第 59 卷 第 3 期 2010 年 3 月
1000-3290/2010/59(03)/1473-08

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 3, March, 2010

离散调制连续变量量子密钥分发的安全边界*

沈 咏 邹宏新†

(国防科学技术大学理学院物理系 长沙 410073)

(2009 年 5 月 8 日收到;2009 年 6 月 22 日收到修改稿)

对一种结合离散调制和反向协调,适用于长距离传输的连续变量量子密钥分发四态协议的安全性进行了严格证明. 这种协议中 Alice 发送的态与高斯调制协议中的有一定差异,这种差异可以等价成信道衰减和额外噪声. 另外,由于 Alice 不可能做到精确调制,这会导致其发送的相干态中含有噪声. 把这种调制引起的噪声看作光源的噪声,并推导出了在光源噪声不能被窃听者所利用的条件下的安全码率的下界. 为了避免实验上快速、随机的控制本地振荡光的相位,还将无开关协议和四态协议相结合,分析了其安全性.

关键词: 离散调制, 四态协议, 连续变量量子密钥分发, 安全码率

PACC: 0367, 4250

1. 引 言

目前,国内外在基于单光子的量子保密通信研究上取得了巨大进展,特别是近年来的诱骗态方案,又将单光子保密通信的安全距离大幅度提高,导致其进一步向实用化靠近. 作为量子保密通信的一个可选方案,物理学家们又提出了利用连续光来进行保密通信的方案. 它们对连续光场两正交分量进行编码,并采用高效的平衡零拍探测,提高了编码效率降低了探测成本.

连续变量量子密钥分发(CV-QKD)在过去几年中取得了非常显著的成就. 人们提出了一些基于高斯调制相干态结合平衡零拍探测[1]或无开关协议[2]的量子密钥分发方案,并进行了实验演示[3—6]. 朱畅华等提出的基于信道估计的自适应连续变量量子密钥分发方法增加了 CV-QKD 的稳定性[7]. 在无条件安全性方面,人们研究了信道和探测器的衰减和额外噪声等非理想因素对 CV-QKD 安全码率的影响[8,9]. 但是,目前 CV-QKD 还只适用于短距离密钥传输,其原因在于从 Alice 和 Bob 共享的连续变量中提取出密钥的经典后处理过程远比从离散变量中提取密钥复杂. 为了使 CV-QKD 能够适用于更长的距离, Leverrier 和 Grangier 小组提出了一种基于离散调制的连续变量量子密钥分发协议:四态协议[10],并对其安全性进行了证明,但是他们在证明过程中忽略了与离散调制协议等价的纠缠方案(entanglement-based scheme)中 Alice 和 Bob 共享纠缠态的协方差矩阵与相应的连续调制协议中协方差矩阵的差异. 另外,离散调制协议只适用于调制方差非常小的情况(每个脉冲的平均光子数小于 1),在如此小的范围内很难做到精确调制. 调制的误差可以看作是光源的噪声,而他们在证明过程中并没有考虑这种噪声. 本文考虑了这些问题,对光源有噪声时的基于离散调制连续变量量子密钥分发的安全性进行了严格证明. 除此之外,由于这种方案需要随机选择光场的一个正交分量进行测量,要求对平衡零拍探测的相对相位进行随机、快速控制,实验难度非常大. 因此本文还将离散调制同无开关协议相结合,分析了其安全性,并同平衡零拍探测方案进行了比较.

* 国防科学技术大学科学研究计划项目(批准号:JC08-02-01),国家自然科学基金(批准号:10904174)和华东师范大学精密光谱国家重点实验室开放研究基金资助的课题.

† E-mail: hxzou@nudt.edu.cn

2. 高斯调制 CV-QKD 的缺陷

基于高斯调制的 CV-QKD,其通信过程可以由以下几个步骤所描述:1)发送端 Alice 随机的选择两个平均值为 0,数值大小服从高斯分布的离散信号分别调制到一束相干光的正交振幅和位相上,并通过量子通道发送给接收端 Bob. 2)Bob 收到发送来的态后,随机地选择一个正交分量进行平衡零拍探测,并告诉 Alice 所选择的正交分量,这样 Alice 和 Bob 就拥有了一组相关联的随机变量. 3)最后,通信双方扔掉未测量的正交分量和明显被窃听的信息,并采用反向协调进行误码校正和保密放大提取密钥. 整个通信过程的安全性由海森伯不确定性原理所保证. 在这个过程中,窃听者 Eve 可以利用一切不违背物理规律的方法来窃取信息. 在信道参数给定的情况下,如果理论推导出的安全码率大于 0,那么 Alice 和 Bob 得到的密钥就是无条件的.

