基于卡尔曼滤波的本地本振连续变量量子秘密共享*

廖骏[1)] 费焯迎[1)] 王一军[2)†]

1) (湖南大学信息科学与工程学院, 长沙 410082)

2) (中南大学自动化学院, 长沙 410083)

(2025 年 2 月 25 日收到; 2025 年 4 月 30 日收到修改稿)

在实际的连续变量量子秘密共享系统中, 经不安全信道传输的本振光或因各种针对性攻击而受到安全威胁. 针对这个问题, 本文提出了一种本地本振连续变量量子秘密共享方案, 本振光在可信端本地生成而无需由各用户发送, 从而彻底堵住相关安全漏洞. 在此基础上, 利用卡尔曼滤波对各个参考相位分别进行最小均方误差估计, 在降低相位漂移估计误差的同时抑制相位测量噪声. 分别开发了涉及标量卡尔曼和矢量卡尔曼的相位补偿方法, 其中矢量卡尔曼一步完成补偿而无需额外处理相位慢漂移. 本文对滤波后系统的过噪声进行建模, 并推导了针对窃听者和不诚实用户的安全界限. 数值模拟结果表明, 与块平均相比, 所提方案在最大传输距离和最大支持用户数方面优势明显, 具有构建大规模量子通信网络的潜力.

关键词: 量子秘密共享, 连续变量, 本地本振, 卡尔曼滤波

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250227

CSTR: 32037.14.aps.74.20250227

1 引 言

量子秘密共享 (quantum secret sharing, QSS)[1,2] 允许可信端 Dealer 与多个远程用户通过不安全量子信道共享密钥. 在经典 (k, n) 阈值 QSS 方案中, 秘密被分成 n 份, 参与方只有掌握其中至少 k 份才能将其完全重构, 保护秘密信息免遭窃听者和不诚实用户窃取. 连续变量量子秘密共享 (continuous-variable quantum secret sharing, CVQSS)[3,4] 作为 QSS 的一个重要分支, 其密钥信息通常编码在正交光场分量上, 在理论安全码率和兼容现有光通信技术方面具有优势 [5]. 基于纠缠态的 CVQSS[6] 的理论无条件安全性首先得到证明, 但其制备和测量难度较大, 之后各种基于相干态的 CVQSS 被相继提出, 其中高斯调制相干态 (Gaussian modulated coherent state, GMCS) 协议 [7,8] 拓宽了对信道损耗的可容忍范围, 并天然抗特洛伊木马攻击; 离散调制相干态 (discretely modulated coherent state, DMCS) 协议 [9] 在低信噪比下具有高协商效率, 适合长距离安全通信, 在采取多环调制策略 [10] 后进一步降低量子探测器识别 DMCSs 的误差概率, 显著提高系统性能.

在 CVQSS 实际实现中, 多路信号的本振光 (local oscillator, LO) 通常需要由各自用户通过不安全信道发送给 Dealer 进行相干检测. 然而, LO 在传输的过程中易受到各种类型的针对性攻击 [11], 如波长攻击 [12]、LO 校准攻击 [13]、LO 波动攻击 [14] 和偏振攻击 [15,16] 等, 这些攻击带来的安全威胁主要可分为两类: 一是外部窃听者通过操纵量子信道窃取信息, 二是内部不诚实用户通过伪造或篡改共享数据破坏协议完整性 [17]. 虽然研究者们提出了

* 国家自然科学基金 (批准号: 62101180) 和湖南省重点研发计划 (批准号: 2025QK3011) 资助的课题.

† 通信作者. E-mail: xxywyj@sina.com

各种应对措施[18,19], 但大多聚焦于抵御外部攻击, 没有一种对策能够完美地堵住所有针对 LO 攻击的安全漏洞. 因此, 亟需研究针对窃听者和不诚实用户的联合优化方案, 以提升 CVQSS 系统的整体安全性. 2023 年, Liao 等[20] 提出了一种基于往返式架构的双相位调制 CVQSS 方案, 其优点是量子信号和 LO 均由 Dealer 产生, 因此 LO 无需再通过不安全信道发送给 Dealer, 从而消除了传输 LO 的漏洞. 然而, 该方案的代价是未经调制的量子信号需要通过不安全的量子信道传输, 由此可能会造成其他安全问题, 因而不能被认为是完美的.

抵御针对 LO 攻击的另一种思路则是从根本上消除 LO 的使用. 避免多路 LO 各自相干检测的复杂情况, 考虑采用本地本振[21–23] 的同时实现单路参考信号同步, 完成多个发射-测量端之间的相位参考[24]. 一般来说, 本地测量得到的参考相位中存在由独立激光器之间初始相位差引起的相位快漂移, 以及由光路传输延迟和激光时钟同步误差引起的相位慢漂移[25,26], 且测量过程会不可避免地引入相位测量噪声[27]. 相位漂移补偿的准确性[28] 是保证系统性能的关键, 直接补偿与量子信号实际相位漂移较大偏差的参考相位会导致信道过噪声的增大从而对实际安全性造成损害[29]. 之前的研究表明, 因相位慢漂移变化缓慢, 其影响可通过块平均最大限度地消除[30], 且通过部署实时检测设备能够控制相位测量噪声并防止潜在的参考相位攻击[31,32]. 尽管如此, 随用户规模扩大, CVQSS 系统性能受相位噪声制约的问题亟待解决.

由于连续变量类协议建立在标准电信技术之上, 其数据处理方面的应用备受关注. 其中卡尔曼滤波 (Kalman filter, KF)[33] 作为一种经典机器学习算法, 能够在动态系统中提供最小均方误差 (minimum mean square error, MMSE) 估计, 在最近的研究中表现出优异的相位噪声处理能力[34,35]. KF 可进一步分为标量 KF[36] 和矢量 KF[37,38], 两者都将相位快漂移纳入状态模型中, 而后者另外对相位慢漂移的线性变化进行建模. 总体而言, 标量 KF 较为简洁且对系统的稳定性要求较高, 而矢量 KF 能够同时处理多个变量的估计, 能很好地适应 CVQSS 系统复杂的信号处理需求.

受上述研究启发, 本文提出一种基于 KF 的本地本振 CVQSS (LLO-CVQSS) 方案. 具体来说, 除了由 Dealer 本地生成 LO 测量各用户量子信号外, 最远用户随路发送仅包含初始相位信息的参考信号并由其余用户和 Dealer 执行测量和相位补偿. 该策略中 LO 无需通过不可信信道进行传输, 整个 CVQSS 系统对针对 LO 的攻击免疫. 在此基础上, 利用 KF 对参考相位实施 MMSE 估计, 大大减小相位漂移估计误差. 开发分别基于标量 KF 和矢量 KF 的 LLO-CVQSS 相位补偿方法, 特别地, 矢量卡尔曼高效地一步进行补偿, 无需额外处理相位慢漂移. 之后对系统过噪声建模, 相位测量噪声被有效抑制. 推导在窃听者和不诚实用户的攻击下基于 KF 的 LLO-CVQSS 安全界限, 数值模拟表明, 与块平均方案相比, 所提方案性能得到显著提升, 最远传输距离从 67.3 km 提升至 82.6 km, 最大支持用户数从 22 提升至 33, 有助于推动大规模量子通信网络的构建.

