



基于相不敏感放大器的高斯调制连续变量量子秘密共享

曾泽齐, 范廉政, 秦哲, 李得龙, 廖骏*

湖南大学计算机学院, 长沙 410082

* 通信作者. E-mail: llqqlq@hnu.edu.cn

收稿日期: 2025-10-22; 修回日期: 2025-11-19; 接受日期: 2026-01-04; 网络出版日期: 2026-05-22

国家自然科学基金 (批准号: 62101180)、湖南省重点研发计划 (批准号: 2025QK3011) 和中国工程科技发展战略湖南研究院战略研究与咨询 (批准号: 2025WK1001) 资助项目

摘要 探测器作为连续变量量子秘密共享系统的核心组件, 其性能对整个系统至关重要. 然而, 在实际情况下, 探测器是非理想的, 其缺陷会对信号造成噪声干扰, 导致连续变量量子秘密共享系统的实际性能下降. 为了解决此问题, 本文提出基于相不敏感放大器的高斯调制连续变量量子秘密共享方案. 其中, 相不敏感放大器能均匀地放大量子信号的每个正交分量, 提高信号的功率, 从而可以相对减小非理想探测器的缺陷对信号造成的噪声干扰, 提高系统的实际性能. 实验结果表明, 相不敏感放大器能够有效提高连续变量量子秘密共享系统的密钥率和安全传输距离, 且在高增益情况下系统实际性能接近理论上采用理想探测器的连续变量量子秘密共享系统性能. 本文提出的方案为解决由非理想探测器缺陷造成的连续变量量子秘密共享系统性能降低问题, 提供了解决思路.

关键词 量子秘密共享, 连续变量, 量子通信, 相不敏感放大器, 量子密码

1 引言

秘密共享将一个秘密信息分割成多份, 并将其分配给不同的参与者, 只有满足特定条件的参与者共同协作, 才能恢复原始秘密^[1]. 随着量子技术的飞速发展, 出现了量子版本的秘密共享, 即量子秘密共享 (quantum secret sharing, QSS)^[2]. QSS 的安全性不再基于数学上的计算复杂性, 而是由量子力学原理保证, 从而将秘密共享的理论安全水平从计算安全提升到无条件安全. 相较于仅允许两名合法通信方进行量子通信的量子密钥分发 (quantum key distribution, QKD) 技术^[3~8], QSS^[9~12] 不仅突破了 QKD 对用户数量的限制, 理论上可以支持任意数量的用户, 更重要的是允许用户之间进行安全的秘密共享.

根据编码方式的不同, QSS 被分为两类: 离散变量 (discrete-variable, DV) QSS^[13,14] 和连续变量 (continuous-variable, CV) QSS^[15~17]. 近年来 DV-QSS 在实验中取得了诸多进展. 2023 年, Shen 等人^[18] 提出了基于相位编码的 QSS 协议, 去除了对纠缠资源的需求和对相位随机化的需要, 降低了实验复杂度. 在此基础上, 2024 年, Wang 等人^[19] 进一步提出了用有限脉冲实现的相干态量子秘密共享, 通过在安全密钥生成和错误率分析过程中对所有参与者采用对称基选择, 在不事先知晓不可信用户身份的情况下实现了安全密钥生成, 解决了之前协议因不对称基选择而产生的安全漏洞. 然而, DV-QSS^[20] 通常需要将密钥信息编码在单个光子偏振态上, 而高纯度单光子态的制备和测量需要使用高质量的单光子源和高灵敏度的单光子探测器完成, 实际实现较困难. 而 CV-

引用格式: 曾泽齐, 范廉政, 秦哲, 等. 基于相不敏感放大器的高斯调制连续变量量子秘密共享. 中国科学: 信息科学, 2026, 56: 1566–1578, doi: 10.1360/SSI-2025-0437

Zeng Z Q, Fan L Z, Qin Z, et al. Gaussian-modulated continuous-variable quantum secret sharing based on phase-insensitive amplifiers. Sci Sin Inform, 2026, 56: 1566–1578, doi: 10.1360/SSI-2025-0437

QSS^[21~24]继承了连续变量技术的优势,将密钥信息编码在量子态相空间的正交分量上,可兼容现有光通信技术实现高质量的测量. CV-QSS 技术实现相对简单,探测设备相对成熟,是 QSS 的重要发展方向. 2004 年, Lance 等人^[25]基于连续变量纠缠态实现了 $(2,3)$ 门限量子态共享,该方案可以扩展到任意 (t,n) 门限方案. 2013 年, Lau 等人^[26]将 QSS 扩展到连续变量簇态领域,并证明了通过分发连续变量簇态可以共享经典信息和量子信息. 2017 年, Kogias 等人^[27]提出了一种基于纠缠态的 CV-QSS 方案,并推导了其在渐近极限下任意 (t,n) 门限方案在对抗窃听者和不诚实参与者的充分条件. 然而,连续变量纠缠态仍然基于多方纠缠,当参与者数量很大时现有技术还难以实现,并且其仍然面临着难以容忍的信道损耗. 为避免连续变量纠缠态的使用,2019 年, Grice 等人^[28]提出了一种基于弱相干态的 CV-QSS 方案,提高了 CV-QSS 可容忍的信道噪声,并提出 CV-QSS 理论上可以通过高斯调制相干态实现,减少了制备过程的困难. 但该方案为 (n,n) 门限的 CV-QSS,需要所有参与者合作才能恢复秘密信息,具有较大的限制. 2020 年, Wang 等人^[29]提出了一种改进的基于弱相干态的 (t,n) 门限的 CV-QSS 方案,通过使用拉格朗日插值法将秘密分成 n 份,使得该方案至少 t 个参与者合作才能恢复原始秘密,少于 t 个则无法获取任何关于秘密的信息,大幅提升了方案的灵活性. 然而实际的高斯调制方案需要高稳定性的高消光比调制器,这大幅提高了调制成本. 为此,2020 年, Wu 等人^[30]提出了一种基于热源的 CV-QSS,该方案的实现不再需要高稳定性的高消光比调制器,降低了调制成本. 2021 年, Liao 等人^[31]将相干态的调制方式拓展到离散调制相干态 (discretely modulated coherent state, DMCS),提出了一种基于 DMCS 的 CV-QSS,进一步降低了实际 CV-QSS 中量子态制备过程中的困难. 在此基础上,2023 年, Liao 等人^[32]进一步提出了一种基于多环离散调制的 CV-QSS,通过多环离散调制降低了探测器分辨 DMCS 的错误率,提高了离散调制 CV-QSS 的性能.

上述 CV-QSS 方案虽对 CV-QSS 的各个方面进行了改进,但均未讨论 CV-QSS 中非理想探测器的缺陷所造成的实际问题. 事实上,由于实际探测器存在缺陷, CV-QSS 系统的密钥率和安全传输距离实际上难以达到理论性能. 幸运的是,在 QKD 领域,针对非理想探测器缺陷这个问题, Fossier 等人^[33]于 2009 年提出了一种基于光学参数放大器的 QKD 方案,证明了光学参数放大器中的相敏放大器 (phase-sensitive amplifier, PSA) 和相不敏感放大器 (phase-insensitive amplifier, PIA) 均可用于解决由于非理想探测器的缺陷导致的 QKD 系统性能下降的问题. 2022 年, Wu 等人^[34]提出了一种基于实际探测器补偿的离散调制连续变量测量设备无关 QKD 方案,使用了 PSA 对零差探测器进行补偿,有效提升了系统的密钥率和安全传输距离. 相比之下,目前 CV-QSS 领域对非理想探测器的缺陷的研究尚不充分,但是,深入研究并解决非理想探测器的缺陷造成的 CV-QSS 系统实际性能下降问题,具有重要的意义,有助于解决 CV-QSS 系统的实际部署问题.

