激光与光电子学进展

基于离散调制的三态连续变量量子密钥分发协议的安全性分析

孙游东，邢永鑫，王天一*

贵州大学大数据与信息工程学院，贵州 贵阳 550025

摘要 目前，基于离散调制的连续变量量子密钥分发(Continuous-Variable Quantum Key Distribution，CV-QKD)协议受到越来越多的关注。提出了一种基于后选择的三态CV-QKD协议，在集体攻击和反向协调的条件下推导了三态CV-QKD协议的安全码率公式，并与四态CV-QKD协议进行了性能比较。数值仿真结果表明，当传输距离较短时，三态CV-QKD协议能够获得高于四态CV-QKD协议的安全码率，这说明三态CV-QKD协议更适用于城域网等规模较小的密钥分发场景。

关键词 量子光学；量子密钥分发；连续变量；离散调制；三态协议；后选择

中图分类号 O431.2 **文献标志码** A **doi**：10.3788/LOP202158.0727004

Security Analysis of Three-State Continuous Variable Quantum Key Distribution Protocol Based on Discrete Modulation

Sun Youdong, Xing Yongxin, Wang Tianyi*

College of Big Data and Information Engineering, Guizhou University, Guiyang, Guizhou 550025, *China*

Abstract At present, the continuous-variable quantum key distribution (CV-QKD) protocol based on discrete modulation has received more attention. In this paper, we propose a three-state CV-QKD protocol based on post-selection. The security key rate of the proposed protocol is calculated under collective attack and reverse reconciliation and compared with that of the four-state protocol. The simulation results show that the proposed three-state protocol can outperform the four-state protocol in security rate if the transmission distance is not too long, indicating that the three-state protocol is more feasible for a short-range application, such as metropolitan area networks.

Key words quantum optics; quantum key distribution; continuous variable; discrete modulation; three-state protocol; post-selection

OCIS codes 270.5565; 060.5565; 270.5568; 270.5585

1 引 言

量子密钥分发(Quantum Key Distribution，QKD)是一种新的通信技术[1-2]，它利用量子物理的特性提高通信双方的保密性。根据技术路径的不同，QKD可以分为连续变量量子密钥分发(Continuous-Variable Quantum Key Distribution，CV-QKD)和离散变量量子密钥分发(Discrete-Variable Quantum Key Distribution，DV-QKD)两类。基于单光子的DV-QKD受技术条件的限制，目前单光子态的检测和制备还存在很大的难度。相比之下，基于相干态的CV-QKD能够与现有的光纤

收稿日期：2020-08-07；**修回日期**：2020-09-17；**录用日期**：2020-09-23

***E-mail**：tywang@gzu.edu.cn

通信器件及网络兼容，具有易实现、成本低的优势，受到了研究者的广泛关注。龚峰等[3]提出了一种利用光放大器改进自参考连续变量量子密钥分发协议的改进方案，该方案较好地补偿了参考脉冲引入的相位噪声的影响。黄彪等[4]针对基于本地本振光的连续变量量子密钥分发协议中参考脉冲传输带来的安全性问题，提出了篡改参考脉冲相位的攻击方法以及监听相位补偿噪声方差的相位攻击探测方法。马识途等[5]研究了基于双边类型低密度奇偶校验码的连续变量量子密钥分发协议的性能。

根据相干态调制方法的不同，CV-QKD 协议又可以分为两种类型，分别是高斯调制协议[1,6]和离散调制协议[7]。高斯调制 CV-QKD 协议的安全性分析可以借助纠缠等价模型[8]和高斯最优定理[9-10]实现，发展较为成熟。相比之下，目前对离散调制 CV-QKD 协议安全性的研究尚不够充分，且绝大多数工作都是针对四态协议进行的[11]，关于离散调制三态协议安全性的讨论很少。2017 年，Bradler 等[12]提出了三态协议安全性分析方案，但是使用的分析方法比较复杂，难以推广。

