基于 GHZ 态的三方量子确定性密钥分配协议*

周南润† 宋汉冲 龚黎华 刘晔

(南昌大学电子信息工程系, 南昌 330031)

(2012 年 4 月 10 日收到; 2012 年 6 月 1 日收到修改稿)

基于连续变量 GHZ 态的纠缠特性, 提出一种三方量子确定性密钥分配协议, 其中密钥由 GHZ 态的振幅产生, 而相位可以用来验证信道的安全性. 现有的量子确定性密钥分配协议一次只能向一个接收方传送密钥, 现实生活中经常要向多个接收方发送确定性密钥. 信息论分析结果表明, 当信道传输效率大于 0.5 时, 该协议可以同时向两个接收方安全传送确定性密钥, 制备多重纠缠态后, 该协议还能够扩展成多方量子确定性密钥分配协议, 这极大提高了密钥的整体传送效率, 而且连续变量量子 GHZ 态信道容量较高, 因此该协议具有重要的现实意义.

关键词: 连续变量 GHZ 态, 量子确定性密钥分配, 密钥管理, 量子通信

PACS: 42.50.Ar, 03.67.−a, 42.79.Sz, 95.75.Kk

1 引 言

最初的量子密钥分配 (QKD) 方案多是基于单光子的离散变量量子密钥分配 (discrete-variable quantum key distribution, DVQKD), 它将光束的偏振方向作为编码依据来实现密钥传输, 但是单光子源难以制备, 信道容量普遍偏低, 这导致 DVQKD 难以满足实际通信需求. 因此, 连续变量量子密钥分配 (continuous-variable quantum key distribution, CVQKD) 引起了人们的广泛关注, 它利用压缩态、相干态等易于产生和操控的连续量子信号作为量子信息的载体, 能获得较高的信道容量, 有利于解决即时通信的难题. 1999 年, Ralph 首次提出将多光子的连续量子信号作为信息载体来进行密钥分发 [1], 随后证明了方案的安全性 [2]. 2001 年, Cerf 等 [3] 采用高斯变量来调制单模压缩态的两个正交分量, 实现了密钥的安全分发, 其安全性由量子测不准原理保证, 窃听者想要获取其中一个正交分量上的信息, 必然会引起另一个正交分量上噪声的增加. 2002 年, Grosshans 和 Grangier[4] 提出了一种只利用相干态即可实现密钥分发的方案, 它不需要依赖于亚散粒噪声的压缩特性, 该方案因采用正向协调, 信道传输效率高于 50% (即信道损耗小于 3 dB) 才可以进行安全的密钥分发. 同年, Silberhorn 等 [5] 采用后向选择协调方案, 打破了正向协调 3 dB 的限制, 使 CVQKD 更接近于实用化. 2003 年, Grosshans 等 [6] 为克服 3 dB 的限制提出利用逆向协调的方法分发密钥, 不管信道传输效率为多少, 均可获得安全密钥. 2005 年, Takesue 等 [7] 借助差分移相键控技术提出一个基于泊松分布光子源的量子密钥分配协议, 该协议具有更强的抗干扰能力, 可以抵御光子数分离攻击, 在 30 km 光纤中密钥传输速率可以达到 1 Mbit/s. 2006 年, Namiki 和 Hirano[8] 将弱相干态的相位进行离散调制, 基于通信双方相位选择上的不同, 提出三态、四态、六态、八态的密钥传输协议, 达到了较高的传输效率, 其中在四态传输协议中效率为 100%. 2007 年, Ma 等 [9] 指出基于纠缠的 QKD 协议具有更好的抗衰落能力, 基于相干态的协议可以获得更高的密钥传输速率. 文献 [10] 分析了平衡零拍测量对连续变量量子密钥分配的影响, 给出了平衡零拍测量的探测噪声、电

* 国家自然科学基金 (批准号: 11174118)、江西省自然科学基金 (批准号: 20122BAB201031)、江西省教育厅科技项目 (批准号: GJJ11339, GJJ12137) 和江西省青年科学家 (井冈之星) 培养对象计划项目 (批准号: 20122BCB23002) 资助的课题.