对于窃听者来说,最优的攻击方式是高斯集体攻击(Gaussian collective attacks),因此只需用考虑高斯集体攻击下的码率就可以证明 CV-QKD 的无条件安全性[11,12]. 在高斯集体攻击下,当 Alice 和 Bob 采用反向协调协议时,其安全码率为[13]

$$K = I(a:b) - \chi(b:E), \tag{1}$$

其中 a, b 分别是 Alice 和 Bob 对自己的子系统进行测量后得到的经典随机变量,$I(a:b)$ 是 Alice 和 Bob 手中经典随机变量之间的 Shannon 互信息量. $\chi(b:E)$ 是 Holevo 界,它界定了 Eve 所能劫获的 Bob 手中经典随机变量的信息:

$$\chi(b:E) = S(\rho_{\mathrm{E}}) - \int \mathrm{d}b p(b) S(\rho_{\mathrm{E}}^{b}), \tag{2}$$

其中 ρ_{E} 是 Eve 手中的态,ρ_{E}^{b} 是 Bob 测量后 ρ_{E} 塌缩得到的态,$p(b)$ 是 Bob 测量结果的概率分布,S 是 von Neumann 熵. (1)式成立有一个条件,那就是 Alice 和 Bob 能进行完美的纠错,将他们之间的互信息 $I(a:b)$ 全部提取出来,但这在实际中是不可能的. 在实际过程中,他们提取的信息可以由 $\beta I(a:b)$ $(0<\beta<1)$ 来表示,β 是考虑非完美协调时引入的一个因子,称为协调效率,定义为[14]

$$\beta = \frac{H(\hat{b}) - I_{\mathrm{red}}}{I(a:b)}, \tag{3}$$

其中 $\hat{b}$ 是 Bob 将 b 进行量化编码后得到的离散随机变量,$H(\hat{b})$ 是 $\hat{b}$ 的 Shannon 熵,I_{red} 是信息协调过程中每个信号平均泄露的信息. 对于给定的信源和信道可以很容易计算出 $H(\hat{b})$ 和 $I(a:b)$. I_{red} 与采用的协调方案以及信道的性质有关,很难直接从理论上推得,一般通过实验的方法来确定. 考虑协调效率时,安全码率表示为[5,15]

$$K = \beta I(a:b) - \chi(b:E). \tag{4}$$

当通信距离较长,信道衰减较大时,信噪比会比短距离通信时明显降低. 连续变量的信息协调效率也会随着信噪比的衰减急剧降低[10]. 通过增大信号的调制方差可以提高信噪比,但是这时 $I(a:b)$ 和 $\chi(b:E)$ 都会变大,而它们的差却得不到明显改善,这就要求协调效率必须很高,否则没有安全码率[5,13]. 即使采用目前 CV-QKD 中最好的纠错方案,如 LDPC 码和 turbo 码,也很难使通信距离超过 30 km[10].

3. 四态协议

为了使 CV-QKD 能适用于更远的距离,Leverrier 和 Grangier 小组提出了一种基于离散调制的连续变量量子密钥分发协议,即四态协议[10]. 如图 1(a)所示,在这个协议中,Alice 随机的选择向 Bob 发送相干态 $|\alpha_k\rangle = |\alpha \mathrm{e}^{\mathrm{i}(2k+1)\pi/4}\rangle$,其中 $k \in \{0,1,2,3\}$,α 是一个实数. 对于一个确定的信道,即给定了透过率和额外噪声(excess noise)的信道,可以通过改变 α 的取值使得安全码率达到最大. Bob 接受到 Alice 发出的态后随机的选择对 X 分量或 P 分量进行平衡零拍探测并得到测量结果 y. Bob 根据 y 的符号的正负得到 1bit 数据,并将测量结果的绝对值 $|y|$ 通过经典信道发送给 Alice. 这样 Alice 和 Bob 就共享了一串相关的比特,然后通过信息协调和保密增强就可以得到密钥. 从经典通信的角度来看,对这种在高斯加性白噪声信道传递的二进制调制数据进行纠错是很容易解决的,即使在信噪比很低的时候也能获得很高的协调效率[10].

