一维高斯调制连续变量量子密钥分发现实源强度误差的影响*

王普† 白增亮 常利伟

(山西财经大学信息学院, 太原 030006)

(2025 年 1 月 7 日收到; 2025 年 2 月 5 日收到修改稿)

本文深入地研究了一维高斯调制连续变量量子密钥分发系统在源强度误差下的现实安全性和性能表现. 详细地分析了源强度误差对协议参数估计过程的影响机制, 并基于发送端的三种现实假设, 提出相应数据优化方案, 以减轻源强度误差的负面影响. 同时, 综合考虑了源强度误差及有限码长效应, 以保障系统的现实安全性. 研究结果表明, 源强度误差不可忽视, 对于显著的强度波动, 系统的最大传输距离将减少约 20 km. 因此, 在协议的实际实施过程中, 必须充分考虑源强度误差的影响, 并采取相应的措施来减少或消除这些误差. 本研究为现实条件下实施一维高斯调制连续变量量子密钥分发提供了理论依据, 为构建高效、低成本、小型化的量子通信网络探索了新方向.

关键词: 连续变量量子密钥分发, 一维调制, 源误差, 现实安全性

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250025

CSTR: 32037.14.aps.74.20250025

1 引 言

量子密钥分发 (quantum key distribution, QKD) 以量子物理基本原理为基础, 在通信双方间分发密钥, 确保信息安全[1,2]. 其安全性不依赖于数学问题的复杂性, 也不受计算能力的限制, 从理论层面上能够实现无条件安全通信[3]. 1984 年, Bennett 和 Brassard[1] 受量子货币思想启发, 提出了首个 QKD 协议, 即 BB84 协议. 从 1992 年第一个 32.5 cm 的自由空间 QKD 实验演示[4] 到现在跨越 4600 km 的天地一体化量子通信网络[5], 经过 30 多年理论和实验的发展, QKD 已经从实验室逐渐走向现实应用[6]. 30 多年来, 各种 QKD 协议被提出[6–8], 根据编码方式的不同主要分为两类: 基于单光子编码的离散变量量子密钥分发 (discrete-variable QKD, DV-QKD) 和基于光场正交分量编码的连续变量量子密钥分发 (continuous-variable QKD, CV-QKD).

CV-QKD 将信息编码于光场的正交分量, 采用相干探测技术, 如零差探测或外差探测. 这使得它在中短距离成码率高, 与现有光纤网络兼容性好, 且无需昂贵的单光子探测器. 同时, 其实现成本低、易集成, 能够有效地满足局域网和城域网络的搭建需求, 近年来受到科研人员的广泛关注[9–12]. 其研究重点主要聚焦于以下三方面: 首要的是确保协议的安全性, 这涵盖了对潜在窃听者 Eve 可能采取的各类攻击策略的防范, 以及针对实际器件不完美性所带来的现实安全性挑战[13–23]; 其次是提升协议的性能, 旨在达到更高的密钥生成速率以及实现更远的传输距离[24–33]; 最后是推动协议物理实现的集成化、小型化和低成本, 这包括探索更为

* 国家自然科学基金 (批准号: 62305198) 和山西省自然科学基金 (批准号: 202303021212168, 202103021224290) 资助的课题.

† 通信作者. E-mail: wangpu@sxufe.edu.cn

简便的协议方案、拓展协议以支持多用户网络化应用等[34–43].

尽管 CV-QKD 在理论和实验方面已取得显著的成就, 但对于真正广泛安全的实际应用仍面临许多关键挑战. 虽然 CV-QKD 的理论安全性分析已较为完善, 但在实际应用过程中, 存在实际系统与理论模型不匹配的情况, 这会导致安全漏洞的出现, 使系统面临被窃听者攻击的风险. 在确保安全的前提下, 实际的 CV-QKD 系统致力于在尽可能简化系统结构的基础上实现高性能. 一维 (unidimensional, UD) CV-QKD 协议仅使用一个调制器 (振幅或者相位调制器) 来完成信息的编码, 在硬件实现上更为简单, 降低了整体系统的搭建成本. 由于信息编码的维度减少, 所需的随机数生成量也相应减少. 这对于随机数生成资源有限的应用场景尤为重要. 因此, UD CV-QKD 对于 CV-QKD 的小型化和低成本应用具有显著优势. 尤其是在构建大规模量子通信网络时更具吸引力, 通过减少每个节点的成本, 可以更容易地实现网络的扩展和普及[44–61]. 但目前 UD CV-QKD 的研究都假定发送端 (Alice) 具有完全稳定的源, 这在实际中是不现实的. 即使用户可以很好地控制源, 也不可避免地会出现一些误差[62–65]. 其中, 最主要的源误差是源的强度误差, 比如光脉冲的强度波动、调制器和衰减器的不精确校准以及不可避免的外部环境干扰等都可能导致光源强度误差的产生. 最近, 单路和测量设备独立的两维高斯调制 CV-QKD 方案 (正交振幅和相位都调制) 在源强度误差下的现实安全性被研究[64,65], 有效地促进了协议的实际应用.

为了完善 UD CV-QKD 的现实安全性, 本文研究了源强度误差对 UD CV-QKD 协议性能和安全性的影响. 为了使得协议能够在各种现实条件下稳定运行并保障通信安全, 我们对用户的能力做出了三种贴近实际的假设, 并针对这些假设提出了相应的数据优化处理方案, 以减少源误差的影响. 同时, 我们强调, 对于潜在窃听者 (Eve) 的能力, 并未施加任何限制, 以确保我们的安全分析具有普遍性和严谨性. 进一步, 我们评估了协议在有限码长下的安全性. 由于在协议的实际实现中, 通信双方能交换的量子态数量总是有限的, 因此必须考虑统计涨落和有限码长效应对安全性的影响. 当源误差和有限码长同时存在时, 它们会相互交织并共同影响 UD CV-QKD 系统的安全性.

本文首先阐述了 UD CV-QKD 协议方案和安全性, 然后详细地分析了不同现实假设下源误差对 UD CV-QKD 的影响, 最后综合考虑了源误差和有限码长效应, 以确保系统的实际安全性.

2 一维高斯调制连续变量量子密钥分发模型

2.1 协议模型

当描述一个 CV-QKD 协议时, 通常包含两种方案: “准备与测量”(preparation and measurement, PM) 和 “基于纠缠”(entanglement-based, EB). 在 PM 方案中, 信息发送方 (Alice) 会先将经典信息编码到量子态中, 然后通过光信号的形式发送给信息接收方 (Bob). Bob 接收到信号后, 会进行一系列测量, 以还原出原始的经典信息. 在 EB 方案中, Alice 会生成一个特殊的双模压缩真空态, 并测量其中一个模式的正交分量. 随后, 她将另一个模式发送给 Bob, Bob 测量相应正交分量, 以完成信息的传递. 在实际应用场景中, 现有的大多数 CV-QKD 系统都是基于 PM 方案来实现的. 而 EB 方案对于协议的安全性分析更加方便.

