文章编号:1000-5862(2013)03-0253-04

基于 4 粒子纠缠态的量子安全直接通信

徐　越[1],李渊华[1,2],桑明煌[1],聂义友[1,2*]
(1. 江西师范大学物理与通信电子学院,江西 南昌　330022;2 江西省光电子与通信重点实验室,江西 南昌　330022)

摘要:提出了一个利用 4 粒子纠缠态实现量子安全直接通信的方案. 在该方案中,由于携带信息的粒子不需要在公共信道上传输,使得这一方案是决定性的和安全的.

关键词:量子信息;安全直接通信;Bell 态
中图分类号:O 431.2　　**文献标志码**:A

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 1 个无条件安全的量子密钥分发(QKD)方案(即 BB84 协议)被提出以来,QKD 受到了人们的广泛关注,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(QSDC)的方案,并吸引了众多研究者的关注. 在文献[4]中,K. Bostrom 和 T. Felbinger 利用 EPR 对作为量子信道,提出了一个 QSDC 的乒乓协议,然而 Zhang Zhanjun 等[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[6-10],这些量子信道包括 EPR 态[6]、GHZ 态[7-8]和团簇态[9-12]等.

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. 本文利用一个 4 粒子纠缠态作为量子信道,提出了一种量子安全直接通信的方案. 在该方案中,通信双方在控制者的帮助下只需传送 1 次粒子,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,就能实现双方的直接通信. 最后,对该方案的安全性进行了分析.

1　基于 4 粒子纠缠态的量子安全直接通信方案

为了实现直接通信,选择如下 4 粒子纠缠态为量子信道

$$|\psi\rangle_{1234}=\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{1234},\quad(1)$$

这个量子态又可以表示为

$$|\psi\rangle_{1234}=\frac{1}{2}(|\phi^+\rangle_{13}|\phi^-\rangle_{24}+|\phi^-\rangle_{13}\cdot|\phi^+\rangle_{24}+|\varphi^+\rangle_{13}|\varphi^+\rangle_{24}+|\varphi^-\rangle_{13}|\varphi^-\rangle_{24}),\quad(2)$$

其中 $|\phi^\pm\rangle=(|00\rangle\pm|11\rangle)/\sqrt{2}$,$|\varphi^\pm\rangle=(|01\rangle\pm|10\rangle)/\sqrt{2}$,为 Bell 态.

下面详细描述该通信方案.

(ⅰ) 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:

$$|\phi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}\longrightarrow 00,$$
$$|\phi^-\rangle=(|00\rangle-|11\rangle)/\sqrt{2}\longrightarrow 11,$$
$$|\varphi^+\rangle=(|01\rangle+|10\rangle)/\sqrt{2}\longrightarrow 01,$$
$$|\varphi^-\rangle=(|01\rangle-|10\rangle)/\sqrt{2}\longrightarrow 10.$$

(ⅱ) 信息发送者 Alice 制备一有序序列纠缠态 $|\psi^i\rangle_{1234}$和足够多的单粒子态. 纠缠态用来建立通信信道,而单粒子态用于产生干扰. 接着,Alice 把有序序列纠缠态 $|\psi^i\rangle_{1234}$ 中的粒子分成两组有序粒子对序列,每个纠缠态中的粒子 1 和 3 为一组有序粒子对序列,用 P^i_{13} 表示;粒子 2 和 4 为另一组,用 P^i_{24} 表示. 然后,Alice 把 P^i_{13} 序列保留在自己手中,而把 P^i_{24} 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^i_{24} 序列粒子对时,把干扰的单粒子

收稿日期:2013-03-13
基金项目:国家自然科学基金(61265001),江西省自然科学基金(20122BAB202005)和江西省教育厅科研课题资助项目.
通信作者:聂义友(1963-),男,江西丰城人,教授,主要从事量子信息方面的研究.

按自己知道的方式随意夹杂在由粒子 2 和 4 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 所示.