为解决非理想探测器缺陷造成的 CV-QSS 系统实际性能下降问题,本文提出基于 PIA 的高斯调制 CV-QSS 方案. 该方案通过将 PIA 部署在分发者 Dealer 端以补偿非理想探测器的缺陷. 具体来说,PIA 可以均匀地放大信号的每个正交分量,提高信号的功率,从而可以相对减小非理想探测器的缺陷对信号造成的噪声干扰,提高 CV-QSS 系统的实际性能. 实验结果表明,本文所提方案有效补偿了非理想探测器的缺陷,在使用非理想探测器情况下的密钥率和最大用户数量均优于传统 CV-QSS 方案.

本文第 2 节详细介绍所提出的方案的具体内容;第 3 节推导基于 PIA 的高斯调制 CV-QSS 方案的密钥率等公式;第 4 节分析比较本文所提方案与传统 CV-QSS 系统的性能差距;第 5 节作出总结.

2 基于 PIA 的高斯调制 CV-QSS

PIA 是一种非简并光学参数放大器^[35],由一个增益因子为 g 的无噪放大器和方差为 N 的 EPR 态组成, EPR 态的其中一个模式进入放大器的第二个输入端口以模拟放大器的固有噪声. PIA 同等程度地放大两种正交分量,其放大作用可以等效为对信号态执行双模压缩操作,但由于放大时信号态要与 PIA 内的真空模式相互作用,因而会额外引入一定的噪声. 图 1 给出了基于 PIA 的高斯调制 CV-QSS 的方案图. 在该方案中 PIA 被部署在分发者 Dealer 内部以保证其无法被窃听者 Eve 攻击. M 个用户与分发者 Dealer 通过一条量子信道依次连接. 每个用户将本地调制的量子信号发送给分发者 Dealer. 当叠加信号发送到量子信道输出端时,PIA 放大发送过

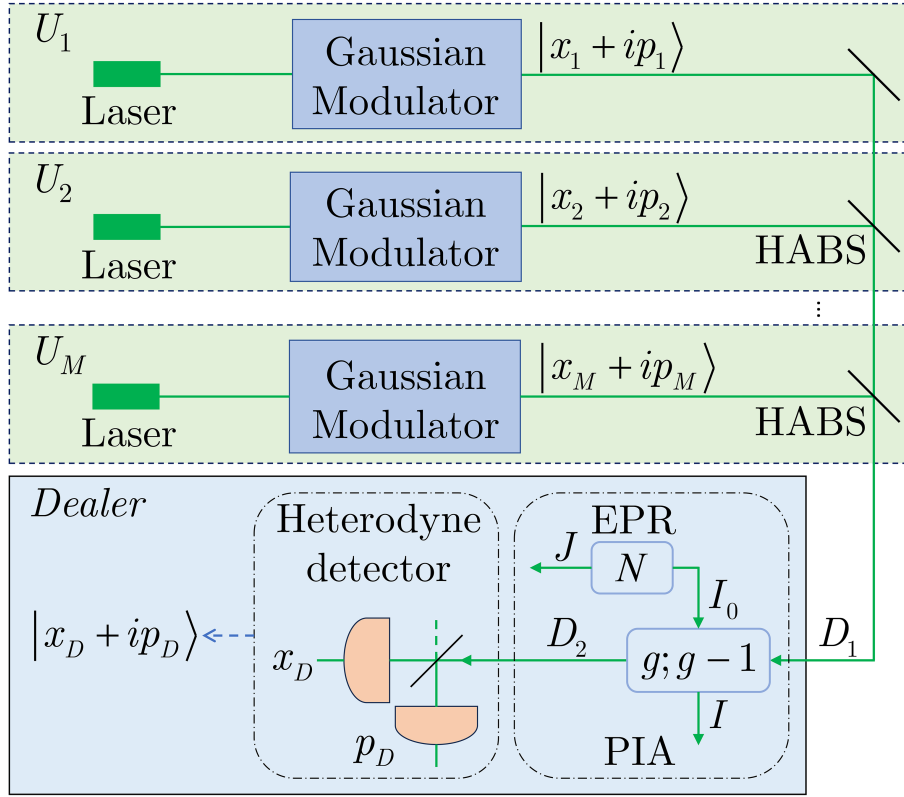


图 1 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案. HABS 为高度非对称分束器.

Figure 1 (Color online) Gaussian-modulated CV-QSS scheme based on PIA. HABS stands for highly asymmetric beam splitter.

来的量子信号, 增大信号的功率. 分发者 Dealer 随后使用外差探测器对放大后的信号进行测量并得到测量结果. 具体的方案步骤如下.

(1) U_1 在本地制备高斯调制相干态 $|x_1 + ip_1\rangle$ 并将其发送入量子信道. U_2 同样独立制备高斯调制相干态 $|x_2 + ip_2\rangle$, 并通过 HABS 将相干态 $|x_2 + ip_2\rangle$ 耦合到与 U_1 输入信号相同的时空模式. 其他用户执行相同的操作. 携带有所有用户信息的相干态经量子信道传输后进入 PIA 输入端. 携带有所有用户信息的相干态表达式为 $|\sum_{r=1}^M \sqrt{T_r} x_r + i \sum_{r=1}^M \sqrt{T_r} p_r\rangle$.

(2) PIA 对发送过来的信号进行放大操作, 增大信号的功率. 原携带有所有用户信息的相干态 $|\sum_{r=1}^M \sqrt{T_r} x_r + i \sum_{r=1}^M \sqrt{T_r} p_r\rangle$ 转化为相干态 $|(\sum_{r=1}^M \sqrt{T_r} x_r)^P + i(\sum_{r=1}^M \sqrt{T_r} p_r)^P\rangle$, 其中 $(\sum_{r=1}^M \sqrt{T_r} x_r)^P$ 和 $(\sum_{r=1}^M \sqrt{T_r} p_r)^P$ 分别表示 PIA 对信号的位置和动量分量进行的放大操作. 分发者 Dealer 使用外差探测器对放大后的相干态进行测量, 保存测量结果 $\{x_D, p_D\}$.

(3) 以上步骤重复多次, 分发者 Dealer 在多次测量结果中随机选择一部分, 要求所有的用户公布相应的数据, 由相应的测量结果估算出信道透过率 $\{T_1, T_2, \dots, T_M\}$ [28]. 所有用户舍弃公布的数据.

(4) 分发者 Dealer 选择一个用户为可信方, 其他 $M - 1$ 个用户为不可信方. 之后随机选择多次测量结果中的一部分, 要求除该用户外的其他所有用户公布相应的数据. 分发者 Dealer 对该部分的测量结果进行置换操作, 即 $x_W = x_D - (\sum_{r=1}^M \sqrt{T_r} x_r)^P$, $p_W = p_D - (\sum_{r=1}^M \sqrt{T_r} p_r)^P$. 之后分发者 Dealer 对 $\{x_W, p_W\}$ 和可信用户 U_1 原始数据两者相同的部分进行分析 [33], 估算出安全密钥率 R_1 . 所有用户舍弃公布的数据.

(5) 将步骤 4 重复 M 次, 每次选择不同的用户作为可信方. 最后, 分发者 Dealer 得到 M 个密钥率 $\{R_1, R_2, \dots, R_M\}$, 选择 M 个密钥率中的最小值确定为安全密钥率 R , 并采用反向协商方法生成最终密钥 $K = K_1 \oplus K_2 \oplus \dots \oplus K_M$ [36, 37].

