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

# 基于光前置放大器的量子密钥分发融合经典通信方案

钟海 叶炜 吴晓东 郭迎

# Optical preamplifier based simultaneous quantum key distribution and classical communication scheme

Zhong Hai Ye Wei Wu Xiao-Dong Guo Ying

引用信息 Citation: Acta Physica Sinica, 70, 020301 (2021) DOI: 10.7498/aps.70.20200855
在线阅读 View online: https://doi.org/10.7498/aps.70.20200855
当期内容 View table of contents: http://wulixb.iphy.ac.cn

# 基于光前置放大器的量子密钥分发融合经典通信方案*

钟海[1)] 叶炜[1)] 吴晓东[2)†] 郭迎[1)2)‡]

1) (中南大学计算机学院, 长沙 410083)

2) (中南大学自动化学院, 长沙 410083)

(2020 年 6 月 5 日收到; 2020 年 8 月 7 日收到修改稿)

量子密钥分发融合经典通信方案将连续变量量子密钥分发和经典通信合并到了一起, 为将来在现有的光网络上同时进行密钥分发和经典通信提供了一个有效的方法. 然而, 在量子信号上叠加一个经典信号将会给连续变量量子密钥分发系统引入过噪声从而大大降低系统的性能. 本文提出基于光前置放大器的量子密钥分发融合经典通信方案, 即在接收端插入光前置放大器来提升系统的性能. 首先, 在相同比特误码率条件下, 光前置放大器对信号的放大能够降低对发送端经典信号调制振幅的要求, 从而降低经典信号对量子信号的噪声影响; 其次, 光前置放大器能够补偿接收端探测器的不完美; 再次, 对于本地本振光的情形, 放大器还能放大弱相位参考脉冲, 从而降低参考脉冲散粒噪声带来的相位过噪声. 在实际可达到的系统参数下, 数值仿真结果表明本文提出的方案相比于原方案在安全密钥率和传输距离上都有很好的提升. 这些结果表明本方案为量子密钥分发融合经典通信方案的进一步发展和实际应用提供了一个十分有效而实用的方法.

**关键词**: 连续变量, 量子密钥分发融合经典通信, 光前置放大器

**PACS**: 03.67.Dd, 03.67.Hk **DOI**: 10.7498/aps.70.20200855

## 1 引 言

量子密钥分发 (quantum key distribution, QKD)[1–6] 使得相隔两地的合法双方 Alice 和 Bob 能够通过一个可能被窃听者 Eve 控制的量子信道进行安全的密钥分发. 目前 QKD 主要分为两个分支, 即离散变量 (discrete variable, DV) QKD[4,7] 和连续变量 (continuous variable, CV) QKD[5,6]. CVQKD 因具有很高的探测效率且能够与现有的相干光通信系统进行很好的兼容而受到研究者的广泛关注. 目前应用最广泛的 CVQKD 协议是基于高斯调制相干态 (Gaussian modulated coherent state, GMCS) 的协议[8]. 该协议的理论无条件安全性已经得到很好的证明[9,10]. 更为重要的一点是, 该协议是基于相干态的, 这就使得它能够在现有的相干光通信系统的框架下来实现量子密钥分发. 无论是传输本振光 (transmitted local oscillator, TLO) 的情形还是本地本振光 (locally local oscillator, LLO) 情形[11,12], 运用现有的相干光学组件和时分、偏振与波分复用技术, 多个实验已经实现了在实验室环境下基于商用单模光纤的 CVQKD 系统[13–15]. 同时, 为了测试 CVQKD 系统与现有经典光网络的兼容性, 多个在实际环境中的实地测试实验也取

* 国家自然科学基金 (批准号: 61871407, 61872390, 61801522) 和中南大学研究生自主探索创新项目 (批准号: 2020zzts136) 资助的课题.

† 通信作者. E-mail: wuxiaodong2018@foxmail.com

‡ 通信作者. E-mail: yingguo@csu.edu.cn

 

得了很好的进展[16,17]. 为了进一步使得 CVQKD 与经典相干光网络能够更好地兼容, CVQKD 与经典通信通过波分复用与空分复用进行共同传输也得到了理论的验证和实验的证明[18–20]. 这些研究成果为今后 CVQKD 在现有相干光网络上的普及奠定了基础.

最近, 一种将 CVQKD 与经典通信进一步融合的新方案引起了研究者们的重视, 即量子密钥分发融合经典通信 (simultaneous quantum key distribution and classical communication, SQCC) 方案[21–26]. 该方案在传统 CVQKD 对信号进行高斯调制 (或者离散调制) 的基础上再叠加调制一个经典信号, 如二进制相移键控 (binary phase-shift keying, BPSK) 或者正交相移键控 (quadrature phase-shift keying, QPSK). 这样, 使每一个传输的相干态同时承载密钥和经典信息, 为 CVQKD 在现有相干光通信网络上的商用普及提供了一个很好的应用方法. 然而, 由于需要在量子信号上叠加调制一个经典信号, 为了保证经典通信有足够低的比特误码率 (bit error rate, BER), 经典调制振幅$\alpha$将会大于量子信号振幅, 这给 CVQKD 系统带来了较大的噪声干扰从而大大降低了 CVQKD 系统的性能. 如何降低经典调制对量子信号的影响对于该方案来说至关重要. 目前能够提升 CVQKD 系统性能的方法有很多, 如一些量子操作包括减光子[27–29] 和量子催化[30–32] 等, 还有就是运用光前置放大器 (optical preamplifier, OPA)[24,33]. 不同于量子操作, OPA 是常用的光学组件, 它在经典通信和 CVQKD 领域都能发挥积极的作用.

