线性光学克隆机改进的离散极化调制连续变量量子密钥分发可组合安全性分析*

贺英 王天一† 李莹莹

(贵州大学大数据与信息工程学院, 贵阳 550025)

(2024 年 8 月 5 日收到; 2024 年 10 月 28 日收到修改稿)

在连续变量量子密钥分发的实验系统中, 由于调制器受限于分辨率有限的驱动电压, 理想的高斯调制会退化成离散极化调制, 进而引发系统性能的下降. 本文提出并研究了线性光学克隆机改进的离散极化调制连续变量量子密钥分发方案. 在接收端插入线性光学克隆机能够有效地补偿由幅度和相位离散化产生的综合效应所造成的系统性能损失, 实现整体性能的提升. 本文推导出了所提方案在非理想外差探测下可组合安全密钥率的表达式, 并进行数值仿真. 仿真结果表明, 所提方案不仅能够通过灵活调谐线性光学克隆机的相关参数, 优化安全密钥率、提升过量噪声抗性, 还能有效克服有限码长效应对安全性的影响, 为推动连续变量量子密钥分发的实用化发展提供了切实有效的方法.

关键词: 量子密钥分发, 连续变量, 离散极化调制, 线性光学克隆机

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20241094

CSTR: 32037.14.aps.73.20241094

1 引 言

量子密钥分发 (quantum key distribution, QKD) 基于量子力学基本原理在理论上为远程通信双方之间共享信息安全的密钥提供了一种前景广阔的解决方案 [1,2], 已成为一种可行的网络安全技术, 是最有希望实现商业化的量子通信协议之一 [3,4]. 连续变量量子密钥分发 (continuous variable quantum key distribution, CVQKD) 得益于承载密钥信息的相干态易于制备、可利用相干光电信系统中的组件来构建系统、便于芯片的集成等优势, 近年来受到广泛关注 [5–8], 在安全性证明 [9,10]、实验实现 [11–15], 以及方案改进与性能提升 [16–19] 等方面已经取得了较大的进展.

在 CVQKD 的实验实现中, 正交分量的高斯调制通常通过独立调制相干态的幅度和相位实现 [20]. 然而, 光电调制器电压的有限分辨率特性将导致调制离散化效应的出现, 即原本服从瑞利分布的连续幅度和服从均匀分布的连续相位均退化为离散输出 [21–23], 两者的耦合导致理想的高斯调制退化为离散极化调制 (discretized polar modulation, DPM)[24,25]. 调制离散化效应会造成调制后的正交分量取值偏离真实值, 其影响在制备-测量模型中可以通过正交分量取值的波动表示, 在纠缠等效模型中可以建模为光源端的可信过量噪声 [24].

虽然 DPM-CVQKD 依然能够实现密钥分发, 但其安全密钥率和传输距离相较于理想高斯调制的 CVQKD 都会有所下降. 为补偿实际物理场景下的调制离散化效应, 本文使用线性光学克隆机 (linear optics cloning machine, LOCM) 对 DPM-CVQKD 进行改进, 在考虑实际探测器的情况下,

* 国家自然科学基金 (批准号: 62361009) 和贵州省科技计划 (批准号: 黔科合基础-ZK[2021] 一般 304) 资助的课题.

† 通信作者. E-mail: tywang@gzu.edu.cn

提出了 LOCM 改进的 DPM-CVQKD 方案 (LOCM DPM-CVQKD), 应用 LOCM 实现可控的放大增益, 进而弥补 DPM 带来的性能下降. LOCM 由线性光学、外差探测, 以及可控位移构成, 被置于接收方一侧 [26,27]. 它借助本征相关性可以生成量子态的近似克隆, 从而代替了传统方案中利用高强度光源泵浦的非线性介质 [28]. 这不仅实现了可控的放大增益, 而且还降低了对高强度光源的依赖, 但其代价则是引入更多的过量噪声. 引入的噪声可以通过在适当的范围内动态调节 LOCM 的相关参数加以补偿, 其调节过程等效于调节信道附加噪声和外差探测器的信噪比, 从而实现对可容忍过量噪声的动态平衡. 可调谐的 LOCM 噪声允许信息协调的参考方对估计的散粒噪声进行偏置 [29], 这增加了 Alice 和 Bob 之间的互信息, 提高了系统的探测效率和对过量噪声的抗性 [30], 将其应用在 DPM-CVQKD 中有助于克服调制离散化效应带来的性能退化, 并提升安全密钥率和传输距离.

本文内容安排如下: 第 2 部分详细介绍了 LOCM DPM-CVQKD 的 PM 方案及其 EB 方案, 并进行安全性分析; 第 3 部分对本文所提方案进行了数值仿真, 验证了幅值和相位离散化的综合效应, 以及 LOCM 相关参数对系统的影响, 评估了可组合安全分析下有效码长对传输距离和安全密钥率的影响; 第 4 部分是对全文的总结.

2 LOCM DPM-CVQKD 安全性分析

LOCM DPM-CVQKD 的 PM 方案如图 1 所示. 在发送端, Alice 通过激光器、随机数生成器以及调制器将经典的随机变量 α 编码在相干态上以完成量子态的制备过程, 最终生成了服从高斯分布 $\mathcal{N}(0,V_{\rm A})$ 的随机数 $(x_{\rm A},p_{\rm A})$, 其幅度 $A=\sqrt{x_{\rm A}^2+p_{\rm A}^2}$, 相位 $\theta=\arctan(p_{\rm A}/x_{\rm A})$ 分别服从瑞利分布和均匀分布. 幅度和相位将被采样和离散化后分别独立地通过高斯调制器调制到相干态 $|\alpha\rangle=|x_{\rm A}+{\rm i}p_{\rm A}\rangle$ 上, 其离散化的联合效应在 PM 方案中由虚乘法系数 T_x/T_p 进行建模.

在调制器引起的离散化中, 相干态的幅度和相位等价于通过了均匀量化器进行离散化. 假设幅度和相位的分辨率分别为 $\delta_{\rm a}$ 和 $\delta_{\rm p}$, 经过离散化后, 幅度 A 被分割成大小为 $\delta_{\rm a}$ 的 N 个等间隔区间的集合, 相位 θ 被分割成大小为 $\delta_{\rm p}$ 的 M 个等间隔区间的集合, 从数值上可分别表示为 [24]

$$\begin{aligned} &I_{\rm a}^j=[j\delta_{\rm a},(j+1)\delta_{\rm a})\,,\ j=0,1,2,\cdots,N-1,\\ &I_{\rm p}^k=[k\delta_{\rm p},(k+1)\delta_{\rm p})\,,\ k=0,1,2,\cdots,M-1, \end{aligned}\tag{1}$$

其中 $M=2\pi/\delta_{\rm p}$. 此时, 任何位于区间 j 内的幅度 A 将被投影输出为 $A^*=(j+0.5)\delta_{\rm a}$, 而任何位于区间 k 内的相位 θ 则将被投影输出为 $\theta^*=(k+0.5)\delta_{\rm p}$.

