基于量子远程通信的连续变量量子确定性密钥分配协议*

宋汉冲 龚黎华 周南润†

(南昌大学电子信息工程系, 南昌 330031)

(2011 年 11 月 14 日收到; 2011 年 11 月 29 日收到修改稿)

基于量子远程通信的原理, 本文借助双模压缩真空态和相干态, 提出一种连续变量量子确定性密钥分配协议. 在利用零差探测法的情况下协议的传输效率达到了 100%. 从信息论的角度分析了协议的安全性, 结果表明该协议可以安全传送预先确定的密钥. 在密钥管理中, 量子确定性密钥分配协议具有量子随机性密钥分配协议不可替代的重要地位和作用. 与离散变量量子确定性密钥分配协议相比, 该协议分发密钥的速率和效率更高, 又协议中用到的连续变量量子态易于产生和操控、适于远距离传输, 因此该协议更具有实际意义.

关键词: 连续变量, 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

自 BB84 协议、EPR 协议、B92 协议提出以来, 量子密码引起了人们的高度重视, 其无条件安全性和潜在商机也引起了政府、军方、企业和国际媒体的关注和支持. 量子密钥分配 (quantum key distribution, QKD) 包括离散变量量子密钥分配 (discrete-variable quantum key distribution, DVQKD) 和连续变量量子密钥分配 (continuous - variable quantum key distribution, CVQKD), 其安全性由量子不可克隆定理和 Heisenberg 不确定性原理等量子物理属性保证. DVQKD 多以单光子、微弱激光脉冲为信息载体, 但是目前单光子源难以制备, 单量子探测效率较低, 容易受到干扰, 以单光子作为信息载体, 极大地限制了密钥传输速率, 导致实用性不强. CVQKD 主要以压缩态、相干态、双模纠缠态等连续量子信号来传送密钥, 这些量子信号可以通过线性光学元器件产生, 容易操作, 与 DVQKD 相比, CVQKD 具有较高的信道容量, 适合远距离传输, 可以很好满足即时通信的要求, 因此 CVQKD 越来越多的受到人们的关注.

1999 年, Ralph 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], 并证明了方案的安全性 [2]. 2001 年, Cerf 等人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 Heisenberg 不确定性原理保证, 窃听者想要获取在其中一个正交分量上的信息, 必然会引起另外一个正交分量上噪声的增加 [3]. 2002 年, Grosshans 提出一种只利用相干态即可实现密钥分发的方案, 不需要依赖于亚散粒噪声的压缩特性, 但是该方案采用的是正向协调, 需要信道传输效率高于 50%(即信道损耗小于 3 dB) 才能进行安全的分发密钥 [4]. 同年, Silberhorn 等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 [5]. 2003 年, Grosshans 为克服 3dB 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, 当信道无失真时, 密钥传输速率达到 1.7 Mbit/s, 当信道损耗为 3.1 dB 时, 密

* 国家自然科学基金 (批准号: 10647133, 11174118), 江西省自然科学基金 (批准号: 2009GQS0080), 江西省教育厅科技项目 (批准号: GJJ11339) 和南昌大学引进人才科研启动费资助的课题.