图 1(a) 展示了一维高斯调制相干态协议的 PM 方案. 协议的主要步骤包括:

1) 量子态的制备. 在发送端, Alice 使用强度为 I 的信号脉冲光准备一系列相干态. 为了完成信息编码, Alice 使用一个调制方差为 V_{M} 的振幅调制器对相干态进行调制, 调制后的量子态在相空间中呈现一维链式结构.

2) 量子态的传输. Alice 通过一个不可信的量子信道将调制好的量子态发送出去.

3) 量子态的测量. 探测端 Bob 接收到信号后, 运用实际的平衡零拍探测器对量子态的正交振幅或者正交相位展开测量.

4) 数据筛选. Bob 公开测量正交的选择, Alice 只保留与 Bob 相同的正交分量. 然后 Alice 和 Bob 得到一组相互关联的数据.

5) 参数估计. Alice 和 Bob 利用公开信道交换一部分数据, 进行参数估计. 通过对量子信道透射率、额外噪声和正交相位方差等参数的估计, 可以估算协议的密钥率, 判断通信是否安全、有效.

6) 数据协调. 若通信有效, Bob 发送一些边信息给 Alice, 进行数据协调、纠错, 使得通信双方得到一组完全相同的数据.

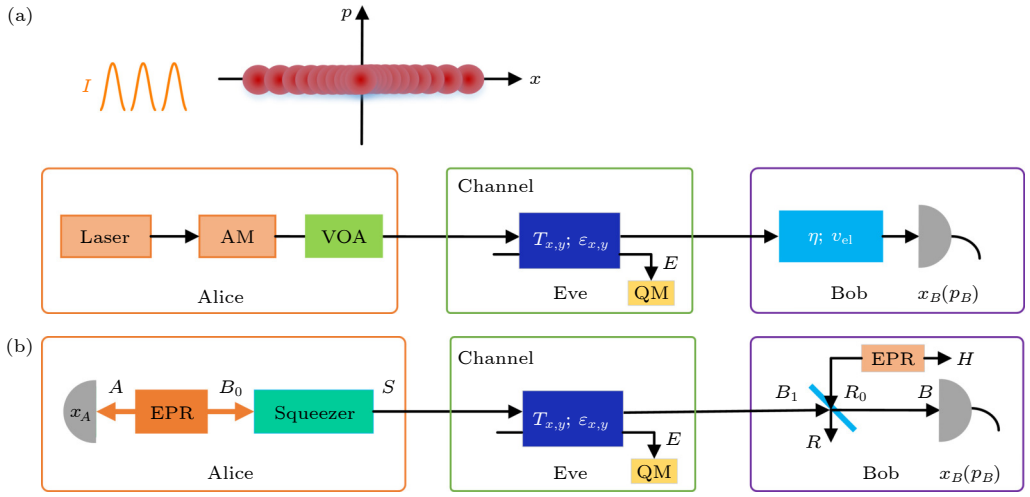


图 1 一维高斯调制连续变量量子密钥分发模型 (a) 准备测量方案; (b) 基于纠缠方案

Fig. 1. Unidimensional Gaussian modulation continuous-variable quantum key distribution models: (a) Preparation and measurement scheme; (b) entanglement-based scheme.

7) 私密放大. 通信双方应用哈希函数消除可能泄漏的信息, 得到安全密钥.

为了便于安全性分析, 我们考虑协议等效的 EB 方案. 如图 1(b) 所示, Alice 准备具有方差 V 的 EPR 态 ρ_{AB_0}, 并对自己保留的模式 A 进行零拍探测, 对另外一个模态 B_0, 用压缩参数 $r=\ln\sqrt{V}$ 的压缩算符 (Squeezer) 对正交相位进行压缩, 产生模式 S. 然后 Alice 将模式 S 通过传输效率为 T_x, T_y, 额外噪声为 ε_x, ε_y, 长度为 L 的量子信道发送给 Bob. Bob 进一步使用传输效率为 η 的分束器将接收到的模式 B_1 转化 B. 这个转化过程用来模拟探测效率为 η, 电子学噪声为 $v_{\rm el}$ 的实际零拍探测器. 其中, 电子学噪声通过在分束器的一个端口注入方差为 $V_{\rm N}$ 的热态 ρ_{R_0} 来模拟, 则 $V_{\rm N}=1+v_{\rm el}/(1-\eta)$. 然后, Bob 使用一个完美的零拍探测器测量模式 B 的正交振幅 x 和部分正交相位 p, 得到测量结果 x_B 和 p_B. 至此, Alice 和 Bob 获得一组相互关联的数据. 最后经过参数估计、数据协调、私密放大步骤, 通信双方可以提取安全的密钥.

上述两种方案的等价关系已经被证明[50]. 通过对 Alice 的零差探测结果乘以一个常数因子, 可以建立 UD 相干态协议的 EB 方案和 PM 方案的一对一等价关系.

2.2 密钥率的计算

利用等价的 EB 方案, 可以方便地进行密钥速率的计算. 在渐近条件下, 以 Bob 端的数据为参考端 (反向协调), 安全密钥速率的计算公式为[44]

$$K^{\rm asy}=\beta I_{AB}-\chi_{BE}, \tag{1}$$

其中 I_{AB} 是 Alice 和 Bob 之间的香农互信息; χ_{BE} 是 Holevo 边界, 代表 Eve 可以从 Bob 端的数据获取的最大信息量; β 代表数据协调效率.