† E-mail: znr21@163.com

子噪声和密钥量之间的定量表达式. 2008 年, Zhao 等 [11] 通过对信号加入任意的噪声, 分析了在集体攻击情况下连续变量离散调制协议中密钥传输速率的最小值, 为量子密钥传输提供了安全性判定依据. 文献 [12] 针对两类不同的集体噪声信道, 提出了两个有效的 QKD 方案. 2009 年, Fossier 等 [13] 用相干态和逆向协调技术设计出一个连续变量的量子密钥分配协议的原型, 在信道噪声 3 dB 时, 速率为 8 kbit/s. 文献 [14] 基于 EPR 纠缠特性提出了一种量子密钥分配协议, 该协议中信号不用进行调制, 只需直接测量就可以得到随机密钥, 在信道传输效率为 80%时, 密钥传输速率为 84 bit/s. 2010 年, Liu 等 [15] 运用极化编码和加入诱骗态思想, 实现了 200 km 光纤中性能良好的密钥传输. 文献 [16] 利用制备-测量的方法对强相干态进行了离散调制, 证明了信源的相位噪声对密钥分配的速率没有影响. 文献 [17] 将诱惑态方法和非正交编码协议相结合, 提出一种可以抵御光子数分离攻击的量子密钥分发方案. 2011 年文献 [18] 采用法拉第-迈克耳孙干涉仪检测的方法实现了基于强度调制的弱相干光脉冲的差分相位编码系统, 系统针对各个可能引起误码的关键环节提出并采用了相关物理方案来减小系统的误码, 实现了 50 km 传输距离时误码率为 3.9%的量子密钥分发. 2011 年, Allati 等 [19] 用三重相干态完成密钥传输, 其中密钥根据纠缠特性产生, 无须协商测量基. 文献 [20] 在实用光源条件下, 分析了有限脉冲数编码对密钥生成率和传输距离的影响, 并比较了主动诱惑态、被动诱惑态、无限长时间极限情况和不同量子效率条件下密钥生成率随传输距离的变化关系, 为实用的量子密钥分配实验提供了重要的理论参数. 2012 年, Yoshino 等 [21] 运用波分复用技术设计了一个高速的量子密钥分发系统, 该系统能够在 45 km 的光纤中稳定工作 12 h, 密钥传输速率达到 208 kbit/s. 文献 [22] 提出了一种改进的四态量子密钥传输协议, 该协议中密度矩阵可以由实验数据直接得到, 克服了以往协议中需要对信道进行线性估计才能获得密度矩阵的难题, 大大简化了密钥传输的过程.

以上的量子密钥分配方案中都只有一个接收方, 即发送方一次只能向一个接收方传送密钥, 我们称之为点对点的密钥传输协议. 在现实生活中人们常需要向多个接收方发送密钥. 为了实现该目标, 人们通常是对该密钥进行加密然后依次向每个接收方传送密文. 当接收方较多时, 这将导致密钥的整体传输效率不高, 实用性不强. 文献 [23] 提出一种基于纠缠交换的多方多级量子密钥分配协议, 该协议可以向两方甚至多方传送密钥, 极大地提高了密钥生成率以及信道容量. 文献 [24] 提出一个可以同时向两个通信方发送信息的密钥分配协议, 该协议实现简单, 不需要利用量子的纠缠特性, 大大提高了密钥分发的效率. 这些基于多方的量子密钥分发协议产生的密钥是随机性的, 不能同时向多个接收方分发事先确定的密钥. 文献 [25] 提出的点对点量子确定性密钥分配协议在一定程度上解决了确定性密钥分发的困难, 然而该协议中单光子难以制备, 信道容量较低, 而且每次通信都只能向一名接收方传送密钥, 难以保证其在短时间内向多个接收方分发确定性密钥, 这大大限制了量子确定性密钥分配的应用范围. 为此本文基于连续变量量子 GHZ 态设计一个全新的三方量子确定性密钥分配协议 (tripartite quantum deterministic key distribution, TQDKD), 协议要先验证密钥发送方和接收方的身份, 在验证通信双方身份后, 只要信道传输效率高于 0.5, 就可以同时向两个接收方发送确定性密钥, 而且在制备多重纠缠态后, 该协议还可以同时向多个接收方发送确定性密钥, 大大缩短了由单一发送方向多个接收方传送密钥的时间, 作为对密钥管理的有益补充, TQDKD 具有以往量子确定性密钥分配不可替代的重要地位和作用, 将进一步扩大确定性密钥分配的应用范围.

2 基础知识

在量子光学中, 压缩态光束可以表示为

$$a = x + \mathrm{i}p = \mathrm{e}^{r}x(0) + \mathrm{i}\,\mathrm{e}^{-r}p(0), \tag{1}$$

其中 $x(0)$, $p(0)$ 表示真空态的振幅和相位, $x(0)$, $p(0) \sim N(0,1)$, $[x(0),p(0)] = 2\mathrm{i}$, 若 $r > 0$, 表示光束相位被压缩, 若 $r < 0$, 表示光束振幅被压缩, 压缩态振幅和相位满足 Heisenberg 测不准关系: $\Delta x \cdot \Delta p \geqslant 1$. 连续变量 GHZ 态产生过程如下 [26]: 令压缩态光束 a_1, a_2 通过一个 1:2 分光镜产生 a_{A} 和 a_3', 再令 a_3' 和 a_3 通过一个 1:1 分光镜产生 a_{B1} 和 a_{B2}. $a_{\mathrm{A}}, a_{\mathrm{B1}}$ 和 a_{B2} 组成一对 GHZ 纠缠态, 表示为

$$x_{\mathrm{A}} = \frac{1}{\sqrt{3}}\mathrm{e}^{r_1}x_1(0) + \sqrt{\frac{2}{3}}\mathrm{e}^{-r_2}x_2(0), \tag{2a}$$