本文第 2 节详细介绍基于 KF 的 LLO-CVQSS 方案设计, 刻画方案的关键流程; 第 3 节中给出根据方案提出的相位补偿方法; 第 4 节对所提方案进行过噪声建模; 第 5 节分析系统性能; 第 6 节得出结论.

2 方案设计

图 1 为基于 KF 的 LLO-CVQSS 的方案示意图, 为简便起见, 以 (2, 2) 阈值方案为例, 用户 1 和用户 2 通过不安全的量子信道与 Dealer 按顺序连接, (n, n) 阈值方案能类似地推广得到. 总体协议过程可以分为制备、测量、参数估计与后处理 3 个部分, 具体如下.

1) 制备

用户 1 用自己的激光器产生光脉冲, 然后通过 50∶50 的分束器分为两路. 一路经调幅器、调相器和可变光衰减器制备成 GMCS, 另一路延迟半个脉冲间隔后形成参考信号. 两路信号经分束器耦合后发送给用户 2, 其中用户 1 的 GMCS 表示为 $|x_1+\mathrm{i}p_1\rangle$.

用户 2 也产生光脉冲并通过分束器, 一路延迟半个脉冲间隔后形成参考信号, 另一路经调幅器、调相器和可变光衰减器后, 通过高度不平衡分束器耦合到与用户 1 输入信号相同的时空模式, 形成混合信号. 该混合信号包括用户 1 的 GMCS $|x_1+\mathrm{i}p_1\rangle$、用户 2 的 GMCS $|x_2+\mathrm{i}p_2\rangle$ 和用户 1 参考信号, 之后被发送给 Dealer.

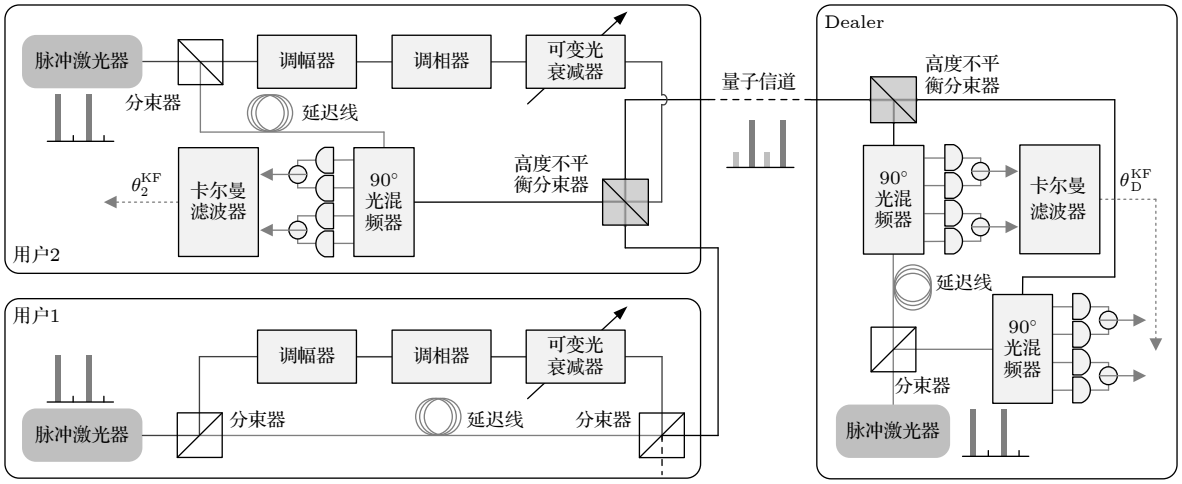


图 1 基于 KF 的 LLO-CVQSS 示意图

Fig. 1. Schematic diagram of KF-based LLO-CVQSS.

2) 测量

用户 2 在本地用参考信号与高度不平衡分束器反射的用户 1 输入信号进行外差检测, 得到用户 2 参考相位 y_2.

Dealer 在本地生成 LO, 然后通过分束器分为两路, 其中一路延迟半个脉冲间隔. 被输入的混合信号也由高度不平衡分束器分成两部分, 一部分与延迟的 LO 外差检测, 得到 Dealer 参考相位 $y_{\rm D}$, 另一部分用未延迟的 LO 外差检测, 得到混合信号测量结果 $\{x_{\rm D}, p_{\rm D}\}$.

重复上述步骤多次以获得足够的数据后, 用户 2 和 Dealer 将各自参考相位送入 KF 进行精细估计, 得到滤波相位 $\theta_2^{\rm KF}$ 和 $\theta_{\rm D}^{\rm KF}$. 滤波相位用于补偿各自相位漂移, 用户 2 和 Dealer 数据分别修正为 $\{x_2', p_2'\}$ 和 $\{x_{\rm D}', p_{\rm D}'\}$.

3) 参数估计与后处理

Dealer 随机选取其数据的一个子集, 要求所有用户披露其对应的原始数据, 从而估计各用户的信道透射率 $\{T_1, T_2\}$. 此后所有参与方丢弃相应数据.

假设用户 1 诚实, 用户 2 不诚实. Dealer 进一步选择其数据的另一个子集, 并要求用户 2 公布相应的值. Dealer 可将该子集替换为 $x_{\rm D1} = x_{\rm D}' - \sqrt{T_2}x_2'$ 和 $p_{\rm D1} = p_{\rm D}' - \sqrt{T_2}p_2'$, 等效在 Dealer 和用户 1 之间建立了一条点对点的连续变量量子密钥分发 (continuous-variable quantum key distribution, CVQKD) 链路 [26]. 应用 CVQKD 标准后处理程序 [39], Dealer 和用户 1 之间的密钥率的下界 R_1 便被估计出来. 之后所有参与方都丢弃相应数据. 利用同样的方法估计出 Dealer 和用户 2 之间的密钥率的下界 R_2. 出于安全考虑, Dealer 应选择 $\{R_1, R_2\}$ 中的最小值作为 LLO-CVQSS 方案的最终密钥率 R.

若 R 为正, 则对剩余未公开数据进行反向协商, 获得用户 1 与 Dealer 之间的密钥 K_1、用户 2 与 Dealer 之间的密钥 K_2. 最后, Dealer 根据表达式 $E = M \oplus K_1 \oplus K_2$ 对消息 M 进行编码, 然后将加密后的消息 E 广播给所有用户. 显然, 只有用户 1 和用户 2 合作才能将加密消息 E 解码.

由上可知, 本文提出的基于 KF 的 LLO-CVQSS 方案不必通过不安全信道传输 LO 因而能够彻底消除攻击者操纵 LO 的安全威胁, 相比传统 CVQSS 系统在实际安全性方面具有明显优势. 在 2) 测量部分的滤波是实现本方案的相位补偿与相位噪声控制的重要操作, 将在第 3 节详细介绍.