以上所描述的是制备和测量方案[16](prepare and measure scheme),这种方案实现起来比较容易,但是很难直接证明其安全性,于是文献[10]给出了与之等价的纠缠方案. 如图 1(b)所示,在纠缠方案中,Alice 手中有一个纠缠源,不断产生纯的纠缠态 $|\Phi_{AB_0}\rangle$,

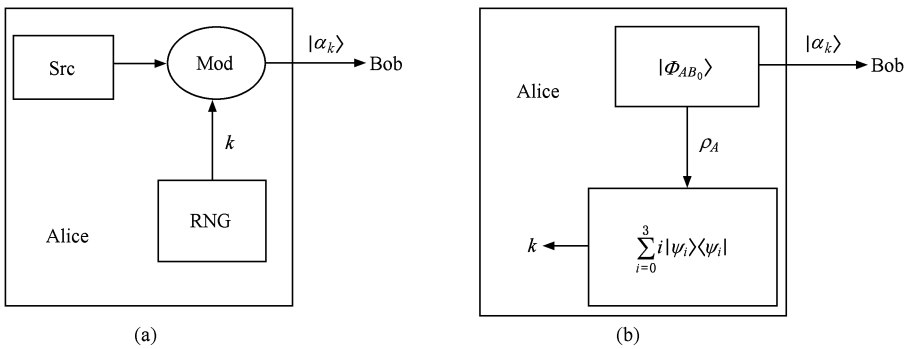

图 1　(a) 四态协议的制备与测量方案(Alice 从随机数发生器(RNG)获得随机数 k,然后通过调制器(Mod)对光源(Src)发出的初始态进行调制);(b) 四态协议的纠缠等价方案(Alice 手中有一个初始的双模纠缠态,她对其中一个模式进行投影测量,获得测量结果为 k,并将另一个分量发送给 Bob)

$$|\Phi_{AB_0}\rangle = \frac{1}{2}\sum_{k=0}^{3} |\psi_k\rangle_A |\alpha_k\rangle_{B_0}, \tag{5}$$

其中

$$|\psi_k\rangle = \sum_{m=0}^{3} \frac{1}{2} e^{-i(1+2k)m\pi/4} |\phi_m\rangle, \tag{6}$$

$$|\phi_m\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_m}} \sum_{n=0}^{\infty} \frac{\alpha^{4n+m}}{\sqrt{(4n+m)!}} (-1)^n |4n+m\rangle, \tag{7}$$

其中

$$\lambda_{0,2} = \frac{1}{2}\exp(-\alpha^2)(\cosh(-\alpha^2) \pm \cos(-\alpha^2)),$$

$$\lambda_{1,3} = \frac{1}{2}\exp(-\alpha^2)(\sinh(-\alpha^2) \pm \sin(-\alpha^2)), \tag{8}$$

很容易验证,不同的 $|\psi_k\rangle$ 之间是相互正交的. 当 Alice 用投影算符 $\sum_{i=0}^{3} i|\psi_i\rangle\langle\psi_i|$ 对自己手中的态进行测量得到结果为 k 时,发送给 Bob 的态就相应塌缩到 $|\alpha_k\rangle$.

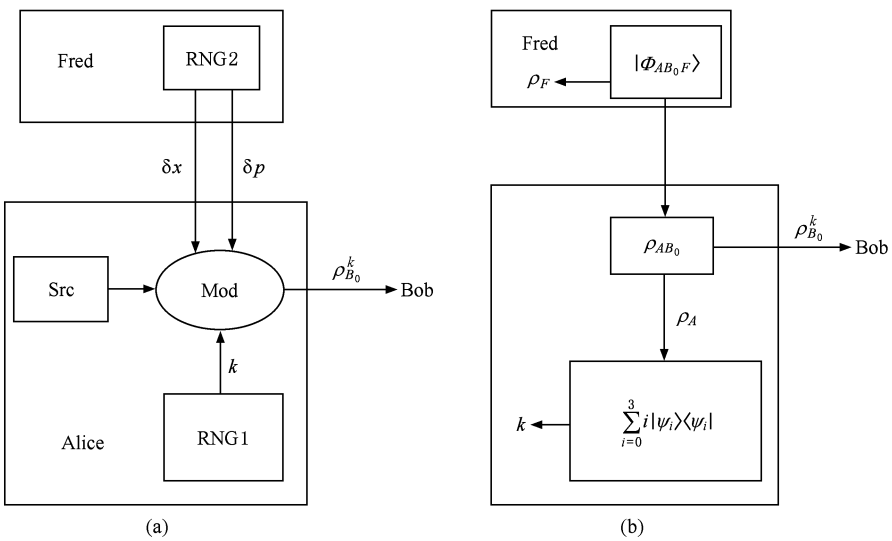

图 2　(a)光源有噪声时四态协议的制备与测量方案(Alice 从随机数发生器(RNG_1)获得随机数 k,然后通过调制器(Mod)对光源(Src)发出的初始态进行调制. Fred 控制 Alice 的调制器,改变其调制结果. 改变量为 Fred 的随机数发生器(RNG_2)产生的随机数 δx 和 δp);(b)光源有噪声时四态协议的纠缠等价方案(Fred 手中有一个三模纠缠态,他保留其中一个模式,将另两个模式发送给 Alice。Aice 对其中一个模式进行投影测量,获得结果为 k,并将另一个模式发送给 Bob)