(6) 分发者 Dealer 通过 $E = M \oplus K$ 对原始消息 M 进行加密, 得到加密消息 E . 之后, 分发者 Dealer 向所

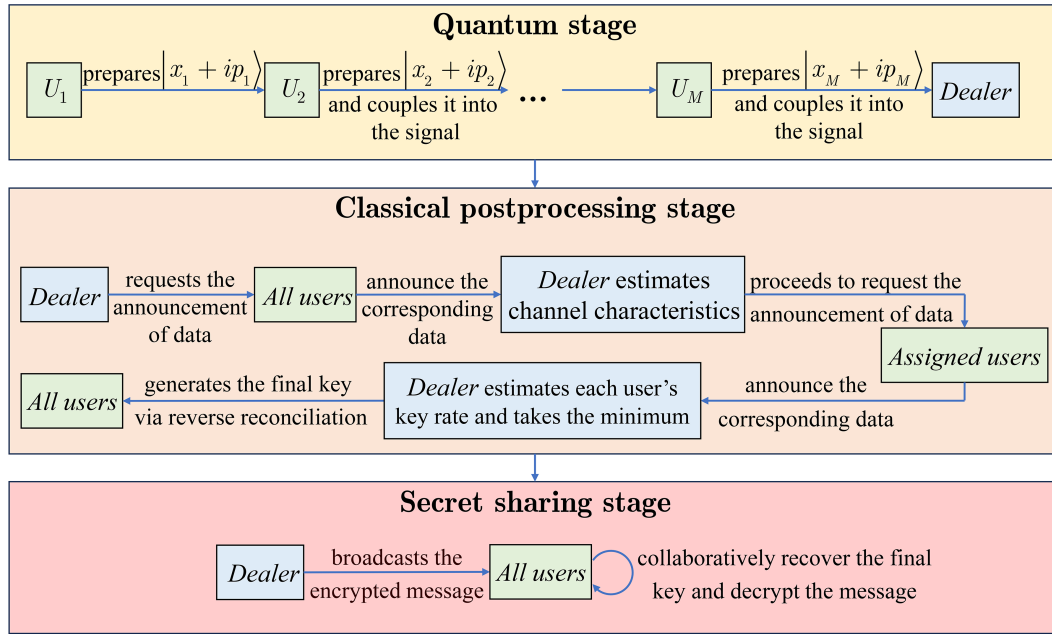


图 2 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案的信息流向图.

Figure 2 (Color online) The information flow diagram of the Gaussian-modulated CV-QSS scheme based on PIA.

有用户广播加密消息 E . 显然, 所有用户需要合作才能恢复出最终密钥 K , 从而解密出原始消息 M .

基于 PIA 的高斯调制 CV-QSS 方案的信息流向主要分为 3 个阶段, 如图 2 所示. 量子阶段的信息流向为所有用户依次向分发者 Dealer 发送本地制备的量子态. 经典后处理阶段的信息流向为分发者 Dealer 首先向所有用户请求公布数据, 随后所有用户向分发者 Dealer 公布相应数据用以估计信道特性, 分发者 Dealer 继续请求对应用户公布数据, 对应用户向分发者 Dealer 公布相应数据用以估算每个用户的点对点密钥率, 分发者 Dealer 通过与每个用户进行反向协商生成最终密钥. 秘密共享阶段的信息流向为分发者 Dealer 向所有用户广播加密消息, 所有用户合作恢复最终密钥并解密消息.

在实际 CV-QSS 方案中, 分发者 Dealer 端的探测器是非理想的, 其非理想特性会导致几个问题. 首先, 非理想探测器的缺陷会导致实际 CV-QSS 系统性能低于理论性能. 其次, 为使 CV-QSS 方案实际性能接近理论性能需要高质量的探测器, 这会增加部署探测器的成本. 为解决上述问题, 本文所提方案在分发者 Dealer 端的探测器前部署 PIA, 以补偿非理想探测器的缺陷. 这是因为 PIA 可以显著提高信号光场的平均光子数, 使得原本因非理想探测器低效率而未能被有效探测到的量子态得以被探测, 在一定程度上能够补偿非理想探测器的低效率缺陷; 此外, PIA 对信号的放大作用会显著提高信号的功率, 从而能够相对减小探测器噪声对信号的噪声干扰. 因此, 由于 PIA 能够通过上述两个机制补偿非理想探测器的缺陷, 本文所提方案不需要高质量的探测器, 使用实际应用条件的探测器即可实现相同的系统性能, 从而有效降低了 CV-QSS 实际应用中了对探测器的要求.

3 密钥率的计算

一般来说, 在对某个量子保密通信系统进行安全性分析时, 通常考虑其基于纠缠 (entanglement based, EB) 的模型. 这是因为 EB 模型在理论安全性分析方面已被证明与其所对应的制备-测量 (prepare-and-measure, PM) 模型等价^[38], 且其更便于进行理论安全性分析. 图 3 给出了基于 PIA 的高斯调制 CV-QSS 的 EB 模型方案图. 该模型假设分发者 Dealer 与用户 1 之间的点对点密钥率为 CV-QSS 系统的最终密钥率, 这是因为用户 1 与分发者 Dealer 之间的距离最远, 理论上来说, 距离越远受到的信道损耗也越大, 若距离最远处的密钥率为正, 则整个系统就是安全的. 因此, 本文基于所提方案的 EB 模型进行密钥率的计算.

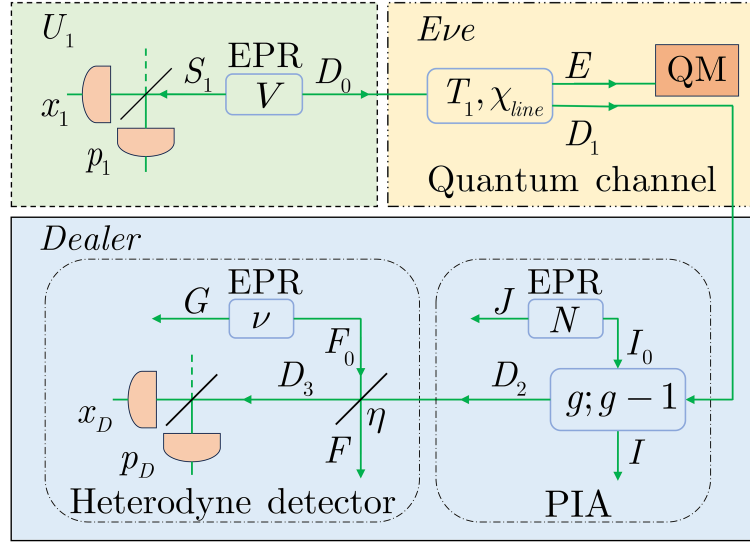


图 3 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 的 EB 模型方案图. 信道透射率 T_1 和信道附加噪声 χ_{line} 由窃听者 Eve 控制, QM 为量子存储器.

Figure 3 (Color online) Schematic diagram of the EB model of the Gaussian-modulated CV-QSS based on PIA. The transmission efficiency T_1 and the channel-added noise χ_{line} are controlled by eavesdropper Eve, QM represents the quantum memory.

假设量子信道的衰减系数为 γ . 分发者 Dealer 和用户 1 之间的光纤长度为 L , 其余 $M - 1$ 个用户顺序分布在用户 1 和分发者 Dealer 之间. 为了简化分析, 假设每个用户都引入相同的过噪声 ε_0 . 则在反向协商情况下, 分发者 Dealer 与用户 1 之间的渐近安全密钥率可由下式表示^[33]:

$$R = f \cdot I_{U_1 D} - \chi_{DE}, \quad (1)$$

其中 $I_{U_1 D}$ 为用户 1 和分发者 Dealer 之间的互信息量; f 为方案的协商效率; χ_{DE} 是窃听者 Eve 和分发者 Dealer 之间的 Holevo 界.