† E-mail: znr21@163.com

钥传输速率达到 75 kbit/s[6]. 2004 年, Weedbrook 提出利用 50/50 分光镜测量的方法, 同时测量光源的振幅和相位, 无需变换测量基, 提高了密钥传输效率, 为量子密钥分配指供了新的研究方法 [7]. 马海强等提出利用两个偏振分束器的量子密钥分发系统, 有效地解决了相位调制器的偏振依赖性问题 [8]. 2006 年, Namiki 将相干态的相位进行离散调制, 达到了较高的传输效率, 其中在 4 态协议中传输效率为 100%[9]. 曾贵华提出了一种基于 EPR 纠缠特性的加密方法, 其中纠缠光束由非简并光学参数放大器 (NOPA) 产生, 安全性由 EPR 关联特性来保证 [10]. 2007 年, Lodewycy 等人完成了 25 km 全光纤相干态连续变量量子密钥分发的实验, 结果表明: 在个体攻击下密钥传输速率为 2.7kbit/s, 集体攻击下密钥传输速率为 2.2 kbit/s[11]. 2009 年, Patron 采用压缩态光源和外差探测法, 提出了一种高效的 QKD 方案, 该方案具有较强的抗干扰能力 [12]. 曾贵华等实现了 CVQKD 的纠错和协商, 提高了协议的效率 [13]. 2010 年, 王金东针对相位编码量子密钥分发系统相位漂移的实际问题, 提出了一种 “五点法” 快速相位漂移参数的扫描方法. 该方法能够对相位漂移进行实时补偿 [14], 该课题组 2011 年提出了一种基于确定性量子密钥分发误码判据的相位调制器半波电压的精确测定方法, 可以用于实际量子密钥分发系统中实时获得不同条件下的行波相位调制器的半波电压以最大程度地减小系统误码率 [15]. Lo 等通过在电信波长上采用密集波分复用技术研究了在同一光纤中进行量子密钥分发与经典通信的可行性问题, 指出诱骗态 BB84 QKD 协议不可行, 而高斯调制相干态 QKD 协议可行性较好 [16]. 2011 年, Namekata 等利用超低噪声正弦门控的雪崩光电二极管, 采用单光子探测器, 在 100 km 的光纤中完成了安全的 QKD, 信道传输速度达到 24 kbit/s, 当改用差分移相的探测方法后, 传输距离可以达到 160 km[17]. Leverrier 设计出非高斯调制的 QKD 协议, 使得在密钥协商阶段的效率大大提高, 并证明它在线性量子信道中是绝对安全的, 该协议还在密钥传输过程中加入了诱骗态, 可以抵御任意的集体攻击 [18].

以上的密钥分配方案都能在合法通信用户之间产生一组安全的随机密钥, 直到协议结束之前, 没有人 (包括发送者和接收者) 知道最终的密钥. 而在现实生活中, 人们经常需要传送一个预先确定的密钥. 例如, 当一个特定秘密的密钥遗失或者破坏时, 为了解开这个秘密, 发送者需要传送一个与之前相同的密钥给指定的接收者. 为了实现该目标, 人们通常是对该密钥进行加密然后传送其密文. 众所周知, 加密至少需要安全的密钥和安全的加密算法, 这就引起两个问题: 如何安全地共享密钥和如何设计安全高效的加解密算法. 前者可以由 QKD 协议来实现, 然而后者除了量子加密算法 [19] 和密钥消耗量大的一次一密便签以外, 很难有绝对安全的加密算法. 文献 [20] 对基于离散变量量子秘密通信的 Ping-Pong 协议做了改进, 提出一种新的连续变量量子对话协议. 此类量子安全直接通信中, “发现窃听即终止策略” 使得在发现窃听者之前可能已经泄露一部分信息, 因此不能直接用来传送确定性密钥 (可用于分配随机密钥), 分配的确定性密钥不具有无条件安全性. 尽管利用离散量子信号也可以产生确定性密钥 [21−23], 但是离散变量量子确定性密钥分发协议的效率、速率等性能不高, 导致实用性不强. 量子远程通信 (quantum teleportation) 可以将一个量子态从一个地方转移到另一个地方, 而不需要移动量子态的载体, 可以用于量子密钥分配. 文献 [24] 借助于双模压缩纠缠态, 证明了任意的单模和双模量子态都可以进行远程传输. 文献 [25] 指出只要纠缠度比较高, 就可以成功地实现相干态的远程传输. 针对上述量子密钥分配协议的不足, 本文基于量子远程通信的原理, 提出连续变量量子确定性密钥分配 (continuous-variable quantum deterministic key distribution, CVQDKD) 协议, 它的主要目的是经由公共信道移交一预先确定的密钥给接收者, 其中密钥对发送者而言是确定的. 作为对密钥管理的有益补充, CVQDKD 将具有不可替代的重要地位和作用.

2 基础知识和判定依据

在量子光学中, 一个光束的两个正则分量振幅 X 和相位 P 可以用产生算符 $a^\dagger$ 和湮没算符 a 表示为 [26]

$$X = a^\dagger + a, \tag{1}$$

$$P = \mathrm{i}(a^\dagger - a), \tag{2}$$

其中 $[a^\dagger, a] = 1$, $[X, P] = 2\mathrm{i}$, 则 X 和 P 满足 Heisenberg 不确定性关系: $\Delta X \cdot \Delta P \geqslant 1$.