4. 光源有噪声时的安全性分析

如图 2(a)所示,在制备与测量方案中,由于非理想调制,Alice 每次并不能把一个相干态精确地调制成 $|\alpha_k\rangle$,其 X 分量和 P 分量的中心位置会分别存在 δx 和 δp 的噪声,我们可以假设这个噪声完全是由一个中立者 Fred 引入的,他和 Eve 没有关系,不会给 Eve 提供任何信息. 因此 Alice 制备的并不是纯态 $|\alpha_k\rangle$,而是一个混合态 $\rho_{B_0}^k$. 考虑到对称性,我们不妨假设叠加在 X 分量和 P 分量上的噪声相等,大小为

$$\begin{aligned} D(\delta x) = D(\delta p) &= \mathrm{tr}(\Delta\hat{x}^2\rho_{B_0}^k) \\ &\quad - \langle\alpha_k|\Delta\hat{x}^2|\alpha_k\rangle \\ &= (1+\delta\varepsilon) - 1 = \delta\varepsilon, \end{aligned} \tag{9}$$

其中 1 是由量子力学特性造成的归一化散粒噪声,$\delta\varepsilon$ 是由 Fred 引入的额外噪声.

下面我们给出与之等价的纠缠方案. 如图 2(b)所示,在这个方案中,Alice, Fred 以及发送给 Bob 的三个子系统构成一个纯态,可以写成

$$|\Phi_{AB_0F}\rangle = \frac{1}{2}\sum_{k=0}^{3}|\psi_k\rangle_A|\varphi_{B_0F}^k\rangle, \tag{10}$$

其中 $|\Phi_{B_0F}^k\rangle$ 满足 $\mathrm{tr}_F(|\varphi_{B_0F}^k\rangle\langle\varphi_{B_0F}^k|) = \rho_{B_0}^k$. Alice 用投影算符 $\sum_{i=0}^{3}k|\psi_i\rangle\langle\psi_i|$ 对自己手中的态 ρ_A 进行测量,当 ρ_A 塌缩成 $|\psi_k\rangle$ 时,发送给 Bob 的态就由 ρ_{B_0} 塌缩成 $\rho_{B_0}^k$. 这样在 Eve 看来,这种方案和前面描述的制备和纠缠方案没有区别,因此这两种方案的安全性是等价的,下面我们将只对纠缠等价方案进行讨论.

当 Eve 对发给 Bob 的态进行集体攻击时,她会用一条无损耗、无噪声的信道代替 Alice 和 Bob 之间的信道,然后将 ρ_{B_0} 和自己手中的态 $|\psi_E\rangle$ 进行纠缠,并使得纠缠后的 ρ_{AB} 与未受到攻击且通过有衰减有噪声的信道之后的态相同. 在假设 Eve 的能力足够强时,我们可以认为 Eve 有能力纯化 ρ_{ABF},即总系统 $|\psi_{ABEF}\rangle$ 是一个纯态. 由于 ρ_{ABE} 是一个混合态,我们很难直接计算出 Eve 所获得的信息 $\chi(b:E)$. 但是可以证明,如果 Fred 把自己手中的态交给 Eve,会使得 Eve 获得更多的信息[17],即

$$\chi(b:EF) - \chi(b:E) \geqslant 0, \tag{11}$$

由于 $|\psi_{ABEF}\rangle$ 是一个纯态,我们容易得到 $\chi(b:EF)$. 因此,虽然我们很难直接得到(4)式给出的安全码率,但是我们可以得到安全码率的一个下界,即

$$\tilde{K} = \beta I(a:b) - \chi(b:EF). \tag{12}$$

Bob 对收到的态进行平衡零拍探测,不防假设他对 X 分量进行测量,得到测量结果为 b,测量后他手中的态塌缩成 $\hat{x}$ 的本征态,而 ρ_{AEF} 塌缩成 $|\psi_{AEF}^b\rangle$. 因为 $|\psi_{ABEF}\rangle$ 是一个纯态,可以得到,$S(\rho_{EF}) = S(\rho_{AB})$,又因为 $|\psi_{AEF}^b\rangle$ 也是一个纯态,同样可以得到 $S(\rho_{EF}^b) = S(\rho_A^b)$. 另外,由于 $S(\rho_A^b)$ 的取值与 b 无关,由(2)式和(12)式可得,安全码率的下界为