$$p_{\rm A} = \frac{1}{\sqrt{3}}\,{\rm e}^{-r_1}p_1(0) + \sqrt{\frac{2}{3}}\,{\rm e}^{r_2}p_2(0), \tag{2b}$$

$$x_{\rm B1} = \frac{1}{\sqrt{3}}\,{\rm e}^{r_1}x_1(0) - \frac{1}{\sqrt{6}}\,{\rm e}^{-r_2}x_2(0) + \frac{1}{\sqrt{2}}\,{\rm e}^{-r_3}x_3(0), \tag{2c}$$

$$p_{\rm B1} = \frac{1}{\sqrt{3}}\,{\rm e}^{-r_1}p_1(0) - \frac{1}{\sqrt{6}}\,{\rm e}^{r_2}p_2(0) + \frac{1}{\sqrt{2}}\,{\rm e}^{r_3}p_3(0), \tag{2d}$$

$$x_{\rm B2} = \frac{1}{\sqrt{3}}\,{\rm e}^{r_1}x_1(0) - \frac{1}{\sqrt{6}}\,{\rm e}^{-r_2}x_2(0) - \frac{1}{\sqrt{2}}\,{\rm e}^{-r_3}x_3(0), \tag{2e}$$

$$p_{\rm B2} = \frac{1}{\sqrt{3}}\,{\rm e}^{-r_1}p_1(0) - \frac{1}{\sqrt{6}}\,{\rm e}^{r_2}p_2(0) - \frac{1}{\sqrt{2}}\,{\rm e}^{r_3}p_3(0). \tag{2f}$$

令 $r_1 = r_2 = r_3$, 计算 $a_{\rm A}$, $a_{\rm B1}$ 和 $a_{\rm B2}$ 之间振幅和相位的关联方差为

$$\left\langle \left[\Delta(x_{\rm A} - x_{\rm B1})\right]^2 \right\rangle = \left\langle \left[\Delta(x_{\rm A} - x_{\rm B2})\right]^2 \right\rangle = 2\,{\rm e}^{-2r}, \tag{3a}$$

$$\left\langle \left[\Delta(p_{\rm A} + p_{\rm B1} + p_{\rm B2})\right]^2 \right\rangle = 3\,{\rm e}^{-2r}. \tag{3b}$$

当压缩参数 $r \to +\infty$ 时, 输出模 $a_{\rm A}$, $a_{\rm B1}$ 和 $a_{\rm B2}$ 之间具有很强的关联性:

$$\lim_{r\to+\infty}(x_{\rm A} - x_{\rm B1}) = \lim_{r\to+\infty}(x_{\rm A} - x_{\rm B2}) = 0, \tag{4a}$$

$$\lim_{r\to+\infty}(p_{\rm A} + p_{\rm B1} + p_{\rm B2}) = 0, \tag{4b}$$

此时输出模中任意两者之间的振幅正关联, 而三者之间的相位也存在纠缠特性. 当纠缠度较高时, Alice, $\rm Bob_1$ 和 $\rm Bob_2$ 分别测量 $a_{\rm A}$, $a_{\rm B1}$ 和 $a_{\rm B2}$ 的振幅分量, 即可使三者获得一个高度相关的随机序列 x. 这样 Alice, $\rm Bob_1$ 和 $\rm Bob_2$ 只需按照一定的编码规则进行协商, 就可获得密钥. 例如 Alice 要发送比特 101, 假定通信三方选择编码规规如图 1 所示 (也可划分为更多区间), 记比特 000 所在编码区间为 $(v_0, v_1]$, 比特 001 所在编码区间为 $(v_1, v_2], \cdots$, 比特 111 所在编码区间为 $(v_7, v_8]$, 若测得 $x \in (v_5, v_6]$, Alice 公布修正信息 0, $\rm Bob_1$ 和 $\rm Bob_2$ 根据 x 所在的区间得到密钥, 若测得 $x \in (v_k, v_{k+1}](k \neq 5)$, 则公布修正信息 $v = v_5 - v_k$, $\rm Bob_1$ 和 $\rm Bob_2$ 根据 v 对所得到的 x 进行修正, 得到 $v' = (x + v_5 - v_k) \in (v_5, v_6]$, 即可获得确定性密钥 101.

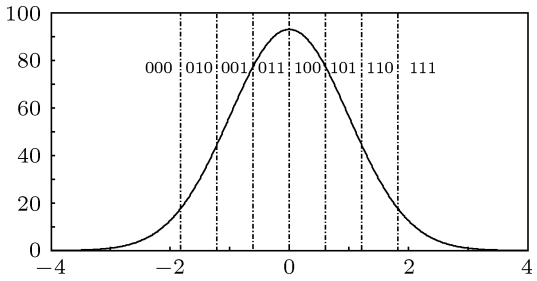

图 1 信道编码区间划分

3 三方量子确定性密钥分配协议

假设 Alice 要同时向 $\rm Bob_1$, $\rm Bob_2$ 传送确定性密钥, 则协议的步骤如下:

1) Alice 产生 GHZ 纠缠态光束 $a_{\rm A}$, $a_{\rm B1}$ 和 $a_{\rm B2}$, Alice 保留光束 $a_{\rm A}$, 并将 $a_{\rm B1}$, $a_{\rm B2}$ 分别发送给 $\rm Bob_1$, $\rm Bob_2$;

2) $\rm Bob_1$, $\rm Bob_2$ 声明收到光束 $a_{\rm C1}$, $a_{\rm C2}$ (若无窃听, 则 $a_{\rm C1} = a_{\rm B1}$, $a_{\rm C2} = a_{\rm B2}$), 并商定随机选取一些时间间隙 t_1, 选取相同的分量测量 $a_{\rm C1}$, $a_{\rm C2}$, 若 $\rm Bob_1$ 在 t_1 测量 $a_{\rm C1}$ 的振幅分量, 则 $\rm Bob_2$ 也在 t_1 测量 $a_{\rm C2}$ 的振幅分量, 反之亦然; 然后 $\rm Bob_1$, $\rm Bob_2$ 公布所选的时间间隙 t_1 和测量分量;

3) Alice 选取与 $\rm Bob_1$, $\rm Bob_2$ 相同的测量分量在 t_1 测量 $a_{\rm A}$, 并公布测量结果;

4) $\rm Bob_1$, $\rm Bob_2$ 合作将测量结果与 Alice 公布的结果进行比对, 若纠缠度不变或未超过错误门限, 则 $\rm Bob_1$, $\rm Bob_2$ 相信 Alice 和通信信道, 继续步骤 4), 否则放弃此次通信;

5) Alice 随机选取一些时间间隙 t_2 对 $a_{\rm A}$ 进行振幅或相位测量, 并公布所选的 t_2 和测量分量;

6) $\rm Bob_1$, $\rm Bob_2$ 根据 Alice 公布的 t_2 和测量分量分别测量 $a_{\rm C1}, a_{\rm C2}$, 并公布测量结果;

7) Alice 将自己测量的结果和 $\rm Bob_1$, $\rm Bob_2$ 公布的结果进行比对, 若纠缠度不变或未超过错误门限, 则 Alice 相信 $\rm Bob_1$, $\rm Bob_2$ 和通信信道, 继续步骤 8), 否则放弃此次通信;

8) $\rm Bob_1$, $\rm Bob_2$ 在剩下的时隙分别测量 $a_{\rm C1}, a_{\rm C2}$ 的振幅分量, 记录测量结果 y, z;

9) Alice 在剩下的时间间隙测量 $a_{\rm A}$ 的振幅分量, 记录下测量结果 x, 并根据所要发送的确定性密钥和编码规则公布校正信息 v;

10) $\rm Bob_1$, $\rm Bob_2$ 根据自己的测量结果及校正信息进行解码, 即可恢复出确定性密钥.

其中 1)—7) 的目的是进行身份认证和信道安全认证, 当通信方较多时, 进行身份认证可以避免窃听者伪装成合法通信方窃取密钥, 而且可以避免中间人攻击, 这在保证多方量子密钥分配的安全性方面显得尤为重要; 8)—10) 为确定性密钥的生成阶段, 由于信道认证过程中已经在一些时间间隙验证了量子 GHZ 态振幅的关联特性, 所以在确认信道安全后, 合法通信方即可从所收光束的振幅中获得安全的随机密钥, 此时只要将随机性密钥进行校正, 就可恢复出确定性密钥, 而窃听者仅根据校正信息则得不到任何有用信息. 三方量子确定性密钥分配协议如图 2 所示.

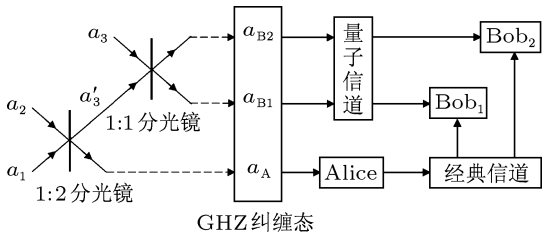

图 2 三方量子确定性密钥分配协议

当 Alice 制备多重纠缠态时, 该协议也可以同时向多个接收方发送密钥, 只需将步骤 1) 改为: Alice 产生压缩态光束 $a_1, a_2, a_3, \cdots, a_{n+1}$, 并将 a_1, a_2 通过 1:n 分光镜产生 $a_{\rm A}$ 和 a_3', 再令 a_3' 和 a_3 通过 1:$(n-1)$ 分光镜产生 $a_{\rm B1}$ 和 $a_4', \cdots$, 最后令 a_{n+1}' 和 a_{n+1} 通过 1:1 分光镜产生 $a_{\rm B}(n-1)$ 和 $a_{{\rm B}n}$, 即产生纠缠态光束 $a_{\rm A}$, $a_{\rm B1}$, $a_{\rm B2}, \cdots, a_{{\rm B}n}$. Alice 保留光束 $a_{\rm A}$, 并将 $a_{\rm B1}, a_{\rm B2}, \cdots, a_{{\rm B}n}$ 分别发送给 $\rm Bob_1$, $\rm Bob_2$, $\rm Bob_n$.