②④②④②④②④…②④⟶②⊙④②④⊙②④⊙②④②⊙④②…④⊙②④

图 1 夹杂粒子序列示意图

(ⅲ) 接收者 Bob 在接到 P_{24}^{i} 粒子对序列后,通过经典信道告诉发送者 Alice 自己已经收到了粒子对序列. 接着,Alice 告诉 Bob 干扰粒子所在的位置,并且 Bob 把干扰粒子从收到的粒子序列中取出并抛弃.

(ⅳ) 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. 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,检验两人的测量结果是否相关联,如果两人的测量结果是按(2)式中的形式相配对,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.

(ⅴ) 在确定信道是安全以后,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 $|\varphi^{\pm}\rangle_{ab}^{i}$,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.

(ⅵ) 最后,Bob 对自己手中的粒子 2 和 4 进行 Bell 基测量,并把自己测得的结果和 Alice 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,举例加以说明: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 和处于纠缠态的粒子 1、3 按(a,1)和(b,3)分别进行 Bell 基测量,并把测量结果告诉 Bob;最后,Bob 对自己手中的粒子 2 和 4 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:

$$|\phi^{+}\rangle_{ab}\otimes|\psi\rangle_{1234}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{ab}\otimes$$

$$\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{1234}=$$

$$\frac{1}{2}|\phi^{+}\rangle_{ab}(|\phi^{+}\rangle_{13}|\phi^{-}\rangle_{24}+|\phi^{-}\rangle_{13}|\phi^{+}\rangle_{24}+|\varphi^{+}\rangle_{13}\cdot$$

$$|\varphi^{+}\rangle_{24}+|\varphi^{-}\rangle_{13}|\varphi^{-}\rangle_{24})=\frac{1}{4}(|\phi^{+}\rangle_{a1}|\phi^{+}\rangle_{b3}+$$

$$|\phi^{-}\rangle_{a1}|\phi^{-}\rangle_{b3}+|\varphi^{+}\rangle_{a1}|\varphi^{+}\rangle_{b3}+|\varphi^{-}\rangle_{a1}|\varphi^{-}\rangle_{b3})\cdot$$

$$|\phi^{-}\rangle_{24}+\frac{1}{4}(|\phi^{+}\rangle_{a1}|\phi^{-}\rangle_{b3}+|\phi^{-}\rangle_{a1}|\phi^{+}\rangle_{b3}-$$

$$|\varphi^{+}\rangle_{a1}|\varphi^{-}\rangle_{b3}-|\varphi^{-}\rangle_{a1}|\varphi^{+}\rangle_{b3})|\phi^{+}\rangle_{24}+$$

$$\frac{1}{4}(|\phi^{+}\rangle_{a1}|\varphi^{+}\rangle_{b3}+|\phi^{-}\rangle_{a1}|\varphi^{-}\rangle_{b3}+|\varphi^{+}\rangle_{a1}\cdot$$

$$|\phi^{+}\rangle_{b3}+|\varphi^{-}\rangle_{a1}|\phi^{-}\rangle_{b3})|\varphi^{+}\rangle_{24}+\frac{1}{4}(|\phi^{+}\rangle_{a1}\cdot$$

$$|\varphi^{-}\rangle_{b3}+|\phi^{-}\rangle_{a1}|\varphi^{+}\rangle_{b3}-|\varphi^{+}\rangle_{a1}|\phi^{-}\rangle_{b3}-|\varphi^{-}\rangle_{a1}\cdot$$

$$|\phi^{+}\rangle_{b3})|\varphi^{-}\rangle_{24}.$$

若 Alice 要发送的经典信息是 01、10 和 11,则她分别制备 $|\varphi^{+}\rangle_{ab}$、$|\varphi^{-}\rangle_{ab}$ 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. 最后,Bob 对粒子 2、4 进行 Bell 基测量,并分析两人的测量结果进行解码. Alice 和 Bob 的测量结果和相应的解码表如表 1 所示.