$$\tilde{K} = \beta I(a:b) - S(\rho_{AB}) + S(\rho_A^b). \tag{13}$$

对于高斯态,von Neumann 熵可以通过协方差矩阵来计算[18]. 设 ρ_{AB}^G 和 ρ_A^G 分别是双模和单模的高斯态,它们的协方差矩阵分别为 γ_{AB}^G 和 γ_A^G,其具体数值可以由实验直接获得,令

$$\gamma_{AB}^G = \begin{bmatrix} A & C \\ C^{\mathrm{T}} & B \end{bmatrix}, \tag{14}$$

其中 A,B,C 都是 2×2 的矩阵,设

$$\begin{aligned} \Delta &= \det A + \det B + 2\det C, \\ s_{1,2} &= \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det(\gamma_{AB})}}{2}}, \end{aligned} \tag{15}$$

则

$$\begin{aligned} S(\rho_{AB}^G) &= g(s_1) + g(s_2), \\ S(\rho_A^G) &= g(\sqrt{\det\gamma_A^G}), \end{aligned} \tag{16}$$

其中

$$\begin{aligned} g(x) &= \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) \\ &\quad - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right). \end{aligned} \tag{17}$$

为了和高斯调制协议进行类比,下面我们计算初始纯态 $|\Phi_{AB_0}\rangle$ 的协方差矩阵 γ_{AB_0}. 归一化到散粒噪声,根据(5)—(8)式容易计算出

$$\gamma_{AB_0} = \begin{pmatrix} (V_A+1)\boldsymbol{I}_2 & Z\boldsymbol{\sigma}_z \\ Z\boldsymbol{\sigma}_z & (V_A+1)\boldsymbol{I}_2 \end{pmatrix}, \tag{18}$$

其中 $Z = \alpha^2(\lambda_0^{3/2}\lambda_1^{-1/2} + \lambda_1^{3/2}\lambda_2^{-1/2} + \lambda_2^{3/2}\lambda_3^{-1/2} + \lambda_3^{3/2}\lambda_0^{-1/2})$,$V_A = \alpha^2$,$\boldsymbol{I}_2$ 为二维单位矩阵,$\sigma_z = \mathrm{diag}(1,-1)$. 这里的 V_A 就是制备与测量方案中 Alice 的调制方差,Z 反映了初始态 $|\Phi_{AB_0}\rangle$ 的纠缠度. 对于处在最大纠缠的 EPR 态,当协方差矩阵中的对角元为 V_A+1 时,非对角元中的 Z 应该替换为 Z_{EPR},$Z_{\mathrm{EPR}} = \sqrt{V_A^2+2V_A}$. 由于 $|\Phi_{AB_0}\rangle$ 并不是最大

纠缠的，所以 $Z < Z_{\mathrm{EPR}}$.

当 Alice 发送给 Bob 的子系统 ρ_{B_0} 通过一个透过率为 T_0，额外噪声为 ε_0 的信道后，ρ_{B_0} 会发生演化变成 ρ_B，很容易得出，此时 ρ_{AB} 的协方差矩阵 γ_{AB} 为[18]

$$\gamma_{AB} = \begin{pmatrix} (V_A + 1)\boldsymbol{I}_2 & \sqrt{T_0}Z\boldsymbol{\sigma}_z \\ \sqrt{T_0}Z\boldsymbol{\sigma}_z & [T_0(V_A + \varepsilon_0 + \delta\varepsilon) + 1]\boldsymbol{I}_2 \end{pmatrix}. \tag{19}$$

根据高斯攻击的最优性，当协方差矩阵相同时（即使在等价的制备与测量方案中 Alice 进行的并不是高斯调制），且 ρ_{AB} 为高斯态时使得 $\tilde{K}$ 达到最小[19]. 因此我们可以认为 ρ_{AB} 是高斯态，这不会对协议的安全性造成影响. 当 Alice 进行高斯调制，信道的透过率为 T，额外噪声为 ε 时，很容易推出在等价的纠缠方案中，Alice 和 Bob 共享混合态的协方差矩阵 γ_{AB}^{G} 为[10]

$$\gamma_{AB}^{G} = \begin{pmatrix} (V_A + 1)\boldsymbol{I}_2 & \sqrt{T}Z_{\mathrm{EPR}}\boldsymbol{\sigma}_z \\ \sqrt{T}Z_{\mathrm{EPR}}\boldsymbol{\sigma}_z & [T(V_A + \varepsilon) + 1]\boldsymbol{I}_2 \end{pmatrix}, \tag{20}$$