当相干态的幅度和相位被离散化后, 调制后的正交分量将会出现相应的波动 [25], 这种波动状态可以被定量表达为

$$\begin{aligned} x_{\rm A}^*&=A^*\cos\theta^*=(A+\Delta A)\cdot\cos(\theta+\Delta\theta)\,,\\ p_{\rm A}^*&=A^*\sin\theta^*=(A+\Delta A)\cdot\sin(\theta+\Delta\theta)\,, \end{aligned}\tag{2}$$

其中, $\Delta A=A-A^*\in[-\delta_{\rm a}/2,\delta_{\rm a}/2)$, $\Delta\theta=\theta-\theta^*\in[-\delta_{\rm p}/2,\delta_{\rm p}/2)$ 分别代表幅值和相位的波动程度, 当 ΔA 和 $\Delta\theta$ 趋近于 0 时, $x_{\rm A}^*/p_{\rm A}^*$ 将逐渐逼近并收敛于理想高斯分布比值 $x_{\rm A}/p_{\rm A}$. 为了更精确地描述高斯调制的离散化效应, 引入虚拟乘法系数 T_x/T_p 来建模正交分量的波动程度 [24], 可以表示为

$$\begin{aligned} T_x&=\frac{x_{\rm A}^*}{x_{\rm A}}=\frac{A+\Delta A}{A}\cdot\frac{\cos(\theta+\Delta\theta)}{\cos\theta}\\ &=\left(1+\frac{\Delta A}{A}\right)(\cos\Delta A-\sin\Delta\theta\tan\theta)\,,\\ T_p&=\frac{x_{\rm p}^*}{x_{\rm p}}=\frac{A+\Delta A}{A}\cdot\frac{\sin(\theta+\Delta\theta)}{\sin\theta}\\ &=\left(1+\frac{\Delta A}{A}\right)(\cos\Delta A-\sin\Delta\theta\cot\theta)\,. \end{aligned}\tag{3}$$

此时, (2) 式可以重写为以下形式:

$$x_{\rm A}^*=T_xx_{\rm A},\quad p_{\rm A}^*=T_pp_{\rm A}.\tag{4}$$

因为低幅度值比低相位值更容易受到离散化影响, 会直接导致 DPM 的估计特性严重偏离于真实统计数据. 因此, 这需要通过预选择过程来剔除最容易被离散化的原始数据样本, 以减小偏离程度, 确保调制估计的准确性 [24,25]. 在本文的预选择过程中, 阈值设定为 $\eta_{\rm th}=\delta_{\rm a}$, 会使得虚乘法系数 T_x/T_p 的分布更为集中, 趋近于理想值 1, 这也意味着 DPM 方案正在向理想高斯调制靠近.

在接收端, Bob 利用 LOCM 来放大 Alice 发送的量子态, 通过 3 dB 分束器将输入的量子态分为两个部分, 其中一部分与真空态在分束器中进行干涉后利用外差探测器分别测量 x 和 p 正交分量. 根据测量结果 x_m 以及增益 λ 对另一部分进行修正后将作为另一模式的位移量, 通过正确选择, Bob

可以得到线性放大器对信号模态的变换, 并应用外差探测完成量子态的传输过程. 最后经过参数估计、误码纠错、保密增强和信息协调这一系列后处理过程完成密钥分发过程.

在 LOCM 中, 受调制离散化效应影响的相干态会经过分束器被分割为两个模式, 其中一个模式被送入一个外差探测器进行探测, 探测后的结果输出会乘以调谐增益 λ 进行修正后作为另一模式的位移量[27]. 最终的输出模式可以表达为

$$x_{\mathrm{B}}=\frac{1}{\sqrt{1-\tau}}x_{\mathrm{B}_1}+\sqrt{\frac{\tau}{1-\tau}}x_{\mathrm{vac}}, \tag{5}$$

其中 τ 是分束器的透射率, x_{vac} 是具有单位方差的真空噪声. LOCM 可视为对输入态的具有等效增益 $G=1/(1-\tau)$ 的线性放大器, 其输出方差为

$$V_{\mathrm{B}}=\frac{V_{\mathrm{B}_1}+\tau}{1-\tau}. \tag{6}$$

LOCM DPM-CVQKD 经过 PM 方案转换的 EB (equivalent entanglement-based) 方案如图 2 所示. 在发送端, Alice 会制备一个方差为 V 的 EPR 态, 对其中一个模式进行外差探测, 得到 $(x_{\mathrm{A}},p_{\mathrm{A}})$ 的值, 并将另一模式投影至以 $(x_{\mathrm{A}},p_{\mathrm{A}})$ 为中心的相干态上. 相干态的幅度和相位离散化的联合效应造成的调制正交分量的波动可建模为在发送端引入的制备噪声. 经过预选择后, Alice 制备的离散化相干态 $(x_{\mathrm{A}}^{*},p_{\mathrm{A}}^{*})$ 将通过不可信的量子信道传输给接收端, 此量子信道特征由透射率 T 和过量噪声 ε 进行描述. 在接收端, Bob 会应用 LOCM 对传输的量子态进行放大, EPR 态的其中一个模式会与传输的离散化相干态在分束器中进行干涉, 利用外差探测器来测量分束器输出的一个模式以得到最终的输出结果. 一方面, 用方差为 N_{LOCM} 的 EPR 态对 LOCM 引入的热噪声进行建模, 另一方面, 可以直接用虚拟分束器的透射率 T_{LOCM} 来等效地描述 LOCM 的探测效率, 在数学上可表达为[28]

$$\begin{aligned}T_{\mathrm{LOCM}}&=\left(\sqrt{1-\tau}+\lambda\sqrt{\frac{\tau}{2}}\right)^2,\\ N_{\mathrm{LOCM}}&=\frac{\left(\lambda\sqrt{\dfrac{1-\tau}{2}}-\sqrt{\tau}\right)^2+\dfrac{\lambda^2}{2}-1}{1-\left(\sqrt{1-\tau}+\lambda\sqrt{\dfrac{\tau}{2}}\right)^2}.\end{aligned} \tag{7}$$

因此, 由 LOCM 引入的噪声可以由下式给出:

$$\begin{aligned}\chi_{\mathrm{LOCM}}&=\frac{1+(1-T_{\mathrm{LOCM}})\,N_{\mathrm{LOCM}}}{T_{\mathrm{LOCM}}}\\ &=\frac{\lambda^2+\left(\lambda\sqrt{1-\tau}-\sqrt{2\tau}\right)^2}{\left[\sqrt{2\,(1-\tau)}+\lambda\sqrt{\tau}\right]^2}.\end{aligned} \tag{8}$$

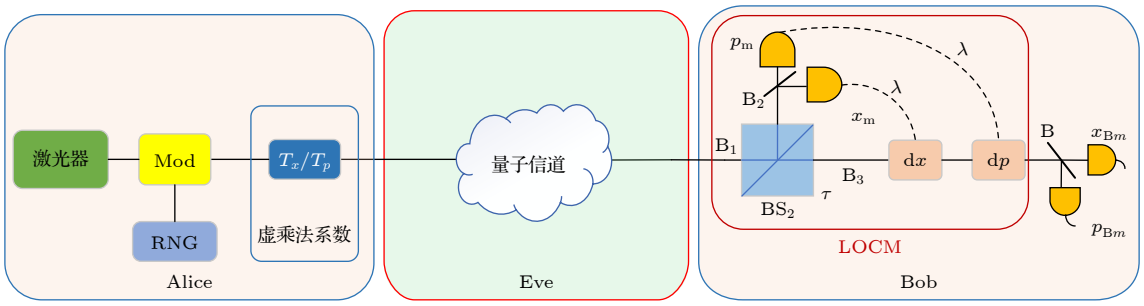

图 1 LOCM DPM-CVQKD 的制备测量方案

Fig. 1. The PM scheme of LOCM DPM-CVQKD protocol.