为了降低 SQCC 方案中经典信号调制对 CVQKD 系统的影响, 本文提出基于 OPA 的 SQCC 方案, 即在原始 SQCC 方案中在接收端内插入 OPA 来对信号进行放大. 一方面, OPA 的加入能够在相同的 BER 条件下降低发送端对经典调制振幅要求. 另一方面, OPA 够补偿接收端探测器的不完美. 再者, 对于 LLO 情形, OPA 对弱相位参考脉冲的放大还能够降低由于参考脉冲散粒噪声带来的相位噪声. 这样在保证经典通信性能的前提下, 使得 CVQKD 系统具有更小的噪声从而能够获得更好的系统鲁棒性和性能. 在实验可达到的参数条件下, 本文对提出的方案进行了数值仿真. 仿真结果显示本文提出的方案能够很好地提升 SQCC 方案的安全密钥率和传输距离, 为将来 SQCC 方案的进一步发展提供一个很好的理论参考和实际应用方法.

本文的具体安排如下: 第 2 节详细描述本文提出的基于 OPA 的 SQCC 方案及其噪声模型、方案特点和渐近安全性分析; 第 3 节给出本文方案的性能分析; 第 4 节总结全文.

## 2 基于前置放大器的量子密钥分发融合经典通信方案

### 2.1 方案描述

如图 1 所示, Alice 对自己产生的相干光脉冲先后进行经典 BPSK/QPSK 调制和量子高斯调制, 同时将经典信息比特和量子信息编码到单个相干态$\left|(x_{\rm A}+{\rm e}^{-{\rm i}m_{\rm A}\pi}\alpha)+{\rm i}(p_{\rm A}+{\rm e}^{-{\rm i}n_{\rm A}\pi}\alpha)\right\rangle$上. $x_{\rm A}$和$p_{\rm A}$为用于 CVQKD 的高斯调制信息, $m_{\rm A}$和$n_{\rm A}$为她编码的经典信息比特, $\alpha$为经典调制的相空间位移. 对于 BPSK, $m_{\rm A}=n_{\rm A}\in\{0,1\}$, 而对于 QPSK, $m_{\rm A},n_{\rm A}\in\{0,1\}$. Alice 将调制的相干态衰减到适当的强度并与参考脉冲 (强本振光或者弱相位参考脉冲) 时分偏振复用后一起通过量子信道传输给 Bob. 接收端 Bob 收到信号后先通过偏振控制器调整信号偏振态, 然后利用 OPA 放大信号并将其解

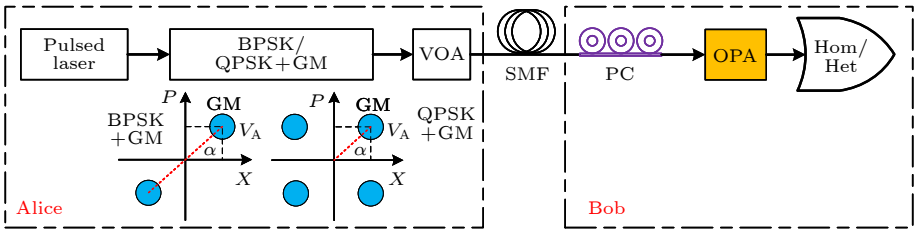


图 1 基于前置光放大器的 SQCC 方案示意图. GM, 高斯调制; VOA, 可调光衰减器; SMF, 单模光纤; PC, 偏振控制器; OPA, 光前置放大器; Hom, 零差探测; Het, 外差探测

Fig. 1. Schematic of the OPA-based SQCC scheme. GM, Gaussian modulation; VOA, variable optical attenuator; SMF, single-mode fiber; PC, polarization controller; OPA, optical preamplifier; Hom, homodyne detection; Het, heterodyne detection.

复用后进行零差或者外差探测来同时获得经典和量子信息. 注意, 当经典调制为 BPSK 调制而接收端测量为外差测量时, Alice 只需要对单个正则分量 ($x_{\rm A}$ 或 $p_{\rm A}$) 进行经典信息调制. 如果 Bob 的正则分量测量结果分别为 $x_{\rm R}$ ($p_{\rm R}$), 那么可以通过如下关系得到经典比特和高斯量子信息[21]:

$$x_{\rm B}=\sqrt{\frac{\delta}{Tg\eta}}x_{\rm R}+(2m_{\rm B}-1)\alpha, \tag{1}$$

$$p_{\rm B}=\sqrt{\frac{\delta}{Tg\eta}}p_{\rm R}+(2n_{\rm B}-1)\alpha, \tag{2}$$

这里 $x_{\rm B}$ ($p_{\rm B}$) 为 Bob 得到的用于后续密钥生成的原始高斯数据, 当 $x_{\rm R}$ ($p_{\rm R}$) $>0$ 时, $m_{\rm B}$ ($n_{\rm B}$) 等于 0, 反之等于 1, $T$ 为信道透射率, $\eta$ 为探测器的量子效率, $g$ 为放大器增益, $\delta=1(2)$代表零差 (外差) 探测. 注意, 本文考虑的 OPA 主要有两类: 理想的相敏感放大器 (phase-sensitive amplifier, PSA)和实际的相不敏感放大器 (phase-insensitive amplifier, PIA). 为了简便和不失一般性, 本文主要考虑基于 PSA 的零差探测且经典调制为 BPSK 和基于 PIA 的外差探测且经典调制为 QPSK 的两种情况.