双模压缩真空态可以由两个真空态通过非简并光学参量放大 (NOPA) 过程来制备. 两个真空

态 $a_{\rm in1}$, $a_{\rm in2}$ 经过双模压缩变换 $S(r)$ 以后, 输出为

$$\begin{aligned} a_{\rm out1} &= S^{\dagger}(r)a_{\rm in1}S(r), \\ &= a_{\rm in1}\cosh(r) + a_{\rm in2}^{\dagger}\sinh(r), \end{aligned} \tag{3}$$

$$\begin{aligned} a_{\rm out2} &= S^{\dagger}(r)a_{\rm in2}S(r) \\ &= a_{\rm in2}\cosh(r) + a_{\rm in1}^{\dagger}\sinh(r), \end{aligned} \tag{4}$$

那么 $a_{\rm out1}$, $a_{\rm out2}$ 的振幅和相位可以分别表示为

$$\begin{aligned} X_{\rm out1} &= X_{\rm in1}\cosh(r) + X_{\rm in2}\sinh(r), \\ P_{\rm out1} &= P_{\rm in1}\cosh(r) - P_{\rm in2}\sinh(r), \\ X_{\rm out2} &= X_{\rm in2}\cosh(r) + X_{\rm in1}\sinh(r), \\ P_{\rm out2} &= P_{\rm in2}\cosh(r) - P_{\rm in1}\sinh(r). \end{aligned} \tag{5}$$

计算两个输出的正交振幅和相位的关联方差, 有

$$\begin{aligned} &\langle[\Delta(X_{\rm out1} - X_{\rm out2})]^2\rangle \\ =&\langle[\Delta(P_{\rm out1} + P_{\rm out2})]^2\rangle = 2\,{\rm e}^{-2r}, \end{aligned} \tag{6}$$

$$\begin{aligned} &\langle[\Delta(X_{\rm out1} + X_{\rm out2})]^2\rangle \\ =&\langle[\Delta(P_{\rm out1} - P_{\rm out2})]^2\rangle = 2\,{\rm e}^{2r}, \end{aligned} \tag{7}$$

当压缩参数 $r \to +\infty$ 时, 输出模 $a_{\rm out1}$, $a_{\rm out2}$ 具有很强的关联性:

$$\begin{aligned} \lim_{r\to+\infty} X_{\rm out1} &= X_{\rm out2}, \\ \lim_{r\to+\infty} P_{\rm out1} &= -P_{\rm out2}, \end{aligned} \tag{8}$$

此时 $a_{\rm out1}$, $a_{\rm out2}$ 的振幅正关联, 相位负关联; 当压缩参数 $r \to -\infty$ 时, 输出模 $a_{\rm out1}$, $a_{\rm out2}$ 也具有很强的关联性, 此时振幅负关联, 相位正关联.

文献 [19] 提出用参数 F 表示双模压缩态的纠缠度:

$$\begin{aligned} F =&\langle[\Delta(X_{\rm out1} - k_1X_{\rm out2})]^2\rangle_{\rm min} \\ &\times\langle[\Delta(P_{\rm out1} + k_2P_{\rm out2})]^2\rangle_{\rm min}. \end{aligned} \tag{9}$$

当 $k_1 = \dfrac{\langle x_{\rm out1}\cdot x_{\rm out2}\rangle}{\langle x_{\rm out2}^2\rangle}$, $k_2 = -\dfrac{\langle p_{\rm out1}\cdot p_{\rm out2}\rangle}{\langle p_{\rm out2}^2\rangle}$ 时, 可得

$$F = \frac{4\sigma^4}{{\rm e}^{2r} + {\rm e}^{-2r}}, \tag{10}$$

其中 $\langle x_{\rm in1}^2\rangle = \langle x_{\rm in2}^2\rangle = \langle p_{\rm in1}^2\rangle = \langle p_{\rm in2}^2\rangle = \sigma^2$. 当 $r \to \infty$, $F \to 0$; 若纠缠被破坏, 则 r 变小, 会引起 F 迅速增大, 即 F 描述了双模压缩态之间的纠缠度, 它会随着纠缠度的增大而减小.