密钥速率计算的关键是推导出量子态传输过程中系统的协方差矩阵. 起始的 EPR 态 ρ_{AB_0}, 对模式 B_0 进行相位压缩后得到量子态 ρ_{AS}, 它的协方差矩阵可以表示为

$$\gamma_{AS}=\begin{bmatrix} V & 0 & \sqrt{V\left(V^2-1\right)} & 0 \\ 0 & V & 0 & -\sqrt{(V^2-1)/V} \\ \sqrt{V\left(V^2-1\right)} & 0 & V^2 & 0 \\ 0 & -\sqrt{(V^2-1)/V} & 0 & 1 \end{bmatrix}. \tag{2}$$

这时模式 S 的相位正交分量方差为 1, 即一个散粒噪声单元. 模式 S 进一步通过量子信道, 发送给 Bob, 得到模式 B_1, 相应的协方差矩阵变为

$$\boldsymbol{\gamma}_{AB_1}=\begin{bmatrix}\sqrt{1+V_{\mathrm{M}}} & 0 & \sqrt{T_xV_{\mathrm{M}}}(1+V_{\mathrm{M}})^{1/4} & 0\\ 0 & \sqrt{1+V_{\mathrm{M}}} & 0 & C_y^{B_1}\\ \sqrt{T_xV_{\mathrm{M}}}(1+V_{\mathrm{M}})^{1/4} & 0 & T_x\left(V_{\mathrm{M}}+1+\chi_{\mathrm{linex}}\right) & 0\\ 0 & C_y^{B_1} & 0 & V_y^{B_1}\end{bmatrix}, \tag{3}$$

其中调制方差 $V_{\mathrm{M}}=V^2-1$, $\chi_{\mathrm{linex}}=(1-T_x)/T_x+\varepsilon_x$ 代表量子态在正交振幅方向上由信道引入的总噪声(相对于信道的输入端), $V_y^{B_1}$ 代表模式 B_1 在正交相位方向上的方差, $C_y^{B_1}$ 代表模式 A 和 B_1 在正交相位方向上关联.

在接收端, 模式 B_1 通过分束器之后, 变为模式 B. 协方差矩阵 $\boldsymbol{\gamma}_{AB}$ 具有如下形式:

$$\boldsymbol{\gamma}_{AB}=\begin{bmatrix}\sqrt{1+V_{\mathrm{M}}} & 0 & \sqrt{\eta T_xV_{\mathrm{M}}}(1+V_{\mathrm{M}})^{1/4} & 0\\ 0 & \sqrt{1+V_{\mathrm{M}}} & 0 & C_y^{B}\\ \sqrt{\eta T_xV_{\mathrm{M}}}(1+V_{\mathrm{M}})^{1/4} & 0 & \eta T_x\left(V_{\mathrm{M}}+1+\chi_{\mathrm{totx}}\right) & 0\\ 0 & C_y^{B} & 0 & V_y^{B}\end{bmatrix}, \tag{4}$$

其中 $\chi_{\mathrm{totx}}=\chi_{\mathrm{linex}}+\chi_{\mathrm{hom}}/T_x$ 是相对于信道输入端, 量子态在正交振幅方向上系统引入的总噪声; $\chi_{\mathrm{hom}}=(1-\eta)/\eta+\nu_{\mathrm{el}}/\eta$ 是相对于 Bob 输入端, 由于探测器的不完美引入的噪声; $V_y^B=\eta\left(V_y^{B_1}+\chi_{\mathrm{hom}}\right)$ 和 $C_y^B=C_y^{B_1}\sqrt{\eta}$ 是量子态在正交相位方向上的方差和关联.

可以求得互信息 I_{AB} 为

$$I_{AB}=\frac{1}{2}\log_2\frac{V_A}{V_A^{x_B}}=\frac{1}{2}\log_2\left(1+\frac{V_{\mathrm{M}}}{1+\chi_{\mathrm{totx}}}\right). \tag{5}$$

Holevo 边界 χ_{BE} 定义为

$$\chi_{BE}=S(\rho_E)-S\left(\rho_E^{x_B}\right), \tag{6}$$

其中 $S(\rho)$ 是量子态 ρ 的冯诺伊曼熵. 基于 Eve 的纯化, 系统 ρ_{AB_1E} 为纯态, 有 $S(\rho_{AB_1})=S(\rho_E)$. 在 Bob 端进行探测之后, $\rho_{ARHE}^{x_B}$ 是纯态, 有 $S(\rho_E^{x_B})=S(\rho_{ARH}^{x_B})$. 所以 χ_{BE} 可以进一步写为

$$\begin{aligned}\chi_{BE}&=S(\rho_{AB_1})-S(\rho_{ARH}^{x_B})\\&=\sum_{i=1}^{2}g\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}g\left(\frac{\lambda_i-1}{2}\right),\end{aligned} \tag{7}$$

其中 $g(x)=(x+1)\log_2(x+1)-x\log_2 x$.

$\lambda_{1,2}$ 是量子态 ρ_{AB_1} 对应的协方差矩阵 $\boldsymbol{\gamma}_{AB_1}$ 的辛本征值, 表示为

$$\lambda_{1,2}^2=\frac{1}{2}\left[A\pm\sqrt{A^2-4B}\right], \tag{8}$$

其中

$$\begin{aligned}A=&1+V_y^{B_1}+V_{\mathrm{M}}+V_y^{B_1}\left(\varepsilon_x+V_{\mathrm{M}}\right)T_x\\&+2C_y^{B_1}(1+V_{\mathrm{M}})^{\frac{1}{4}}\sqrt{V_{\mathrm{M}}T_x},\end{aligned} \tag{9}$$

$$B=\left[V_y^{B_1}(1+V_{\mathrm{M}})-\left(C_y^{B_1}\right)^2\sqrt{1+V_{\mathrm{M}}}\right](1+\varepsilon_xT_x). \tag{10}$$

$\lambda_{3,4,5}$ 是量子态 $\rho_{ARH}^{x_B}$ 对应的协方差矩阵 $\boldsymbol{\gamma}_{ARH}^{x_B}$ 的辛本征值, 表示为

$$\lambda_{3,4}^2=\frac{1}{2}\left[C\pm\sqrt{C^2-4D}\right],\ \lambda_5=1. \tag{11}$$

其中

$$C=\frac{A(1+\nu_{\mathrm{el}})+[(\varepsilon_xT_x+1)(V_{\mathrm{M}}+2)+V_{\mathrm{M}}T_x-A]\eta}{1+\varepsilon_xT_x\eta+V_{\mathrm{M}}T_x\eta+\nu_{\mathrm{el}}}, \tag{12}$$

$$D=\frac{B(1+\nu_{\mathrm{el}}-\eta)+(1+V_{\mathrm{M}})(1+\varepsilon_xT_x)\eta}{1+\varepsilon_xT_x\eta+V_{\mathrm{M}}T_x\eta+\nu_{\mathrm{el}}}. \tag{13}$$

基于以上结果, 可以计算密钥速率. 对于上述未知参数 $C_y^{B_1}$ 和 $V_y^{B_1}$, $V_y^{B_1}$ 可以通过在 Bob 端随机地探测量子态的正交相位分量来估计, 而 $C_y^{B_1}$ 不能被估计, 因为在 Alice 端起始的量子态在正交相位分量上没有调制. 窃听者 Eve 可以通过操控 $C_y^{B_1}$ 执行攻击, 然而它的攻击必须符合基本的物理原则. 因此, 未知参数 $C_y^{B_1}$ 可以利用海森伯不确定关系进行限制.