## 2.2 噪声分析

基于 OPA 的 SQCC 方案的噪声来源主要有 6 个方面: 1) 真空噪声; 2) 原始 CVQKD 系统中不依赖于信号的过噪声 $\xi_0$; 3) 探测器电噪声 $\xi_{\rm ele}$; 4) 经典通信比特误码率引入的过噪声 $\xi_{\rm BER}$; 5) 参考脉冲光子泄露造成的过噪声 $\xi_{\rm leak}$; 6) 相位噪声 $\xi_{\rm phase}$[22]. 经典通信存在一定的误码率, 会给 CVQKD 带来过噪声, 其大小为[22]

$$\xi_{\rm BER}=\frac{4\alpha^2}{N_0}C_{\rm BER}, \tag{3}$$

其中 $C_{\rm BER}$ 为比特误码率, $N_0=1/4$ 为散粒噪声方差. 参考脉冲会产生泄露噪声主要是由于有限的振幅调制和偏振复用消光比. 对于 TLO 方案, 该噪声可以估计为[13]

$$\xi_{\rm leak}^{\rm TLO}=\frac{2\langle n_{\rm ref}^{\rm B}\rangle}{T}10^{-\eta_{\rm A}}10^{-\eta_{\rm P}}, \tag{4}$$

这里 $\langle n_{\rm ref}^{\rm B}\rangle$ 为 Bob 端参考脉冲的平均光子数, $\eta_{\rm A}$ 为振幅调制器的消光率, $\eta_{\rm P}$ 为偏振消光率, $T=10^{-\chi L/10}$ 为信道透射率, $\chi$ 为光纤衰减系数, $L$ 为光纤长度. 对于 LLO 方案, 该噪声可以估计为[22]

$$\xi_{\rm leak}^{\rm LLO}=\frac{\langle n_{\rm ref}^{\rm B}\rangle\Delta t}{TN_0\tau_{\rm c}}10^{-\eta_{\rm A}}10^{-\eta_{\rm P}}, \tag{5}$$

其中 $\Delta t$ 为参考脉冲与信号脉冲的时域时延, $\tau_{\rm c}$ 为 Alice 端信号激光器的相干时间. 由于在高斯调制的基础上对信号叠加了一个经典调制, 信号强度增大的同时对相位噪声也进行了放大, 因此 SQCC 方案中相位噪声是一个重要的噪声来源. 对于 TLO 方案, 相位噪声主要来源于信号和 LO 之间的相位噪声以及其他调制误差带来的相位噪声, 其引入的过噪声大小为[21]

$$\xi_{\rm phase}^{\rm TLO}=\frac{\alpha^2\sigma_\varphi}{N_0}, \tag{6}$$

其中 $\sigma_\varphi$ 为相位噪声方差. 对于 LLO 方案, 其相位噪声 $\sigma_\varphi$ 主要来源于两部分, 一个是不平衡干涉仪结构带来的路径不平衡引入的相位噪声 $\sigma_{\rm I}$; 另一个是由于散粒噪声引起的相位参考脉冲相位测量浮动噪声 $\sigma_{\rm B}$, 它与参考脉冲强度成负相关, 根据文献 [22] 中的实验结果, 参考脉冲强度提升 10 倍, 相位噪声将约为原来的 1/3, 故为了使我们的数值仿真更接近实际的情况, 本文假定加了 OPA 后, 由于弱相位参考信号的散粒噪声引入的相位噪声 $\sigma_{\rm B}=\sigma_{\rm B_0}/3^{\lg g}$. 因此, 总的相位噪声可以表示为[22]

$$\begin{aligned}\xi_{\rm phase}^{\rm LLO}&=\left(\frac{\alpha^2}{N_0}+V_{\rm A}\right)\sigma_\varphi=\left(\frac{\alpha^2}{N_0}+V_{\rm A}\right)(\sigma_{\rm I}+\sigma_{\rm B})\\&=\xi_{\rm I}+\xi_{\rm B},\end{aligned} \tag{7}$$

$$\xi_{\rm I}=\left(\frac{\alpha^2}{N_0}+V_{\rm A}\right)\sigma_{\rm I}, \tag{8}$$

$$\xi_{\rm B}=\left(\frac{\alpha^2}{N_0}+V_{\rm A}\right)\sigma_{\rm B}=\left(\frac{\alpha^2}{N_0}+V_{\rm A}\right)\frac{\sigma_{\rm B_0}}{3^{\lg g}}, \tag{9}$$

其中 $V_{\rm A}$ 为 Alice 的高斯调制方差, $\sigma_{\rm B_0}$ 为原始方案中由于散粒噪声所引起的参考脉冲相位测量浮动噪声.