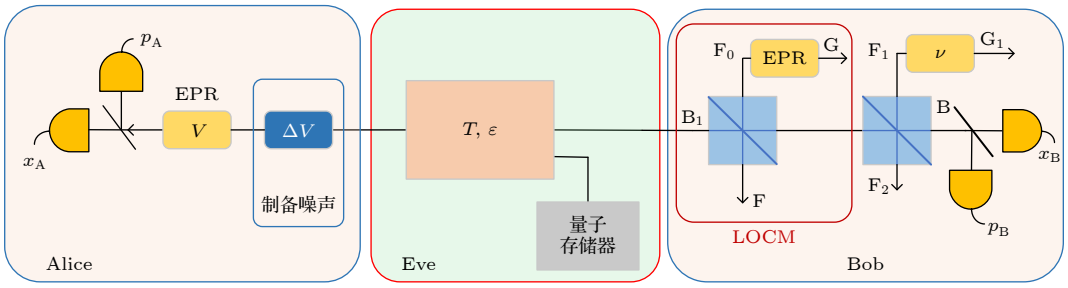

图 2 LOCM DPM-CVQKD 的纠缠等价方案

Fig. 2. The EB scheme of LOCM DPM-CVQKD protocol.

传输的量子态经 LOCM 放大后, 利用实际外差探测器进行测量, 用方差为 υ 的 EPR 态和传输效率为 η 的分束器分别对探测器的电子噪声 $\upsilon_{\rm el}$ 和探测效率进行建模. 此时, 系统经过正交分量的波动以及插入 LOCM 之后, 其协方差矩阵可表示为

$$\gamma_{\rm AB}=\begin{pmatrix}\sigma_{\rm A}^2\boldsymbol{I}_2 & c_{\rm AB}\boldsymbol{\sigma}_z\\ c_{\rm AB}\boldsymbol{\sigma}_z & \sigma_{\rm B}^2\boldsymbol{I}_2\end{pmatrix}$$
$$=\begin{pmatrix}V\boldsymbol{I}_2 & \sqrt{T\left(V^2-1\right)}\boldsymbol{\sigma}_z\\ \sqrt{T(V^2-1)}\boldsymbol{\sigma}_z & T[V+(\langle T_x^2\rangle-1)V_{\rm A}+\chi_{\rm tot}]\boldsymbol{I}_2\end{pmatrix}, \tag{9}$$

其中, $V=V_{\rm A}+1$, $\boldsymbol{I}_2$ 为单位矩阵 $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\boldsymbol{\sigma}_z$ 为泡利矩阵 $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $T=10^{-\frac{0.2L}{10}}$, L 代表着通信双方之间的传输距离, $\langle\cdot\rangle$ 表示均值操作, DPM 引起的离散化效应可被建模为方差为 $E=\left(\langle T_x^2\rangle-1\right)V_{\rm A}$ 的制备噪声. $\chi_{\rm tot}$ 代表归因于信道输入的总噪声, 可以表达为[31]

$$\chi_{\rm tot}=\chi_{\rm line}+\frac{\chi_{\rm LOCM}}{T}+\frac{\chi_{\rm het}}{TT_{\rm LOCM}}, \tag{10}$$

其中, $\chi_{\rm line}=1/T-1+\varepsilon$ 为信道传输过程中引入的总噪声, $\chi_{\rm LOCM}$ 为 LOCM 引入的噪声, $\chi_{\rm het}=(2-\eta+2\upsilon_{\rm el})/\eta$ 为外差探测器引入的噪声, 其中 η 和 $\upsilon_{\rm el}$ 分别表示 Bob 探测器的量子效率和电子噪声.

LOCM DPM-CVQKD 方案在反向协调和集体攻击下的安全密钥率可表示为[32]

$$K=p_{\rm ps}\left(\beta I_{\rm AB}-S_{\rm BE}\right), \tag{11}$$

其中, $p_{\rm ps}$ 是经过预选择和用于密钥分发的信号态的百分比, $I_{\rm AB}$ 是 Alice 和 Bob 之间的香农互信息, $S_{\rm BE}$ 是 Bob 和 Eve 之间的互信息的 Holevo 界, 代表集体攻击下 Eve 的最大窃取信息, β 是反向协调的协调效率. 一方面, 根据协方差矩阵 $\gamma_{\rm AB}$ 可以计算 $I_{\rm AB}$, 由下式给出:

$$I_{\rm AB}=\log_2\left[\frac{\sigma_{\rm B}^2+1}{\sigma_{\rm B}^2+1-c_{\rm AB}^2/(\sigma_{\rm A}^2+1)}\right]. \tag{12}$$

另一方面, $S_{\rm BE}$ 可以表达为

$$S_{\rm BE}=S\left(E\right)-S\left(E\left|B\right.\right), \tag{13}$$

其中, $S(E)$ 为量子态 E 的冯诺依曼熵, $S(E|B)$ 为条件冯诺依曼熵, 取决于协方差矩阵的辛特征值. 在 Bob 进行外差探测后, Eve 可以纯化整个系统, 有 $S(E)=S(AB)$ 以及 $S\left(E\left|B\right.\right)=S\left(A\left|B\right.\right)$. 因此, (13) 式又可重写为

$$\begin{aligned}S_{\rm BE}&=S\left(AB\right)-S\left(A\left|B\right.\right)\\&=G\left(\frac{\lambda_1-1}{2}\right)+G\left(\frac{\lambda_2-1}{2}\right)-G\left(\frac{\lambda_3-1}{2}\right)\\&\quad-G\left(\frac{\lambda_4-1}{2}\right)-G\left(\frac{\lambda_5-1}{2}\right),\end{aligned} \tag{14}$$

其中, $G\left(x\right)=\left(x+1\right)\log_2\left(x+1\right)-x\log_2\left(x\right)$, λ_i, $i=1,2,3,4,5$ 为辛特征值, 且 $\lambda_5=1$. λ_1 和 λ_2 可由协方差矩阵 $\gamma_{\rm AB}$ 确定, 表示为

$$\begin{aligned}\lambda_1&=\sqrt{\frac{1}{2}\left(A+\sqrt{A^2-4B}\right)},\\ \lambda_2&=\sqrt{\frac{1}{2}\left(A-\sqrt{A^2-4B}\right)},\end{aligned} \tag{15}$$