当 Alice 和 Bob 共享纠缠的双模压缩真空态 $a_{\rm out1}$, $a_{\rm out2}$ 时, Alice 制备相干态 $|x + {\rm i}p\rangle_1$, 并和 $a_{\rm out1}$ 通过 50/50 分光镜进行联合 Bell 基测量, 得到

$$\begin{aligned} x_u &= \frac{1}{\sqrt{2}}(x_1 - x_{\rm out1}), \\ p_u &= \frac{1}{\sqrt{2}}(p_1 + p_{\rm out1}), \end{aligned} \tag{11}$$

考虑到信道增益, Bob 可以先对收到的信号进行增益补偿, 不会对收到的信号造成额外影响. 记 Bob 收到的信号为

$$\begin{aligned} x_{\rm B} &= x_{\rm out} + \sqrt{2}x_u - \sqrt{2}x_u \\ &= x_1 - (x_{\rm out1} - x_{\rm out2}) - \sqrt{2}x_u, \end{aligned} \tag{12}$$

$$\begin{aligned} p_{\rm B} &= p_{\rm out} + \sqrt{2}p_u - \sqrt{2}p_u \\ &= p_1 + (p_{\rm out1} + p_{\rm out2}) - \sqrt{2}p_u. \end{aligned} \tag{13}$$

Alice 公布测量结果后, Bob 执行相应的幺正变换, 得到

$$x'_{\rm B} = x_{\rm B} + \sqrt{2}x_u = x_1 - (x_{\rm out1} - x_{\rm out2}), \tag{14}$$

$$p'_{\rm B} = p_{\rm B} + \sqrt{2}p_u = p_1 + (p_{\rm out1} + p_{\rm out2}), \tag{15}$$

当纠缠度 $r \to +\infty$ 时, $x'_{\rm B} = x_1$, $p'_{\rm B} = p_1$, 即 Alice 和 Bob 可以得到两个高度相关的序列, 可以用来传送密钥, 若 $a_{\rm out1}$, $a_{\rm out2}$ 纠缠度比较低则无法得到正确结果. 当 Alice 要传送确定性密钥时, 令 $x_1 = p_1$, 此时无论 Bob 选择振幅或相位进行测量, 均能得到和 Alice 高度相关的序列 x_1, 实现确定性密钥分发.

3 连续变量量子确定性密钥分配协议

假设 Alice 需要将确定性密钥传给指定的接收者 Bob, 则方案的步骤如下:

1) Alice 将双模压缩算符 $S(r)$ 作用于真空态 $|00\rangle_{23}$, 产生纠缠的光学模 a_2, a_3, 其中 $S(r) = \exp[r(a_2^{\dagger}a_3^{\dagger} - a_2a_3)]$.

2) Alice 随机选择时间间隙计算 a_2, a_3 之间的纠缠度 F, 并且记录下相应的时间间隙和结果 F, 然后将 a_3 发送给 Bob.

3) 记 Bob 收到的光学模为 a_4(若无窃听, 则 $a_4 = a_3$). 当 Bob 确认收到 a_4 以后, Alice 公布相应的时间间隙和计算结果, Bob 选择相应的时间间隙随机进行振幅或相位测量, 计算纠缠度 F'. 若 $F' > F$, 则说明有窃听存在, 放弃此次通信, 转回步骤 1), 若 $F' = F$, 则继续步骤 4).

4) Alice 将所要发送的离散信息按照一定的编码规则进行区间划分 (LDPC 码或 Turbo 码). 假

设 Alice 把坐标区间分为 $(-\infty, x_1)$, $[x_1, x_2), \cdots,$ $[x_{n-1}, x_n)$, $[x_n, +\infty)$, 如果要发送的比特序列是 01001, 对应的区间为 $[x_{k-1}, x_k)$, 则产生随机变量 x, y, z, 其中实数 $x \in [x_{k-1}, x_k)$, y, z 为任意实数. Alice 将位平移算符 $D(\alpha_1 = (x+y) + \mathrm{i}(x+y))$ 作用于真空态 $|0\rangle_1$, 产生相干态 a_1, 同时选取位平移算符 $D(\alpha_1' = (x+z) + \mathrm{i}(x+z))$ 作用于真空态 $|0\rangle_1'$, 产生相干态 a_1'(诱骗态), 并随机选择时间间隙将 a_1' 插入 a_1 中, 产生混合的量子态 a. 然后, Alice 将 a 和 a_2 通过 50/50 分光镜进行联合 Bell 基测量, 记录下 a 与 a_2 的振幅和 X_u 与相位差 P_u, 并将测量结果通过经典信道告知 Bob.

5) Bob 根据 Alice 的测量结果对 a_4 进行相应的幺正变换 $D(\mu = \sqrt{2}(X_u + \mathrm{i}P_u))$, 然后随机选择测量基 (振幅 X 或相位 P) 进行测量, 即可获得一个与 Alice 高度相关的序列 ξ.

6) Alice 公布自己加入诱骗态 a_1' 的时间间隙, Bob 公布相应时间间隙的测量结果, 若双方结果不一样, 则放弃此次通信, 否则 Alice 公布步骤 4) 中的 y, 继续步骤 7).