因此, 现在可以估计全部信道增加的噪声 $\chi_{\rm line}$ 和探测器增加的噪声 $\chi_{\rm det}$ 了. 对于零差和外差探测, 归一化到 Bob 输入端的探测器增加的噪声分别为 $\chi_{\rm hom}=(1-\eta+\xi_{\rm ele}+T\eta\xi_{\rm B})/(g\eta)$ 和 $\chi_{\rm het}=[2-\eta+2\xi_{\rm ele}+T\eta\xi_{\rm B}+\eta N(g-1)]/(g\eta)$[33], 其中 $N$ 为 PIA 内部闲波模的噪声方差. 对于 TLO 和 LLO 方案, 归一化到信道输入端的信道增加的噪声分别

为 $\chi_{\text{line}}^{\text{TLO}}=(1-T)/T+\xi_{\text{phase}}^{\text{TLO}}+\xi_0+\xi_{\text{leak}}^{\text{TLO}}$ 和 $\chi_{\text{line}}^{\text{LLO}}=(1-T)/T+\xi_{\text{I}}+\xi_0+\xi_{\text{BER}}+\xi_{\text{leak}}^{\text{LLO}}$. 这样, 归一化到信道输入端的总噪声就等于 $\chi_{\text{tot}}=\chi_{\text{line}}+\chi_{\text{det}}/T$. 注意, 零差探测时 $\chi_{\text{det}}=\chi_{\text{hom}}$, 外差探测时 $\chi_{\text{det}}=\chi_{\text{het}}$.

## 2.3 方案特点

相比于原方案, OPA 的引入对 SQCC 系统有几个方面的益处. 首先, 它对信号放大的同时能够补偿探测器的不完美, 这在文献 [24,25,33] 中已经证明了这一点. 其次, 之前研究已经表明 SQCC 方案中经典调制对量子系统的影响是限制该方案的主要因素. 本文提出的方案放大了接收端的经典调制信号, 使得相同 BER 下对发送端的经典调制振幅大小的要求可以降低, 这将减少经典调制对 CV-QKD 系统的噪声影响. 根据文献 [21,22] 中的结果和放大器对探测器的补偿作用 [33], 加了放大器之后发送端经典调制相空间位移将变为

$$\alpha=w\sqrt{fN_0}\frac{\sqrt{gT\eta(V_{\text{A}}+\xi_{\text{leak}}+\xi_0)+\delta(1+\xi_{\text{ele}})+(\delta-1)\eta N(g-1)}}{\sqrt{gT\eta(\delta-fw^2\sigma_\varphi)}},\tag{10}$$

其中 $w=\text{erf}^{-1}(1-2C_{\text{BER}})$, $f=2(4)$对应经典 BPSK(QPSK) 调制. 根据 (10) 式, 图 2 给出了 $\alpha$ 与距离之间函数关系的数值仿真结果, 其中 $g=1$ 代表不加放大器. 从图 2 可以很明显地看到两种情况下都有 $\alpha$ 随着增益 $g$ 的增加而变小. 这说明加了 OPA 之后误码率带来的噪声以及相位噪声都能得到一定的缓解, 尤其是基于 PSA 零差探测的情形. 由于实际的 PIA 会引入一定的噪声, 因此基于 PIA 外差探测情形下的 $\alpha$ 降低程度要小一些. 再次, 对于 LLO 方案, OPA 同样能够放大弱相位参考信号, 从而降低由于弱相位参考信号的散粒噪声引入的相位噪声. 因此, 相比于原方案, 基于 OPA 的 SQCC 方案能够在相等的 BER 下具有更好的系统鲁棒性和稳定性, 系统的安全密钥率和传输距离都能够得到提升.

## 2.4 渐近安全性

基于 OPA 的 CVQKD 在集体攻击下的渐近密钥率可以表示为 [33]

$$R=\beta I_{\text{AB}}-\chi_{\text{BE}},\tag{11}$$

其中 $I_{\text{AB}}$ 为 Alice 和 Bob 之间的香浓互信息量, $\chi_{\text{BE}}$ 为 Eve 和 Bob 之间互信息的 Holevo 界, $\beta$ 为反向协商效率.