其中 $A=\det\gamma_{\rm A}+\det\gamma_{\rm B}+\det\sigma_{\rm AB}$ 和 $B=\det\gamma_{\rm AB}$. λ_3 和 λ_4 可由矩阵 $\gamma_{{\rm AF_0GF_2G_1}}$ 确定, 表示为

$$\gamma_{{\rm AF_0GF_2G_1}}^{x_{\rm B},p_{\rm B}}=$$
$$\gamma_{{\rm AF_0GF_2G_1B}}-\sigma_{{\rm AF_0GF_2G_1B}}^{\rm T}(\gamma_{\rm B}+I_2)^{-1}\sigma_{{\rm AF_0GF_2G_1B}}. \tag{16}$$

此时, λ_3 和 λ_4 可通过下式进行计算:

$$\begin{aligned}\lambda_3&=\sqrt{\frac{1}{2}\left[C+\sqrt{C^2-4D}\right]},\\ \lambda_4&=\sqrt{\frac{1}{2}\left[C-\sqrt{C^2-4D}\right]},\end{aligned} \tag{17}$$

其中,

$$\begin{aligned}C=&\frac{1}{\left[T\left(V+\chi_{\rm tot}+{\rm E}\right)\right]^2}[A\chi_{\rm com}^2+B+1\\&+2\chi_{\rm com}[V\sqrt{B}+T(V+\chi_{\rm line}+E)]\\&+2T\left(V^2-1\right)],\end{aligned}$$
$$D=\left(\frac{V+\sqrt{B}\chi_{\rm com}}{T\left(V+\chi_{\rm tot}\right)}\right)^2,$$
$$\chi_{\rm com}=\chi_{\rm LOCM}+\chi_{\rm het}/T_{\rm LOCM}.$$

基于上述详尽的推导与分析, 将 (12) 式和 (14) 式代入 (11) 式, 我们可以得到渐进情况下安全密钥率的表达式, 进而可以对 LOCM DPM-CVQKD 方案的安全性进行评估. 然而, 考虑到实际应用中安全密钥长度的固有局限性, 直接实现这一理论安全性是十分困难的. 因此, 本文采用可组合安全性分析框架进一步对所提方案进行评估, 可使得 DPM-CVQKD 与 LOCM 结合使用时, 即使是在有限码长的情形下, 整体协议的安全性仍然能够得到保证[33–35].

可组合安全性分析允许密钥具有较小的失效概率ε, 这是因为在密钥生成过程中, 受限于样本量的规模, 统计结果往往难以完全符合理论预期, 存在一定程度的偏差或波动. 通过设置一个较小的失效概率阈值ε, 在统计波动的允许范围内, 可以确保生成的密钥仍然具有足够高的安全性[33]. 这一设置有效地平衡了安全性的保障与实际操作中的限制, 使得整个量子密钥分发协议在复杂多变的现实环境中依然能够稳健运行. 如果 LOCM DPM-CVQKD 是$\varepsilon_{\rm cor}$正确, $\varepsilon_{\rm sec}$保密, 满足$\varepsilon \geqslant \varepsilon_{\rm cor}+\varepsilon_{\rm sec}$, 那么此方案是$\varepsilon$-secure 安全的[34]. 具体而言, $\varepsilon_{\rm cor}$代表通过纠错后不同字符串的残差概率的界限量, $\varepsilon_{\rm sec}$代表最终密钥与窃听者完全解耦的理想输出经典量子态之间距离的界限量, 满足

$$\varepsilon_{\rm sec}=\varepsilon_{\rm s}+\varepsilon_{\rm h}, \tag{18}$$

其中$\varepsilon_{\rm s}$是平滑参数, $\varepsilon_{\rm h}$是哈希参数. 在本文提出的方案中, 使用下式作为安全参数可保证 LOCM DPM-CVQKD 是ε - secure 安全的:

$$\varepsilon=2p_{\rm ec}\varepsilon_{\rm PE}+\varepsilon_{\rm cor}+\varepsilon_{\rm sec}, \tag{19}$$

其中$p_{\rm ec}$是误码纠错步骤中的成功概率, $\varepsilon_{\rm PE}$是参数估计的失败概率. 与此同时, (11) 式中$\beta I_{\rm AB}$和$S_{\rm BE}$又可重写为

$$\begin{aligned}&\beta I_{\rm AB}=H(l|E)_{\rho}+S(l:E)_{\rho}-\frac{{\rm leak}_{\rm ec}}{n},\\&S_{\rm BE}\geqslant H(l)-H(l|E)_{\rho},\end{aligned} \tag{20}$$

其中, $H(l|E)_{\rho}$是在单克隆态ρ下进行计算的条件冯诺依曼熵, $S(l:E)_{\rho}$是 Eve 对代表d比特字符的离散变量l的 Holeve 界, $H(l)$是l的香农熵, ${\rm leak}_{\rm ec}$是误码纠错期间 Bob 发送给 Alice 的侧信息大小. 因此, LOCM DPM-CVQKD 方案的可组合性安全密钥率的最低界可表示为[33]

$$\begin{aligned}K_n\geqslant{}&nH(l|E)_{\rho}-\sqrt{n}\Delta_{\rm aep}\left(p_{ec}\varepsilon_s^2/3,d\right)\\&+\log_2\left[p_{\rm ec}\left(1-\varepsilon_{\rm s}^2/3\right)\right]\\&+2\log_2\left(\sqrt{2}\varepsilon_{\rm h}\right)-{\rm leak}_{\rm ec}\\={}&nK-\sqrt{n}\Delta_{\rm aep}\left(p_{\rm ec}\varepsilon_{\rm s}^2/3,d\right)\\&+\log_2\left[p_{\rm ec}\left(1-\varepsilon_{\rm s}^2/3\right)\right]+2\log_2\left(\sqrt{2}\varepsilon_{\rm h}\right)\\={}&n\left(K-\frac{\Delta_{\rm aep}\left(p_{\rm ec}\varepsilon_{\rm s}^2/3,d\right)}{\sqrt{n}}+\frac{\Theta}{\sqrt{n}}\right),\end{aligned} \tag{21}$$

其中, d是每个测量结果的编码位数, n是用于密钥分发的码长数量. $\Delta_{\rm aep}(\varepsilon_{\rm s},d)$和$\Theta$可表示为

$$\begin{aligned}&\Delta_{\rm aep}(\varepsilon_s,d)\\&=4\log_2\left(2\sqrt{d}+1\right)\sqrt{-\log_2\left(1-\sqrt{1-\varepsilon_{\rm s}^2}\right)}\\&\simeq 4\log_2\left(2\sqrt{d}+1\right)\sqrt{\log_2\left(2/\varepsilon_{\rm s}^2\right)},\\&\Theta=\log_2\left[p_{\rm ec}\left(1-\frac{\varepsilon_{\rm s}^2}{3}\right)\right]+2\log_2\left(\sqrt{2}\varepsilon_h\right).\end{aligned} \tag{22}$$

3 数值仿真

基于上述分析, 我们推导出了 LOCM DPM-CVQKD 的可组合安全密钥率, 现对此方案的系统性能进行评估. 本文设置的参数如下: $V_{\rm A}=25$, $p_{\rm ps}=1$, $\beta=0.96$, $\varepsilon=0.02$, $\eta=0.6$, $v_{\rm el}=0.01$, $p_{\rm ec}=0.9$, $d=2^5$, $n=10^{10}$, $\varepsilon_{\rm h}=\varepsilon_{\rm s}=10^{-10}$, LOCM 参数取值为: $\lambda=0.47$, $\tau=0.20$.