3 相位补偿方法设计

本节介绍基于 KF 的 LLO-CVQSS 相位补偿方法. 在第 2 节测量部分 Dealer 混合信号测量结果 $\{x_{\rm D}, p_{\rm D}\}$ 可表示为

$$\begin{aligned}\begin{bmatrix} x_{\rm D} \\ p_{\rm D} \end{bmatrix} &= \begin{bmatrix} x_{\rm D_1} + x_{\rm D_2} \\ p_{\rm D_1} + p_{\rm D_2} \end{bmatrix} \\ &= \sqrt{\frac{\eta T_1}{2}} \begin{bmatrix} \cos\Phi_1 & \sin\Phi_1 \\ -\sin\Phi_1 & \cos\Phi_1 \end{bmatrix} \begin{bmatrix} x_1 \\ p_1 \end{bmatrix} \\ &\quad + \sqrt{\frac{\eta T_2}{2}} \begin{bmatrix} \cos\Phi_2 & \sin\Phi_2 \\ -\sin\Phi_2 & \cos\Phi_2 \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} + \begin{bmatrix} x_{\rm N} \\ p_{\rm N} \end{bmatrix}, \end{aligned} \tag{1}$$

式中, η 为外差检测效率, T_1 和 T_2 为各用户与 Dealer

之间的信道透过率, $x_{\rm N}$ 和 $p_{\rm N}$ 为高斯噪声, 相位差 Φ_1 为用户 1 与 Dealer 之间相位快漂移、Φ_2 为用户 2 与 Dealer 之间相位快漂移:

$$\Phi_1 = \theta_1^{\rm init} - \theta_{\rm D}^{\rm init}, \tag{2}$$

$$\Phi_2 = \theta_2^{\rm init} - \theta_{\rm D}^{\rm init}, \tag{3}$$

式中, $\theta_1^{\rm init}$, $\theta_2^{\rm init}$ 和 $\theta_{\rm D}^{\rm init}$ 分别为用户 1、用户 2 和 Dealer 激光器的初始相位. 另外, 外差检测得到的用户 2 参考相位 y_2 和 Dealer 参考相位 $y_{\rm D}$ 测量方程分别表示为[40]

$$y_2 = \theta_2^{\rm R} + n_2, \tag{4}$$

$$y_{\rm D} = \theta_{\rm D}^{\rm R} + n_{\rm D}, \tag{5}$$

式中 n_2 和 $n_{\rm D}$ 分别为用户 2、Dealer 端相位测量噪声, $\theta_2^{\rm R}$ 为用户 1 与用户 2 参考信号之间相位漂移、$\theta_{\rm D}^{\rm R}$ 为用户 1 与 Dealer 参考信号间相位漂移. 具体表示为

$$\theta_2^{\rm R} = \theta_1^{\rm init} + \theta_1^{\rm delay} - \left(\theta_2^{\rm init} + \theta_2^{\rm delay}\right) = \Phi_1 - \Phi_2 + \varphi_2^{\rm R}, \tag{6}$$

$$\theta_{\rm D}^{\rm R} = \theta_1^{\rm init} + \theta_1^{\rm delay} - \left(\theta_{\rm D}^{\rm init} + \theta_{\rm D}^{\rm delay}\right) = \Phi_1 + \varphi_{\rm D}^{\rm R}, \tag{7}$$

式中, $\theta_1^{\rm delay}$, $\theta_2^{\rm delay}$ 和 $\theta_{\rm D}^{\rm delay}$ 分别为用户 1、用户 2 和 Dealer 光路传输延迟和激光时钟同步误差, 其两两差值 $\varphi_2^{\rm R}$ 为用户 1 与用户 2 之间相位慢漂移、$\varphi_{\rm D}^{\rm R}$ 为用户 1 与 Dealer 之间相位慢漂移.

由于标量 KF 不处理相位慢漂移, 可由矢量 KF(详见补充材料 A(online)) 退化得到, 因此不作为重点介绍. 用户 2 和 Dealer 通过矢量 KF 对各自参考相位进行估计, 从估计状态向量 $\hat{\boldsymbol{s}}_2 = \begin{bmatrix} \hat{\theta}_2^{\rm R} \\ \hat{\varphi}_2^{\rm R} \end{bmatrix}$ 和 $\hat{\boldsymbol{s}}_{\rm D} = \begin{bmatrix} \hat{\theta}_{\rm D}^{\rm R} \\ \hat{\varphi}_{\rm D}^{\rm R} \end{bmatrix}$ 中得到相位漂移估计值 $\hat{\theta}_2^{\rm R}$, $\hat{\theta}_{\rm D}^{\rm R}$ 和相位慢漂移估计值 $\hat{\varphi}_2^{\rm R}$, $\hat{\varphi}_{\rm D}^{\rm R}$ 两部分. 进一步, 用户 2 滤波相位 $\theta_2^{\rm KF}$ 和 Dealer 滤波相位 $\theta_{\rm D}^{\rm KF}$ 可由估计状态向量提取如下:

$$\theta_2^{\rm KF} = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} \hat{\theta}_2^{\rm R} \\ \hat{\varphi}_2^{\rm R} \end{bmatrix} = \hat{\theta}_2^{\rm R} - \hat{\varphi}_2^{\rm R} = \hat{\Phi}_1 - \hat{\Phi}_2, \tag{8}$$

$$\theta_{\rm D}^{\rm KF} = \begin{bmatrix} 1 & -1 \end{bmatrix} \begin{bmatrix} \hat{\theta}_{\rm D}^{\rm R} \\ \hat{\varphi}_{\rm D}^{\rm R} \end{bmatrix} = \hat{\theta}_{\rm D}^{\rm R} - \hat{\varphi}_{\rm D}^{\rm R} = \hat{\Phi}_1. \tag{9}$$

可见滤波相位由相位快漂移估计值 $\hat{\Phi}_1$, $\hat{\Phi}_2$ 组成. 根据滤波相位进行相位旋转操作, 用户 2 和 Dealer 的数据分别修正为

$$\begin{bmatrix} x_2' \\ p_2' \end{bmatrix} = \begin{bmatrix} \cos\left(-\theta_2^{\rm KF}\right) & \sin\left(-\theta_2^{\rm KF}\right) \\ -\sin\left(-\theta_2^{\rm KF}\right) & \cos\left(-\theta_2^{\rm KF}\right) \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} = \begin{bmatrix} \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) & \sin\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) \\ -\sin\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) & \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix}, \tag{10}$$