其中 $Z_{\mathrm{EPR}} = \sqrt{V_A^2 + 2V_A}$. 令 $\gamma_{AB}^{G} = \gamma_{AB}$ 可以推得

$$T = T_0 \frac{Z^2}{Z_{\mathrm{EPR}}^2},$$

$$\varepsilon = \frac{Z_{\mathrm{EPR}}^2}{Z^2}(V_A + \varepsilon_0 + \delta\varepsilon) - V_A, \tag{21}$$

在信道的透过率和额外噪声相同的情况下，由于离散调制协议的纠缠等价方案中使用的纠缠态并不是最大纠缠，所以协方差矩阵中的 Z 比高斯调制协议中对应的 Z_{EPR} 小. 为了使两个协方差矩阵相等，只能通过降低高斯调制协议中信道的透过率、增大额外噪声来实现，即四态协议中所用的纠缠态由于没有达到最大纠缠，所产生的影响可以等价成信道的衰减和额外噪声. 因此，在协调效率相同的条件下，当信道的透过率为 T_0，额外噪声为 ε_0 时，离散调制协议的安全码率下界与高斯调制协议中信道透过率为 T，额外噪声为 ε 时的安全码率相同，其中 $T < T_0$，$\varepsilon > \varepsilon_0 + \delta\varepsilon$. 在信道透过率很小的情况下，四态协议能达到的协调效率比高斯调制协议的协调效率高很多，因此在长距离通信过程中四态协议有很大的优势.

5. 平衡零拍方案和无开关方案的安全边界

在基于高斯调制的 CV-QKD 协议中，Alice 和 Bob 采用反向协调，Bob 采用平衡零拍探测，信道的透过率为 T，额外噪声为 ε 时，Bob 所接收到的态中的总噪声为[20]

$$\chi = \frac{(1 - T)}{T} + \varepsilon, \tag{22}$$

其中 T，ε 由(21)式定义. Alice 和 Bob 之间的互信息为[20]

$$I(a:b) = \frac{1}{2}\log_2\left(\frac{V + \chi}{\chi + 1}\right), \tag{23}$$

定义

$$A = V^2(1 - 2T) + 2T + [T(V + \chi)]^2, \tag{24}$$

$$B = [T(V\chi + 1)]^2, \tag{25}$$

Eve 能够对 Fred 手中的态进行测量时可以获得的信息为[20]

$$\chi(b:EF) = g(\tau_1) + g(\tau_2) - g(\tau_3), \tag{26}$$

其中

$$\tau_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})},$$

$$\tau_3 = \sqrt{V\frac{1 + V\chi}{V + \chi}}, \tag{27}$$

根据高斯攻击的最优性，这样得到的当信道的透过率和额外噪声分别为 T 和 ε 时基于高斯调制的 CV-QKD 协议的安全码率就是当信道透过率和额外噪声分别为 T_0 和 ε_0、光源噪声为 $\delta\varepsilon$ 时四态协议的安全码率的下界，其中 T 和 ε 由(21)式给出. 通过数值模拟我们可以得到不同透过率和额外噪声所对应的最优调制方差. 以 $\varepsilon_0 + \delta\varepsilon = 0.001$ 为例，假设信息协调的效率为 0.8，信道的衰减为 0.2 dB/km，Bob 的探测效率为 0.6，我们可以得到最优调制方差随距离的变化如图 3 所示. 当调制方差取最优值时我们可以得到安全码率的下界随距离的变化如图 4 所示. 和高斯调制方案不同，四态协议的协调效率在信噪比很低的情况下仍能达到 0.8，因此四态协议的安全传输距离很容易超过目前基于高斯调制的 CV-QKD 协议的极限距离 30 km. 如果能够有效地抑制光源和信道中的额外噪声，那么安全传输距离有望突破 200 km.