第 r 个用户的信道透射率 T_r 可表示为

$$T_r = 10^{-\frac{\gamma l_r}{10}}, \quad (2)$$

其中, l_r 为分发者 Dealer 与第 r 个用户的距离, 由用户的具体位置决定. 假设每个用户的分束器的透射率为 $t_B \cong 1$. 由于安全密钥率是使用等效到信道输入端 (在用户 1 处) 的噪声来估计的, 因此通过将 ε_0 除以从用户 1 到第 r 个用户的透射率 $\frac{T_1}{T_r}$ 来计算来自第 r 个用户的过噪声. 第 r 个用户引入的等效到信道输入端的过噪声 ε_r 可表示为

$$\varepsilon_r = \frac{T_r}{T_1} \varepsilon_0. \quad (3)$$

因此等效到信道输入端的信道附加噪声 χ_{line} 表达式可表示为

$$\chi_{line} = \frac{1}{T_1} - 1 + \sum_{r=1}^M \varepsilon_r, \quad (4)$$

其中, $\frac{1}{T_1} - 1$ 表示由于信道损耗而产生的真空噪声.

接下来计算 PIA 和外差探测器引入的噪声. PIA 对模 D_1, I_0 引起的变换可描述为辛变换矩阵 $Y_{D_1 I_0}^{PIA}$, 辛变换矩阵 $Y_{D_1 I_0}^{PIA}$ 可表示为

$$Y_{D_1 I_0}^{PIA} = \begin{bmatrix} \sqrt{g} \cdot I_2 & \sqrt{g-1} \cdot \sigma_z \\ \sqrt{g-1} \cdot \sigma_z & \sqrt{g} \cdot I_2 \end{bmatrix}, \quad (5)$$

其中 $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 为二维单位矩阵和 $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

则模 D_2 和模 I 的表达式可表示为

$$\begin{cases} x_{D_2} = \sqrt{g}x_{D_1} + \sqrt{g-1}x_{I_0}, \\ p_{D_2} = \sqrt{g}p_{D_1} - \sqrt{g-1}p_{I_0}, \\ x_I = \sqrt{g}x_{I_0} + \sqrt{g-1}x_{D_1}, \\ p_I = \sqrt{g}p_{I_0} - \sqrt{g-1}p_{D_1}. \end{cases} \quad (6)$$

由上式可知 PIA 将信号功率放大为原来的 g 倍, 同时模 I_0 的噪声通过 $\sqrt{g-1}$ 项耦合到信号中. 则 PIA 对放大后信号增加的噪声为 $N(g-1)$, 其中 N 为模 I_0 的方差. 由于安全密钥率是使用等效到信道输入端 (在用户 1 处) 的噪声来估计的, 而 PIA 对输入的噪声同样放大了 g 倍, 因而等效到放大器输入端的 PIA 引入噪声 χ^{PIA} 需除以 PIA 的增益 g , 具体表达式为

$$\chi^{PIA} = \frac{N(g-1)}{g}. \quad (7)$$

外差探测器引入的噪声 χ_h [28] 为

$$\chi_h = \frac{1 + (1-\eta) + 2\nu_{el}}{\eta}, \quad (8)$$

其中 η 和 ν_{el} 为分发者 Dealer 外差探测器的效率和噪声方差.

等效到放大器输入端的外差探测器引入噪声 χ_{het} 同样需除以 PIA 增益 g , 具体表达式为

$$\chi_{het} = \frac{\chi_h}{g} = \frac{1 + (1-\eta) + 2\nu_{el}}{g\eta}. \quad (9)$$

则等效到放大器输入端的由 PIA 和外差探测器引入的噪声 χ_{het}^{PIA} 表达式为

$$\chi_{het}^{PIA} = \chi_{het} + \chi^{PIA} = \frac{1 + (1-\eta) + 2\nu_{el} + N(g-1)\eta}{g\eta}. \quad (10)$$

而等效到信道输入端的由 PIA 和外差探测器引入的噪声需在式 (10) 基础上除以用户 1 的信道透射率 T_1 , 具体为 $\frac{\chi_{het}^{PIA}}{T_1}$. 则等效到信道输入端的总噪声 χ_{tot} 表达式可表示为

$$\chi_{tot} = \chi_{line} + \frac{\chi_{het}^{PIA}}{T_1}. \quad (11)$$

由于采用外差探测, 信号态的两个正交分量都可以用来生成安全密钥, 用户 1 和分发者 Dealer 之间的互信息量 I_{U_1D} 可表示为

$$I_{U_1D} = \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \quad (12)$$

其中 $V = V_1 + 1$, V_1 为用户 1 的调制方差.

通过香农方程将调制方差 V_1 与信噪比 SNR 联系起来, 则调制方差 V_1 可表示为

$$V_1 = (1 + \chi_{tot}) SNR. \quad (13)$$

窃听者 Eve 能够从分发者 Dealer 的密钥中获得的最大信息量 χ_{DE} 表达式可由下式表示:

$$\chi_{DE} = S(\rho_E) - \int d\phi_D p(\phi_D) S(\rho_E^{\phi_D}), \quad (14)$$

其中, ϕ_D 表示分发者 Dealer 采用外差探测所获得的探测结果, $p(\phi_D)$ 表示 ϕ_D 的概率密度, $\rho_E^{\phi_D}$ 表示基于分发者 Dealer 测量结果的窃听者 Eve 量子态, $S(\rho_E)$ 和 $S(\rho_E^{\phi_D})$ 分别表示量子态 ρ_E 和量子态 $S(\rho_E^{\phi_D})$ 的冯·诺依曼熵.

由于窃听者 Eve 系统纯化了系统 $S_1 D_1$, 分发者 Dealer 端的测量纯化了系统 $S_1 IJFG$, 所以 χ_{DE} 可表示为

$$\chi_{DE} = S(\rho_{S_1 D_1}) - S(\rho_{S_1 IJFG}^{x_D p_D}). \quad (15)$$

由于窃听者 Eve 无法入侵分发者 Dealer 的设备以获取系统的经典随机数据, 因此分发者 Dealer 的外差探测器的缺陷和噪声是可信的, 窃听者无法攻击^[36, 38]. 在此模型下, χ_{DE} ^[38, 39] 可表示为

$$\chi_{DE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^7 G\left(\frac{\lambda_i - 1}{2}\right), \quad (16)$$

其中 $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2,3,4,5,6,7}$ 的计算过程详见附录 A.

根据以上的公式, 可以计算出基于 PIA 的高斯调制 CV-QSS 系统的渐近安全密钥率.

4 性能分析

上文详细介绍了所提方案的具体步骤, 推导了该方案产生的密钥率公式. 本节将对基于 PIA 的高斯调制 CV-QSS 方案进行性能分析, 并比较其与传统 CV-QSS 方案的性能差异. 显然, 用户数为 2 的 QSS 是 QSS 中最基础的情况. 这是因为 QSS 实现的是秘密共享, 具有多用户的共享性, 而用户数为 1 的 QSS 的密钥信息仅在用户和分发者 Dealer 两者之间传递, 不具备共享性, 即无法实现秘密共享, 其实质是退化成为点对点的 QKD. 因此, 在未强调用户数情况下本节的仿真分析默认使用最基础的用户数为 2 的高斯调制 CV-QSS 系统来验证所提方案的有效性. 此外, 由于当 PIA 增益 $g = 1$ 时, 式 (10) 中的 χ_{het}^{PIA} 退化为 χ_h , 此时整个系统可以等效为使用非理想探测器且不使用 PIA 补偿的传统 CV-QSS 方案, 因此本文用 PIA 增益 $g = 1$ 的情况模拟使用非理想探测器的传统 CV-QSS 方案.