$$\begin{aligned}
\begin{bmatrix} x_{\rm D}' \\ p_{\rm D}' \end{bmatrix} &= \begin{bmatrix} \cos\left(-\theta_{\rm D}^{\rm KF}\right) & \sin\left(-\theta_{\rm D}^{\rm KF}\right) \\ -\sin\left(-\theta_{\rm D}^{\rm KF}\right) & \cos\left(-\theta_{\rm D}^{\rm KF}\right) \end{bmatrix} \begin{bmatrix} x_{\rm D} \\ p_{\rm D} \end{bmatrix} = \sqrt{\frac{\eta T_1}{2}} \begin{bmatrix} \cos(\Phi_1 - \hat{\Phi}_1) & \sin\left(\Phi_1 - \hat{\Phi}_1\right) \\ -\sin(\Phi_1 - \hat{\Phi}_1) & \cos\left(\Phi_1 - \hat{\Phi}_1\right) \end{bmatrix} \begin{bmatrix} x_1 \\ p_1 \end{bmatrix} \\
&+ \sqrt{\frac{\eta T_2}{2}} \begin{bmatrix} \cos\left(\Phi_2 - \hat{\Phi}_1\right) & \sin\left(\Phi_2 - \hat{\Phi}_1\right) \\ -\sin\left(\Phi_2 - \hat{\Phi}_1\right) & \cos\left(\Phi_2 - \hat{\Phi}_1\right) \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} + \begin{bmatrix} x_{\rm N}' \\ p_{\rm N}' \end{bmatrix} = \sqrt{\frac{\eta T_1}{2}} \begin{bmatrix} \cos(\delta\Phi_1) & \sin(\delta\Phi_1) \\ -\sin(\delta\Phi_1) & \cos(\delta\Phi_1) \end{bmatrix} \begin{bmatrix} x_1 \\ p_1 \end{bmatrix} \\
&+ \sqrt{\frac{\eta T_2}{2}} \begin{bmatrix} \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1 + \delta\Phi_2\right) & \sin\left(\hat{\Phi}_2 - \hat{\Phi}_1 + \delta\Phi_2\right) \\ -\sin\left(\hat{\Phi}_2 - \hat{\Phi}_1 + \delta\Phi_2\right) & \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1 + \delta\Phi_2\right) \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} + \begin{bmatrix} x_{\rm N}' \\ p_{\rm N}' \end{bmatrix} \\
&= \sqrt{\frac{\eta T_1}{2}} \begin{bmatrix} \cos(\delta\Phi_1) & \sin(\delta\Phi_1) \\ -\sin(\delta\Phi_1) & \cos(\delta\Phi_1) \end{bmatrix} \begin{bmatrix} x_1 \\ p_1 \end{bmatrix} \\
&+ \sqrt{\frac{\eta T_2}{2}} \begin{bmatrix} \cos(\delta\Phi_2) & \sin(\delta\Phi_2) \\ -\sin(\delta\Phi_2) & \cos(\delta\Phi_2) \end{bmatrix} \begin{bmatrix} \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) & \sin\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) \\ -\sin\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) & \cos\left(\hat{\Phi}_2 - \hat{\Phi}_1\right) \end{bmatrix} \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} + \begin{bmatrix} x_{\rm N}' \\ p_{\rm N}' \end{bmatrix} \\
&= \sqrt{\frac{\eta T_1}{2}} \begin{bmatrix} \cos(\delta\Phi_1) & \sin(\delta\Phi_1) \\ -\sin(\delta\Phi_1) & \cos(\delta\Phi_1) \end{bmatrix} \begin{bmatrix} x_1 \\ p_1 \end{bmatrix} + \sqrt{\frac{\eta T_2}{2}} \begin{bmatrix} \cos(\delta\Phi_2) & \sin(\delta\Phi_2) \\ -\sin(\delta\Phi_2) & \cos(\delta\Phi_2) \end{bmatrix} \begin{bmatrix} x_2' \\ p_2' \end{bmatrix} + \begin{bmatrix} x_{\rm N}' \\ p_{\rm N}' \end{bmatrix},
\end{aligned} \tag{11}$$

式中, $\delta\Phi_1$ 和 $\delta\Phi_2$ 为补偿误差相位[41], $x'_{\rm N}$ 和 $p'_{\rm N}$ 依然为高斯噪声. 至此, 多方相位漂移根据矢量 KF 完成一步补偿. 而对于标量 KF, 除以上步骤外, 需额外补偿相位慢漂移[30]: 将数据 $\{x_1,p_1\}$, $\{x'_2,p'_2\}$ 和 $\{x'_{\rm D},p'_{\rm D}\}$ 分成若干块, Dealer 对块中数据随机披露, 用户 1、用户 2 完成互相关计算并补偿, 最后所有参与方丢弃相应数据.

4 系统过噪声建模

为简便起见, 假设基于 KF 的 LLO-CVQSS 各用户量子信号调制方差均为 $V_{\rm A}$, 施加在量子信号上总的过噪声可表示为

$$\varepsilon=\varepsilon_{\rm AM}+\varepsilon_{\rm LE}+\varepsilon_{\rm ADC}+\varepsilon_{\rm phase}+\varepsilon_{\rm rest}, \tag{12}$$

其中 $\varepsilon_{\rm rest}$ 为一般 CVQKD 已考虑的其余过噪声, 而在调制过程中, 因实际调幅器的动态范围有限[42], 引入调制噪声:

$$\begin{aligned}\varepsilon_{\rm AM}&=\varepsilon_{\rm AM_1}+\varepsilon_{\rm AM_2}\\&=|\alpha_{\rm S}|^2 10^{-d_{\rm dB}/10}+\frac{T_2}{T_1}|\alpha_{\rm S}|^2 10^{-d_{\rm dB}/10},\end{aligned} \tag{13}$$

式中, 调幅器动态范围取典型值 $d_{\rm dB}=40$, 信号最大振幅 $\alpha_{\rm S}=\sqrt{10V_{\rm A}}$. 另外, 用户 1 参考信号与量子信号耦合时, 其脉冲间隔的残余光子进入信号脉冲[43], 引起光子泄漏噪声:

$$\varepsilon_{\rm LE}=\varepsilon_{\rm LE_1}+\varepsilon_{\rm LE_2}=\frac{2|\alpha_{\rm R}|^2}{R_{\rm e}}+\frac{T_2}{T_1}\cdot\frac{2|\alpha_{\rm R}|^2}{R_{\rm e}}, \tag{14}$$

式中 $|\alpha_{\rm R}|^2$ 为所选取的 CVQKD 链路用户参考信号幅值, 调幅器有限消光比取 $R_{\rm e}=60$ dB. 其次在 Dealer 端测量时, 输出电压经模数转换器 (analog-to-digital converter, ADC) 量化[44], 引入 ADC 量化噪声记为

$$\varepsilon_{\rm ADC}=\varepsilon_{\rm ADC_1}+\varepsilon_{\rm ADC_2}\geqslant\frac{|\alpha_{\rm S}|^2}{12\cdot 2^q}+\frac{T_2}{T_1}\cdot\frac{|\alpha_{\rm S}|^2}{12\cdot 2^q}, \tag{15}$$

式中, ADC 量化比特数 q=10. 本地本振系统相位噪声由相位快、慢漂移补偿误差构成, 如下式:

$$\varepsilon_{\rm phase}=V_{\rm A}\left(V_{\rm fast}+V_{\rm slow}\right)=V_{\rm A}\left(V_{\rm drift}+V_{\rm error}+V_{\rm slow}\right), \tag{16}$$

式中因各用户量子信号与参考信号由同一激光器产生, 量子信号与参考信号之间相位漂移方差 $V_{\rm drift}=0$; 相位慢漂移补偿误差 $V_{\rm slow}$ 因补偿方式的区别而有所不同, 这一点会在第 5 节中重点分析; 由于信道损耗与噪声客观存在[45], 用户 2 和 Dealer 测量参考相位时的误差可计算为

$$V_{\rm error}=V_{\rm error_D}+V_{\rm error_2}=\frac{\chi_{\rm D}+1}{|\alpha_{\rm R}|^2}+\frac{T_2}{T_1}\cdot\frac{\chi_2+1}{|\alpha_{\rm R}|^2}, \tag{17}$$

式中, 参考信号上总噪声为

$$\chi_{\rm D}=\frac{2-\eta T_1+2v_{\rm el}}{\eta T_1}+\varepsilon_{\rm ch},$$

$$\chi_2=\frac{2-\eta T_2+2v_{\rm el}}{\eta {\rm T}_2}+\varepsilon_{\rm ch},$$

其中, 参考信号信道噪声[46] $\varepsilon_{\rm ch}=0.002$, $v_{\rm el}$ 为电噪声.