7) Bob 将序列 ξ 中剩余的测量结果分别减去 y, 然后按照和 Alice 同样的编码规则进行解码, 能够得到 $x \in [x_{k-1}, x_k)$, 即获得 Alice 要发送的比特序列 01001.

其中 1)—3) 的目的是安全地共享连续变量量子纠缠态, 4)—7) 为密钥传送、接收和生成阶段, 插入诱骗态 a_1' 的目的是使得确定性密钥对除发送者以外的人来说是随机性的, 随机平移 y 的目的是使得确定性的结果与确定性密钥之间并不等价, 只有信道安全和接收者通过了身份认证后再扣除诱骗态和随机平移才能得到最终需要的确定性密钥. 这两种随机化手段使得接收者完全接收信号后仍不能判断真实的确定性密钥是什么, 这对确定性密钥分发的安全性显得尤为重要.

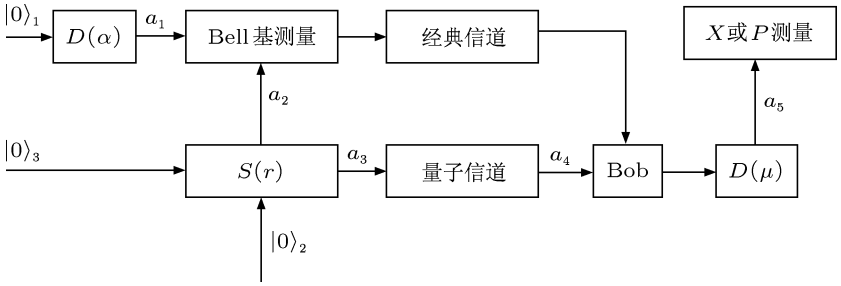

图 1 连续变量量子确定性密钥分配协议模型

4 安全性分析

该方案的安全性基于量子纠缠、随机插入诱骗态和随机平移, 他们的本质都是信息分割. 而插入的诱骗态和平移态主要是在生成密钥阶段发挥作用, 一旦信道安全即可获得密钥, 不会影响双方之间最后的信息量. 在进行安全性分析时, 只需考虑在没有加入诱骗态时信道的安全性, 即可保证 CVQDKD 协议的安全性.

4.1 Alice 和 Bob 之间的互信息量

在协议中 Bob 选取 x 或者 p 测量是随机的, 假设其概率各为 1/2, 有

$$\Delta I = \frac{1}{2}(\Delta I_x + \Delta I_{\mathrm{p}}), \tag{16}$$

由于 x 和 p 的对称性, $\Delta I_x = \Delta I_{\mathrm{p}}$, 信息传输速率可简写为

$$\Delta I = \Delta I_x. \tag{17}$$

当采用逆向协调时, $\Delta I_x = I(x_{\mathrm{B}}, x_{\mathrm{A}}) - I(x_{\mathrm{B}}, x_{\mathrm{E}})$, 其中 $I(x_{\mathrm{B}}, x_{\mathrm{A}})$ 表示 Bob 和 Alice 之间的互信息量, $I(x_{\mathrm{B}}, x_{\mathrm{E}})$ 表示 Bob 和 Eve 之间的互信息量, 由香农信息论可知

$$\begin{aligned} I(x_{\mathrm{B}}, x_{\mathrm{A}}) &= \frac{1}{2}\log_2\left(\frac{V_{\mathrm{B}}}{V_{\mathrm{A|B}}}\right), \\ I(x_{\mathrm{B}}, x_{\mathrm{E}}) &= \frac{1}{2}\log_2\left(\frac{V_{\mathrm{E}}}{V_{\mathrm{E|B}}}\right), \end{aligned} \tag{18}$$

$$\Delta I = \frac{1}{2}\log_2\left(\frac{V_{\mathrm{E|B}}}{V_{\mathrm{A|B}}}\right), \tag{19}$$