本文对基于离散调制的三态 CV-QKD 协议在纠缠克隆攻击和反向协调[13]下的安全性进行了分析，从理论上评估了三态协议的安全码率并通过数值仿真对结果进行了计算。仿真结果表明：当传输距离较短时，三态协议能够取得高于常见四态协议的安全码率。

2　三态 CV-QKD 协议

三态协议在相空间上的编码方案如图 1 所示[14]。由于光场的湮灭算符 $\hat{a}^{\dagger}$ 和产生算符 $\hat{a}$ 都不是厄米算符，为了便于对光场进行测量，两个正交分量算符 $\hat{x}$ 和 $\hat{p}$ 被定义为

$$\begin{cases} \hat{x}=\dfrac{\hat{a}+\hat{a}^{\dagger}}{2} \\ \hat{p}=\dfrac{\hat{a}-\hat{a}^{\dagger}}{2\mathrm{i}} \end{cases}。 \tag{1}$$

利用(1)式可以将相空间用平面直角坐标系表示，其中 x、p 分别表示横、纵坐标，也就是 $\hat{x}$ 和 $\hat{p}$ 两个正交分量的取值，如图 1 所示，“1”和“0”代表与 Bob 基相关联的 Alice 的位编码。在发送端，Alice 发送相干态 $|S\rangle=\left|\alpha'\exp(\mathrm{i}\phi_{\mathrm{A}})\right\rangle$，其中 $\phi_{\mathrm{A}}\in\left\{0,2\pi/3,4\pi/3\right\}$，$\alpha'=2/\sqrt{3}\,\alpha$，$\alpha$ 为调制方差，$\alpha>0$。在接收端，Bob 通过随机选择相位 ϕ_{B} 来测量正交分量，测量结果可以表示为

$$x\left(\phi_{\mathrm{B}}\right)=x\cos\phi_{\mathrm{B}}+p\sin\phi_{\mathrm{B}}, \tag{2}$$

式中：$\phi_{\mathrm{B}}\in\left\{\pi/2,-\pi/6,-5\pi/6\right\}$。如表 1 所示，只有利用基于(2)式计算出的测量值的正负才能进一步完成 Alice 的编码。

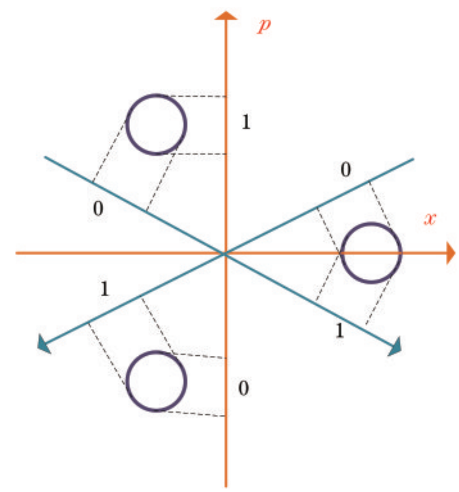

图 1　三态协议的相空间示意图

Fig. 1　Phase space diagram of three-state protocol

此三态协议包括以下 8 个步骤。1) Alice 发送一个量子态 $|S\rangle$ 给 Bob。2) Bob 使用随机选择的 x 基或 p 基对接收到的状态进行测量。3) Alice 和 Bob 重复步骤 1)、2)多次。4)Alice 通过经典信道公布每个过程所使用的基并随机公布部分状态。5) Bob 使用 Alice 公布的数据来估算量子信道的参数，并根据自己的测量结果和估计的信道参数选择用于密钥生成的数据。Bob 仅使用正确的测量基组。在此定义当 $(\left|\phi_{\mathrm{B}}-\phi_{\mathrm{A}}\right| \bmod \pi)\neq\dfrac{\pi}{2}$ 时，组合 $(\phi_{\mathrm{A}},\phi_{\mathrm{B}})$ 为错误的测量基组，否则为正确的测量基组。然后 Bob 通知 Alice 他选择的测量基。在理论分析中，我们假设 Bob 还揭示了其结果 m 的绝对值 $|m|$。6)Bob 为所选测量值 m 的负值分配 0、为正值分配 1 以制作位串。7)如表 1 所示，Alice 为 $-\alpha$ 分配“0”、为 α 分配“1”以生成字符串。8)Alice 和 Bob 通过对所获得的位串进行纠错和隐私放大来共享安全密钥。在表 1 中，$\langle x\rangle$ 表示 Bob 测量正交分量的测量结果；A 表示 Alice 为测量值 $\langle x\rangle$ 所分配的二进制数值，其中正值被分配为“1”，负值被分配为“0”，测量值为 0 时则不计。