根据海森伯不确定关系, 一个高斯态是物理态, 则其协方差矩阵 $\boldsymbol{\gamma}$ 必须满足 [66]:

$$\boldsymbol{\gamma}+\mathrm{i}\cdot\boldsymbol{\Omega}\geqslant 0, \tag{14}$$

其中

$$\boldsymbol{\Omega} = \bigoplus_{i=1}^{n} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{15}$$

因此, 参数 $C_y^{B_1}$ 和 $V_y^{B_1}$ 可以被限制, 通过如下关系式:

$$\gamma_{AB_1} + \mathrm{i}\cdot\boldsymbol{\Omega} \geqslant 0, \tag{16}$$

得到抛物线方程:

$$(C_y^{B_1} - C_0)^2 \leqslant \frac{V_{\mathrm{M}}}{\sqrt{(1+V_{\mathrm{M}})}} \frac{\chi_{\mathrm{linex}}}{1+\chi_{\mathrm{linex}}} (V_y^{B_1} - V_0), \tag{17}$$

其中

$$C_0 = -\frac{V_0\sqrt{T_x V_{\mathrm{M}}}}{(1+V_{\mathrm{M}})^{1/4}}, \quad V_0 = \frac{1}{T_x\,(1+\chi_{\mathrm{linex}})}. \tag{18}$$

在理论仿真中, 对于一个固定 $V_y^{B_1}$, 可以通过扫描 $C_y^{B_1}$, 找到一个 $C_y^{B_1\mathrm{opt}}$, 使得协议的密钥速率最低, 这个密钥率是可获得的安全密钥率[44,45,50].

3 源误差影响

上述密钥率的计算基于一个假设, 态的制备过程是完美的. 然而在协议的实际实施过程中, 当 Alice 准备相干态时, 不可避免地会产生一些误差, 如光源强度误差. 如图 2, 实际的光脉冲强度 I' 随着时间 t 进行变化, 这使得准备发送的目标相干态和实际制备的相干态有偏差.

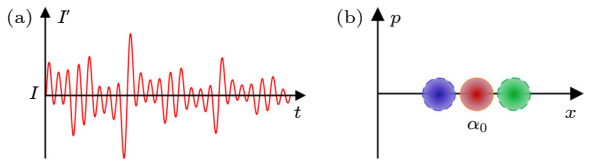


图 2 (a) 实际的光脉冲强度 I' 随时间 t 呈现出动态变化; (b) 在相空间中, 由于源强度误差的影响, 实际制备的相干态可能会偏离目标相干态的位置

Fig. 2. (a) Actual optical pulse intensity dynamically changes over time; (b) the actual prepared coherent state may deviate from the target coherent state's location in the phase space under the influence of source intensity errors.

通过对协议运行中的实际源强度误差建模, 有两种误差来源: 一种是由于源器件 (调制器或衰减器) 的不精确校准引起的强度偏置; 一种是由于源脉冲强度的不精确控制导致的强度波动. 假设发送者 Alice 原本打算使用强度为 I 的信号脉冲光制备一系列相干态, 但在任何时刻 t_i, 她实际使用的信号脉冲光强度为 $I_i' = I\,(1+\varphi)\,(1+\delta_i)$. φ 代表强度偏置, 因为在每一轮 QKD 的传输中, 它的漂移比较缓慢, 可以被视为一个常数. δ_i 是强度波动, 其均值为 0, 方差为 V_{f}. 由于现实中强度波动的方差远小于调制方差, 因此, 经过调制之后量子态的正交振幅仍然可以近似为高斯分布. 因为 $I \propto |\alpha|^2$, Alice 实际编码的高斯随机变量是

$$x_A' = \sqrt{(1+\varphi)\,(1+\delta_i)}\,x_A. \tag{19}$$

制备的量子态经过量子信道传输到 Bob 端, 进行探测后得到:

$$x_B' = t_x x_A' + z_x, \tag{20}$$

其中 $t_x = \sqrt{\eta T_x}$; z_x 代表噪声项, 服从均值为零, 方差为 $\sigma_x^2 = 1 + \eta T_x \varepsilon_x + \nu_{\mathrm{el}}$ 的高斯分布.

下面我们对 Alice 的能力制定不同的假设, 以适应于各种现实情况, 并提出不同的数据处理方案来保证协议在各种情况下的安全性. 而我们对窃听者 (Eve) 的能力没有进行任何限定, 即考虑最差的情况, 假设 Eve 知道每个脉冲的强度边信息.

3.1 Alice 知道信号源每个脉冲的强度变化

首先给出最强假设, 也就是 Alice 知道每个脉冲的强度边信息. 此情形下, 从理论上来说, Alice 完全有能力对每个脉冲的误差进行精准校正, 例如对光源进行实时反馈控制. 但这样做会使系统的复杂程度大幅提升, 同时也会增加成本投入. 于是, 我们提出一种新的方案, 即在不增添任何硬件设备的前提下, 仅仅借助简单的数据后处理手段, 可以对安全密钥率进行估算. 具体的操作方法是, 依据强度边信息, Alice 直接对她手头的数据 x_A 做出相应调整, 使其变为 x_A'. 如此一来, 信道参数可以被正确估计, 最终的密钥率表达为

$$K_{\mathrm{final}}^{\mathrm{asy}} = \int_{-\infty}^{+\infty} f\,(\delta_i)\,K^{\mathrm{asy}}\,(V_{\mathrm{M}i})\,\mathrm{d}\delta_i, \tag{21}$$

其中 $f\,(\delta_i)$ 是 δ_i 的概率密度函数, $V_{\mathrm{M}i} = (1+\varphi)\,(1+\delta_i)V_{\mathrm{M}}$. 不难发现, 经过数据修正之后的密钥率近似于理想情况 (没有源误差) 的密钥率.

3.2 Alice 只知道信号源强度变化的统计分布

在一般情况下, Alice 并不能掌握每个脉冲的强度边信息, 在此假定她仅仅了解脉冲强度变化的统计分布情况. 比如, 在 QKD 正式启动运行前的测试阶段, 对未知参数 φ 和 δ_i 实施评估. 下面, 我们考虑 δ_i 的两种常见分布形式: 高斯分布和均匀分布.