基于 KF 的 LLO-CVQSS 对相位补偿的优化主要体现在相位漂移估计误差上. 根据不完全相位补偿噪声模型[47] 可知, 在消除光频差的理想情况下, 相位漂移估计误差为相位测量误差 $\sigma_{\rm n}^2{=}V_{\rm error}$. 而经过 KF, 估计误差减小为[37]

$$\begin{aligned}\mu&=\frac{1}{2}\left[\sqrt{\sigma_{\rm w}^2\left(\sigma_{\rm w}^2+4\sigma_{\rm n}^2\right)}-\sigma_{\rm w}^2\right]\\&<\frac{1}{2}\left[\left(\sigma_{\rm w}^2+2\sigma_{\rm n}^2\right)-\sigma_{\rm w}^2\right]=\sigma_{\rm n}^2,\end{aligned} \tag{18}$$

详细数学推导过程见补充材料 A (online). 其物理意义为 KF 通过动态调整卡尔曼增益, 将相位测量误差 $\sigma_{\rm n}^2$ 与状态噪声方差 $\sigma_{\rm w}^2$ 联合优化, 最终使得估计误差 μ 始终小于原始测量误差 $\sigma_{\rm n}^2$. 相应地, 相位补偿精度计算为[48]

$$\kappa=(1-\mu/2)^2. \tag{19}$$

补偿后相位噪声可重写为[49]

$$\varepsilon'_{\rm phase}=(\varepsilon+V_{\rm A})(1-\kappa)/\kappa. \tag{20}$$

而信道实际过噪声和用户 1 实际信道透过率分别为[50]

$$\begin{aligned}\varepsilon'&=\varepsilon_{\rm AM}+\varepsilon_{\rm LE}+\varepsilon_{\rm ADC}+\varepsilon'_{\rm phase}+\varepsilon_{\rm rest}\\&=\frac{\varepsilon+(1-\kappa)V_{\rm A}}{\kappa},\end{aligned} \tag{21}$$

$$T'_1=\kappa T_1. \tag{22}$$

密钥率计算过程与一般 CVQSS 一致, 详见补充材料 B(online). 由上可知, 受益于过噪声的降低和信道透过率的增大, 基于 KF 的 LLO-CVQSS 在渐近性能方面具有优势, 下一节将对其进行定量评估.

5 数值模拟分析

目前为止, 已经详细介绍了基于 KF 的 LLO-

CVQSS 方案, 包括相位补偿方法和具体的过噪声模型. 其优势在于, 不仅克服了 LO 容易遭受针对性攻击的安全弱点, 还降低了相位估计误差, 实现对系统的实际安全性能的优化. 本节对其效果进行模拟. 根据实际实验环境, 衰减系数设置为 $\alpha = 0.2$ dB/km[51], 反向协商效率 $\beta = 0.95$[52], 外差检测效率 $\eta = 0.6$[53], 电噪声 $v_{\mathrm{el}} = 0.01$[46], 量子信号调制方差 $V_{\mathrm{A}} = 4$, 与块平均方案[54]的标准值保持一致, 以确保实验结果的可比性.

图 2 为基于矢量 KF 和标量 KF 的 LLO-CVQSS 两种系统的渐近性能, 为方便比较也给出理想补偿和块平均系统性能, 无特别说明 σ_{w}^2=10^{-4}. 结果表明, 矢量 KF 方案的密钥率与理想补偿情况十分接近, 且相位快漂移方差相同时, 矢量 KF 方案的补偿结果优于标量 KF 方案和块平均方案. 这是由于矢量 KF 不仅处理了相位慢漂移, 还提供较小的相位漂移估计误差 μ, 如插图所示, μ 在数值上远小于相位测量误差 σ_{n}^2 的结果证明了这一点. 由 (18) 式可知, KF 直接降低相位估计误差 μ, 从而过噪声中的相位噪声分量减少至 $\varepsilon'_{\mathrm{phase}}$ (见 (20) 式) 并最终提升密钥率 R. 而进一步观察不同相位快漂移方差 σ_{w}^2 情况的矢量 KF 方案可发现, σ_{w}^2 越小系统密钥率越高, 这表明采用初始相位较为接近的独立激光器将对矢量 KF 方案性能提升起到一定作用. 需注意的是, 标量 KF 本身缺乏对相位慢漂移的处理, 相位慢漂移补偿误差 V_{slow} 不可忽略. 考虑到 LLO-CVQSS 系统规模等复杂因素, 相位慢漂移补偿误差较大时 (如浅灰色虚线所示 $V_{\mathrm{slow}} = 0.005$ rad^2 或 16.4 deg^2) 将严重削弱其性能, 标量 KF 系统性能与块平均相比不具有明显优势, 由此可见第 3 节提到标量 KF 方案对相位慢漂移的额外补偿十分必要.

上述模拟中为使结果更具说服力, 采用了对块平均方案最优的用户参考信号幅值 $|\alpha_{\mathrm{R}}|^2_{\mathrm{optimal}}$[55,56]. 而图 3 表示幅值 $|\alpha_{\mathrm{R}}|^2$ 对矢量 KF 和块平均系统性能的具体影响, 其中黑色、深灰色和浅灰色线条分别代表 $|\alpha_{\mathrm{R}}|^2$ 为 1000, 3000 和块平均最优的情况. 从图 3 插图中得到的信息是, 除了矢量 KF 的过噪声小于块平均的过噪声外, 当 $|\alpha_{\mathrm{R}}|^2$ 在 (0, 10000] 的范围内增大时, 矢量 KF 和块平均的过噪声分别增长和先减后增, 这解释了图 3 中二者密钥率随 $|\alpha_{\mathrm{R}}|^2$ 变化而呈现不同趋势的原因. 根据第 4 节的噪声模型可知, $|\alpha_{\mathrm{R}}|^2$ 与相位噪声 $\varepsilon_{\mathrm{phase}}$ 成反比而与光子泄露噪声 $\varepsilon_{\mathrm{LE}}$ 成正比, 不难得出经过 KF, 相位噪声 $\varepsilon'_{\mathrm{phase}}$ 不再是过噪声主导因素. 矢量 KF 系统的优势可概括为受 $|\alpha_{\mathrm{R}}|^2$ 影响较小, 且可以用较小的 $|\alpha_{\mathrm{R}}|^2$ 获得更好的性能. 本地本振系统对用户参考信号的取值远小于 LO[57] 的初衷之一是减少对量子信号的干扰[43], 上述分析结果很好地满足了这一需求.

