

[38] Lu H, Fung C H F, Ma X, Cai Q Y 2011 *Phys. Rev. A* **84** 042344

Cluster state based controlled quantum secure direct communication protocol with controllable channel capacity*

Zheng Xiao-Yi† Long Yin-Xiang

(*Automation Engineering Department, Guangdong Technical College of Water Resource and Electric Engineering, Guangzhou 510635, China*)

(Received 10 May 2017; revised manuscript received 2 June 2017)

Abstract

Controllable quantum secure direct communication is an important branch of quantum communication. In this paper, we propose a controlled quantum secure direct communication protocol with channel capacity controllable based on a five-particle cluster state. To start with, the sender Alice prepares the five-particle cluster state sequence and inserts decoy photon randomly, and then sends two parts of the particle sequence to the receiver Bob and the controller Cindy, and meanwhile keeps one part of the particle sequence himself. After Bob and Cindy receive the particle sequence, Alice performs a Z-based single-particle measurement and publishes the measurement results and the position information of the decoy photon through the classical channel. According to the information published by Alice, Bob and Cindy remove the decoy photon and perform a Bell-state measurement to their own part particle sequence. Three sides of communication complete the first safety examination of the channel by checking the bit error rate of the measurement results. After that, the controller Cindy determines the channel capacity by selecting the measurement base (Z basis or X basis) to measure its own particle sequence, and then announces the measured results with classical channel. The sender Alice inserts decoy photon and codes the information by doing a unitary transformation to its own particle sequence and then sends the receiver Bob and tells him the position information of the decoy photon with classical channel. Combining the information published by Cindy with the information transmitted by Alice, Bob can complete the second safety examination of the channel and decode the information Alice has sent by removing decoy photon and performing a Bell-state measurement of his own two groups of particle with appropriate rules. Through an analysis of the entangled structural properties of the five-particle cluster state, it has been confirmed that this protocol is designed to make full use of the entanglement properties of the five-particle cluster in different entangled structures. Therefore the protocol can obviously be generalized into the two-way controlled quantum secure direct communication by simply changing the rules of the measurement and the particles used for unitary coding. Through analyzing the security of this protocol, it reveals that this protocol can effectively both prevent eavesdroppers from eavesdropping useful information and monitor this kind of act, and therefore the controlled quantum secure direct communication can theoretically be established in a certain noise environment.

Keywords: Bell-state measurement, five-particle cluster state, unitary transformation, controlled quantum secure direct communication

PACS: 03.67.Hk, 03.67.Ac, 03.65.Ud **DOI:** 10.7498/aps.66.180303

* Project supported by the Natural Science Foundation of Guangdong Province, China (Grant No. 2016a030313736).

† Corresponding author. E-mail: kyle87@126.com