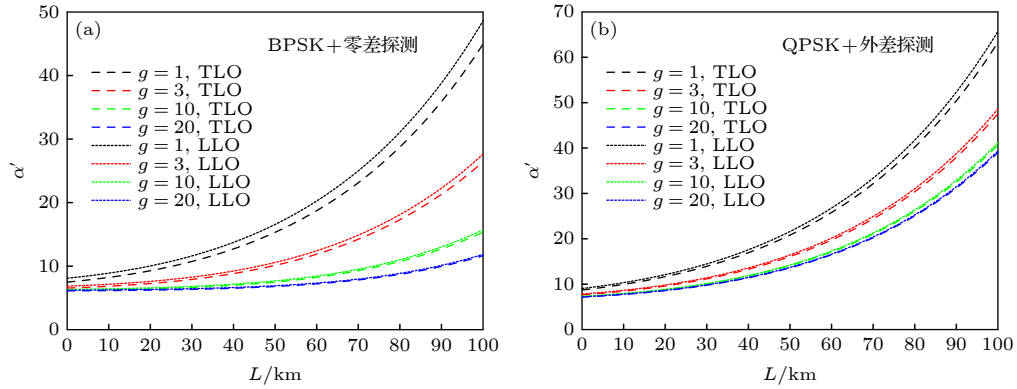


图 2 BER 达到 $10^{-9}$ 所需要的相空间位移 $\alpha$ 与距离的函数关系 (a) 基于 PSA 的零差探测情况下的结果; (b) 基于 PIA 的外差探测情况下的结果. 仿真参数设定如下: $V_{\text{A}}=4$, $\gamma=0.2$ dB/km, $\eta=0.5$, $\xi_{\text{ele}}=0.1$, $\Delta t=10^{-9}$ s, $\tau_{\text{c}}=1$ μs, $\xi_0=0.01$, $N=1.5$; 对于 TLO 方案, $\eta_{\text{A}}=65$ dB, $\eta_{\text{P}}=35$ dB, $n_{\text{ref}}^{\text{B}}=10^6$, $\sigma_\varphi=10^{-4}$ rad$^2$; 对于 LLO 方案, $\eta_{\text{A}}=30$ dB, $\eta_{\text{P}}=30$ dB, $n_{\text{ref}}^{\text{B}}=10^3$, $\sigma_{\text{I}}=10^{-4}$ rad$^2$, $\sigma_{\text{B}_0}=2\times10^{-3}$ rad$^2$

Fig. 2. The needed phase space displacement $\alpha'$ as a function of transmission distance while BER = $10^{-9}$: (a) The results under the case of homodyne detection based on PSA; (b) the results under the case of heterodyne detection based on PIA. Simulation parameters are set as follows: $V_{\text{A}}=4$, $\gamma=0.2$ dB/km, $\eta=0.5$, $\xi_{\text{ele}}=0.1$, $\Delta t=10^{-9}$ s, $\tau_{\text{c}}=1$ μs, $\xi_0=0.01$, $N=1.5$; for the scheme of TLO, $\eta_{\text{A}}=65$ dB, $\eta_{\text{P}}=35$ dB, $n_{\text{ref}}^{\text{B}}=10^6$, $\sigma_\varphi=10^{-4}$ rad$^2$; for the scheme of LLO, $\eta_{\text{A}}=30$ dB, $\eta_{\text{P}}=30$ dB, $n_{\text{ref}}^{\text{B}}=10^3$, $\sigma_{\text{I}}=10^{-4}$ rad$^2$, $\sigma_{\text{B}_0}=2\times10^{-3}$ rad$^2$.

对于基于 PSA 零差探测的情形, Alice 和 Bob 之间的互信息为

$$I_{\mathrm{AB}}=\frac{1}{2}\log_2\frac{V_{\mathrm{A}}+1+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}. \tag{12}$$

Eve 和 Bob 之间互信息的 Holevo 界为

$$\chi_{\mathrm{BE}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right), \tag{13}$$

其中 $G(x)=(x+1)\log_2(x+1)-x\log_2 x$, 特征值 $\lambda_{1,2}$ 为

$$\lambda_{1,2}^2=\frac{1}{2}(A\pm\sqrt{A^2-4B}), \tag{14}$$

$$A=(V_{\mathrm{A}}+1)^2(1-2T)+2T+T^2(V_{\mathrm{A}}+1+\chi_{\mathrm{line}})^2, \tag{15}$$

$$B=T^2[(V_{\mathrm{A}}+1)\chi_{\mathrm{line}}+1]^2; \tag{16}$$

特征值 $\lambda_{3,4}$ 为

$$\lambda_{3,4}^2=\frac{1}{2}\left(C_{\mathrm{hom}}\pm\sqrt{C_{\mathrm{hom}}^2-4D_{\mathrm{hom}}}\right), \tag{17}$$

$$C_{\mathrm{hom}}=\frac{A\chi_{\mathrm{hom}}+(V_{\mathrm{A}}+1)\sqrt{B}+T(V_{\mathrm{A}}+1+\chi_{\mathrm{line}})}{T(V_{\mathrm{A}}+1+\chi_{\mathrm{tot}})}, \tag{18}$$

$$D_{\mathrm{hom}}=\sqrt{B}\frac{V_{\mathrm{A}}+1+\sqrt{B}\chi_{\mathrm{hom}}}{T(V_{\mathrm{A}}+1+\chi_{\mathrm{tot}})}; \tag{19}$$

特征值 $\lambda_5=1$.

对于基于 PIA 外差探测的情形, Alice 和 Bob 之间的互信息为

$$I_{\mathrm{AB}}=\log_2\frac{V_{\mathrm{A}}+1+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}. \tag{20}$$

Eve 和 Bob 之间互信息的 Holevo 界为

$$\chi_{\mathrm{BE}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{7}G\left(\frac{\lambda_i-1}{2}\right), \tag{21}$$

特征值 $\lambda_{1,2}$ 与 (14) 式相同, 特征值 $\lambda_{5,6,7}=1$, 而特征值 $\lambda_{3,4}$ 为

$$\lambda_{3,4}^2=\frac{1}{2}\left(C_{\mathrm{het}}\pm\sqrt{C_{\mathrm{het}}^2-4D_{\mathrm{het}}}\right), \tag{22}$$

$$\begin{aligned}C_{\mathrm{het}}=&\frac{1}{[T(V_{\mathrm{A}}+1+\chi_{\mathrm{tot}})]^2}\{A(\chi_{\mathrm{het}})^2+B+1+2\chi_{\mathrm{het}}\\&\times[(V_{\mathrm{A}}+1)\sqrt{B}+T(V_{\mathrm{A}}+1+\chi_{\mathrm{line}})]\\&+2T[(V_{\mathrm{A}}+1)^2-1]\},\end{aligned} \tag{23}$$

$$D_{\mathrm{het}}=\left[\frac{V_{\mathrm{A}}+1+\sqrt{B}\chi_{\mathrm{het}}}{T(V_{\mathrm{A}}+1+\chi_{\mathrm{tot}})}\right]^2. \tag{24}$$