假设量子信道不是理想的，其特征由过量噪声 ξ 和信道透射率 η 描述，可以得出以 S 为条件的 m 的概率密度[15]为

表 1 三态协议的 Alice 位编码

Table 1 Alice's bit encoding in three-state protocol

Result	$\phi_A=0$, $\phi_B=\pi/2$	$\phi_A=0$, $\phi_B=-\pi/6$	$\phi_A=0$, $\phi_B=-5\pi/6$	$\phi_A=2\pi/3$, $\phi_B=\pi/2$	$\phi_A=2\pi/3$, $\phi_B=-\pi/6$	$\phi_A=2\pi/3$, $\phi_B=2\pi/3$	$\phi_A=4\pi/3$, $\phi_B=\pi/2$	$\phi_A=4\pi/3$, $\phi_B=-\pi/6$	$\phi_A=4\pi/3$, $\phi_B=-5\pi/6$
$\langle x\rangle$	0	α	$-\alpha$	α	$-\alpha$	0	$-\alpha$	0	α
A		1	0	1	0		0		1

$$P(m|S)=\sqrt{\frac{2}{\pi(1+\xi)}}\exp\left[-2\frac{\left(m-\sqrt{\eta}\,S\right)^2}{1+\xi}\right],\tag{3}$$

式中:真空噪声方差为1/4。

概率 ε 被定义为 Alice 发送 0 或 1 而 Bob 收到 1 或 0 的概率,简称为误码率(BER),即

$$\varepsilon=\left[1+\exp\left(8\frac{\sqrt{\eta}}{1+\xi}|m|\alpha\right)\right]^{-1}。\tag{4}$$

因此,根据 Shannon 公式,Alice 和 Bob 之间的互信息 I_{AB} 可表示为

$$I_{AB}=1-h(\varepsilon),\tag{5}$$

式中:$h(\varepsilon)=-\varepsilon\,\mathrm{lb}\,\varepsilon-(1-\varepsilon)\,\mathrm{lb}(1-\varepsilon)$是二元熵。

3 集体攻击

如图 2 所示,假设量子信道是高斯型,在协议的每次运行中,Eve 都会准备一份双模压缩真空(EPR)态,并从中选出一对 EPR 态放在 Alice 发送给 Bob 的态中以进行干扰。Eve 将自己的状态保存在量子记忆中,并对自己保持的状态进行集体攻击,获得了有关 Alice 和 Bob 共享的比特序列的信息。再考虑针对集体攻击协议的密钥率。当量子信道是对称的并且是高斯型时,所有集体攻击都被认为是酉等价的[16]。因此,下面我们计算对抗纠缠克隆攻击的安全密钥率。

对于纠缠克隆攻击,Eve 准备了模式为 E_1 和 E_2 的 EPR 态:

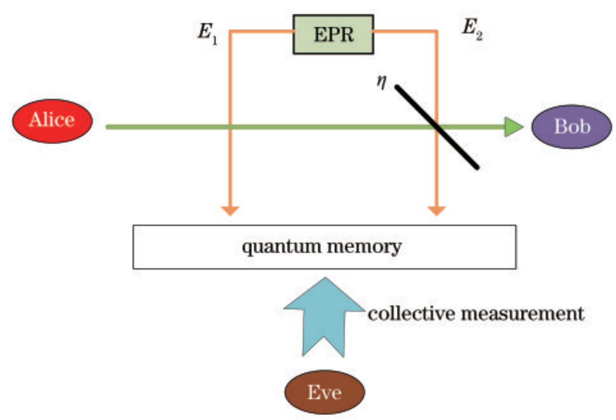

图 2 纠缠克隆攻击的示意图

Fig. 2 Schematic of entangled clone attack

$$|E_{EPR}\rangle=\sqrt{\frac{\pi}{2}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\,\mathrm{d}x_2\exp\left(-Vx_1^2-x_2^2/V\right)\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\frac{x_1-x_2}{\sqrt{2}}\right\rangle_{E_2},\tag{6}$$

式中:x_i 为正交算子,$i=0,1$;$|x\rangle_{E_i}$ 为模式 E_i 的特征向量;参数 $V\geqslant 1$,且满足

$$\frac{1}{2}\left(V+\frac{1}{V}\right)=\frac{1-\eta+\xi}{1-\eta}。\tag{7}$$

相干态$|S\rangle$表示为

$$|S\rangle=\left(\frac{2}{\pi}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\mathrm{d}x\exp\left[-(x-s)^2\right]|x\rangle。\tag{8}$$

由于透射率为 η 的分束器变换为

$$|x\rangle_A|x_2\rangle_{E_2}\rightarrow\left|\sqrt{\eta}\,x-\sqrt{1-\eta}\,x_2\right\rangle_A\left|\sqrt{1-\eta}\,x+\sqrt{\eta}\,x_2\right\rangle_{E_2},\tag{9}$$

将 $m=\sqrt{\eta}\,x-\sqrt{1-\eta}\left(x_1-x_2\right)/\sqrt{2}$ 代入(8)式与(6)式中,可以得到

$$|x\rangle_A\left|\frac{x_1-x_2}{\sqrt{2}}\right\rangle_{E_2}\rightarrow|m\rangle_A\left|\sqrt{\frac{1-\eta}{\eta}}\,m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}。\tag{10}$$

由于模式 E_1 不需要分束器变换,因此最后整合(6)、(8)、(10)式,得出了最终的整合干扰模式为

$$\left|\varphi(S,\mathrm{m})\right\rangle=\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\,\mathrm{d}x_2\,\varphi(S,m)\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2},\tag{11}$$

这里

$$\varphi(S,m)=\exp\left\{-\left[\sqrt{\frac{1-\eta}{\eta}(x_1-x_2)}+\frac{m}{\sqrt{\eta}}-S\right]^2-Vx_1^2-x_2^2/V\right\}。\tag{12}$$

注意$\left|\varphi(S,m)\right\rangle$具有以下归一性

$$\left\langle\varphi(S,m)\middle|\varphi(S,m)\right\rangle=P(m/S)。\tag{13}$$

为了后面计算方便，我们引入

$$\left|e_{ij}\right\rangle=N\left|\varphi\left[(-1)^i|S|,\varphi(-1)^j|m|\right]\right\rangle,\tag{14}$$

式中：i, j=0,1并且N是一个依赖于i, j的归一化因子。具体表达式分别为

$$\begin{cases}\left|e_{00}\right\rangle=N\left\{\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\mathrm{d}x_2\exp\left\{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{|m|}{\sqrt{\eta}}-|s|\right]^2-Vx_1^2-x_2^2/V\right\}\times\right.\\\qquad\left.|m\rangle_{\mathrm{A}}\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}\right\}\\\left|e_{01}\right\rangle=N\left\{\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\mathrm{d}x_2\exp\left\{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{-|m|}{\sqrt{\eta}}-|s|\right]^2-Vx_1^2-x_2^2/V\right\}\times\right.\\\qquad\left.|m\rangle_{\mathrm{A}}\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}\right\}\\\left|e_{10}\right\rangle=N\left\{\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\mathrm{d}x_2\exp\left\{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{|m|}{\sqrt{\eta}}+|s|\right]^2-Vx_1^2-x_2^2/V\right\}\times\right.\\\qquad\left.|m\rangle_{\mathrm{A}}\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}\right\}\\\left|e_{11}\right\rangle=N\left\{\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\mathrm{d}x_1\mathrm{d}x_2\exp\left\{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{-|m|}{\sqrt{\eta}}+|s|\right]^2-Vx_1^2-x_2^2/V\right\}\times\right.\\\qquad\left.|m\rangle_{\mathrm{A}}\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}\right\}\end{cases}。\tag{15}$$