为了对所提方案的性能进行评估, 我们将 DPM-CVQKD 方案与 LOCM DPM-CVQKD 方案在不同幅度分辨率和相位分辨率下进行了详细的对比研究, 结果如图 3 所示. 在传输损耗较小的场景中, LOCM DPM-CVQKD 的安全密钥率低于 DPM-CVQKD 方案. 其原因在于 LOCM 以引入过量噪声为代价来提高系统性能, 在传输损耗较小时, 传输的信号衰减相对较小, 此时 LOCM 引入的过量噪声会导致信噪比下降, 即使通过设置 LOCM 的相关参数对其进行调节, 也无法在损耗较小时完全对幅度和相位的离散化效应进行补偿, 此时 LOCM 对系统性能具有负面影响.

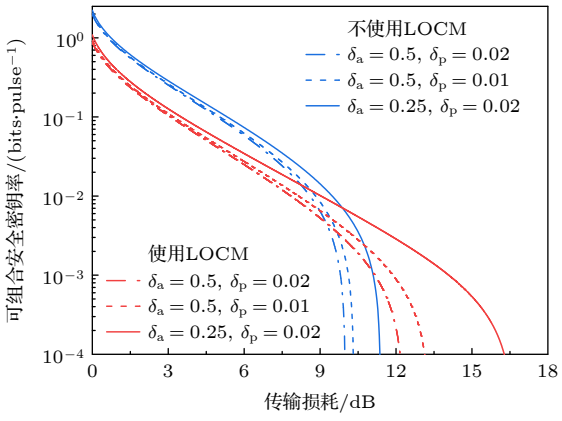

图 3 LOCM 对 DPM-CVQKD 可组合安全密钥率的改进

Fig. 3. Enhancement of LOCM on the composable secret key rate of DPM-CVQKD.

然而随着传输损耗的不断增大, LOCM 的应用展现出了显著的优势, 在 $\delta_{\rm a}=0.25$, $\delta_{\rm p}=0.02$ 的情形下, 其最大传输损耗达到了 16.67 dB, 比未使用 LOCM 时高出了 5.29 dB. 这是因为在传输一定距离之后, 信号衰减明显增加, LOCM 能够有效补偿这种衰减, 通过放大接收信号提升系统性能. 而 DPM CVQKD 方案在传输损耗稍大时, 信号衰减无法得到补偿, 离散化带来的综合效应对系统的影响也变得显著. 这证明了本文所提方案不仅能够优化安全密钥率, 还能够提升最大传输损耗, 且在传输损耗增大时表现出了更为明显的优势.

此外, 从图 3 中可以清晰地看出 LOCM 调制离散化效应起到了补偿作用. 随着 $\delta_{\rm a}$ 和 $\delta_{\rm p}$ 的变化, LOCM DPM-CVQKD 的可组合安全密钥率和传输损耗均有所改进, 尤其是对幅度离散化的补偿作用更为显著. 在添加 LOCM 后, 在 $\delta_{\rm a}=0.5$, $\delta_{\rm p}=0.02$ 的配置下, 最大安全传输损耗改进了 1.5 dB, 而 $\delta_{\rm a}=0.25$, $\delta_{\rm p}=0.02$ 的配置要比前一种情况多改进了 3.79 dB. 这凸显了 LOCM 能够有效地补偿正交分量的波动, 抑制幅度和相位的离散化过程对系统性能的负面影响, 这是因为通过调节相关参数提供的可调谐放大增益, LOCM 对传输过程中的离散化的量子态进行了等效放大, 增强了传输量子态的强度, 提高了传输信号的信噪比, 使得幅度波动和相位波动相对于整体信号功率的占比下降, 从而提升了系统性能. 相比之下, 幅度离散化导致的正交分量波动要强于相位离散化导致的正交分量波动, 因而 LOCM 对幅度离散化的补偿效果体现得更加明显. 以上结果表明 LOCM 不仅有效地弥补了离散化过程带来的信息损失造成的性能下降, 还补偿了传输过程中的信号衰减, 也表明了即使量子态经历了离散化过程, 系统仍然能够维持较高的安全密钥生成率和较大的可容忍传输损耗, 提升了系统的稳定性和效率.

LOCM DPM-CVQKD 方案通过引入一定程度的噪声来实现系统性能的提升, 系统的可容忍过量噪声也因此发生改变, 其与传输损耗之间的关系如图 4 所示. DPM-CVQKD 方案和 LOCM DPM-CVQKD 方案均呈现逐渐下降的趋势, 但是因为 LOCM 能够弥补幅度和相位离散化过程造成的影响, 所以添加了 LOCM 的可容忍噪声要比未添加 LOCM 的略高. 值得注意的是, 添加 LOCM 后方案相位分辨率对可容忍过量噪声基本上可以忽略不计, 而幅值分辨率的降低则会显著提高系统的可容忍过噪声水平. 具体来说, LOCM DPM-CVQKD 方案在 $\delta_{\rm a}=0.5$, $\delta_{\rm p}=0.02$ 的情形下, 可容忍过量噪声达到最大值 0.2827; 而在 $\delta_{\rm a}=0.25$, $\delta_{\rm p}=0.02$ 的情形下, 可容忍过量噪声达到最大值 0.3641, 相比前一种情况提高了 0.0814. 这种改善是源于 LOCM 通过可调谐的参数将引入的噪声转变成了有利于系统的噪声范围之内, 等价于调节了探测器的信噪比, 从而增加了 Alice 和 Bob 之间的互信息, Bob 和 Eve 之间的互信息则保持不变. 因此, 利用 LOCM 改进, 可以提高 CVQKD 系统对过量噪声的可容忍能力.

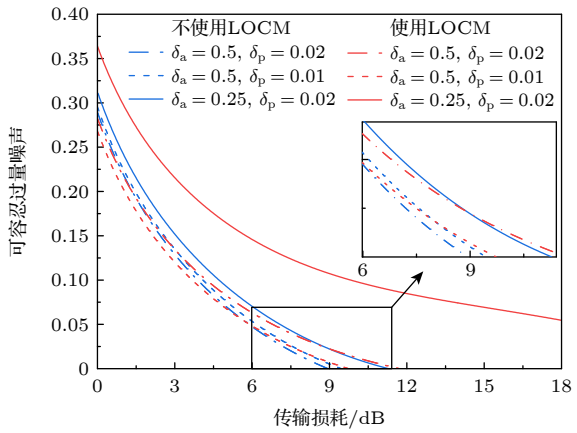

图 4 LOCM 对 DPM-CVQKD 可容忍过量噪声的改进

Fig. 4. Enhancement of LOCM on the tolerable excess noise of DPM-CVQKD.