在采用平衡零拍探测方案时，Bob 需要随机的选择平衡零拍探测的相位分别进行 X 分量或 P 分

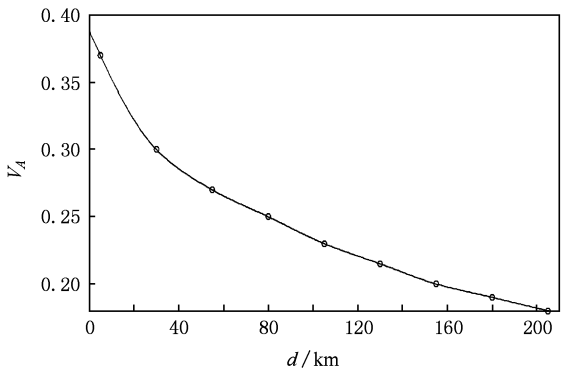

图 3 最优调制方差随距离的变化(其中 ◦为数值模拟时得到的点)

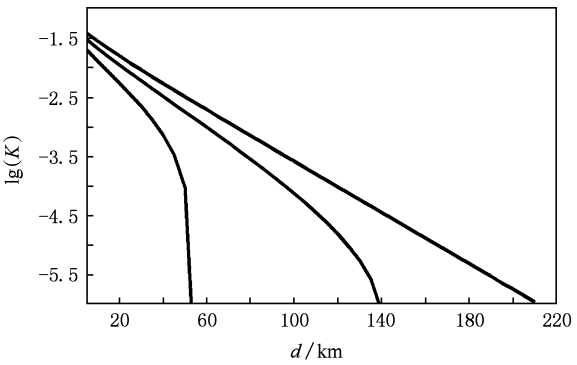

图 4 安全码率的下界随距离的变化,从上到下 $\varepsilon_0+\delta\varepsilon$ 的取值分别为 0.001, 0.005, 0.01

量的测量. 这里,本地振荡光和信号光相对相位的精确控制是一个必备条件,直接决定了通信的安全码率[3],而当光源重复频率很高时这是很难做到的. 为了避免这个问题,这里引入无开关方案[2],在这个方案中 Bob 用一个 50:50 的分束片将信号光分成两束,然后用平衡零拍探测分别测量其中一束的 X 分量和另一束的 P 分量. Bob 测量之前,Alice 和 Bob 共享的态 ρ_{AB} 的协方差矩阵 γ_{AB} 仍然由(20)式给出. 设 $\chi'=\frac{(2-T)}{T}+\varepsilon$, Bob 测量后 Alice 手中的态 ρ_A 塌缩成 ρ_A^b, 容易推得 ρ_A^b 的协方差矩阵 γ_A^b 为

$$\gamma_A^b=\begin{pmatrix}\frac{V\chi'+1}{V+\chi'} & 0\\ 0 & \frac{V\chi'+1}{V+\chi'}\end{pmatrix}. \tag{28}$$

定义

$$\tau'_1=\tau_1,\tau'_2=\tau_2,\tau'_3=\frac{V\chi'+1}{V+\chi'}, \tag{29}$$

与前面类似可以推出 Alice 和 Bob 之间的互信息

$$I'(a:b)=\log_2\left(\frac{V+\chi'}{\chi'+1}\right), \tag{30}$$

Eve 能够对 Fred 手中的态进行测量时可以获得的信息为

$$\chi'(b:EF)=g(\tau'_1)+g(\tau'_2)-g(\tau'_3), \tag{31}$$

这时安全码率的下界为

$$\tilde{K}'=\beta I'(a:b)-\chi'(b:EF). \tag{32}$$

当 $\varepsilon_0+\delta\varepsilon=0.01$ 时,无开关方案的安全码率和平衡零拍探测方案的安全码率下界之差 $\delta K=\tilde{K}'-\tilde{K}$ 如图 5 所示. 在无开关方案中,Bob 对两个分量都进行了测量,看起来似乎码率应该是采用平衡零拍探测时的两倍,但事实上在无开关方案中进行探测之前,Bob 先要将接收到的信号光通过分束片与真空态干涉,这样就引入了附加的噪声,使得 Bob 探测的两个分量比采用平衡零拍时探测的分量含有更多的噪声,因此平均从每个分量上获得的安全码率比采用平衡零拍探测时的都要低,其总的结果只比采用平衡零拍探测时的稍大一点[20]. 但由于无开关方案无需像平衡零拍探测那样对信号光和本地震荡光的相对相位进行快速、精确控制,降低了实验难度.