$V_{\mathrm{A|B}}$ 表示 Alice 关于 Bob 的条件方差, 记为 $V_{\mathrm{A|B}} = \min_{g_\mathrm{A}}\langle(x_\mathrm{B} - g_\mathrm{A}x_\mathrm{A})^2\rangle$, 同理 $V_{\mathrm{E|B}}$ 表示 Eve 关于 Bob 的条件方差, 记为 $V_{\mathrm{E|B}} = \min_{g_\mathrm{E}}\langle(x_\mathrm{B} - g_\mathrm{E}x_\mathrm{E})^2\rangle$, $V_{\mathrm{A|B}}$ 和 $V_{\mathrm{E|B}}$ 满足关系 [6,7]

$$V^x_{\mathrm{A|B}} \cdot V^\mathrm{p}_{\mathrm{E|B}} \geqslant 1, \quad V^\mathrm{p}_{\mathrm{A|B}} \cdot V^x_{\mathrm{E|B}} \geqslant 1. \tag{20}$$

Alice 和 Eve 能够同时获得关于 Bob 的信息量是有一定限制的, 它们满足 Heisenberg 不确定性关系. 在 $V^\mathrm{p}_{\mathrm{A|B}}$ 取得最小值时, 我们可以确定 Eve 所能获取的最大信息量的下限 $V^x_{\mathrm{E|B}}$.

4.2 基于分光镜攻击的安全性分析

在本协议中 Alice 和 Bob 只在量子信道中进行了一次量子信号的传输, 假定窃听者 Eve 采取截取 – 重发策略. 他的一种做法是截取全部由 Alice 发出的信号, 随机的选取 X 或 P 分量进行测量 (或者同时测量 X 和 P), 然后根据测量结果制备量子态发送给 Bob, 然而无论进行哪种测量, 由于量子测不准原理的约束, Eve 都会不可避免地引入额外噪声, 从而引起纠缠度发生变化, 最终会被合法的通信双方在安全检测的过程中发现. 另一种可能做法则是截取部分由 Alice 发出的信号进行相应的操作, 根据量子不可克隆定理, 为了不被 Alice 和 Bob 发现的同时获取最大信息量, Eve 所能采取的最好的做法是截取 Alice 发出的光束, 让其通过一个透射系数为 η 的分光镜, 其中 η 的值必须与信道传输效率相等, 自己截取其中 $(1-\eta)$ 的部分, 让剩下的 η 部分通过无损信道传送给 Bob, 然后通过 Alice 公开的信息进行相应的操作. 本文将主要分析此种情况下协议的安全性.

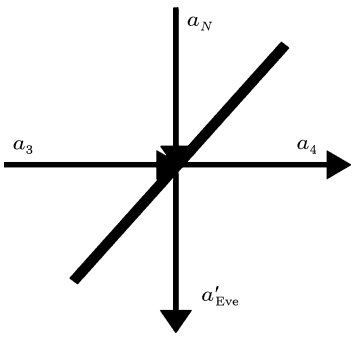

图 2 分光镜攻击

Alice 制备的相干态可以描述为: $a_1 = \alpha_1 + a_{\mathrm{vac}}$, 相应的在 x 分量上 $x_1 = x + x_{\mathrm{vac}}$, 则 $V^x_1 = \sigma^2 + V_{\mathrm{vac}}$, 而双模压缩真空态的表达式可由 (5) 式求得, 如图所示, Eve 截取 Alice 发出的光束经过分光镜以后,

$$a_4 = \sqrt{\eta}a_3 + \sqrt{1-\eta}a_N, \tag{21}$$

$$a'_{\mathrm{Eve}} = \sqrt{\eta}a_N - \sqrt{(1-\eta)}a_3, \tag{22}$$

其中 a_N 为量子信道噪声, Bob 和 Eve 在 Alice 公布信息之后, 分别进行相应的操作和幺正变换后:

$$a_5 = a_4 + \sqrt{\eta}\mu, \tag{23}$$

$$a_{\mathrm{Eve}} = a'_{\mathrm{Eve}} - \sqrt{(1-\eta)}\mu. \tag{24}$$

根据 $V_{\mathrm{A|B}}$ 定义, 需要 $g_\mathrm{A} = \dfrac{\langle x_\mathrm{A} \cdot x_\mathrm{B}\rangle}{\langle x^2_\mathrm{A}\rangle}$, 在本方案中, $V_{\mathrm{A|B}} = \langle x_5\rangle^2 - \dfrac{\langle x \cdot x_5\rangle^2}{\langle x^2\rangle}$, 而根据 (22) 式可得到在 x 分量上:

$$\begin{aligned} x_5 &= x_4 + \sqrt{\eta}(x_1 - x_2) \\ &= \sqrt{\eta}x_3 + \sqrt{(1-\eta)}x_N + \sqrt{\eta}(x_1 - x_2), \\ \langle x \cdot x_5\rangle &= \sqrt{\eta}\sigma^2 \\ V_{\mathrm{A|B}} &= 1 - \eta + 2\eta(\cosh^2(r) + \sinh^2(r)) \\ &\quad - 4\eta\cosh(r)\sinh(r) + \eta V_1 - \eta V \\ &= 1 - \eta + \eta V_{\mathrm{vac}} + 2\eta\,\mathrm{e}^{-2r}. \end{aligned} \tag{25}$$