本节数值仿真的默认参数设置如下: 协商效率 $f = 0.95$, 光纤衰减系数 $\gamma = 0.2$ dB/km, PIA 的内在噪声 $N = 1$, 用户引入过噪声 $\varepsilon_0 = 0.01$, 非理想外差探测器的参数取值为 $\eta = 0.6$, $\nu_{el} = 0.1$, 理想外差探测器的参数取值为 $\eta = 1$, $\nu_{el} = 0$. 以上参数取值均为实验通常情况下使用的数值.

图 4 给出了基于 PIA 的高斯调制 CV-QSS 方案的渐进密钥率与传输距离的关系. 由图中可以看出, 本文所提方案性能明显优于使用非理想探测器的传统 CV-QSS 方案的性能, 并且本文所提方案的安全传输距离还可以通过增大 PIA 增益 g 进一步补偿. 例如, 当 PIA 增益 g 提高到 3 时, 本文所提方案补偿了 5.28 km 的安全传输距离; 当 PIA 增益 g 进一步提高到 20 时, 本文所提方案又进一步补偿了 3 km 的安全传输距离. 此外, 值得注意的是, 本文所提方案在 PIA 增益 g 等于 20 情况下的最大传输距离与使用理想外差探测器的 CV-QSS 方案的最大传输距离十分接近. 这一结果表明, PIA 的高增益有效补偿了原本由非理想探测器缺陷而降低的 CV-QSS 系统实际性能, 并使实际 CV-QSS 系统的最大传输距离能够接近使用理想探测器的情况.

为探究 PIA 的高增益能够有效补偿原本因非理想探测器缺陷而降低的 CV-QSS 系统实际性能的原因, 图 5 显示了基于 PIA 的高斯调制 CV-QSS 方案的噪声 χ_{het}^{PIA} 与 PIA 增益 g 的关系. 可以发现, 与使用非理想探测器的传统 CV-QSS 方案 ($g = 1$) 中的噪声 χ_{het}^{PIA} 相比, 本文所提方案中的噪声 χ_{het}^{PIA} 明显下降, 且随着 PIA 增益 g 越大, 本文所提方案中的噪声 χ_{het}^{PIA} 越小, 尤其是在 PIA 增益 g 等于 20 的情况下本文所提方案中的噪声 χ_{het}^{PIA} 为 1.08, 已经十分接近理想外差探测器所引入的噪声, 即 1. 这一结果表明, PIA 的高增益有效抑制了非理想探测器的缺陷对信号造成的噪声干扰. 此外, 由于噪声 χ_{het}^{PIA} 与用于计算 CV-QSS 密钥率的 Holevo 界 χ_{DE} 密切相关, 图 5 还显示了基于 PIA 的高斯调制 CV-QSS 方案的 Holevo 界 χ_{DE} 与 PIA 增益 g 的关系. 从图中可以看出, 随着 PIA 增益 g 的增大, 本文所提方案中的 Holevo 界不断降低. 这一结果表明, 随着 PIA 增益 g 的增大, 窃听者 Eve 在集体高斯攻击下可以窃取的信息上限将越来越小. 结合上述分析可知, PIA 的高增益通过抑制非

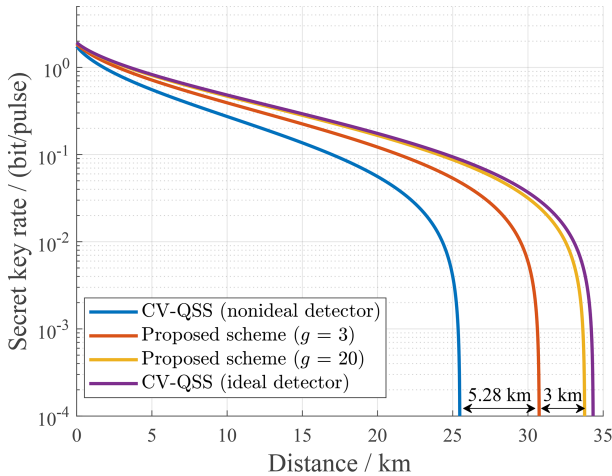


图 4 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案的渐进密钥率与传输距离的关系。

Figure 4 (Color online) Asymptotic secret key rate of the Gaussian-modulated CV-QSS scheme based on PIA as a function of transmission distance.

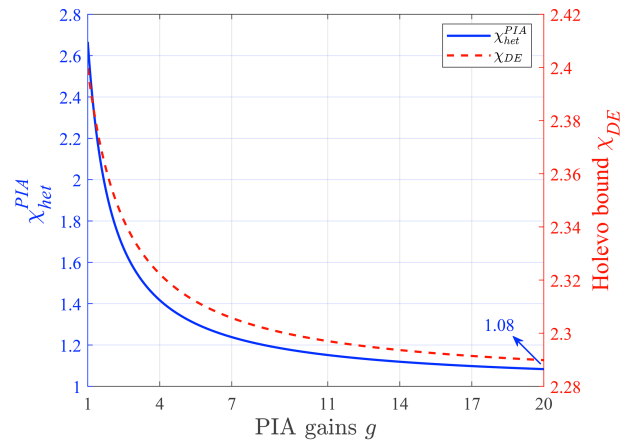


图 5 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案的噪声 χ_{het}^{PIA} 和 Holevo 界 χ_{DE} 与 PIA 增益 g 的关系, 其中传输距离 $L = 20$ km。

Figure 5 (Color online) The noise χ_{het}^{PIA} and Holevo bound χ_{DE} of the Gaussian-modulated CV-QSS scheme based on PIA as a function of the gain of PIA g , with the transmission distance being 20 km.

理想探测器缺陷对信号造成的噪声干扰, 有效降低了窃听者 Eve 在集体高斯攻击下可以窃取的信息上限, 从而使原本因非理想探测器缺陷而降低的 CV-QSS 系统的实际性能得以补偿。

由于 PIA 能够补偿非理想探测器的缺陷, 因此本文所提方案对所需的探测器性能要求应比传统 CV-QSS 更宽松。为比较本文所提方案所需探测器性能与传统 CV-QSS 方案的差异, 图 6 绘制了基于 PIA 的高斯调制 CV-QSS 方案的密钥率与探测器效率的关系。从图 6 中可以看出, 相较于使用非理想探测器的传统 CV-QSS 方案, 本文所提方案在探测器性能要求方面具有优势。例如, 在传输距离 $L = 32$ km 的情况下, 对于传统 CV-QSS 方案中需要使用探测器效率为 0.937 的高质量探测器才能达到的系统性能, 本文所提方案在 PIA 增益 g 等于 20 时仅需使用探测器效率为 0.245 的探测器即可达到相同的系统性能。这一结果表明, 本文所提方案不需要依赖于高质量探测器, 使用更接近实际应用条件的探测器即可实现相同的系统性能, 在实际部署中具有更强的适用性。