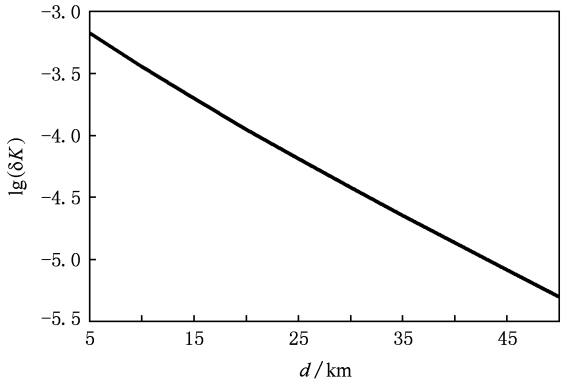

图 5 无开关方案和平衡零拍探测方案的码率之差

6. 结 论

本文根据最新提出的连续变量离散调制方案,首先讨论了非理想调制时四态协议的安全性. 非理想调制引入的噪声可以归结为光源噪声,为了方便计算,这里引入了一个中立者 Fred,假设 Eve 能对 Fred 手中的态进行测量(事实上是不可能的),采用放缩法,得到了其安全码率的下界. 其次,由于四态协议的纠缠等价方案中初始纠缠态没有达到最大

纠缠，导致了其协方差矩阵与高斯调制协议中的协方差矩阵存在微小区别. 本文根据高斯攻击的最优性，将四态协议的安全码率等效于信道透过率更小、额外噪声更大的高斯调制协议的安全码率，得到了四态协议安全码率的下界，从而证明这种新的协议是安全的. 最后，本文还将无开关协议和四态协议相结合，计算结果表明采用无开关方案的安全码率与平衡零拍探测方案相当. 但无开关方案比平衡零拍探测方案更容易实现，因此在实验上更有优势.

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

[2] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2004 *Phys. Rev. Lett.* **93** 170504

[3] Grosshans F, Van Assche G, Wenger J, Tualle-Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238

[4] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C, Lam P K 2005 *Phys. Rev. Lett.* **95** 180503

[5] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev.* A **76** 042305

[6] Qi B, Huang L L, Qian L, Lo H K 2007 *Phys. Rev.* A **76** 052323

[7] Zhu C H, Pei C X, Quan D X, Chen N, Yi Y H 2009 *Acta Phys. Sin.* **58** 2184 (in Chinese) [朱畅华、裴昌幸、权东晓、陈　南、易运晖 2009 物理学报 **58** 2184]

[8] Lodewyck J, Debuisschert T, Tualle-Brouri R, Grangier P 2005 *Phys. Rev.* A **72** 050303

[9] Chen J J, Hua Z F, Zhao Y B, Gui Y Z, Guo G C 2007 *Acta Phys. Sin.* **56** 5 (in Chinese) [陈进建、韩正甫、赵义博、桂有珍、郭光灿 2007 物理学报 **56** 5]

[10] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504

[11] Renner R, Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504

[12] Leverrier A, Karpov E, Grangier P, Cerf N J www. arxiv. org/pdf/quant-ph/0809. 2252

[13] Renner R, König R www. arxiv. org/pdf/quant-ph/0403133

[14] Bloch M, Thangaraj A, McLaughlin S W www. arxiv. org/pdf/cs. IT/0509041

[15] Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P 2008 *Phys. Rev.* A **77** 042325

[16] Grosshans F, Cerf N J 2003 *Quantum Inf. Comput.* **3** 535

[17] Shen Y, Yang J, Guo H 2009 *J. Phys.* B **42** 235506

[18] Serafini A, Illuminati F, De Siena S 2004 *J. Phys.* B **37** L21

[19] García-Patrón R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[20] Scarani V, Pasquinucci H B, Cerf N J, Dušek M, Lütkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301

Security bound of continuous-variable quantum key distribution with discrete modulation*

Shen Yong Zou Hong-Xin†

(*Department of Physics*, *National University of Defense Technology*, *Changsha* 410073, *China*)

(Received 8 May 2009; revised manuscript received 22 June 2009)

Abstract

Security of continuous-variable quantum key distribution with four-state protocol based on discrete modulation of noisy coherent states is analyzed. Combing discrete modulation and reverse reconciliation, this protocol can be used for long distance cryptography. There is a small difference between the state Alice sends in the discrete modulation protocol and the Gaussian modulation protocol, and it can be treated as excess noise and loss in the channel. As Alice cannot do a precise modulation, she will induce noise to the coherent state. We look this noise as the source noise and derive a lower bound to the secure key rate assuming the eavesdropper cannot benefit from the noise in the source. For avoiding the fast and random phase locking between the signal and local oscillator in experiment, we also analyze the security of four-state protocol using no-switching scheme.

Keywords: discrete modulation, the four-state protocol, continuous variable quantum key distribution, secure key rate

PACC: 0367, 4250

* Project supported by the Science Research Program of National University of Defense Technology, China (Grant No. JC08 – 02 – 01), the National Natural Science Foundation of China (Grant No. 10904174), and the Opening Research Foundation of State Key Laboratory of Precision Spectroscopy, ECNU.

† E-mail: hxzou@nudt.edu.cn