由于相干态在两个分量上的方差是一样的, 而压缩态可以将一个分量压缩至无限小, 所以这里选取压缩态来得到 $V_{\mathrm{A|B}}$ 的最小值. 当 Alice 制备的 x_1 是压缩态的时候, $V_1 = \sigma^2 + V_{\mathrm{sqz}}$, 而由压缩态的性质, $V^\mathrm{p}_{\mathrm{sqz}} \geqslant \dfrac{1}{V^x_1}$, 从而有

$$(V^\mathrm{p}_{\mathrm{A|B}})_{\min} = 1 - \eta + \frac{\eta}{V^x_1} + 2\eta\,\mathrm{e}^{-2r}, \tag{26}$$

由 (20) 式得

$$\begin{aligned} (V^x_{\mathrm{E|B}}) &\geqslant \frac{1}{(V^\mathrm{p}_{\mathrm{A|B}})_{\min}} \\ &= \left(1 - \eta + \frac{\eta}{V^x_1} + 2\eta\,\mathrm{e}^{-2r}\right)^{-1}, \end{aligned} \tag{27}$$

$$\begin{aligned} \Delta I \geqslant{}& -\frac{1}{2}\log_2(1 - \eta + \eta/V_1 + 2\eta\,\mathrm{e}^{-2r}) \\ &\times (1 - \eta + \eta V_N + 2\eta\,\mathrm{e}^{-2r}). \end{aligned} \tag{28}$$

在 $V_N = 1$, $V_1 = 100$ 时, 结果如图 3 所示: 在 $r = 0$ 时, 由于不存在纠缠, $\Delta I < 0$, 不能传输密

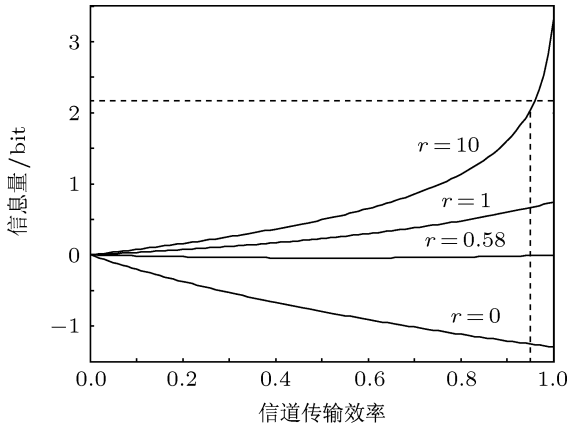

图 3 信息量 ($V_N = 1, V_1 = 100$)

钥, 这说明量子远程通信依赖于量子的纠缠特性, 若 Alice 和 Bob 之间共享的纠缠对纠缠特性被破坏, 则不能传送密钥给 Bob. 而由于 Alice 和 Bob 之间共享的是压缩态要满足 (26) 式, 得到在 $r \geqslant 0.58$ 时成立, 此时 $\Delta I \approx 0$. 在 $r = 1$ 时 $\Delta I > 0$, 表示在 $r = 1$ 时, 只要信道传输效率 $\eta > 0$, 均能够传送安全密钥. 随着纠缠度的增加, Alice 和 Bob 之间的互信息量逐步增大. 由信息论可知, 文献 [23] 中提出的离散变量量子确定性密钥分发协议中每个量子态最多只能传送 1 bit 的密钥, 本文提出的 CVQDKD 使用连续变量量子态, 在 $r = 10$ 的情况下, 从图中可以发现当信道传输效率 $\eta \approx 0.75$ 时, 密钥传输速率为 1 bit/s, 当信道传输效率 $\eta \approx 0.95$ 时, 密钥传输速率几乎达到 2 bit/s, 是文献 [23] 中协议密钥信息传输速率的两倍. 随着信道传输效率的提高, CVQDKD 分发密钥的速度也随之增大, 明显优于离散量子态的确定性密钥分发协议.