本文所提方案的另一个优势是能够容忍更大的用户引入过噪声 ε_0 , 有利于实际 CV-QSS 系统的实现。图 7 给出了基于 PIA 的高斯调制 CV-QSS 方案在不同用户引入过噪声 ε_0 情况下的性能。从图 7 中可知, 随着用户引入过噪声的逐渐增大, 系统的密钥率呈现出下降趋势。因此, 通过降低用户引入过噪声可以提高本文所提方案的性能。此外, 在相同传输距离情况下, 本文所提方案可容忍的用户引入过噪声范围大于传统 CV-QSS 方案可容忍的用户引入过噪声范围。例如, 在传输距离 $L = 25$ km 的情况下, 本文所提方案在 PIA 增益 g 为 20 时的可容忍的用户引入过噪声范围为 $[0, 0.034]$, 远大于传统 CV-QSS 方案的可容忍的用户引入过噪声范围 $[0, 0.0116]$ 。这意味着相较于传统 CV-QSS 方案, 本文所提方案能容忍更大的用户引入过噪声 ε_0 , 换句话说, 本文所提方案降低了 CV-QSS 系统对用户端的要求, 更能满足实际应用场景需求。

在上述的仿真中, 为简化分析, 用户 2 部署在用户 1 与分发者 Dealer 链路正中间, 然而事实上用户的部署位置应具备灵活性, 以适应不同的应用场景需求。为深入研究所提方案在不同用户部署位置情况下的性能表现, 图 8 给出了在不同传输距离比情况下基于 PIA 的高斯调制 CV-QSS 方案的密钥率与传输距离的关系, 其中 L_{12} 表示用户 1 和 2 之间的距离, 传输距离比 L_{12}/L 越大意味着用户 2 越远离用户 1 且越靠近分发者 Dealer。从图 8 中可以看出, 与用户 2 靠近用户 1 的情况 ($L_{12}/L = 0.1$) 相比, 用户 2 靠近分发者 Dealer 情况 ($L_{12}/L = 0.9$) 下的最大传输距离有所降低。原因在于当用户 2 从靠近用户 1 变为靠近分发者 Dealer 时, 透射率 $T_2 = 10^{-\frac{\gamma L_2}{10}}$ 会增大, 而透射率的增大会导致窃听者 Eve 能够获得更多有关用户数据的信息, 从而使得系统的最大传输距离

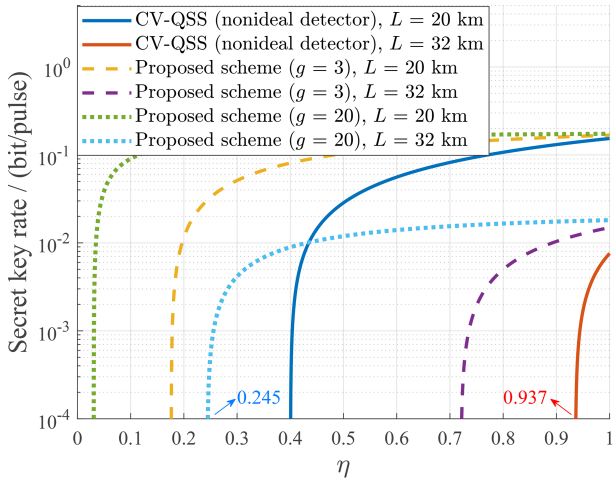


图 6 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案的密钥率与探测器效率 η 的关系。

Figure 6 (Color online) The relationship between the detector efficiency η and the secret key rate of the Gaussian-modulated CV-QSS scheme based on PIA.

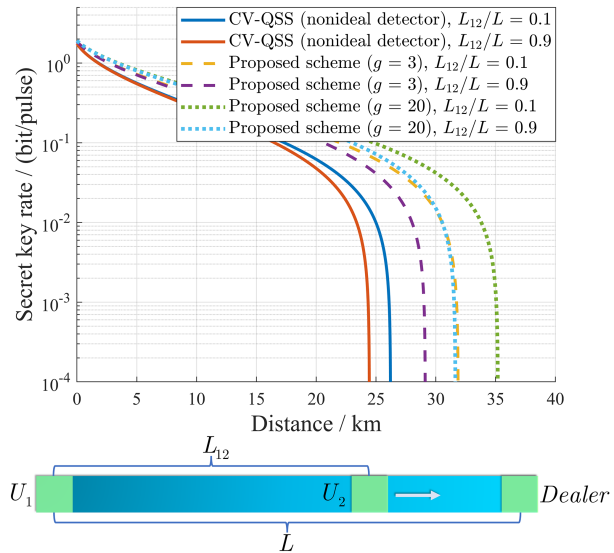


图 8 (网络版彩图) 在不同传输距离比情况下基于 PIA 的高斯调制 CV-QSS 方案的密钥率与传输距离的关系。

Figure 8 (Color online) The relationship between the secret key rate of the Gaussian-modulated CV-QSS scheme based on PIA and the transmission distance at different transmission distance ratios.

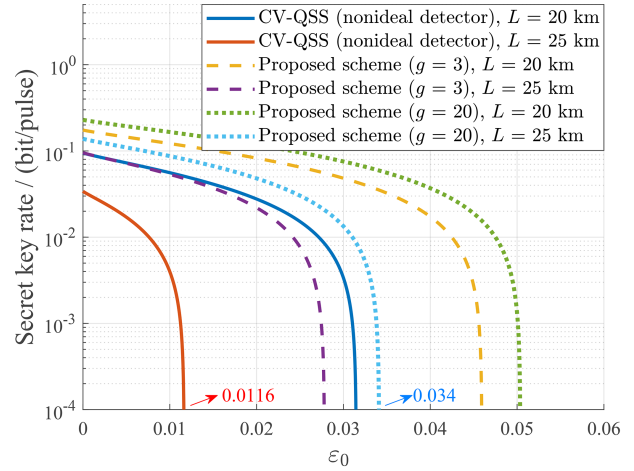


图 7 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案在不同用户引入过噪声情况下的性能。

Figure 7 (Color online) The performance of the Gaussian-modulated CV-QSS scheme based on PIA under the different conditions of the excess noise introduced by each user.

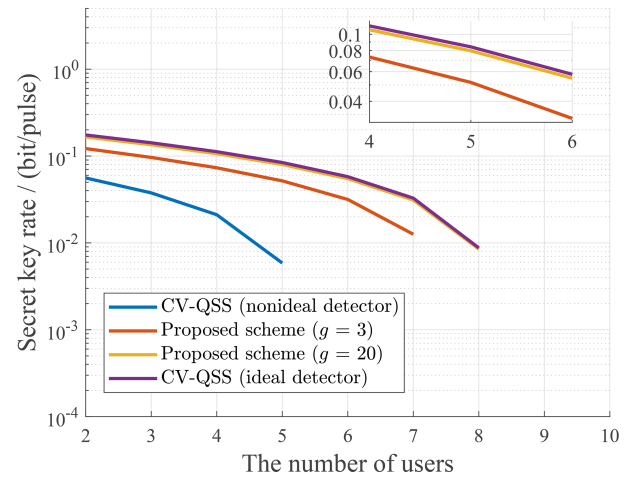


图 9 (网络版彩图) 基于 PIA 的高斯调制 CV-QSS 方案在不同用户数量情况下的性能, 其中传输距离 $L = 20$ km。

Figure 9 (Color online) The performance of the Gaussian-modulated CV-QSS scheme based on PIA under different numbers of users, with the transmission distance being 20 km.

有所下降. 因此, 为获得本文所提方案的最佳性能, 可以将用户 2 尽可能部署在靠近用户 1 的位置, 但这种部署是以牺牲用户部署位置的灵活性为代价的. 另一方面, 在对最大传输距离要求不高的场景下, 可以考虑以牺牲最大传输距离为代价, 使本文所提方案的用户部署位置更加灵活, 以适应更加复杂的网络拓扑结构.