方差的选择会影响系统的最大可容忍传输损耗, 如图 5 所示. 当方差低于阈值 8.4 时, 未添加 LOCM 的 DPM-CVQKD 的可容忍传输损耗明显要优于加入 LOCM 后的 DPM-CVQKD, 但是当方差大于阈值 8.4 时, LOCM DPM-CVQKD 方案反而优于未加入 LOCM 的 DPM-CVQKD 方案. 这种变化的原因在于, 当方差较小时, LOCM 引入的可调谐噪声无法被有效地控制在有利范围内, 甚至会对系统性能造成衰退, 严重限制了对幅值离散化和相位离散化所产生的综合效应的补偿效果, 其优化作用未能得到充分发挥. 在本文的研究中, 所提出方案的最大可容忍传输损耗能够达到 16.67 dB, 而 DPM-CVQKD 只能达到 11.38 dB, 体现出了对系统参数优化的必要性, 也充分证明了 LOCM 在特定条件下对系统性能提升的重要作用.

基于上述分析可知, 通过调节 LOCM 的调谐增益 λ 以及透射率 τ 可实现对 LOCM 噪声的灵活

控制, 这两个参数对可组合安全密钥率的影响如图 6 所示. 从图 6 可以观察到, 随着 τ 的不断增大, 可组合性安全密钥率呈现单调减小的趋势. 但是, 随着 λ 的不断增大, 可组合性安全密钥率呈现先增大后减小的趋势. 这种结果表明, 对于固定的 τ 值, 总能在可控制的范围内找到一个与之匹配的 λ 值, 从而使得可组合安全密钥率达到最优值. 这也是因为 LOCM 引入的可调谐噪声必须控制在有利的范围内才能使其转变成有益于系统的噪声. 通过这种调控, 我们能灵活地优化系统性能, 有效弥补幅值和相位离散化带来的影响.

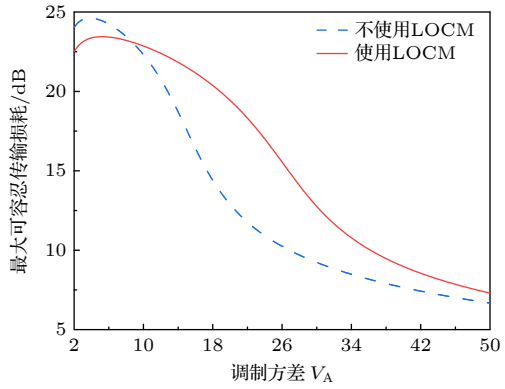

图 5 调制方差对最大传输距离的影响, 幅值分辨率和相位分辨率分别设置为 $\delta_a = 0.25$, $\delta_p = 0.02$

Fig. 5. The effect of modulation variance on maximum transmission distance, the amplitude resolution and phase resolution are $\delta_a = 0.25$, $\delta_p = 0.02$, respectively.

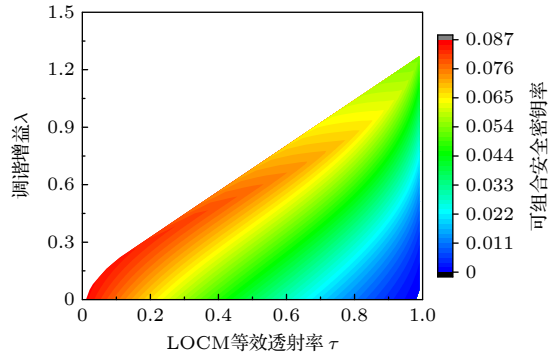

图 6 LOCM 参数对可组合安全密钥率的影响, 幅值分辨率和相位分辨率分别设置为 $\delta_a = 0.25$, $\delta_p = 0.02$

Fig. 6. Effect of LOCM-related parameters on the composable secret key rate, the amplitude resolution and phase resolution are $\delta_a = 0.25$, $\delta_p = 0.02$, respectively.

LOCM 参数的选择对于系统的性能也具有至关重要的影响, 不仅体现在对可组合安全密钥率的作用上, 还体现在对传输损耗的作用上, 如图 7 所示. 从图 7(a) 可以看出, 随着 λ 的逐渐增大, 传输损耗会呈现单调增大的趋势, 而图 7(b) 表明随着 τ 的不断增大, 传输损耗则会呈现单调减小的趋势. 在所选择的参数配置中, 当 $\lambda = 0.47$, $\tau = 0.2$ 时, 传输损耗达到了 16.67 dB, 这一配置即可满足系统性能提升的需求. 基于前述分析可知, LOCM 可视作一个具有线性放大特性的放大器, 其等效放大增益主要受到 τ 的直接影响. 当 τ 保持不变的情况下, 其放大增益就是固定的, 那么此时 LOCM 引入的噪声也只与 τ 相关. 因此, 在保证 LOCM 引入的噪声仍然处于对系统有利的范围内的前提下, 只要调节参数 λ 至使传输损耗达到最大值, 就可以实现系统性能的最优化.

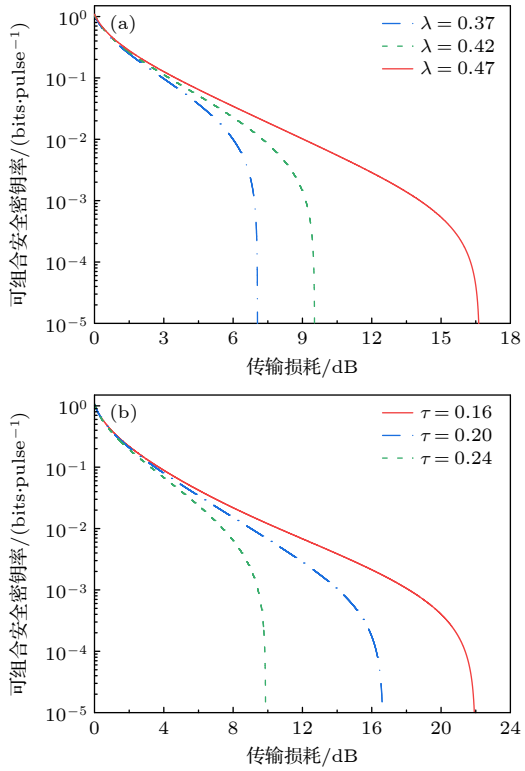

图 7 LOCM 参数对最大传输距离的影响, 幅值分辨率和相位分辨率分别设置为 $\delta_a = 0.25$, $\delta_p = 0.02$ (a) 调谐增益 λ 与传输损耗的关系; (b) 等效透射率 τ 与传输损耗的关系

Fig. 7. Effect of LOCM parameters on maximum transmission distance, the amplitude resolution and phase resolution are set to $\delta_a = 0.25$, $\delta_p = 0.02$, respectively: (a) The tuning gain λ versus losses; (b) the equivalent transmittance τ versus losses.