## 3 性能分析

本节从安全密钥率和传输距离的角度讨论所提出方案的性能提升. 基本的全局仿真参数及其设定如下: Alice 端的调制方差 $V_{\mathrm{A}}=4$, 量子信道衰减系数 $\gamma=0.2$ dB/km, 探测器量子效率 $\eta=0.5$, 探测器电噪声 $\xi_{\mathrm{ele}}=0.1$, 参考脉冲与信号脉冲的时域时延 $\Delta t=10^{-9}$ s, 发送端激光器相干时间 $\tau_{\mathrm{c}}=1$ μs, 系统原始过噪声 $\xi_0=0.01$[22], PIA 引入的噪声为 $N=1.5$[33]; 对于 TLO 方案, 振幅调制器消光率 $\eta_{\mathrm{A}}=65$ dB, 偏振复用消光率 $\eta_{\mathrm{P}}=35$ dB[13], Bob 端 LO 平均光子数 $n_{\mathrm{ref}}^{\mathrm{B}}=10^6$, 相位噪声 $\sigma_\varphi=10^{-4}$ (或 $10^{-5}$) rad$^2$[34]; 对于 LLO 方案, 振幅调制器消光率 $\eta_{\mathrm{A}}=30$ dB, 偏振复用消光率 $\eta_{\mathrm{P}}=30$ dB, Bob 端参考脉冲平均光子数 $n_{\mathrm{ref}}^{\mathrm{B}}=10^3$, 路劲不平衡相位噪声 $\sigma_{\mathrm{I}}=10^{-4}$ (或 $10^{-5}$) rad$^2$, 参考脉冲的散粒噪声引入的相位噪声 $\sigma_{\mathrm{B}_0}=2\times10^{-3}$ rad$^2$[22].

图 3 给出了基于 PSA 零差探测和基于 PIS 外差探测两种情况下安全密钥率在不同距离下的数值仿真结果, 其中黑线代表原始 SQCC 方案的结果, 其他颜色线代表本文提出的基于 OPA 的 SQCC 方案在不同增益 $g$ 下的结果, 虚线表示 TLO 情形而点线表示 LLO 情形. 图 3(a) 和图 3(b) 表示当 $\sigma_\varphi=10^{-4}$ rad$^2$ 和 $\sigma_{\mathrm{I}}=10^{-4}$ rad$^2$ 时, 基于 PSA 的零差探测和基于 PIA 的外差探测两种情形下的结果. 图 3(c) 和图 3(d) 表示当 $\sigma_\varphi=10^{-5}$ rad$^2$ 和 $\sigma_{\mathrm{I}}=10^{-5}$ rad$^2$ 时两种情形下的结果. 从图 3 中的结果可以看出, 无论是 TLO 还是 LLO 情形, 本文提出方案相比于原始方案不管在安全密钥率还是传输距离上都有很好的性能提升, 且放大器增益 $g$ 越大提升效果越明显, 这种提升相比文献 [33] 中基于 OPA 的传统 CVQKD 协议要更好, 这主要得益于 OPA 对信号的放大使得对 CVQKD 有较大影响的经典调制相空间位移 $\alpha$ 在不影响 BER 的情况下能够变小, 从而使得 CVQKD 系统有更小的过噪声, 系统的鲁棒性、稳定性和性能将更好. 同时, 在放大器的增益作用下, LLO 情形下的相位噪声得到了更好的缓解, 使得加了放大器之后 LLO 情形的性能与 TLO 情形的性能更为接近.

比较图 3(a) 和图 3(c) 或者图 3(b) 和图 3(d) 可以发现, 在系统本身的过噪声更小的时候, OPA 给系统带来的性能提升效果将会变小, 这是因为