假设Bob对模式A执行x基测量，并得到结果m。在这种情况下，对于反向协调(RR)，Eve攻击Bob的目的是估计他的比特。则有

$$\begin{cases}\boldsymbol{\rho}_{\mathrm{B}}^0=(1-\varepsilon)\left|e_{00}\right\rangle\left\langle e_{00}\right|+\varepsilon\left|e_{10}\right\rangle\left\langle e_{10}\right|\\\boldsymbol{\rho}_{\mathrm{B}}^1=(1-\varepsilon)\left|e_{11}\right\rangle\left\langle e_{11}\right|+\varepsilon\left|e_{01}\right\rangle\left\langle e_{01}\right|\end{cases},\tag{16}$$

式中：$\boldsymbol{\rho}_{\mathrm{B}}^0$和$\boldsymbol{\rho}_{\mathrm{B}}^1$分别为Bob端测量值为0和1时的密度矩阵。

Eve的可访问信息χ受Holevo界[17]的影响，其通式为

$$\chi=S(\boldsymbol{\rho})-S(\boldsymbol{\rho}_{\mathrm{B}}^0)/2-S(\boldsymbol{\rho}_{\mathrm{B}}^1)/2,\tag{17}$$

式中：$\boldsymbol{\rho}=(\boldsymbol{\rho}_{\mathrm{B}}^0+\boldsymbol{\rho}_{\mathrm{B}}^1)/2$，且$S(\boldsymbol{\rho})=-\mathrm{Tr}(\boldsymbol{\rho}\,\mathrm{lb}\,\boldsymbol{\rho})=-\sum_k n_k\,\mathrm{lb}\,n_k$表示冯·诺依曼熵[18]，其中$n_k$为密度矩

阵$\boldsymbol{\rho}$所对应的特征值，k为有限维希尔伯特空间上的一组正交基。

根据冯·诺依曼熵的定义可知，为了求出(17)式中的χ，我们将算出(17)式中所有密度矩阵的特征值。根据Leverrier等[19]的证明，通过Gramian矩阵可以轻松找到其特征值。

对于$\boldsymbol{\rho}_{\mathrm{B}}^{i}$，其Gramian矩阵表示为

$$\boldsymbol{G}=\begin{bmatrix}1-\varepsilon & \delta t\\ \delta t & \varepsilon\end{bmatrix},\tag{18}$$

计算公式分别为

$$t=\left\langle e_{00}\middle|e_{10}\right\rangle=\left\langle e_{11}\middle|e_{01}\right\rangle=\exp\left(-2\frac{1+\xi-\eta}{1+\xi}\alpha^{2}\right),\tag{19}$$

$$\delta=\sqrt{\varepsilon(1-\varepsilon)},\tag{20}$$

所以其特征值为

$$\frac{1}{2}\left[1\pm\sqrt{1-4\delta^{2}(1-t)^{2}}\right]。\tag{21}$$

由于(21)式与m无关，因此有

$$S\left(\boldsymbol{\rho}_{\mathrm{B}}^{0}\right)=S\left(\boldsymbol{\rho}_{\mathrm{B}}^{1}\right)。\tag{22}$$