4 安全性分析

连续变量量子态的测量主要采用平衡零拍测量技术, 由于其 Hilbert 空间是无限维的, 人们在分析 CVQKD 的安全性时通常都是假定一种特定的攻击方式, 并分析在该攻击方式中 Eve 所能窃取的最大信息量. 本协议安全性基于量子 GHZ 态的纠缠特性以及量子测不准原理, 其中只有 Alice→$\rm Bob_1$, Alice→$\rm Bob_2$ 两条量子信道用来传输量子信号, 而量子密钥信息被调制在光束的振幅上, 窃听者 Eve 可采取的一种攻击方式是采用分光镜截取信号进行测量并企图获取密钥 (图 3). 假设 Eve 所用的分光镜透射系数为 $\varepsilon(0 \leqslant \varepsilon \leqslant 1)$, 则 Alice 发出的两条光束 $a_{\rm B1}$, $a_{\rm B2}$ 经过分光镜后变为

$$a'_{\rm C1} = \sqrt{\varepsilon} a_{\rm B1} + \sqrt{1-\varepsilon} a_{\rm N1}, \tag{5a}$$

$$a'_{\rm C2} = \sqrt{\varepsilon} a_{\rm B2} + \sqrt{1-\varepsilon} a_{\rm N2}. \tag{5b}$$

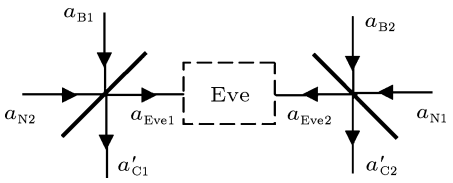

图 3 Eve 分光镜攻击

Eve 获得 $a_{\rm Eve1}$, $a_{\rm Eve2}$, 即

$$a_{\rm Eve1} = \sqrt{\varepsilon} a_{\rm N1} - \sqrt{1-\varepsilon} a_{\rm B1}, \tag{6a}$$

$$a_{\rm Eve2} = \sqrt{\varepsilon} a_{\rm N2} - \sqrt{1-\varepsilon} a_{\rm B2}. \tag{6b}$$

根据 Eve 选取分光镜透射系数的不同, 本文分三种情况来进行安全性分析.

1) $\varepsilon = 0$, 即 Eve 把信号全部拦截下来此时 Eve 的一种做法是将 $a_{\rm Eve1}$, $a_{\rm Eve2}$ 进行联合 Bell 基测量, 得到:

$$x_{\rm u} = \frac{1}{\sqrt{2}}(x_{\rm Eve1} - x_{\rm Eve2}) = \frac{1}{\sqrt{2}}(x_{\rm B2} - x_{\rm B1}), \tag{7a}$$

$$\begin{aligned} p_{\rm v} &= \frac{1}{\sqrt{2}}(p_{\rm Eve1} + p_{\rm Eve2}) \\ &= -\frac{1}{\sqrt{2}}(p_{\rm B1} + p_{\rm B2}). \end{aligned} \tag{7b}$$

虽然密钥信息调制在光束的振幅分量上, 但是 $a_{\rm B1}$, $a_{\rm B2}$ 的振幅具有关联特性, Eve 在振幅分量上所测结果 $x_{\rm u} \to 0$, 得不到任何有效信息, 而 $a_{\rm B1}$, $a_{\rm B2}$ 两者间的相位无关联特性, 经过测量后也得不到有效信息.

Eve 的另一种做法是分别测量 $a_{\rm B1}$, $a_{\rm B2}$. 根据密钥调制所采用的原理, 假设 Eve 分别测量 $a_{\rm B1}$ 的振幅和 $a_{\rm B2}$ 的相位, 由于 $a_{\rm B1}$, $a_{\rm B2}$ 的振幅具有关联特性, 测量后 Eve 可准确恢复出 $a_{\rm B2}$. 然而由于量子测不准原理, Eve 不可能准确恢复出 $a_{\rm B1}$ 的相位, 从而使 GHZ 态的相位纠缠度降低. 假设通信方进行信道认证时选取 m 个时间间隙测量相位, 则 Eve 被发现的概率为 $p = 1 - 0.5^m$, 当 m 较大时, Eve 被发现的概率接近于 1.

由此可知, $\varepsilon = 0$ 时 Eve 不能保证自己不被合法通信方发现, 所以此种窃听方式下本协议可以安全传送确定性密钥.

2) $\varepsilon = 1$, 即 Eve 不采取任何操作, 自然无法获得有效信息.

3) $0 < \varepsilon < 1$, 即 Eve 只截取信号的一部分, 而让另外一部分信号传送给接收方.