为了得到密钥率, Alice 和 Bob 需要公开部分数据对信道参数 T_x, ε_x 进行估计, 假设 Alice 使用记录的数据 x_A 进行估计, 那么:

$$t'_x=\frac{\langle x_A x'_B\rangle}{\langle x_A^2\rangle}=\frac{\langle x_A t_x x'_A\rangle}{\langle x_A^2\rangle}=\sqrt{1+\varphi}\left\langle\sqrt{1+\delta_i}\right\rangle t_x. \tag{22}$$

对函数 $\sqrt{1+\delta_i}$ 在 $\delta_i=0$ 附近实施泰勒展开, 从而获得

$$\left\langle\sqrt{1+\delta_i}\right\rangle\approx 1-\frac{1}{8}V_{\rm f}. \tag{23}$$

定义 $T_{\rm f}:=(1-V_{\rm f}/8)^2$, 则估计的信道传输效率 T'_x 为

$$T'_x=t'^2_x/\eta=(1+\varphi)\,T_{\rm f}t_x^2/\eta=(1+\varphi)\,T_{\rm f}T_x. \tag{24}$$

对于额外噪声 ε'_x 的精确表达, 可依据下述等价关系实现. 设想起始相干态已被理想制备, 即不存在源误差, 当该相干态经由量子信道 T'_x, ε'_x 完成传输后, Bob 所得到的探测结果 x'_B 可重新表示为

$$x'_B=t'_x x_A+z'_x. \tag{25}$$

此时,

$$V\left(x'_B\right)=\eta T'_x V_{\rm M}+\eta\left(\varepsilon'_x T'_x+1\right)+\eta\chi_{\rm hom}. \tag{26}$$

Bob 端得到的 $V\left(x'_B\right)$ 为

$$V\left(x'_B\right)=\eta T_x\left(1+\varphi\right)V_{\rm M}+\eta\left(\varepsilon_x T_x+1\right)+\eta\chi_{\rm hom}. \tag{27}$$

建立上述两个方程的等价关系, 得到:

$$T'_x V_M+\varepsilon'_x T'_x=T_x\left(1+\varphi\right)V_{\rm M}+\varepsilon_x T_x. \tag{28}$$

经过简单的代数运算, 得到:

$$\varepsilon'_x\approx\varepsilon_x/(1+\varphi)\,T_{\rm f}+\frac{1}{4}V_{\rm M}V_{\rm f}. \tag{29}$$

最终得到估计结果为

$$\begin{cases}T'_x=(1+\varphi)\,T_{\rm f}T_x\,,\\ \varepsilon'_x\approx\varepsilon_x/\left(1+\varphi\right)T_{\rm f}+\dfrac{1}{4}V_{\rm M}V_{\rm f}\,.\end{cases} \tag{30}$$

当源端存在向下强度偏置 (即 $\varphi<0$) 的情况下, 这时:

$$T'_x<T_x,\ \varepsilon'_x>\varepsilon_x. \tag{31}$$

信道传输效率被低估, 额外噪声被高估, 进而致使估计的密钥率降低, 不过此情形下并不存在安全隐患.

当源端存在一个向上的强度偏置, 即 $\varphi>0$, 这时, 信道传输效率可能被高估, 额外噪声被低估, 导致估计的密钥率增加. 由于 Eve 掌握强度边信息, 其能够利用被低估的噪声, 实施特定的攻击, 比如截取重发攻击, 使得估计的总额外噪声与原始额外噪声数值相等, 以此隐匿攻击行为, 最终引发安全漏洞. 为了避免这个安全漏洞, Alice 可以对其所持有的原始数据 x_A 予以修正, 得到修正后的数据 $\sqrt{(1+\varphi)}x_A$, 并以此数据进行参数估计, 得到:

$$\begin{cases}T'_x=T_{\rm f}T_x\,,\\ \varepsilon'_x\approx\varepsilon_x/T_{\rm f}+\dfrac{1}{4}\left(1+\varphi\right)V_{\rm M}V_{\rm f}\,.\end{cases} \tag{32}$$

这时, 对于 $\varphi<0$, 可以得到相比于之前更好的参数估计结果. 而对于 $\varphi>0$, 信道传输效率总是被低估, 额外噪声总是被高估, 因此以上提及的潜在安全漏洞可以被克服.

考虑到强度波动 δ_i, 由于 Eve 掌握强度边信息, Alice 和 Bob 只能采用低强度信号脉冲光提取密钥[65]. 因此, Alice 可以进一步扩大自己手中的数据, 以获取更多的低强度脉冲用于密钥提取. 假设 Alice 进一步调整她的数据为 $\sqrt{(1+\varphi)\,d}x_A$, 其中 $d\geqslant 1$. 然后, Alice 发送低强度信号脉冲的概率为

$$P=\int_{-\infty}^{d-1}f\left(\delta_i\right)\mathrm{d}\delta_i. \tag{33}$$

这时, 参数估计结果为

$$\begin{cases}T'_x=T_{\rm f}T_x/d\,,\\ \varepsilon'_x\approx\varepsilon_x d/T\ +\dfrac{1}{4}\left(1+\varphi\right)dV_{\rm M}V_{\rm f}\,.\end{cases} \tag{34}$$

最终可获得的密钥率为[64,65]

$$K_{\rm final}^{\rm asy}=\beta I_{AB}-\left(1-P\right)H\left(x_B\right)-P\chi_{BE}, \tag{35}$$

其中 $\left(1-P\right)H\left(x_B\right)$ 代表不可以用于提取密钥的信息熵 (高强度脉冲光). 当 d 越大时, 则可用于提取密钥的信号数量越多. 然而, 与此同时, 信号传输过程中的损耗估计值以及额外噪声估计值也会相应增大. 因此, 存在一个最佳参数 $d^{\rm opt}$ 使得协议的密钥率达到最大值, 这个可以通过搜索得到.

接下来分析不同的源强度误差对协议密钥率的影响. 涉及的仿真系统参数分别设定为 $\beta=0.97$, $\varepsilon_x=0.03$, $\eta=0.6$, $\nu_{\rm el}=0.1$. 为了公平比较, 采用最优的调制方差 $V_{\rm M}^{\rm opt}$ 和 $d^{\rm opt}$. 考虑经典的对称的信道, 则 $T_y=T_x$, $\varepsilon_y=\varepsilon_x$, 这时: $V_y^{B_1}=1+T_x\varepsilon_x$. 图 3 展示了在不同强度偏置和强度波动下, 密钥速率随着传输距离的变化情况. 图 3(a) 是均匀分布强度波动的结果, 以 δ_i 的绝对值表示波动范围. 图 3(b) 是高斯分布强度波动的结果, 以 δ_i 的方差 $V_{\rm f}$ 表示波动强弱. 黑色实线代表没有源强度误差的密钥率. 分析图 3 可以发现, 在 Alice 优化调整自

身的数据之后, 几乎可以消除光源的强度偏置对协议的影响. 对于一个较大的强度偏置 $\varphi=0.2$, 密钥率几乎没有变化. 这是因为, 经过数据后处理之后, 强度偏置对参数估计结果的影响较小. 强度波动对协议的性能影响较大, 随着波动强度的增加, 协议的密钥率和传输距离快速减少. 说明在协议的实际实施过程中, 源误差不能被忽略不计. 因此, 在协议的实际实施过程中, 必须充分考虑源误差的影响, 并采取相应的措施来减少或消除这些误差.