对于$\boldsymbol{\rho}$，有

$$\boldsymbol{G}=\begin{bmatrix}1-\varepsilon & \delta s & \delta t & (1-\varepsilon)stu\\ \delta s & \varepsilon & \varepsilon st/u & \delta t\\ \delta t & \varepsilon st/u & \varepsilon & \delta s\\ (1-\varepsilon)stu & \delta t & \delta s & 1-\varepsilon\end{bmatrix},\tag{23}$$

计算公式分别为

$$s=\left\langle e_{00}\middle|e_{01}\right\rangle=\left\langle e_{11}\middle|e_{10}\right\rangle=\exp\left[-2\frac{\xi(2+\xi)}{1+\xi}m^{2}\right],\tag{24}$$

$$u=\exp\left(4\frac{\xi\sqrt{\eta}}{1+\xi}\alpha|m|\right)。\tag{25}$$

求出(23)式的特征值为

$$\begin{cases}\dfrac{1}{4u}\left(v_{+}\pm\sqrt{v_{+}-w_{+}}\right)\\ \dfrac{1}{4u}\left(v_{-}\pm\sqrt{v_{-}+w_{-}}\right)\end{cases},\tag{26}$$

计算公式分别为

$$v_{\pm}=u\pm st\left[\varepsilon+(1-\varepsilon)u^{2}\right],\tag{27}$$

$$w_{\pm}=4\delta^{2}u\left[st(1-u)^{2}\pm\left(1-s^{2}\right)\left(1-t^{2}\right)u\right]。\tag{28}$$

4　安全码率及其仿真结果

前面已经给出了Alice和Bob之间的互信息I_{AB}以及Eve的可访问信息χ，现在可以直接给出三态CV-QKD协议的安全码率公式为

$$K=\eta_{\mathrm{pr}}\left(I_{\mathrm{AB}}-\chi\right),\tag{29}$$

式中：η_{pr}为协议的效率，由表1可以轻易得出三态协议下的协议效率$\eta_{\mathrm{pr}}=2/3$。

基于上述推导出的三态协议的安全码率表达式，我们对其进行了数值仿真分析，并将它与相同情况下的四态协议的安全码率仿真图进行了比较。在光纤信道中，信道透射率η表征了光信号在信道中的衰减，其与传输距离L(km)之间的对应关系为$\eta=10^{-\tau L/10}$，其中τ为光纤损耗系数，$\tau=0.2\ \mathrm{dB}\cdot\mathrm{km}^{-1}$。本文主要绘制了在反向协调以及集体攻击下基于离散调制的三态协议及其安全码率在不同过量噪声ξ下的曲线图，其中协议效率$\eta_{\mathrm{pr}}=2/3$。协议在不同过量噪声下的安全码率如图3所示，其中粗线表示三态协议的安全码率，细线表示相同情形下四态协议的安全码率。

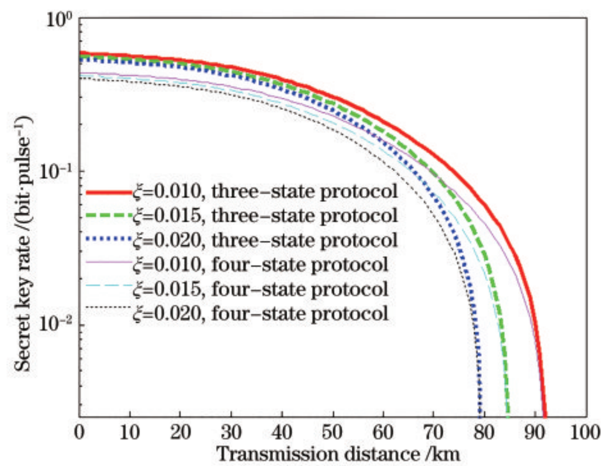

图3　三态协议和四态协议在不同过量噪声下的安全码率

Fig. 3　Security key rates of three-state protocol and four-state protocol under different excess noises