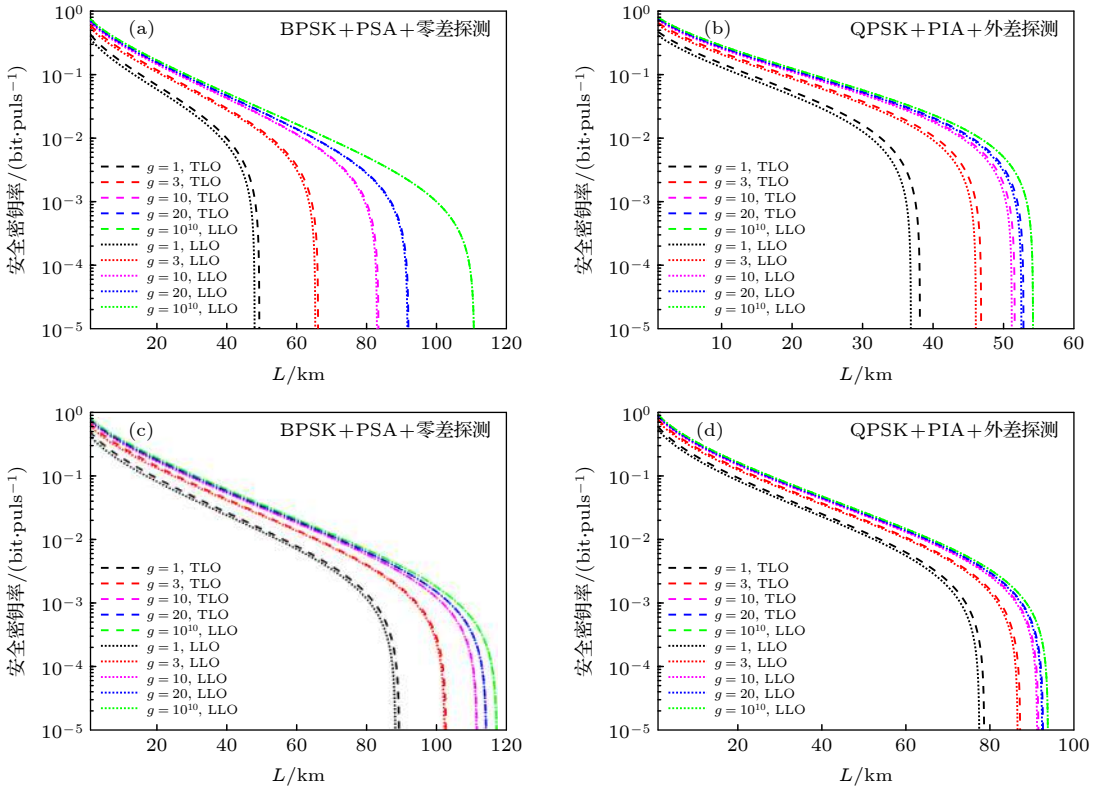


图 3 基于 OPA 的 SQCC 方案安全密钥率与传输距离的关系 (a), (b) 当 $\sigma_\varphi = 10^{-4}$ rad$^2$ 和 $\sigma_{\rm I} = 10^{-4}$ rad$^2$ 时, 基于 PSA 的零差探测和基于 PIA 的外差探测情形下的安全密钥率与传输距离的关系; (c), (d) 当 $\sigma_\varphi = 10^{-5}$ rad$^2$ 和 $\sigma_{\rm I} = 10^{-5}$ rad$^2$ 时, 与 (a) 和 (b) 同样情形下的仿真结果

Fig. 3. The secure key rate as a function of transmission distance for the proposed OPA-based SQCC scheme: (a), (b) The secure key rate as a function of transmission distance for the PSA-based case with homodyne detection and the PIA-based case with heterodyne detection, while $\sigma_\varphi = 10^{-4}$ rad$^2$ and $\sigma_{\rm I} = 10^{-4}$ rad$^2$; (c), (d) the simulation results for the same cases with (a) and (b), while $\sigma_\varphi = 10^{-5}$ rad$^2$ and $\sigma_{\rm I} = 10^{-5}$ rad$^2$.

系统本身过噪声更小时, 系统性能与加了 OPA 之后系统能够达到的极限性能 (当$g = 10^{10}$时) 的差距相对来说变小了, 也就是图 3 中绿线和黑线之间的差距变小了. 当$g = 10^{10}$时 (相当于无穷大), 可以发现探测器增加的噪声将趋近于 0, 这相当于 OPA 完全补偿了探测器的不完美, 使得系统性能达到最大.

## 4 结 论

本文提出了基于 OPA 的 SQCC 方案. 相比于原始的 SQCC 方案, 本文提出的方案不仅能够补偿实际探测器的不完美, 而且能够在保证同样低的经典通信 BER 的情况下降低对发送端经典调制相空间位移$\alpha$的要求, 从而降低经典调制对 CVQKD 系统过噪声方面的影响, 使得系统的鲁棒性和稳定性更好, 性能也能得到提升. 在实验可达到的参数假设下, 数值仿真结果证明了本文所提出的基于 OPA 的方案相比原方案在安全密钥率和传输距离上确实具有更好的性能. 同时, OPA 是常见的光学设备, 在经典通信领域有着广泛的应用, 基于 OPA 的 SQCC 方案与现有的相干光通信网络有着良好的融合度. 因此, 本文提出的方案具有很好的实用价值, 为 SQCC 方案在复杂环境中的实际应用提供了一种切实可行的办法, 也让该方案具有更广的适用性.