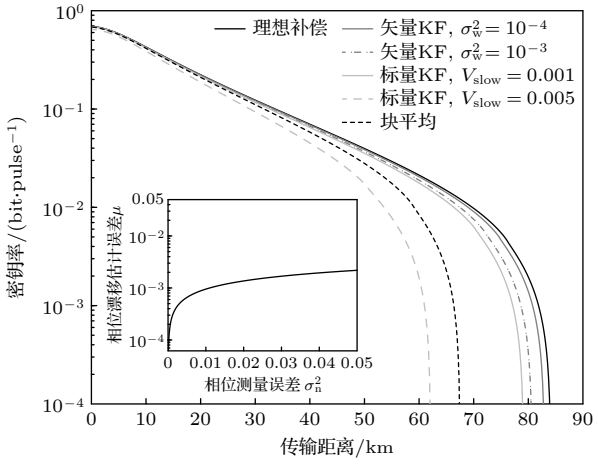


图 2 不同相位补偿方法下所提方案性能, 插图为相位漂移估计误差与相位测量误差的函数关系

Fig. 2. Performance of the proposed scheme with different phase compensation methods, and the subplot shows the phase drift estimation error as a function of the phase measurement error.

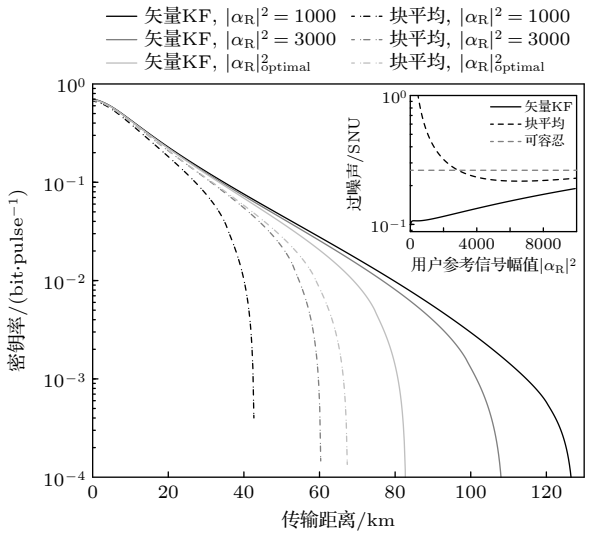


图 3 不同参考信号幅值下所提方案与块平均方案性能; 小图为传输距离 60 km 时系统过噪声与 $|\alpha_{\mathrm{R}}|^2$ 的函数关系

Fig. 3. Performance of the proposed scheme and block averaging for different reference signal amplitudes, and the small figure shows the excess noise as a function of $|\alpha_{\mathrm{R}}|^2$ at a transmission distance of 60 km.

最后, 用户数 n 作为 QSS 系统容量的重要衡量指标, 有必要此在框架内对所提方案展开研究. 图 4 表示推广 (2, 2) 阈值实现的 (n, n) 阈值矢量 KF 和块平均方案密钥率与传输距离的函数关系, 从右到左不同颜色不同标记线条分别代表用户数 n 为 2, 4, 10, 22 和 33 的情况. 容易发现, 随着用户数的增加, 两种方案密钥率都会下降, 这是因为出于安全性考虑, $n-1$ 个用户必须被视为不诚实, 而增加的用户引入了更多的过噪声. 对于这一限制系统规模的消极因素, 矢量 KF 明显比块平均控制得更好. 数值上来看, 矢量 KF 将最远传输距离从 67.3 km 提升至 82.6 km, 并将系统支持的最大用户数从 22 提升至 33, 表明基于 KF 的 LLO-CVQSS 更有利于构建大规模量子通信网络.

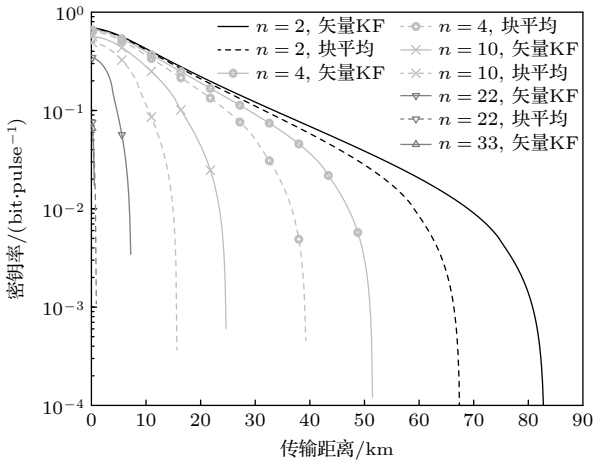


图 4 不同 (n, n) 阈值下所提方案和块平均方案性能

Fig. 4. Performance of the proposed scheme and block averaging for different (n, n) thresholds.

6 结 论

本文提出了一种实用的基于 KF 的 LLO-CVQSS, 采取由 Dealer 本地生成 LO 的策略, 消除了由用户经不安全信道传输 LO 的必要, 从而能够抵御针对 LO 的攻击, 与现有的 CVQSS 协议相比具有更高实际安全性. 在该基础之上, 通过 KF 实现对参考相位的 MMSE 估计, 从而大幅降低相位漂移估计误差. 开发了矢量 KF 和标量 KF 各自相位补偿方法, 其中矢量 KF 无需对相位慢漂移进行额外处理便可高效地一步完成补偿. 对 LLO-CVQSS 过噪声建模, 发现滤波有效抑制了相位测量噪声. 推导了在窃听者和不诚实用户的攻击下基于 KF 的 LLO-CVQSS 的安全界限, 数值模拟表明性能优化效果显著. 与块平均方案相比, 所提方案最远传输距离从 67.3 km 提升至 82.6 km, 最大支持用户数从 22 提升至 33, 构建大规模实用量子通信网络的潜力得到体现. 本文的局限性在于, 尚未考虑多用户动态加入或退出场景下的实时相位补偿问题. 未来的工作将致力于探索基于深度学习的自适应拓展卡尔曼滤波算法 [58], 以支持动态量子网络的构建. 同时, 我们也计划利用量子机器学习技术 [59], 进一步提升基于 KF 的 LLO-CVQSS 的性能.