图3显示了三态协议在不同过量噪声下的安全码率。在小于30 km的短距离内，这三种情况并没有太大的区别。但是在大于30 km远距离的情况下，三态协议的性能随着过量噪声的增大而显著变弱，如同高斯调制的CV-QKD所示[13]。而与四态协议比较发现，在相同情况下三态协议的性能要优于四态协议，在最远传输距离上两者并没有明显的差别。但是在传输距离相同的情况下，三态协议的安全码率明显要高于四态协议，这点在小于30 km的近距离内表现尤为明显。仿真结果与理论预测结果相符，因为三态协议的协议效率2/3是高于四态协议效率1/2的。所以在小于30 km的短距离内，安全码率是接近1的高码率，协议效率对其的影响

要远大于远距离情况。

对不同调制方差下的三态协议性能进行了比较，结果如图4所示，可以明显看到，随着调制方差的增大，协议的性能明显下降。所以从理论上来说，调制方差越小，三态协议的性能就越好，因为离散调制的调制方差更小时，协议的概率分布更加接近高斯分布，安全码率更高。如图4所示，当调制方差 α 小于0.1时，协议的性能并没有多大的提升，而且当调制方差过小时，Alice和Bob之间的误码率 ε 会增大，从而影响其安全码率。所以这里认为，当调制方差取0.1时就能得三态协议的最佳性能。

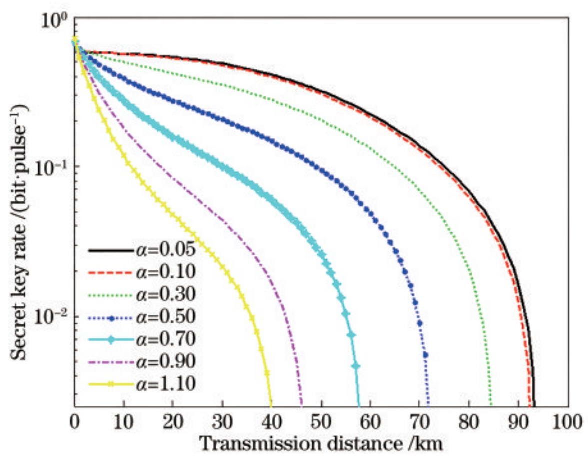

图4　不同调制方差下三态协议的性能比较

Fig. 4　Performance comparison of three-state protocols under different modulation variances

不同过量噪声下三态协议的安全码率随调制方差的变化情况如图5所示，其中Alice和Bob之间的传输距离设置为30 km。由图5可知，当调制方差接近1时，其安全码率下降得最快。从整体上看，安全码率随着调制方差的增大而呈现出先下降再上升的趋势，当调制方差大约为1.2时，安全码率存在一个最小值。这是由于当调制方差在1.2附近时，Bob端的测量值 m 和调制方差 α 的值最为接近，因此Alice和Bob之间的误码率 ε 增大，从而安全码率降低。结合图4也可以验证，当调制方差在0～1.2区间时，0.1是其性能的最佳点。

5　结　　论

分析了基于后选择的离散三态调制CV-QKD协议的安全性，给出了协议的密钥率公式。通过数值仿真，计算出三态协议的安全码率与过量噪声抗

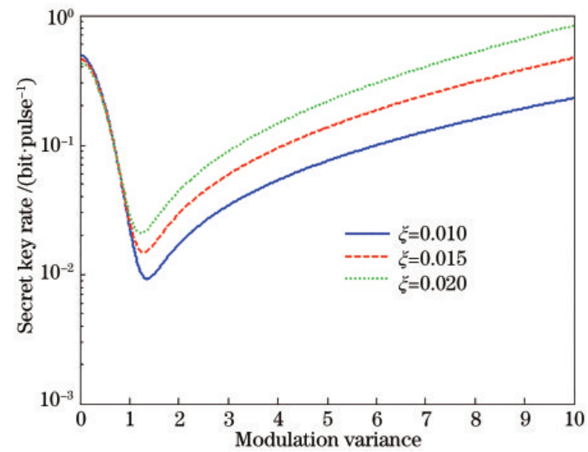

图5　不同过量噪声下三态协议安全码率随调制方差的变化

Fig. 5　Security key rate of three-state protocol versus modulation variance under different excess noises

性。仿真结果表明，当调制方差与传输距离相同时，三态协议的安全码率要高于四态协议。在未来的工作中，将考虑实际实验环境下的非理想因素对三态协议的影响。

参　考　文　献

[1] Bennett C, Brassard G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560(1): 7-11.