5 结 论

现有 CVQKD 协议中不能传送确定性密钥, 本文基于连续变量量子远程通信提出了一个量子确定性密钥分配协议, 用于传送预先确定的密钥, 在协议结束之前, 只有 Alice 拥有最终的密钥. 在典型 CVQKD 方案中, 协议的安全性主要依赖于测量基的随机选择, 仅测量基相同的序列被保留作为密钥, 协议效率只有 50%, 而本协议中, 安全性是由纠缠度决定的, 无论 Bob 选取哪个分量进行测量, 均能得到和 Alice 高度相关的一个序列, 在用诱骗态验证信道安全性之后, Bob 利用 Alice 加入的随机平移进行相应的解码操作, 即可生成确定性密钥序列, 没有窃听的情况下, 效率可以达到 100%. 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可以安全传送预先确定的密钥. 作为对密钥管理的有益补充, CVQDKD 将具有不可替代的重要地位和作用.

[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] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[8] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强, 李亚玲, 赵环, 吴令安 2005 物理学报 **54** 5014]
[9] Namiki R 2006 *Phys. Rev.* A **74** 032302
[10] He G Q, Zeng G H 2006 *Commun. Theor. Phys.* **46** 16
[11] Lodewyck J, Bloch M, Patron R G, Fossier S, Karpov E, Diamanti E, Debuisschert T 2007 *Phys. Rev.* A **76** 042305
[12] Patron R G, Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
[13] Qian X D, He G Q, Zeng G H 2009 *Sci. China. Ser.* F **52** 2072
[14] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东, 秦晓娟, 魏正军, 刘小宝, 廖常俊, 刘颂豪 2010 物理学报 **59** 281]
[15] Wei Z J, Wan W, Wang J D, Liao C J, Liu S H 2011 *Acta Phys. Sin.* **60** 094217 (in Chinese) [魏正军, 万伟, 王金东, 廖常俊, 刘颂豪 2011 物理学报 **60** 094217]
[16] Qi B, Zhu W, Qian L, Lo H K 2010 *New J. Phys.* **12** 103042
[17] Namekata N, Takesue H, Honjo T, Tokura Y, Inouen S 2011 *Opt. Expr.* **19** 10632
[18] Leverrier A, Grangier P 2011 *Phys. Rev.* A **83** 042312
[19] Zhou N R, Zeng G H, Nie Y Y, Xiong J, Zhu F C 2006 *Physica* A **362** 305
[20] He G Q, Zhu J, Zeng G H 2006 *Phys. Rev.* A **73** 012314
[21] Zhou N R, Wang L J, Ding J, Gong L H 2010 *Phys. Scr.* **81** 045009
[22] Zhou N R, Wang L J, Ding J, Gong L H, Zuo X W 2010 *Int. J. Theor. Phys.* **49** 2035
[23] Zhou N R, Wang L J, Gong L H, Zuo X W Liu Y 2010 *Opt. Commun.* **284** 4836
[24] Song T Q 2004 *Acta Phys. Sin.* **53** 3358 (in Chinese) [宋同强 2004 物理学报 **53** 3358]
[25] Yan W, Zhang W J 2007 *Chin. Phys.* **16** 2584
[26] Weedbrook C 2003 Quantum cryptography without basis switching, University of Queensland

Continuous-variable quantum deterministic key distribution protocol based on quantum teleportation*

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

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

(Received 14 November 2011; revised manuscript received 29 November 2011)

Abstract

By exploiting quantum teleportation, we propose a continuous-variable quantum deterministic key distribution (CVQDKD) protocol using two-mode squeezed vacuum state and coherent state. The efficiency is 100% under the homodyne detection. The security of CVQDKD is analyzed in detail from information theory, and the result shows that the proposed protocol can securely hand over the pre-deterministic key. By contrast with the quantum random key distribution, the quantum deterministic key distribution plays an irreplaceable role in the field of key management. Furthermore, the CVQDKD can obtain a higher rate and better efficiency than the quantum deterministic key distribution protocols with discrete variables, and the quantum states used in the protocol are also easy to produce and manipulate, which i suitable for long-distance transmission. Therefore, the CVQDKD protocol is more practical.

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 Nos. 10647133 and 11174118), the Natural Science Foundation of Jiangxi Province, China (Grant No. 2009GQS0080), the Research Foundation of the Education Department of Jiangxi Province (Grant No. GJJ11339), and the Scientific Research Start-up Funds for the Recruitment of Talent of Nanchang University.

† E-mail: znr21@163.com