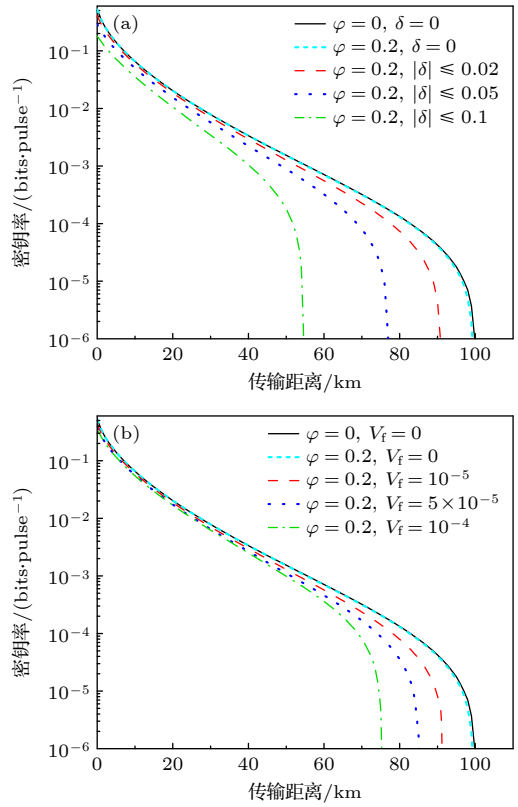


图 3 (a) 不同均匀分布强度波动下密钥率随着传输距离的变化; (b) 不同高斯分布强度波动下密钥率随着传输距离的变化

Fig. 3. (a) Comparison of secret key rates at various transmission distances for intensity fluctuation models following a uniform distribution; (b) comparison of secret key rates at various transmission distances for intensity fluctuation models adhering to a Gaussian distribution.

3.3 Alice 只知道信号源强度变化的上下边界

接下来, 我们探讨一种极端情形, 即不对信号源强度变化的具体概率分布做任何预设假设, 仅假定 Alice 知晓强度变化范围的上下边界. 具体而言, 假定 Alice 所对应的信号源脉冲强度变化区间为 $\left[I^{\rm L}, I^{\rm U}\right]$, $I^{\rm L}$ 和 $I^{\rm U}$ 分别代表上下边界. 因为概率分布的具体形式未知, 我们无法像之前的情况那样直接量化 Eve 可能窃取的信息量. 但是, Alice 和 Bob 可以从低强度脉冲提取密钥. 为了简化, 设定 $I'=gI$, 则 $I^{\rm L(U)}=g^{\rm L(U)}I$. Alice 可以采取一种策略: 将她的原始数据 x_A 直接调整为上边界值 $\sqrt{g^{\rm U}}x_A$, 并基于这些调整后的数据进行参数估计和密钥提取. 这种做法的合理性在于, 即便在强度变化范围的最大值处, 协议仍然能够保持其安全性.

当 Alice 和 Bob 使用修订后的数据 $\sqrt{g^{\rm U}}x_A$ 进行参数估计时, 我们有

$$\begin{cases} T'_x = T_g T_x / g^{\rm U}, \\ \varepsilon'_x \approx \varepsilon_x g^U / T_g + \dfrac{V_g}{4m_g^2} g^{\rm U} V_{\rm M}. \end{cases} \tag{36}$$

其中 $T_g = m_g\left(1 - V_g/8m_g^2\right)^2$, m_g 和 V_g 是强度变化因子 g 的固有均值和方差. 最终的密钥率可表达为

$$K_{\rm final}^{\rm asy} = \beta I_{AB}(g^{\rm U}V_{\rm M}, T'_x, \varepsilon'_x) - \chi_{BE}(g^{\rm U}V_{\rm M}, T'_x, \varepsilon'_x). \tag{37}$$

图 4 给出了不同源强度误差下, 协议密钥率随着传输距离的变化情况. 其他参数设定为 $\beta=0.97$, $\varepsilon_x=0.03$, $\eta=0.6$, $\nu_{\rm el}=0.1$. 采用最优调制方差以最大化密钥率. 黑色实线代表没有源强度误差的密钥率. 随着波动区间范围 ($g^{\rm U}$) 的扩大, 密钥率和传输距离减少. 在短距离处, 影响较少, 但随着传输距离的增加, 影响逐级放大.

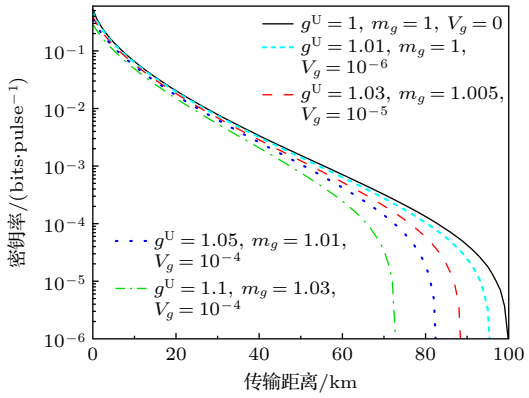


图 4 不同源强度误差对协议性能的影响

Fig. 4. Influence of different source intensity errors on protocol performance.