上述仿真已初步验证了所提方案在两名用户场景下的有效性, 为了进一步探究所提方案在多用户环境中的性能表现, 图 9 给出了所提方案在不同用户数量情况下的性能, 其中各参与者之间间距相等. 从图 9 中可知, 系

统密钥率随用户数量的增加而呈下降趋势. 这是因为更多的用户数会增大 CV-QSS 系统中的总噪声, 使信号受到的噪声干扰增强. 此外, 相较于传统 CV-QSS 方案, 本文所提方案能够容纳更多用户进行安全的量子通信. 从图 9 中可以看出, 在传输距离 $L = 20$ km 的情况下, 传统 CV-QSS 方案最多仅能容纳 5 个用户进行安全的秘密共享, 而本文所提方案在 PIA 增益为 20 时最多能容纳 8 个用户进行安全的秘密共享, 与使用理想探测器情况下所能达到的最大用户容量完全一致. 这一结果表明, 相较于传统 CV-QSS 方案, 本文所提方案在大规模用户场景下展现出优势, 能够满足更大规模用户群体的安全通信需求.

5 结论

本文提出了一种基于 PIA 的高斯调制 CV-QSS 方案. 针对非理想探测器的缺陷导致的 CV-QSS 系统实际性能下降问题, 本文所提方案通过在分发者 Dealer 端部署 PIA 补偿了非理想探测器的缺陷, 提高了 CV-QSS 在实际情况下的性能. 实验结果表明, 本文所提方案有效降低了非理想探测器缺陷对信号造成的噪声干扰, 在多种情况下的系统性能均优于使用非理想探测器的传统 CV-QSS 方案. 此外, 本文所提方案不需要依赖于高质量探测器, 使用实际应用条件的探测器即可实现相同的系统性能, 有效降低了 CV-QSS 实际应用中对探测器的要求. 本文为解决非理想探测器的缺陷导致的 CV-QSS 实际性能下降问题提供了一种可行方案, 推动了 CV-QSS 系统的实用化发展.

参考文献

- 1 Shamir A. How to share a secret. *Commun ACM*, 1979, 22: 612–613
- 2 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. *Phys Rev A*, 1999, 59: 1829–1834
- 3 Liao Q, Fei Z Y, Liu J Y, et al. High-rate discretely-modulated continuous-variable quantum key distribution using quantum machine learning. *Chaos Soliton Fract*, 2025, 196: 116331
- 4 Shao S F, Zhou L, Lin J P, et al. High-rate measurement-device-independent quantum communication without optical reference light. *Phys Rev X*, 2025, 15: 021066
- 5 Yan Z H, Jia X J. Quantum key distribution with chromatic codes. *Light Sci Appl*, 2025, 14: 126
- 6 Hajomer A A E, Kanitschar F, Jain N, et al. Experimental composable key distribution using discrete-modulated continuous variable quantum cryptography. *Light Sci Appl*, 2025, 14: 255
- 7 Wu Q, Ribezzo D, Di Sciullo G, et al. Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers. *Light Sci Appl*, 2025, 14: 274
- 8 Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. *Sci China Inf Sci*, 2025, 68: 180501
- 9 Liao Q, Liu H J, Gong Y P, et al. Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation. *Opt Express*, 2022, 30: 3876–3892
- 10 Kang Y, Guo Y, Feng Y Y. Quantum secret sharing based on continuous-variable GHZ states. *Int J Theor Phys*, 2020, 59: 2308–2320
- 11 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. *Phys Rev A*, 2004, 69: 052307
- 12 You Z X, Wang Y R, Dou Z, et al. Dynamic quantum secret sharing between multiparty and multiparty based on single photons. *Phys A Stat Mech its Appl*, 2023, 624: 128893
- 13 Xing D, Wang Y F, Dou Z, et al. Efficient semi-quantum secret sharing protocol using single particles. *Chin Phys B*, 2023, 32: 070308
- 14 Zhou Y Y, Yu J, Yan Z H, et al. Quantum secret sharing among four players using multipartite bound entanglement of an optical field. *Phys Rev Lett*, 2018, 121: 150502
- 15 Lance A M, Symul T, Bowen W P, et al. Continuous variable (2, 3) threshold quantum secret sharing schemes. *New J Phys*, 2003, 5: 4
- 16 Yang F L, Qiu D W, Mateus P. Continuous-variable quantum secret sharing in fast-fluctuating channels. *IEEE Trans Quantum Eng*, 2023, 4: 1–9
- 17 Liao Q, Fei Z Y, Huang L, et al. Practical continuous-variable quantum secret sharing using local local oscillator. *Commun Phys*, 2025, 8: 138

- 18 Shen A, Cao X Y, Wang Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci China-Phys Mech Astron*, 2023, 66: 260311
- 19 Wang Y Z, Sun X R, Cao X Y, et al. Experimental coherent-state quantum secret sharing with finite pulses. *Phys Rev Appl*, 2024, 22: 044018
- 20 Gaertner S, Kurtsiefer C, Bourennane M, et al. Experimental demonstration of four-party quantum secret sharing. *Phys Rev Lett*, 2007, 98: 020503
- 21 Liu C J, Zhu C H, Li Z H, et al. Continuous-variable quantum secret sharing based on thermal terahertz sources in inter-satellite wireless links. *Entropy*, 2021, 23: 1223
- 22 Zhou N R, Song H C, Gong L H. Continuous variable quantum secret sharing via quantum teleportation. *Int J Theor Phys*, 2013, 52: 4174–4184
- 23 Liao Q, Huang L, Fei Z Y, et al. Measurement-device-independent continuous-variable quantum secret sharing. *Adv Quantum Technol*, 2025, 8: 2400505
- 24 Qin Y, Cheng J L, Ma J X, et al. Efficient and secure quantum secret sharing for eight users. *Phys Rev Res*, 2024, 6: 033036
- 25 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. *Phys Rev Lett*, 2004, 92: 177903
- 26 Lau H K, Weedbrook C. Quantum secret sharing with continuous-variable cluster states. *Phys Rev A*, 2013, 88: 042313
- 27 Kogias I, Xiang Y, He Q Y, et al. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys Rev A*, 2017, 95: 012315
- 28 Grice W P, Qi B. Quantum secret sharing using weak coherent states. *Phys Rev A*, 2019, 100: 022339
- 29 Wang Y J, Jia B, Mao Y, et al. Improving continuous variable quantum secret sharing with weak coherent states. *Appl Sci*, 2020, 10: 2411
- 30 Wu X D, Wang Y J, Huang D. Passive continuous-variable quantum secret sharing using a thermal source. *Phys Rev A*, 2020, 101: 022301
- 31 Liao Q, Liu H J, Zhu L J, et al. Quantum secret sharing using discretely modulated coherent states. *Phys Rev A*, 2021, 103: 032410
- 32 Liao Q, Liu X Q, Ou B, et al. Continuous-variable quantum secret sharing based on multi-ring discrete modulation. *IEEE Trans Commun*, 2023, 71: 6051–6060
- 33 Fossier S, Diamanti E, Debuisschert T, et al. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J Phys B-At Mol Opt Phys*, 2009, 42: 114014
- 34 Wu X D, Huang D, Huang P, et al. Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation. *Acta Phys Sin*, 2022, 71: 240304 [吴晓东, 黄端, 黄鹏, 等. 基于实际探测器补偿的离散调制连续变量测量设备无关量子密钥分发方案. *物理学报*, 2022, 71: 240304]
- 35 Caves C M. Quantum limits on noise in linear amplifiers. *Phys Rev D*, 1982, 26: 1817–1839
- 36 Grosshans F, van Assche G, Wenger J, et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, 421: 238–241
- 37 Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy*, 2015, 17: 6072–6092
- 38 Lodewyck J, Bloch M, García-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev A*, 2007, 76: 042305
- 39 Huang D, Huang P, Lin D K, et al. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci Rep*, 2016, 6: 19201

附录 A 辛特征值 $\lambda_{1,2,3,4,5,6,7}$ 的计算

该部分详细推导有关辛特征值 $\lambda_{1,2,3,4,5,6,7}$ 的计算过程.