[2] Ekert A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.

[3] Gong F, Yang X, Wang T Y. Improvement of self-referenced continuous variable quantum key distribution using optical amplifier[J]. Laser & Optoelectronics Progress, 2019, 56(21): 212702.
龚峰，杨鑫，王天一. 利用光放大器改进自参考连续变量量子密钥分发[J]. 激光与光电子学进展，2019, 56(21): 212702.

[4] Huang B, Huang Y M, Peng Z M. Attack and detection on reference-pulse phase of continuous-variable quantum-key distribution[J]. Acta Optica Sinica, 2019, 39(11): 1127001.
黄彪，黄永梅，彭真明. 连续变量量子密钥分发的参考脉冲相位攻击与探测[J]. 光学学报，2019, 39(11): 1127001.

[5] Ma S T, Guo D B, Xue Z, et al. Multidimensional reconciliation for continuous-variable quantum key distribution based on two-edge type low-density parity-check codes[J]. Acta Optica Sinica, 2019, 39(5): 0527001.

马识途，郭大波，薛哲，等．基于双边类型低密度奇偶校验码的连续变量量子密钥分发多维数据协调[J]．光学学报，2019，39(5)：0527001.

[6] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states[J]. Physical Review Letters, 2002, 88(5): 057902.

[7] Shen Y, Zou H, Tian L, et al. Experimental study on discretely modulated continuous-variable quantum key distribution[J]. Physical Review A, 2012, 82(2): 022317.

[8] Grosshans F, Cer N J, Wenger J, et al. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables[J]. Quantum Information and Computation, 2003, 3: 535-552.

[9] Garcia-Patron R, Cerf N J. Unconditional optimality of Gaussian attacks against continuous variable quantum key distribution[J]. Physical Review Letters, 2006, 97(19): 190503.

[10] Navascues M, Grosshans F, Acin A. Optimality of Gaussian attacks in continuous-variable quantum cryptography[J]. Physical Review Letters, 2006, 97(19): 190502.

[11] Hirano T, Ichikawa T, Matsubara T, et al. Implementation of continuous-variable quantum key distribution with discrete modulation[J]. Quantum Science and Technology, 2017, 2(2): 024010.

[12] Bradler K, Weedbrook C. A security proof of continuous-variable QKD using three coherent states[J]. Physical Review A, 2017, 97(2): 022310.

[13] Grosshans F, Assche G V, Wenger J, et al. Quantum key distribution using gaussian-modulated coherent states[J]. Nature, 2003, 421: 238-241.

[14] Namiki R and Hirano T. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection[J]. Physical Review A, 2006, 74(3): 032302.

[15] Symul T, Alto D J, Assad S M, et al. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise[J]. Physical Review A, 2007, 76(3): 030303.

[16] Heid M, Lütkenhaus, Norbert. Security of coherent state quantum cryptography in the presence of Gaussian noise[J]. Physical Review A, 2009, 76(2): 022313.

[17] Holevo A S. Bounds for the quantity of information transmittable by a quantum communications channel[J]. Problems of Information Transmission, 1973, 9(3): 177–183.

[18] Panagiotis P, Cosmo L, Christian W, et al. Quantum key distribution with phase-encoded coherent states: asymptotic security analysis in thermal-loss channels[J]. Physical Review A, 2018, 98(1): 012340.

[19] Leverrier A, Grangier P. Erratum: unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation[J]. Physical Review Letters, 2009, 106(25): 259902.