4 源误差和有限码长情形下协议性能

在协议的实际实现中, 由于硬件限制、存储容量和计算复杂度等原因, Alice 和 Bob 之间交换的

信号总数总是有限的. 接下来, 我们考虑有限码长情形下, 一维连续变量密钥分发协议源误差的影响. 在有限码长场景中, 由于统计波动的影响, 在源误差的基础上, 必须考虑期望值与实际观测值之间可能存在的最大差异. 假设在协议执行期间, Alice 与 Bob 交换的总信号数量记作 N, 其中 n 个信号被专门用于密钥的提取, 而剩余的 $N-n$ 个信号则用于系统参数的估计, 密钥速率的计算公式变为 [45]

$$K^{\text{finite}}=\frac{n}{N}(\beta I_{AB}^{\delta_{\text{PE}}}-\chi_{BE}^{\delta_{\text{PE}}}-\Delta(n)), \tag{38}$$

其中 $I_{AB}^{\delta_{\text{PE}}}$ 和 $\chi_{BE}^{\delta_{\text{PE}}}$ 是包含统计波动的互信息和 Holevo 边界; δ_{PE} 代表参数估计失败的概率; $\Delta(n)$ 是与私密放大有关的修正项, 定义如下:

$$\Delta(n)\simeq 7\sqrt{\frac{\log_2(2/\xi)}{n}},\quad n\geqslant 10^4. \tag{39}$$

在 UD 协议中, 除了要估计正交振幅方向上的信道参数 T_x 和 ε_x, 还要估计正交相位方差 $V_y^{B_1}$. 假设用 m 关联数据估计信道参数 T_x 和 ε_x, 用 l 数据估计相位方差 $V_y^{B_1}$. 在源误差的基础上, 由于统计波动, 参数的估计值和真实值有偏差. 为了保证协议的安全性, 我们考虑最糟糕情况, 采用参数估计边界值, 得到 [45]:

$$T'_{x\min}\approx\frac{1}{\eta}\left(\sqrt{\eta T'_x}-z_{\delta_{\text{PE}}/2}\sqrt{\frac{1+\eta T'_x\varepsilon'_x+\nu_{\text{el}}}{mV_{\text{M}}}}\right)^2, \tag{40}$$

$$\varepsilon'_{x\max}\approx\varepsilon'_x+z_{\delta_{\text{PE}}/2}\frac{(1+\eta T'_x\varepsilon'_x+\nu_{\text{el}})\sqrt{2}}{\eta T'_x\sqrt{m}}, \tag{41}$$

$$V_{y\max}^{B_1}\approx V_y^{B_1}+z_{\delta_{\text{PE}}/2}\frac{\left[\eta\left(V_y^{B_1}-1\right)+1+\nu_{\text{el}}\right]\sqrt{2}}{\eta\sqrt{l}}. \tag{42}$$

同时考虑源误差和有限码长, 图 5 对比了不同码长下, 协议的密钥率随着传输距离的变化. 图 5(a) 代表第二种源误差模型, Alice 只知道信号源强度变化的统计分布, 考虑强度偏置 $\varphi=0.2$ 和具有方差 $V_{\text{f}}=10^{-4}$ 的高斯分布统计波动. 图 5(b) 代表第三种源误差模型, Alice 只知道信号源强度变化的上下边界, 设定源误差参数: $g^{\text{U}}=1.05$, $m_g=1.01$, $V_g=10^{-4}$. 从图 5 可以发现, 有限码长限制了协议的密钥率和传输距离. 随着信号数量的减少, 可用于参数估计的数据量减少, 产生更大的估计误差, 导致密钥率和传输距离显著减少. 同时, 私密放大步骤也受到限制, 因为需要更多的原始密钥比特来生成相同数量的安全密钥比特. 在源误差存在时, 有限码长效应更加明显, 因为此时可用于参数估计的样本数量有限, 误差的累积导致密钥率的显著下降.

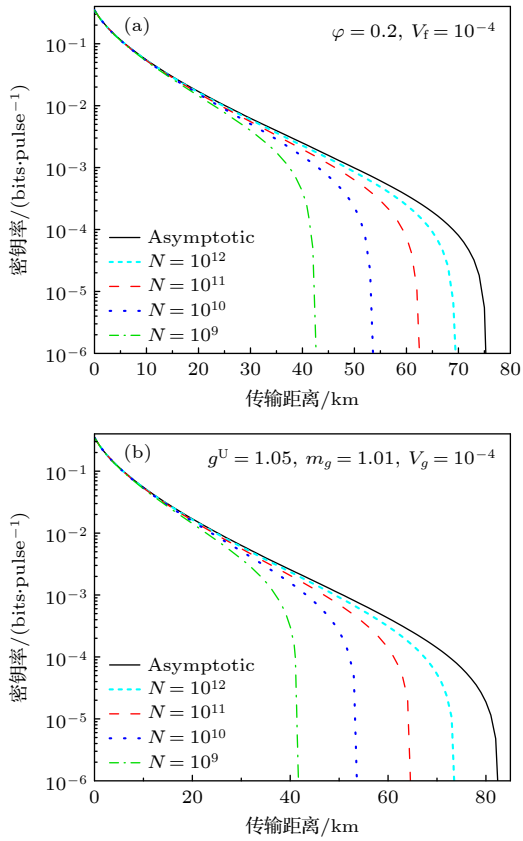


图 5 不同码长下协议性能比较 (a) 考虑第二种源误差模型; (b) 考虑第三种源误差模型

Fig. 5. Comparison of protocol performance under different total exchanged signals sizes: (a) Considering the second source error model; (b) considering the third source error model.

为了进一步研究有限码长下源强度误差的影响, 仿真了信号源脉冲数量 $N=10^{10}$ 条件下, 不同强度误差对应的协议密钥率和传输距离, 结果如图 6 所示. 图 6(a) 是第二种情况下不同高斯分布源强度波动模型. 图 6(b) 是第三种情况下不同源误差模型. 从图 6 可以发现, 尽管有限码长限制了协议的密钥率和传输距离, 但在不同的源误差条件下, 协议仍然是可行的. 对于 $N=10^{10}$ 码长, 较大的源误差 $\varphi=0.2$, $V_{\text{f}}=10^{-4}$, 45 km 下可得到大约 0.001 bit/pulse 的安全密钥率.

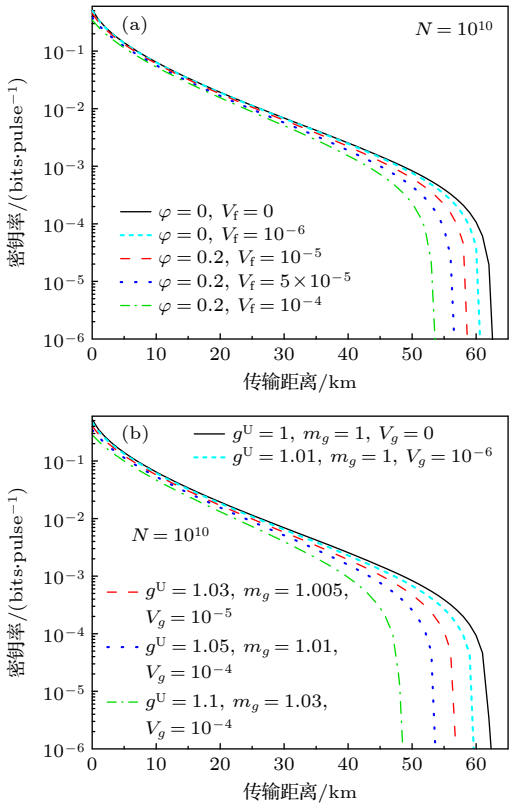


图 6 $N = 10^{10}$ 码长下不同源误差对应的协议密钥率和传输距离 (a) 考虑第二种源误差模型; (b) 考虑第三种源误差模型

Fig. 6. Protocol key rate and transmission distance corresponding to different source errors under the total exchanged signals of $N = 10^{10}$: (a) Considering the second source error model; (b) considering the third source error model.