从上面的分析可知,该通信方案有一个优点,即携带秘密信息的粒子不需要在公共信道上传输,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_{24}^{i} 有序序列粒子对给 Bob 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,仅对建立信道的安全性进行分析.

(ⅰ) 假设窃听者 Eve 对传送 P_{24}^{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_{24}^{i} 有序序列粒子对后,制备数量相等的处于纠缠态的粒子对发送给 Bob. 由于 Alice 在发送 P_{24}^{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,

表 1　Alice 和 Bob 的测量结果以及解码信息表

Alice 的测量结果	Bob 的测量结果	解码对应的信息	Alice 的测量结果	Bob 的测量结果	解码对应的信息
$\|\phi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$	$\|\phi^-\rangle_{24}$	00	$\|\phi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$	$\|\phi^-\rangle_{24}$	11
$\|\phi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$	$\|\phi^+\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$	$\|\phi^+\rangle_{24}$	
$\|\phi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$	$\|\varphi^+\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^+\rangle_{b3}$	$\|\varphi^+\rangle_{24}$	
$\|\phi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^+\rangle_{b3}$	$\|\varphi^-\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^-\rangle_{b3}$	$\|\varphi^-\rangle_{24}$	
$\|\phi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^-\rangle_{b3}$	$\|\phi^-\rangle_{24}$	01	$\|\phi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^+\rangle_{b3}$	$\|\phi^-\rangle_{24}$	10
$\|\phi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^+\rangle_{b3}$	$\|\phi^+\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\phi^-\rangle_{b3}$	$\|\phi^+\rangle_{24}$	
$\|\phi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$	$\|\varphi^+\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$	$\|\varphi^+\rangle_{24}$	
$\|\phi^+\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^-\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^+\rangle_{b3}$	$\|\varphi^-\rangle_{24}$		$\|\phi^+\rangle_{a1}\|\phi^+\rangle_{b3}$ $\|\phi^-\rangle_{a1}\|\phi^-\rangle_{b3}$ $\|\varphi^+\rangle_{a1}\|\varphi^+\rangle_{b3}$ $\|\varphi^-\rangle_{a1}\|\varphi^-\rangle_{b3}$	$\|\varphi^-\rangle_{24}$	

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. 这样就会破坏纠缠态原有的关联性,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.

(ii) 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 $|0\rangle_5$ 和 $|0\rangle_6$ 态的粒子 5 和 6 纠缠到处于纠缠态的粒子 2 和 4 上,执行 CNOT 操作时,分别把粒子 2 和 4 作为控制比特,把粒子 5 和 6 作为目标比特,则量子信道就处于 6 粒子纠缠态,且有

$$
\begin{aligned}
|\psi\rangle_{123456} &= \frac{1}{2}(|000000\rangle + |001101\rangle + |110010\rangle - \\
&\quad |111111\rangle)_{123456} = \frac{1}{2\sqrt{2}}\{|\phi^+\rangle_{13}(|0000\rangle - \\
&\quad |1111\rangle)_{2456} + |\phi^-\rangle_{13}(|0000\rangle + |1111\rangle)_{2456} + \\
&\quad |\varphi^+\rangle_{13}(|0101\rangle + |1010\rangle)_{2456} + |\varphi^-\rangle_{13}\cdot \\
&\quad (|0101\rangle - |1010\rangle)_{2456} = \frac{1}{2\sqrt{2}}\{|\phi^+\rangle_{13}(|\phi^+\rangle_{24}\cdot \\
&\quad |\phi^-\rangle_{56} + |\phi^-\rangle_{24}|\phi^+\rangle_{56}) + |\phi^-\rangle_{13}(|\phi^+\rangle_{24}\cdot \\
&\quad |\phi^+\rangle_{56} + |\phi^-\rangle_{24}|\phi^-\rangle_{56}) + |\varphi^+\rangle_{13}(|\varphi^+\rangle_{24}\cdot \\
&\quad |\varphi^+\rangle_{56} + |\varphi^-\rangle_{24}|\varphi^-\rangle_{56}) + |\varphi^-\rangle_{13}(|\varphi^+\rangle_{24}\cdot \\
&\quad |\varphi^-\rangle_{56} + |\varphi^-\rangle_{24}|\varphi^+\rangle_{56})\}, \qquad (3)
\end{aligned}
$$