由于 GHZ 态的纠缠特性, Eve 进行联合 Bell 基测量得不到任何有效信息, 因此 Eve 只能对 $a_{\rm Eve1}$, $a_{\rm Eve2}$ 进行单独操作, 此时两条量子信道具有对称性, 本文选取 Alice→Bob$_1$ 的量子信道进行分析. 假设量子信道传输效率为 η, 则 Bob$_1$ 端应该收到的信号为

$$a_{\rm C1} = \sqrt{\eta} a_{\rm B1} + \sqrt{1-\eta} a_{\rm N1}, \tag{8}$$

为避免被通信方发现, Eve 需要对 $a_{\rm Eve1}$ 进行相应的放大处理, 并和 $a'_{\rm C1}$ 一起发送给 Bob$_1$, Bob$_1$ 收到的信号为

$$a = g a_{\rm Eve1} + a'_{\rm C1}, \tag{9}$$

其中 g 为增益补偿. 为了让 Bob$_1$ 收到的信号为 $\sqrt{\eta} a_{\rm B1}$, 需要满足:

$$-g\sqrt{1-\varepsilon} a_{\rm B1} + \sqrt{\varepsilon} a_{\rm B1} = \sqrt{\eta} a_{\rm B1}, \tag{10}$$

得到 $g = \dfrac{\sqrt{\varepsilon} - \sqrt{\eta}}{\sqrt{1-\varepsilon}}$, 则 Eve 发送给 Bob$_1$ 的噪声信号为

$$a_{\rm N} = \frac{1 - \sqrt{\eta\varepsilon}}{\sqrt{1-\varepsilon}} x_{\rm N1}, \tag{11}$$

若 $\varepsilon \neq \eta$, 则 $a_{\rm N} \neq \sqrt{1-\eta} x_{\rm N1}$, 这将导致 Bob$_1$ 端所收到信号的信噪比发生变化, 从而使通信方在信道认证阶段的数据误码率增大, 最终会发现 Eve; 若 $\varepsilon = \eta$, 则 $a_{\rm N} = \sqrt{1-\eta} x_{\rm N1}$, $g = 0$, 即不需要增益补偿, 此时 Eve 也不会被通信方发现.

由此可知, $0 < \varepsilon < 1$ 时, Eve 在没有被发现的情况下所能采取的最好的攻击方法是采用透射系数为 η 的分光镜进行拦截, 其中 η 的值与信道传输效率相等, 这样 Eve 端收到的信号为

$$a_{\rm Eve1} = \sqrt{\eta} a_{\rm N1} - \sqrt{1-\eta} a_{\rm B1}, \tag{12}$$

Bob$_1$ 端收到的信号为

$$a_{\rm C1} = \sqrt{\eta} a_{\rm B1} + \sqrt{1-\eta} a_{\rm N1}, \tag{13}$$

根据 (2c) 式, 得到 Bob$_1$ 和 Eve 的振幅分量为

$$x_{\rm C1} = \sqrt{\eta}\left(\frac{1}{\sqrt{3}} {\rm e}^{r} x_1(0) - \frac{1}{\sqrt{6}} {\rm e}^{-r} x_2(0) + \frac{1}{\sqrt{2}} {\rm e}^{-r} x_3(0)\right) + \sqrt{1-\eta} x_{\rm N1}, \tag{14a}$$

$$x_{\rm Eve1} = \sqrt{\eta} x_{\rm N1} - \sqrt{1-\eta}\left(\frac{1}{\sqrt{3}} {\rm e}^{r} x_1(0) - \frac{1}{\sqrt{6}} {\rm e}^{-r} x_2(0) + \frac{1}{\sqrt{2}} {\rm e}^{-r} x_3(0)\right), \tag{14b}$$

其中 $x_i(0)(i = 1,2,3)$ 为真空态, 服从高斯分布, 即 $x_i(0) \sim N(0,1)$, 记量子信道噪声 $x_{\rm N1} \sim N(0, V_{\rm N1})$. 当测量 $a_{\rm C1}$ 的振幅时, 只有 $\sqrt{\dfrac{\eta}{3}} {\rm e}^{r} x_1(0)$ 为信号, 其余均为噪声, 得到 Bob 端信噪比为

$$\frac{S_{\rm B}}{N_{\rm B}} = \frac{\eta {\rm e}^{2r}}{2\eta {\rm e}^{-2r} + 3(1-\eta) V_{\rm N1}}, \tag{15}$$

则 Alice 和 Bob 间的信息量为

$$I_{\rm AB} = \frac{1}{2} \log_2 \left(1 + \frac{S_{\rm B}}{N_{\rm B}}\right). \tag{16}$$

同理, Eve 端的信噪比为

$$\frac{S_{\rm Eve1}}{N_{\rm Eve1}} = \frac{(1-\eta) {\rm e}^{2r}}{2(1-\eta) {\rm e}^{-2r} + 3\eta V_{\rm N1}}, \tag{17}$$

Alice 和 Eve 间的信息量为

$$I_{\rm AE} = \frac{1}{2} \log_2 \left(1 + \frac{S_{\rm Eve1}}{N_{\rm Eve1}}\right). \tag{18}$$