由图 6 和图 7 可以看出, 本方案对系统性能的提升效果依赖于对 LOCM 参数的精准优化. 由于在实际场景下, LOCM 的最优参数组合会受到发送端的调制方差、量子信道的过量噪声和接收端的

接收效率等多重因素的影响, 难以求出精确的解析解, 因而可以通过应用机器学习算法估计. 机器学习已被广泛应用于 QKD 参数的实时预测与动态补偿中, 并取得了良好的效果[36–40]. 针对本文所提方案, 在参数估计阶段可使用启发式优化算法基于估计结果对 LOCM 的参数进行寻优; 在系统运行过程中则可构建面向时间序列的机器学习模型, 预测信道过量噪声的潜在变化并主动搜寻 LOCM 的最优参数配置, 以充分发挥 LOCM 的改进作用.

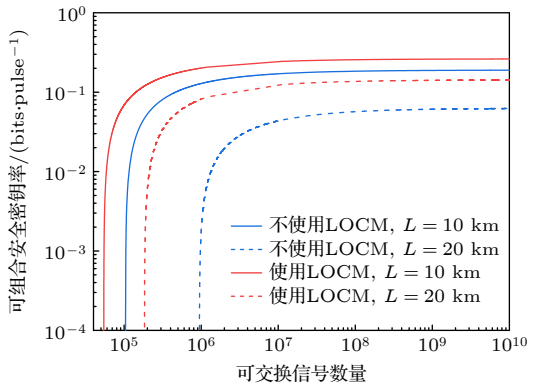

图 8 不同传输距离下码长对可组合安全密钥率的影响, 幅值分辨率和相位分辨率分别设置为 $\delta_{\mathrm{a}}=0.25$, $\delta_{\mathrm{p}}=0.02$

Fig. 8. Effect of block length on the composable secret key rate under different transmission distances, the amplitude resolution and phase resolution are set to $\delta_{\mathrm{a}}=0.25$, $\delta_{\mathrm{p}}=0.02$, respectively.

为探究可组合安全性分析中码长对安全密钥率的影响, 我们展示了在不同传输距离下, DPM-CVQKD 以及 LOCM DPM-CVQKD 方案的可交换信号数量与可组合安全密钥率的关系, 如图 8 所示. 随着码长的逐渐增大, 可组合安全密钥率会经历一个显著的急速上升阶段, 而后在码长为 10^8 附近趋于平稳. 值得注意的是, LOCM DPM-CVQKD 在可组合安全密钥率方面展现出了显著的优势, 明显优于原来的 DPM-CVQKD 方案. 当传输距离为 20 km, 且需要实现 0.0611 bit/pulse 的安全密钥率时, DPM-CVQKD 所需码长为 1.2×10^9, 而 LOCM DPM-CVQKD 仅需要 5.6×10^5 的码长, 两者之间存在近 4 个数量级的差异. 这意味着 LOCM DPM-CVQKD 减小了系统对码长的需求度和复杂度, 同时也减少了实际应用中的成本. 此外, 在传输距离分别为 10 km 和 20 km 的情形时, DPM-CVQKD 的可组合安全密钥率存在近 1 个数量级的差异, 而本文提出的方案则仅存在远不到 1 个数量级的差异, 进一步证明了 LOCM DPM-CVQKD 在减小因传输距离增大而导致的码长增大需求方面的有效性, 从而提高了系统的灵活性和实用性.

4 结论与展望

在 CVQKD 的实验装置中, 调制器驱动电压的有限分辨率会使理想的高斯调制退化成 DPM, 导致系统性能下降. 本文提出了 LOCM DPM-CVQKD 方案, 考虑了接收端探测器噪声的影响, 通过在接收端添加 LOCM 以补偿调制离散化效应, 实现系统性能的提升. 由于 LOCM 会引入额外的过量噪声, 因此需要对 LOCM 的相关参数进行优化, 以利用引入的过量噪声优化安全密钥率及传输距离. 仿真结果表明了 LOCM 不仅能够补偿调制离散化带来的性能损失, 还能在可组合安全性分析框架下显著降低对码长的需求, 从而为连续变量量子密钥分发的实际应用提供了一种高效的理论方案.

LOCM DPM-CVQKD 的实验实现需要高信噪比的外差探测器等光电模块, 并对发送端和接收端的光学结构集成化封装, 这些器件与技术能够与当前相干光通信系统高度兼容, 具备一定的实验可行性. 然而当 LOCM DPM-CVQKD 的传输距离超过一定范围后, 需要更强的本振光, 可能会导致引入较大的过量噪声, 降低安全传输距离. 未来对 LOCM 的更深入研究需要聚焦 LOCM 的实验实现, 构建与实验系统相匹配的安全性分析精确模型, 在此基础上利用机器学习模型实现对 LOCM 最优参数组合的高效搜寻与动态调整, 以便进一步提升所提方案的实用价值.

参考文献

[1] Portmann C, Renner R 2022 *Rev. Mod. Phys.* **94** 025008
[2] Pirandola S, Andersen U L, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C, Pereira J L, Razavi M, Shaari J S, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photonics* **12** 1012
[3] Zhang C X, Wu D, Cui P W, Ma J C, Wang Y, An J M 2023 *Chin. Phys. B* **32** 124207
[4] Zapatero V, Navarrete A, Curty M 2024 *Adv. Quantum Technol.* 202300380
[5] Diamanti E, Leverrier A 2015 *Entropy* **17** 6072
[6] Laudenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hubel H 2018 *Adv. Quantum Technol.* **1** 1800011

[7] Guo H, Li Z, Yu S, Zhang Y C 2021 *Fundam. Res.* **1** 96

[8] Zhang Y C, Bian Y M, Li Z Y, Yu S 2024 *Appl. Phys. Rev.* **11** 011318

[9] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[10] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501

[11] Zhang Y C, Li Z Y, Chen Z Y, Weedbrook C; Zhao Y J, Wang X Y, Huang Y D, Xu C C, Zhang X X, Wang Z Y, Li M, Zhang X Y, Zheng Z Y, Chu B J, Gao X Y, Meng N, Cai W W, Wang Z, Wang G, Yu S, Guo H 2019 *Quantum Sci. Technol.* **4** 035006

[12] Zhang Y C, Chen Z Y, Pirandola S, Wang X Y, Zhou C, Chu B J, Zhao Y J, Xu B J, Yu S, Guo H 2020 *Phys. Rev. Lett.* **125** 010502

[13] Jain N, Chin H M, Mani H, Lupo C, Nikolic D S, Kordts A, Pirandola S, Pedersen T B, Kolb M, Omer B, Pacher C, Gehring T, Andersen U L 2022 *Nat. Commun.* **13** 4740

[14] Hajomer A A E, Derkach I, Jain N, Chin H M, Andersen U L, Gehring T 2024 *Sci. Adv.* **10** eadi9474