参考文献

[1] Hillery M, Bužek V, Berthiaume A 1999 *Phys. Rev. A* **59** 1829

[2] Karlsson A, Koashi M, Imoto N 1999 *Phys. Rev. A* **59** 162

[3] Tyc T, Sanders B C 2002 *Phys. Rev. A* **65** 042310

[4] Lance A M, Symul T, Bowen W P, Tyc T, Sanders B C, Lam P K 2003 *New J. Phys.* **5** 4

[5] Liao Q, Xiao G, Xu C G, Xu Y, Guo Y 2020 *Phys. Rev. A* **102** 032604

[6] Kogias I, Xiang Y, He Q, Adesso G 2017 *Phys. Rev. A* **95** 012315

[7] Grice W P, Qi B 2019 *Phys. Rev. A* **100** 022339

[8] Wang Y J, Jia B, Mao Y, Wu X L, Guo Y 2020 *Appl. Sci.* **10** 2411

[9] Liao Q, Liu H J, Zhu L J, Guo Y 2021 *Phys. Rev. A* **103** 032410

[10] Liao Q, Liu X Q, Ou B, Fu X Q 2023 *IEEE Trans. Commun.* **71** 6051

[11] Liao Q, Wang Z, Liu H, Mao Y, Fu X 2022 *Phys. Rev. A* **106** 022607

[12] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A-Atom. Mol. Opt. Phy.* **87** 052309

[13] Jouguet P, Kunz-Jacques S, Diamanti E 2013 *Phys. Rev. A-Atom. Mol. Opt. Phy.* **87** 062313

[14] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A-Atom. Mol. Opt. Phy.* **88** 022339

[15] Zhao Y J, Zhang Y C, Huang Y D, Xu B J, Yu S, Guo H 2018 *J. Phys. B-At. Mol. Opt. Phy.* **52** 015501

[16] Zheng Y, Huang P, Peng J Y, Zeng G H 2019 *Inf. Commun. Technol. Policy* **45** 43 (in Chinese) [郑异, 黄鹏, 彭进业, 曾贵华 2019 信息通信技术与政策 **45** 43]

[17] Liao Q, Huang L, Fei Z Y, Fu X Q 2025 *Adv. Quantum Technol.* **8** 2400505

[18] Kunz-Jacques S, Jouguet P 2015 *Phys. Rev. A* **91** 022307

[19] Mao Y Y, Huang W T, Zhong H, Wang Y J, Qin H, Guo Y, Huang D 2020 *New J. Phys.* **22** 083073

[20] Liao Q, Liu H J, Gong Y P, Wang Z, Peng Q Q, Guo Y 2022 *Opt. Express* **30** 3876

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

[22] Wang T, Huang P, Zhou Y M, Liu W Q, Ma H X, Wang S Y, Zeng G H 2018 *Opt. Express* **26** 2794

[23] Wang H, Li Y, Pi Y D, Pan Y, Shao Y, Ma L, Zhang Y C, Yang J, Zhang T, Huang W, Xu B J 2022 *Commun. Phys.* **5** 162

[24] Marie A, Alléaume R 2017 *Phys. Rev. A* **95** 012316

[25] Wang H, Pi Y D, Huang W, Li Y, Shao Y, Yang J, Liu J L,

Zhang C L, Zhang Y C, Xu B J 2020 *Opt. Express* **28** 32882
[26] Zhang Y C, Bian Y M, Li Z Y, Yu S, Guo H 2024 *Appl. Phys. Rev.* **11** 011318
[27] Huang B, Ma T T, Huang Y M, Peng Z M 2021 *Laser Optoelectron. Prog.* **58** 1127001 (in Chinese) [黄彪, 麻甜甜, 黄永梅, 彭真明 2021 激光与光电子学进展 **58** 1127001]
[28] Roy S, Petersen I R, Huntington E H 2015 *New J. Phys.* **17** 063020
[29] Liu X C, Wen J X, Li S B, Li H G, Sun S L 2023 *Chin. J. Lasers* **50** 1412002 (in Chinese) [刘旭超, 温佳旭, 李少波, 李华贵, 孙时伦 2023 中国激光 **50** 1412002]
[30] Shen T, Wang X Y, Chen Z Y, Tian H P, Yu S, Guo H 2023 *IEEE Photonics J.* **15** 7600109
[31] Ren S J, Kumar R, Wonfor A, Tang X K, Penty R, White I 2019 *JOSA B* **36** B7
[32] Huang B, Huang Y M, Peng Z M 2019 *Acta Opt. Sin.* **39** 1127001 (in Chinese) [黄彪, 黄永梅, 彭真明 2019 光学学报 **39** 1127001]
[33] Roy S, Rehman O U, Petersen I R, Huntington E H 2014 *European Control Conference Strasbourg, France* pp896-901
[34] Wang T, Huang P, Wang S Y, Zeng G H 2019 *Opt. Express* **27** 26689
[35] Hajomer A A, Derkach I, Jain N, Chin H M, Andersen U L, Gehring T 2024 *Sci. Adv.* **10** eadi9474
[36] Su Y, Guo Y, Huang D 2019 *Phys. Lett. A* **383** 2394
[37] Huang B, Huang Y M, Peng Z M 2020 *Opt. Express* **28** 28727
[38] Zhong H, Ye W, Zuo Z Y, Huang D, Guo Y 2022 *Opt. Express* **30** 5981
[39] Diamanti E, Leverrier A 2015 *Entropy* **17** 6072
[40] Inoue T, Namiki S 2014 *Opt. Express* **22** 15376
[41] Huang B, Huang Y M, Peng Z M 2019 *Opt. Express* **27** 20621
[42] Shao Y, Pan Y, Wang H, Pi Y D, Li Y, Ma L, Zhang Y C, Huang W, Xu B J 2022 *Entropy* **24** 992
[43] Shao Y, Wang H, Pi Y D, Huang W, Li Y, Liu J L, Yang J, Zhang Y C, Xu B J 2021 *Phys. Rev. A* **104** 032608
[44] Kish S P, Villaseñor E, Malaney R, Mudge K A, Grant K J 2021 *IEEE International Conference on Communications Montreal, Quebec* pp1–6
[45] Shao Y, Li Y, Wang H, Pan Y, Pi Y D, Zhang Y C, Huang W, Xu B J 2022 *Phys. Rev. A* **105** 032601
[46] Wang T, Huang P, Zhou Y M, Liu W Q, Zeng G H 2018 *Phys. Rev. A* **97** 012310
[47] Huang P, Lin D K, Huang D, Zeng, G H 2015 *Int. J. Theor. Phys.* **54** 2613-2622
[48] Jouguet P, Kunz-Jacques S, Diamanti E, Leverrier A 2012 *Phys. Rev. A-Atom. Mol. Opt. Phy.* **86** 032309
[49] Huang D, Huang P, Lin D K, Zeng G H 2016 *Sci. Rep.* **6** 19201
[50] Chin H M, Jain N, Zibar D, Andersen U L, Gehring T 2021 *Npj Quantum Inf.* **7** 20
[51] Sun Y H, Chen Z Y, Wang X Y, Yu S, Guo H 2025 *Phys. Rev. Appl.* **23** 014056
[52] Oruganti A N, Derkach I, Filip R, Usenko V C 2025 *Quantum Sci. Technol.* **10** 025023
[53] Liu Y M, Jiang X Q, Dai J S, Hai H, Huang P 2025 *Quantum Sci. Technol.* **10** 025043
[54] Liao Q, Fei Z Y, Huang L, Fu X Q 2025 *Commun. Phys.* **8** 138
[55] Ren S J, Yang S, Wonfor A, White I, Penty R 2021 *Sci. Rep.* **11** 9454
[56] Soh D B, Brif C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J, Sarovar M 2015 *Phys. Rev. X* **5** 041010
[57] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev. A-Atom. Mol. Opt. Phy.* **76** 042305
[58] Rui X, He H W, Sun F C, Zhao K 2013 *IEEE Trans. Veh. Technol.* **62** 108
[59] Liao Q, Fei Z Y, Liu J Y, Huang A Q, Huang L, Wang Y J 2025 *Chaos Soliton. Fract.* **196** 116331