本协议采用正向协调技术, 即 Bob$_1$ 和 Bob$_2$ 根据自己所获得的信息来推断 Alice 的密钥, 根据香农信息论可得 Alice→Bob$_1$ 的量子信道信息传输速率为

$$\begin{aligned}\Delta I =& I_{\rm AB} - I_{\rm AE} \\ =& \frac{1}{2} \log_2 \left(\frac{\eta({\rm e}^{2r} + 2{\rm e}^{-2r}) + 3(1-\eta) V_{\rm N1}}{2\eta {\rm e}^{-2r} + 3(1-\eta) V_{\rm N1}} \right. \\ & \left. \times \frac{2(1-\eta) {\rm e}^{-2r} + 3\eta V_{\rm N1}}{(1-\eta)({\rm e}^{2r} + 2{\rm e}^{-2r}) + 3\eta V_{\rm N1}}\right).\end{aligned} \tag{19}$$

本协议中量子信道具有对称性, Alice→Bob$_2$ 的量子信道也有相同的信息传输速率, 若接收方增加到多方, 每条量子信道也都具有相同的安全性. 在 $V_{\rm N1} = 1$ 时, Alice→Bob$_1$ 的信息传输速率如图 4 所示: 其中密钥信息传输速率与量子信道传输效率成正比, 随着信道传输效率的提高而增大, 当信道传输效率 $\eta < 0.5$ 时, Alice→Bob$_1$ 的信息传输速率 $\Delta I < 0$, 即 Eve 能获得的信息量大于 Bob 所能获得的信息量, 不能获得安全密钥; 当信道传输效率 $\eta > 0.5$ 时, $\Delta I > 0$, 能够安全传送密钥. 该协议依赖量子的纠缠特性, 在压缩参数 $r = 0$ 时, 由于连续变量量子 GHZ 态的关联方差较大, 使得信道传输速率趋近于 0, 几乎无法传送密钥, 随着压缩参

数 r 的增大, 量子 GHZ 态的纠缠度增加, 密钥传输速率也随之提高.

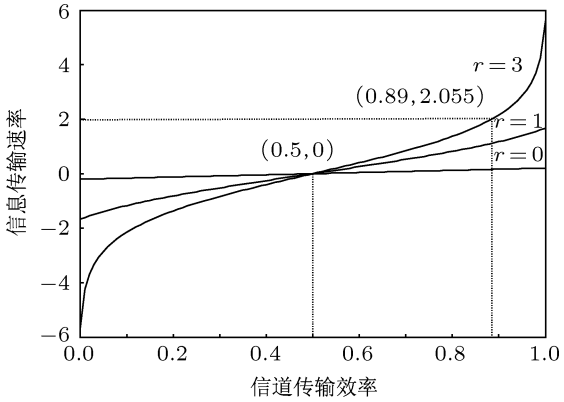

图 4 信息传输速率 ($V_{\mathrm{N1}}=1$)

三方量子确定性密钥分配协议在实际生活中具有重要意义, 例如一个发送方要向两个接收方每人传送 1000 bits 的确定性密钥, 若用基于点对点的离散变量量子确定性密钥传输协议来进行传送, 由于其每个量子比特最多只能传送 1 bit 的经典密钥, 完成密钥传输至少需要 2000 bits 的量子态. 本协议中, 发送方可以同时向两名接收方发送确定性密钥, 而且在 $r=3$, 信道传输效率为 0.89 时, 密钥传输速率达到 2.055 bit/s, 此时只需 487 bits 的量子态即可完成相同的任务, 这表明 TQDKD 能够大大减少密钥传输所需要制备的量子态, 缩短密钥传输所需要的时间, 并且提高密钥传输的效率.

5 结 论

现有的多方量子密钥分配协议都只能产生随机性密钥, 不能完成确定性密钥分发, 而点对点的量子确定性密钥分配协议一次只能向单个接收方传送密钥, 效率较低. 本文基于连续变量量子 GHZ 态, 提出一个三方量子确定性密钥分配协议, 其安全性由量子 GHZ 态的纠缠特性和量子测不准原理来保证. 当信道传输效率大于 0.5 时, 该协议可以同时向两个接收方传送确定性密钥, 当制备多重纠缠态后, 该协议还能够同时向多个接收方发送确定性密钥. 本文从信息论的角度对协议的安全性进行了详细的分析, 分析结果表明该协议中的密钥传输速率与量子信道的传输效率和压缩参数成正比, 而且连续变量的量子信道具有较高的信道容量, 在接收方较多时, 该协议能够极大地提高密钥的整体传输效率. 作为对密钥管理的有益补充, TQDKD 将进一步扩大确定性密钥分配的应用范围.