## 参考文献

[1] Li J, Chen Y H, Pan Z S, Sun F Q, Li N, Li L L 2016 *Acta Phys. Sin.* **3** 030302 (in Chinese) [李剑, 陈彦桦, 潘泽世, 孙风琪, 李娜, 黎蕾蕾 2016 物理学报 **3** 030302]

[2] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙, 莫小范, 桂有珍, 韩正甫, 郭光灿 2004 物理学报 **53** 2123]

[3] Cao Z W, Zhang S H, Peng X Y, Zhao G, Chai G, Li D W 2017 *Acta Phys. Sin.* **66** 020301 (in Chinese) [曹正文, 张爽浩, 冯晓毅, 赵光, 柴庚, 李东伟 2017 物理学报 **66** 020301]

[4] Lo H K, Curty M, Tamaki K 2014 *Nat. Photonics* **8** 595

[5] Braunstein S L, van Loock P 2005 *Rev. Mod. Phys.* **77** 513

[6] 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. Photon.* **12** 1012

[7] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers Systems, and Signal Processing* Bangalore, India, December 10–12, 1984 p175

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

[9] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343

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

[11] Qi B, Lougovski P, Pooser R, Grice W, Bobrek M 2015 *Phys. Rev. X* **5** 041009

[12] Huang D, Huang P, Lin D K, Wang C, Zeng G H 2015 *Opt. Lett.* **40** 3695

[13] Huang D, Huang P, Lin D, Zeng G 2016 *Sci. Rep.* **6** 19201

[14] Huang D, Lin D K, Wang C, Liu W Q, Fang S H, Peng J Y, Huang P, Zeng G H 2015 *Opt. Express* **23** 17511

[15] 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

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

[17] Huang D, Huang P, Li H, Wang T, Zhou Y, Zeng G 2016 *Opt. Lett.* **41** 3511

[18] Qi B, Zhu W, Qian L, Lo H K 2010 *New J. Phys.* **12** 103042

[19] Kumar R, Qin H, Alleaume R 2015 *New J. Phys.* **17** 043027

[20] Eriksson T A, Puttnam B J, Rademacher G, Luís R S, Fujiwara M, Takeoka M, Awaji Y, Sasaki M, Wada N 2019 *IEEE Photonics Technol. Lett.* **31** 467

[21] Qi B 2016 *Phys. Rev. A* **94** 042340

[22] Qi B, Lim C C W 2018 *Phys. Rev. Appl.* **9** 054008

[23] Yang C, Ma C, Hu L, He G 2018 *Int. J. Theor. Phys.* **57** 2775

[24] Wu X, Wang Y, Liao Q, Zhong H, Guo Y 2019 *Entropy* **21** 333

[25] Wu X D, Wang Y J, Huang D, Guo Y 2020 *Front. Phys.* **15** 31601

[26] Pan D, Ng S X, Ruan D, Yin L, Long G, Hanzo L 2020 *Phys. Rev. A* **101** 012343

[27] Guo Y, Liao Q, Wang Y, Huang D, Huang P, Zeng G 2017 *Phys. Rev. A* **95** 032304

[28] Zhong H, Wang Y J, Wang X D, Liao Q, Wu X D, Guo Y 2018 *Entropy* **20** 578

[29] Wu X D, Wang Y J, Zhong H, Liao Q, Guo Y 2019 *Front. Phys.* **14** 41501

[30] Guo Y, Ye W, Zhong H, Liao Q 2019 *Phys. Rev. A* **99** 032327

[31] Ye W, Zhong H, Liao Q, Huang D, Hu L, Guo Y 2019 *Opt. Express* **27** 17186

[32] Ye W, Guo Y, Xia Y, Zhong H, Zhang H, Ding J Z, Hu L Y 2020 *Acta Phys. Sin.* **69** 060301 (in Chinese) [叶炜, 郭迎, 夏莹, 钟海, 张欢, 丁建枝, 胡利云 2020 物理学报 **69** 060301]

[33] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 114014

[34] 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

# Optical preamplifier based simultaneous quantum key distribution and classical communication scheme*

Zhong Hai [1)] Ye Wei [1)] Wu Xiao-Dong [2)†] Guo Ying [1)2)‡]

1) (*School of Computer Science and Engineering, Central South University, Changsha* 410083, *China*)

2) (*School of Automation, Central South University, Changsha* 410083, *China*)

( Received 5 June 2020; revised manuscript received 7 August 2020 )

**Abstract**

That the simultaneous quantum key distribution and classical communication (SQCC) scheme are combined with the continuous variable quantum key distribution (CVQKD) and the classical communication together, will provide an effective method to implement the simultaneous CVQKD and the classical communication in the existing optical networks in the future. However, superimposing a classical signal on the quantum signal will introduce excess noise into the CVQKD system, thus greatly reducing the performance of the system. In this paper, a novel scheme of SQCC based on optical preamplifier (OPA) is proposed, that is, the OPA is inserted into the receiver to improve the performance of the system. On the one hand, under the condition of the same bit error rate, the amplification of the signal by the OPA can reduce the requirement for the modulation amplitude of the classical signal at the sending end, thereby reducing the noise effect of the classical signal on the quantum signal. On the other hand, the OPA can compensate for the imperfection of the receiver detector. Moreover, in the case of locally generated local oscillator, the amplifier can also amplify the weak phase reference pulse, and thus reducing the phase excess noise caused by the shot noise of the weak phase reference pulse. Numerical simulation results show that the proposed scheme has better performance than the original scheme in the sense of security key rate and transmission distance. These results show that this scheme provides an effective and practical method for the further development and practical application of the SQCC scheme.

**Keywords:** continuous variable, simultaneous quantum key distribution and classical communication, optical preamplifier

**PACS:** 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.70.20200855

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61872390, 61801522) and the Postgraduate Independent Exploration and Innovation Project of Central South University, China (Grant No. 2020zzts136).

† Corresponding author. E-mail: wuxiaodong2018@foxmail.com

‡ Corresponding author. E-mail: yingguo@csu.edu.cn