从(3)式可见,现在 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 在随机选择一些相对应的粒子对进行 Bell 基测量后,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 结论

提出了一个基于 4 粒子纠缠态的量子安全直接通信方案. 在这个方案中,首先信息发送者 Alice 和信息接收者 Bob 共享由 Alice 制备的一有序序列纠缠态作为量子信道. 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,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,并通过分析两人的测量结果,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.

4 参考文献

[1] Deng Feguo, Long Guilu. Controlled order rearrangement encryption for quantum key distribution [J]. Phys Rev A, 2003, 68(4): 42315.

[2] Deng Feguo, Long Guilu. Bidirectional quantum key distribution protocol with practical faint laser pulses [J]. Phys Rev A, 2004, 70(1): 12311.

[3] Zhang Zhanjun, Man Zhongxiao, Shi Shouhua. An efficient multiparty quantum key distribution scheme [J]. Int J Quantum Inf, 2005, 3(3): 555-559.

[4] Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement [J]. Phys Rev Lett, 2002, 89(18): 187902.

[5] Zhang Zhanjun, Man Zhongxiao, Li Yong. Improving Wójcik's eavesdropping attack on the ping-pong protocol [J]. Phys Lett A, 2004, 333(1): 46-50.

[6] Yi Xiaojie, Nie Yiyou, Zhou Nanrun, et al. Quantum secure direct communication using entangled photon pairs and local measurement [J]. Commun Theor Phys, 2008, 50(1): 81-84.

[7] Jin Xingri, Ji Xin, Zhang Yingqiao, et al. Three-party quantum secure direct communication based on GHZ states [J]. Phys Lett A, 2006, 354(1): 67-70.

[8] Wang Jian, Zhang Quan, Tang Chaojing. Multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state [J]. Opt Commun, 2006, 266(2): 732-737.

[9] Gao Fei, Guo Fenzhuo, Wen Qiaoyan, et al. Forcible-measurement attack on quantum secure direct communication protocol with cluster state [J]. Chin Phys Lett, 2008, 25(8): 2766-2769.

[10] Cao Weifeng, Yang Yuguang, Wen Qiaoyan. Quantum secure direct communication with cluster states [J]. China Phys Mech Astron, 2010, 53(7): 1271-1275.

[11] 李渊华,金翠平,王永胜,等. 基于 6 粒子团簇态实现 2 粒子任意态的量子信息分离 [J]. 江西师范大学学报: 自然科学版, 2010, 34(5): 502-505.

[12] 刘坤,李渊华,梁章坦,等. 基于 6 粒子团簇态的可控量子隐形传态 [J]. 江西师范大学学报: 自然科学版, 2010, 34(6): 612-614.

Quantum Secure Direct Communication via Four-Partile Entangled States

XU Yue[1], LI Yuan-hua[1,2], SANG Ming-huang[1], NIE Yi-you[1,2*]

(1. College of Physics & Communication Electronics, Jiangxi Normal University, Nanchang Jiangxi 330022, China;
2. Key Laboratory of Optoelectronic & Telecommunication of Jiangxi province, Nanchang Jiangxi 330022, China)

Abstract: A novel quantum secure direct communication scheme by using four-partile entangled states is proposed. In the scheme, the information-carrying qubits do not need to be transmitted over the public channel. Therefore, this scheme is determinate and secure.

Key words: quantum information; quantum secure direct communication; Bell-state

(责任编辑: 冉小晓)