$\lambda_{1,2}$ 是表征 $\rho_{S_1 D_1}$ 的协方差矩阵 $\gamma_{S_1 D_1}$ 的辛特征值, 协方差矩阵 $\gamma_{S_1 D_1}$ 可表示为

$$\gamma_{S_1 D_1} = \begin{bmatrix} \gamma_{S_1} & \sigma_{S_1 D_1}^T \\ \sigma_{S_1 D_1} & \gamma_{D_1} \end{bmatrix} = \begin{bmatrix} V \cdot I_2 & \sqrt{T_1(V^2 - 1)} \cdot \sigma_z \\ \sqrt{T_1(V^2 - 1)} \cdot \sigma_z & T_1(V + \chi_{line}) \cdot I_2 \end{bmatrix}. \quad (A1)$$

$\lambda_{3,4,5,6,7}$ 是表征 $\rho_{S_1 IJFG}^{x_D, p_D}$ 的协方差矩阵 $\gamma_{S_1 IJFG}^{x_D, p_D}$ 的辛特征值, 协方差矩阵 $\gamma_{S_1 IJFG}^{x_D, p_D}$ 可以表示为

$$\gamma_{S_1 IJFG}^{x_D, p_D} = \gamma_{S_1 IJFG} - \sigma_{S_1 IJFG D_3}^T H_{het} \sigma_{S_1 IJFG D_3}, \quad (A2)$$

其中, H_{het} 是描述对模 D_3 进行外差探测的辛矩阵, 且 $H_{het} = (\gamma_{D_3} + I_2)^{-1}$, 表达式中的单位矩阵表示外差探测器中包含的分束器.

而矩阵 γ_{D_3} , $\gamma_{S_1 IJFG}$, $\sigma_{S_1 IJFGD_3}$ 都可以由协方差矩阵 $\gamma_{S_1 IJFGD_3}$ 分解得出:

$$\gamma_{S_1 IJFGD_3} = \begin{bmatrix} \gamma_{S_1 IJFG} & \sigma_{S_1 IJFGD_3}^T \\ \sigma_{S_1 IJFGD_3} & \gamma_{D_3} \end{bmatrix}. \quad (A3)$$

$\gamma_{S_1 IJFGD_3}$ 可以由以下表达式表示:

$$\gamma_{S_1 IJFGD_3} = (Y^{BS})^T \gamma_{S_1 D_2 F_0 IJG} Y^{BS}, \quad (A4)$$

其中 $Y^{BS} = I_{S_1} \oplus Y_{D_2 F_0}^{BS} \oplus I_I \oplus I_J \oplus I_G$, 而 $Y_{D_2 F_0}^{BS}$ 可表示为

$$Y_{D_2 F_0}^{BS} = \begin{bmatrix} \sqrt{\eta} \cdot I_2 & \sqrt{1-\eta} \cdot I_2 \\ -\sqrt{1-\eta} \cdot I_2 & \sqrt{\eta} \cdot I_2 \end{bmatrix}. \quad (A5)$$

$\gamma_{S_1 D_2 F_0 IJG}$ 可以由以下表达式表示:

$$\gamma_{S_1 D_2 F_0 IJG} = (Y^{PIA})^T [\gamma_{S_1 D_1} \oplus \gamma_{I_0 J} \oplus \gamma_{F_0 G}] Y^{PIA}, \quad (A6)$$

其中 $Y^{PIA} = I_{S_1} \oplus Y_{D_1 I_0}^{PIA} \oplus I_J \oplus I_{F_0} \oplus I_G$.

$\gamma_{F_0 G}$ 是描述 EPR 态的方差 ν 的矩阵, 其中 ν 被用于模拟探测器的电子噪声, 在使用外差探测器条件下 ν 取值为 $1 + \frac{2\nu_{el}}{1-\eta}$. $\gamma_{F_0 G}$ 可以表示为

$$\gamma_{F_0 G} = \begin{bmatrix} \nu \cdot I_2 & \sqrt{(\nu^2-1)} \cdot \sigma_z \\ \sqrt{(\nu^2-1)} \cdot \sigma_z & \nu \cdot I_2 \end{bmatrix}. \quad (A7)$$

此外, 矩阵 $\gamma_{I_0 J}$ 描述了 EPR 态的方差 N , 而 N 被用于模拟 PIA 的内在噪声. $\gamma_{I_0 J}$ 可表示为

$$\gamma_{I_0 J} = \begin{bmatrix} N \cdot I_2 & \sqrt{N^2-1} \cdot \sigma_z \\ \sqrt{N^2-1} \cdot \sigma_z & N \cdot I_2 \end{bmatrix}. \quad (A8)$$

结合正文式 (2), (4), (5), (10), (11), (13) 和上述公式, 辛特征值 $\lambda_{1,2}$ 可以表示为

$$\lambda_{1,2}^2 = \frac{1}{2} [A \pm \sqrt{A^2 - 4B}], \quad (A9)$$

其中

$$A = V^2 (1 - 2T_1) + 2T_1 + T_1^2 (V + \chi_{line})^2, \quad (A10)$$

$$B = T_1^2 (V \chi_{line} + 1)^2. \quad (A11)$$

$\lambda_{3,4}$ 的表达式可表示为

$$\lambda_{3,4}^2 = \frac{1}{2} [C \pm \sqrt{C^2 - 4D}], \quad (A12)$$

其中,

$$C = \frac{1}{[T_1 (V + \chi_{tot})]^2} [A(\chi_{het}^{PIA})^2 + B + 1 + 2\chi_{het}^{PIA} [V\sqrt{B} + T_1(V + \chi_{line})] + 2T_1(V^2 - 1)], \quad (A13)$$

$$D = \left[\frac{V + \sqrt{B} \cdot \chi_{het}^{PIA}}{T_1 (V + \chi_{tot})} \right]^2. \quad (A14)$$

最终, $\lambda_{5,6,7}$ 的值可表示为

$$\lambda_{5,6,7} = 1. \quad (A15)$$

Gaussian-modulated continuous-variable quantum secret sharing based on phase-insensitive amplifiers

Zeqi ZENG, Lianzheng FAN, Zhe QIN, Delong LI & Qin LIAO*

College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

* Corresponding author. E-mail: llqqlq@hnu.edu.cn

Abstract As a core component of the continuous variable quantum secret sharing system, the performance of the detector is crucial to the entire system. Nevertheless, in practical circumstances, the detector is nonideal, whose defects can introduce noise interference into the signal and result in the performance degradation of the continuous-variable quantum secret sharing system. To solve this problem, we present a Gaussian-modulated continuous-variable quantum secret sharing based on phase-insensitive amplifiers. The phase-insensitive amplifier can uniformly amplify each orthogonal component of the signal and increase the signal power, thereby relatively reducing the noise interference caused by the defects of nonideal detectors to the signal and significantly improving the actual performance of the system. The numerical simulation shows that the phase-insensitive amplifier effectively increases the secret key rate and the secure transmission distance of the system, and the actual performance of the system under the high gain of the phase-insensitive amplifier closely approaches the performance of the system using an ideal detector. This work provides a novel approach to addressing the issue of reduced performance of continuous-variable quantum secret sharing caused by the defects of nonideal detectors.

Keywords quantum secret sharing, continuous variable, quantum communication, phase-insensitive amplifiers, quantum cryptography