Kalman filter based local local oscillator continuous-variable quantum secret sharing*

LIAO Qin [1)] FEI Zhuoying [1)] WANG Yijun [2)†]

1) (*College of Computer Science and Electronic Engineering, Hunan University, Changsha* 410082, *China*)

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

(Received 25 February 2025; revised manuscript received 30 April 2025)

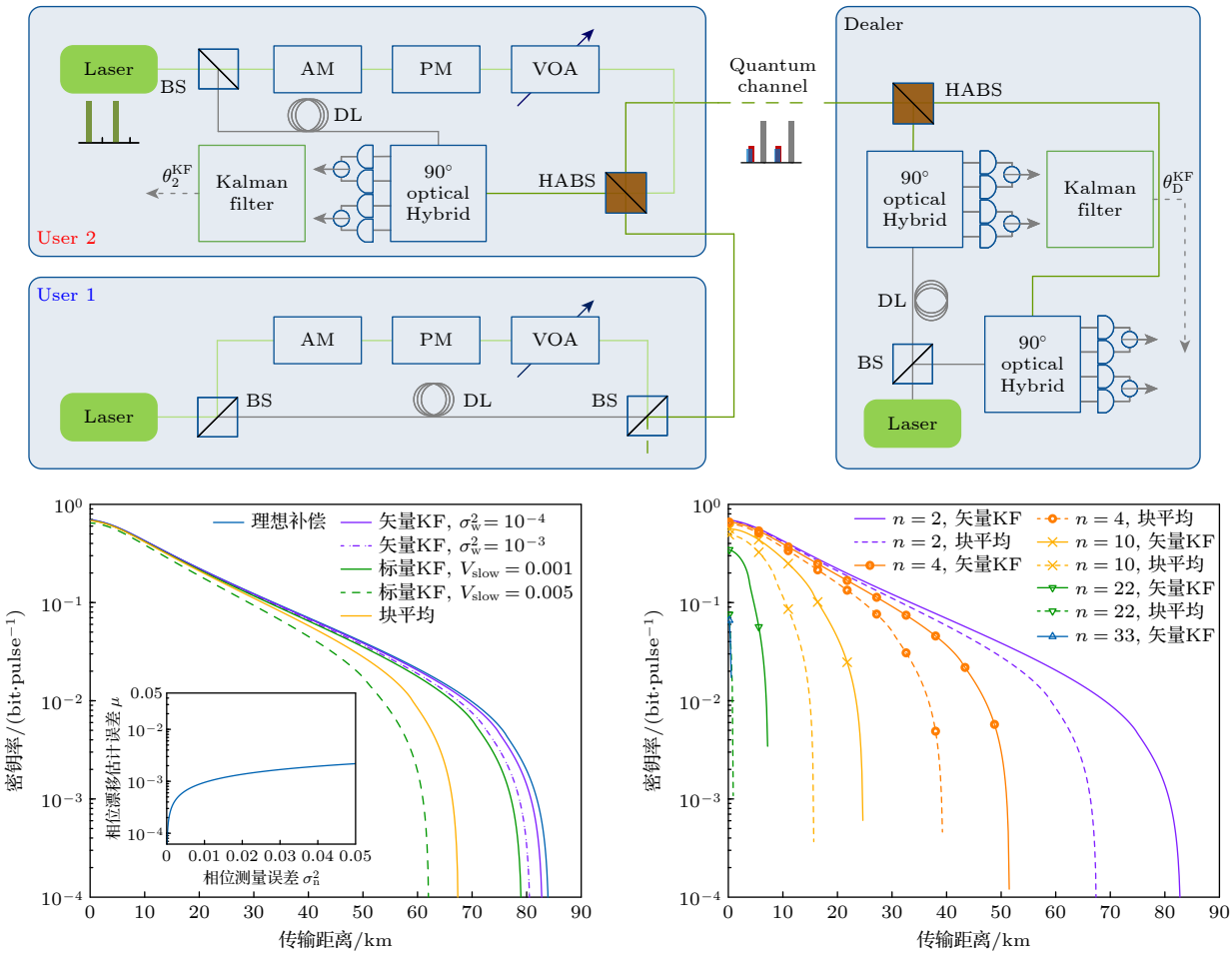
Abstract

In a practical continuous-variable quantum secret sharing system, the local oscillator transmitted via an insecure channel may be subjected to security threats due to various targeted attacks. To solve this problem, this paper proposes a continuous-variable quantum secret sharing scheme with local intrinsic oscillator, in which the intrinsic oscillator is generated locally at the trusted end without being sent by each user, thus completely

* Project supported by the National Natural Science Foundation of China (Grant No. 62101180) and the Key Research and Development Program of Hunan Province, China (Grant No. 2025QK3011).

† Corresponding author. E-mail: xxywyj@sina.com

plugging the relevant security loopholes. The scheme consists of three stages: preparation, where users generate Gaussian-modulated coherent states and reference signals; measurement, where the dealer performs heterodyne detection by using the local intrinsic oscillator and reference phases; post-processing, which involves parameter estimation, phase compensation, and secure key extraction. On this basis, Kalman filter (KF) is utilized to estimate the minimum mean square error for each reference phase separately, reducing the phase drift estimation error and suppressing the phase measurement noise. Phase compensation methods for scalar KF and vector KF are developed respectively, where scalar KF requires additional block averaging for slow phase drift, while vector KF simultaneously models fast and slow drifts, enabling one-step compensation with minimized estimation errors. The excess noise of the filtered system including modulation noise, phase noise, photon leakage noise, and ADC quantization noise is modeled, with KF reducing phase measurement noise via dynamic gain optimization. Security bound against eavesdroppers and dishonest users is derived. Numerical simulations under practical parameters demonstrate significant improvements: vector KF achieves a maximum transmission distance of 82.6 km (*vs.* 67.3 km for block averaging) and supports 33 users (*vs.* 22), with excess noise reduced by 40% at 60 km. The scheme's robustness is further validated under varying reference signal amplitudes, showing stable performance even at lower levels, minimizing interference with quantum signals. These results highlight that the proposed scheme has significant advantages in terms of maximum transmission distance and maximum number of supported users, and has the potential to build adaptive KF algorithms for dynamic user scenarios and quantum machine learning integration.



Keywords: quantum secret sharing, continuous variable, local local oscillator, Kalman filter

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250227

CSTR: 32037.14.aps.74.20250227

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

基于卡尔曼滤波的本地本振连续变量量子秘密共享

廖骏　费焯迎　王一军

Kalman filter based local local oscillator continuous-variable quantum secret sharing

LIAO Qin　FEI Zhuoying　WANG Yijun

引用信息 Citation: Acta Physica Sinica, 74, 160303 (2025)　DOI: 10.7498/aps.74.20250227
CSTR: 32037.14.aps.74.20250227
在线阅读 View online: https://doi.org/10.7498/aps.74.20250227
当期内容 View table of contents: http://wulixb.iphy.ac.cn