[15] Wang T, Huang P, Li L, Zhou Y M, Zeng G H 2024 *New J. Phys.* **26** 023002

[16] Liao Q, Liu H J, Wang Z, Zhu L J 2023 *Acta Phys. Sin.* **72** 040301 (in Chinese) [廖骎, 柳海杰, 王铮, 朱凌瑾 2023 物理学报 **72** 040301]

[17] Chen Z Y, Wang X Y, Yu S, Li Z Y, Guo H 2023 *npj Quantum Inf.* **9** 28

[18] Zheng Y, Wang Y L, Fang C L, Shi H B, Pan W 2024 *Phys. Rev. A* **109** 022424

[19] Zhang G W, Bai J D, Jie Q, Jin J J, Zhang Y M, Liu W Y 2024 *Acta Phys. Sin.* **73** 060301 (in Chinese) [张光伟, 白建东, 颉琦, 靳晶晶, 张永梅, 刘文元 2024 物理学报 **73** 060301]

[20] Jouguet P, Kunz-Jacques S, Diamanti E, Leverrier A 2012 *Phys. Rev. A* **86** 032309

[21] Wu X D, Huang D, Huang P, Guo Y, 2022 *Acta Phys. Sin.* **71** 240304 (in Chinese) [吴晓东, 黄端, 黄鹏, 郭迎 2022 物理学报 **71** 240304.]

[22] Zhang Y J, Wang X Y, Zhang Y, Wang N, Jia Y X, Shi Y Q, Lu Z G, Zou J, Li Y M 2024 *Acta Phys. Sin.* **73** 060302 (in Chinese) [张云杰, 王旭阳, 张瑜, 王宁, 贾雁翔, 史玉琪, 卢振国, 邹俊, 李永民 2024 物理学报 **73** 060302]

[23] Lupo C 2020 *Phys. Rev. A* **102** 022623

[24] Wang T Y, Li M, Wang X 2022 *Opt. Express* **30** 36122

[25] Wang T Y, Li M, Wang X, Hou L 2023 *Opt. Express* **31** 21014

[26] Guo Y, Lv G, Zeng G H 2015 *Quantum Inf. Process.* **14** 4323

[27] Wu X D, Liao Q, Huang D, Wu X H, Guo Y 2017 *Chin. Phys. B* **26** 110304

[28] Zhang H, Mao Y, Huang D, Guo Y, Wu X D, Zhang L 2018 *Chin. Phys. B* **27** 090307

[29] Yang F L, Qiu D W 2020 *Quantum Inf. Process.* **19** 99

[30] He Y, Wang T Y 2024 *Quantum Inf Process.* **23** 135

[31] Mao Y Y, Wang Y J, Guo Y, Mao Y H, Huang W T 2021 *Acta Phys. Sin.* **70** 110302 [毛宜钰, 王一军, 郭迎, 毛堉昊, 黄文体 2021 物理学报 **70** 110302]

[32] Wu X D, Huang D 2023 *Acta Phys. Sin.* **72** 050303 (in Chinese) [吴晓东, 黄端 2023 物理学报 **72** 050303]

[33] Stefano P 2021 *Phys. Rev. Res.* **3** 013279

[34] Pirandola S 2021 *Phys. Rev. Res.* **3** 043014

[35] Mountogiannakis A G, Papanastasiou P, Pirandola S 2022 *Phys. Rev. A* **106** 042606

[36] Liu J Y, Ding H J, Zhang C M, Xie S P, Wang Q 2019 *Phys. Rev. Appl.* **12** 014059

[37] Liu J Y, Jiang Q Q, Ding H J, Ma X, Sun M S, Xu J X, Zhang C H, Xie S P, Li J, Zeng G H, Zhou X Y, Wang Q 2023 *Sci. China Inf. Sci.* **66** 189402

[38] Zhang Z K, Liu W Q, Qi J, He C, Huang P 2023 *Phys. Rev. A* **107** 062614

[39] Chin H M, Jain N, Zibar D, Andersen U L, Gehring T 2021 *npj Quantum Inf.* **7** 20

[40] Xu J X, Ma X, Liu J Y, Zhang C H, Li H W, Zhou X Y, Wang Q 2024 *Sci. China Inf. Sci.* **67** 202501

Composable security analysis of linear optics cloning machine improved discretized polar modulation continuous-variable quantum key distribution*

He Ying Wang Tian-Yi† Li Ying-Ying

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

(Received 5 August 2024; revised manuscript received 28 October 2024)

Abstract

In experimental setups of continuous-variable quantum key distribution (CVQKD) independently modulating the amplitude and phase of coherent states, the ideal Gaussian modulation will be degraded into discretized polar modulation (DPM) due to the finite resolution of the driving voltages of electro-optical modulators. To compensate for the performance degradation induced by the joint effect of amplitude and phase discretization, linear optics cloning machine (LOCM) can be introduced on the receiver side. Implemented by linear optical elements, heterodyne detection and controlled displacement, LOCM introduces extra noise that can be transformed into an advantageous one to combat channel excess noise by dynamically adjusting the relevant parameters into a suitable range. In this paper, the prepare-and-measure version of LOCM DPM-CVQKD is presented, where the incoming signal state enters a tunable LOCM before being measured by the nonideal heterodyne detector. The equivalent entanglement-based model is also established to perform security analysis, where the LOCM is reformulated into combination of the incoming signal state and a thermal state on a beam splitter. The composable secret key rate is derived to investigate the security of LOCM DPM-CVQKD. Simulation results demonstrate that the composable secret key rate and transmission distance are closely related to the tuning gain and the transmittance of LOCM. Once these two parameters are set to appropriate values, LOCM can improve the secret key rate and transmission distance of DPM-CVQKD, as well as its resistance to excess noise. Meanwhile, taking finite-size effect into consideration, the LOCM can also effectively reduce the requirement for the block size of the exchanged signals, which is beneficial to the feasibility and practicability of CVQKD. Owing to the fact that the performance of LOCM DPM-CVQKD is largely reliant on the calibration selection of relevant parameters, further research may concentrate on the optimization of LOCM in experimental implementations, where machine learning related methods may be utilized.

Keywords: quantum key distribution, continuous variable, discretized polar modulation, linear optics cloning machine

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20241094

CSTR: 32037.14.aps.73.20241094

* Project supported by the National Natural Science Foundation of China (Grant No. 62361009) and the Science and Technology Projects of Guizhou Province, China (Grant No. ZK[2021]304).

† Corresponding author. E-mail: tywang@gzu.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

线性光学克隆机改进的离散极化调制连续变量量子密钥分发可组合安全性分析

贺英　王天一　李莹莹

Composable security analysis of linear optics cloning machine improved discretized polar modulation continuous-variable quantum key distribution

He Ying　Wang Tian-Yi　Li Ying-Ying

引用信息 Citation: Acta Physica Sinica, 73, 230303 (2024)　DOI: 10.7498/aps.73.20241094
在线阅读 View online: https://doi.org/10.7498/aps.73.20241094
当期内容 View table of contents: http://wulixb.iphy.ac.cn