[1] Ralph T C 1999 *Phys. Rev.* A **61** 010303

[2] Ralph T C 2000 *Phys. Rev.* A **62** 062306

[3] Cerf N J, Levy M, Assche G V 2001 *Phys. Rev.* A **63** 052311

[4] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[5] Silberhorn C, Ralph T C, Lutkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[6] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238

[7] Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M M, Inoue K, Yamamoto Y 2005 *New J. Phys.* **7** 232

[8] Namiki R, Hirano T 2006 *Phys. Rev.* A **74** 032302

[9] Ma X F, Lo H K, Fung C F 2007 *Phys. Rev.* A **76** 012307

[10] Chen J J, Han Z F, Zhao Y B, Gui Y Z, Guo G C 2007 *Acta Phys. Sin.* **56** 9 (in Chinese) [陈进建, 韩正甫, 赵义博, 桂有珍, 郭光灿 2007 物理学报 **56** 9]

[11] Zhao Y B, Heid M, Rigas J, Lutkenhaus N 2009 *Phys. Rev.* A **79** 012307

[12] Li X H, Deng F G, Zhou H Y 2008 *Phys. Rev.* A **78** 022321

[13] Fossier S, Diamanti E, Debuisschert T, Villing A, Brouri R T, Grangier P 2009 *New J. Phys.* **11** 045023

[14] Su X L, Wang W Z, Wang Y, Jia X J, Xie C D, Peng K C 2009 *Europhys. Lett.* **87** 20005

[15] Liu Y, Chen T Y, Wang J, Cai W Q, Wan X, Chen L K, Wang J H, Liu S B, Yang L, Chen K, Chen Z B, Pan J W, Peng C Z, Liang H 2010 *Opt. Express.* **18** 8587

[16] Shen Y, Zou H X, Tian L, Chen P X, Yuan J M 2010 *Phys. Rev.* A **82** 022317

[17] Hu H P, Wang J D, Huang Y X, Liu S H, Lu W 2010 *Acta Phys. Sin.* **59** 292 (in Chinese) [胡华鹏, 王金东, 黄宇娴, 刘颂豪, 路巍 2010 物理学报 **59** 292]

[18] Wei Z J, Wan W, Wang J D, Liao C J, Liu S H 2011 *Acta Phys. Sin.* **60** 094216 (in Chinese) [魏正军, 万伟, 王金东, 廖常俊, 刘颂豪 2011 物理学报 **60** 094216]

[19] Allati A E, Baz M E, Hassouni Y 2011 *Quantum Inf. Process.* **10** 589

[20] Jiao R Z, Zhang C, Ma H Q 2011 *Acta Phys. Sin.* **60** 110303 (in Chinese) [焦荣珍, 张弼, 马海强 2011 物理学报 **60** 110303]

[21] Yoshino K, Fujiwara M, Tanaka A, Takahashi S, Nambu Y, Tomita A, Miki S, Yamashita T, Wang Z, Sasaki M, Tajima A 2012 *Opt. Lett.* **37** 223

[22] Yang J, Xu B J, Peng X, Guo H 2012 arXiv: 1202.0883v1 [quant-ph]

[23] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 5548 (in Chinese) [杨宇光, 温巧燕, 朱甫臣 2005 物理学报 **54** 5548]

[24] Matsumoto R 2007 *Phys. Rev.* A **76** 062316
[25] Zhou N R, Wang L J, Gong L H, Zuo X W, Liu Y 2011 *Opt. Commun.* **284** 4836
[26] Furusawa A, Takei N 2007 *Phys. Rep.* **443** 97

Tripartite quantum deterministic key distribution based on GHZ states*

Zhou Nan-Run† Song Han-Chong Gong Li-Hua Liu Ye

(*Department of Electronic Information Engineering, Nanchang University, Nanchang* 330031, *China*)

(Received 10 April 2012; revised manuscript received 1 June 2012)

Abstract

By exploiting the entanglement properties of continuous variable quantum GHZ state, we propose a tripartite quantum deterministic key distribution, in which the key is generated from its amplitude and the phase can be used to test and verify the channel security. The existing quantum deterministic key distribution can only hand over deterministic key to one receiver in one communication. However, we always have to transmit deterministic key to more than one receiver in real life. The analysis results of information theory show that when the channel transmission efficiency is greater than 0.5, the proposed protocol can securely hand over the pre-deterministic key to two receivers simultaneously, and it can also be extended to multiparty quantum deterministic key distribution when preparing multiple entangled state, this will greatly improve the overall efficiency of the key transmission, furthermore, the continuous variable quantum GHZ state could have a higher channel capacity, so the protocol has the important practical significance.

Keywords: continuous-variable, quantum deterministic key distribution, key management, quantum communication

PACS: 42.50.Ar, 03.67.−a, 42.79.Sz, 95.75.Kk

* Project supported by the National Natural Science Foundation of China (Grant No. 11174118), the Natural Science Foundation of Jiangxi Province, China (Grant No. 20122BAB201031), the Research Foundation of the Education Department of Jiangxi Province, China (Grant Nos. GJJ11339, GJJ12137), and the Foundation for Young Scientists of Jiangxi Province (Jinggang Star), China (Grant No. 20122BCB23002).

† E-mail: znr21@163.com