5 结论与展望

本文研究了 UD CV-QKD 在源强度误差下的现实安全性和性能表现. 结果表明, 源误差对系统的安全性和性能产生了显著影响. 源强度误差可能会为潜在的窃听者提供额外的信息, 从而增加系统的安全性风险. 为了提升协议的现实安全性和减少源误差的影响, 针对不同的现实条件, 提出了不同的数据优化方案. 同时, 研究了有限码长下, 源误差对协议的影响, 验证了具有源强度误差 UD CV-QKD 的可行性, 为现实环境下 UD CV-QKD 的安全实施提供了理论依据.

下一步研究, 可以探索更加精确的源误差模型和更高效的数据优化方法, 以提高 UD CV-QKD 系统的安全性和性能表现. 也可以考虑将 UD CV-QKD 技术与其他量子通信技术相结合, 以构建更加安全、高效和可靠的量子通信网络系统.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore: IEEE) p175

[2] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

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

[4] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *J. Cryptology* **5** 3

[5] Chen Y A, Zhang Q, Chen T Y, Cai W Q, Liao S K, Zhang J, Chen K, Yin J, Ren J G, Chen Z, Han S L, Yu Q, Liang K, Zhou F, Yuan X, Zhao M S, Wang T Y, Jiang X, Zhang L, Liu W Y, Li Y, Shen Q, Cao Y, Lu C Y, Shu R, Wang J Y, Li L, Liu N L, Xu F, Wang X B, Peng C Z, Pan J W 2021 *Nature* **589** 214

[6] Xu F H, Ma X F, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002

[7] 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, Shamsul Shaari J, Tomamichel M, Usenko V C, Vallone G, Villoresi P, Wallden P 2020 *Adv. Opt. Photonics* **12** 1012

[8] Portmann C, Renner R 2022 *Rev. Mod. Phys.* **94** 025008

[9] Diamanti E, Leverrier A 2015 *Entropy* **17** 6072

[10] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S, Peng K C 2017 *Chin. Phys. B* **26** 040303

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

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

[13] Lin J, Upadhyaya T, Lütkenhaus N 2019 *Phys. Rev. X* **9** 041064

[14] Du S N, Tian Y, Li Y M 2020 *Phys. Rev. Appl.* **14** 024013

[15] Li L, Huang P, Wang T, Zeng G H 2021 *Phys. Rev. A* **103** 032611

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

[17] Liu J Q, Cao Y X, Wang P, Liu S S, Lu Z G, Wang X Y, Li Y M 2022 *Opt. Express* **30** 27912

[18] 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]

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

[20] Huang L Y, Wang X Y, Chen Z Y, Sun Y H, Yu S, Guo H 2023 *Phys. Rev. Appl.* **19** 014023

[21] Zapatero V, van Leent T, Arnon-Friedman R, Liu W Z, Zhang Q, Weinfurter H, Curty M 2023 *npj Quantum Inf.* **9** 10

[22] Xu Y H, Wang T, Liao X J, Zhou Y M, Huang P, Zeng G H 2024 *Photonics Res.* **12** 2549

[23] Fletcher A I, Harney C, Ghalaii M, Papanastasiou P, Mountogiannakis A, Spedalieri G, Hajomer A A E, Gehring T, Pirandola S 2025 arXiv: 2501.09818 [quant-ph]

[24] Wang P, Wang X Y, Li Y M 2019 *Phys. Rev. A* **99** 042309

[25] 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

[26] Dequal D, Trigo Vidarte L, Roman Rodriguez V, Vallone G, Villoresi P, Leverrier A, Diamanti E 2021 *npj Quantum Inf.* **7** 3

[27] Jeong S, Jung H, Ha J 2022 *npj Quantum Inf.* **8** 6

[28] Ma L, Yang J, Zhang T, Shao Y, Liu J L, Luo Y J, Wang H,

Huang W, Fan F, Zhou C, Zhang L L, Zhang S, Zhang Y C, Li Y, Xu B J 2023 *Sci. China Inf. Sci.* **66** 180507
[29] Pi Y D, Wang H, Pan Y, Shao Y, Li Y, Yang J, Zhang Y C, Huang W, Xu B J 2023 *Opt. Lett.* **48** 1766
[30] Wang P, Zhang Y, Lu Z G, Wang X Y, Li Y M 2023 *New J. Phys.* **25** 023019
[31] Yang S S, Yan Z L, Yang H Z, Lu Q, Lu Z G, Cheng L Y, Miao X Y, Li Y M 2023 *EPJ Quantum Technol.* **10** 40
[32] Chen Z Y, Wang X Y, Yu S, Li Z Y, Guo H 2023 *npj Quantum Inf.* **9** 28
[33] Hajomer A A E, Derkach I, Jain N, Chin H M, Andersen U L, Gehring T 2024 *Sci. Adv.* **10** eadi9474
[34] Zhang G, Haw J Y, Cai H, Xu F, Assad S M, Fitzsimons J F, Zhou X, Zhang Y, Yu S, Wu J, Ser W, Kwek L C, Liu A Q 2019 *Nat. Photonics* **13** 839
[35] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M, Peters N A 2020 *Phys. Rev. Appl.* **13** 054065
[36] Milovančev D, Vokić N, Laudenbach F, Pacher C, Hübel H, Schrenk B 2021 *J. Lightwave Technol.* **39** 3445
[37] Tian Y, Wang P, Liu J Q, Du S N, Liu W Y, Lu Z G, Wang X Y, Li Y M 2022 *Optica* **9** 492
[38] Du S N, Wang P, Liu J Q, Tian Y, Li Y M 2023 *Photonics Res.* **11** 463
[39] Wang X Y, Chen Z Y, Li Z H, Qi D K, Yu S, Guo H 2023 *Opt. Lett.* **48** 3327
[40] Zhang M Q, Huang P, Wang P, Wei S R, Zeng G H 2023 *Opt. Lett.* **48** 1184
[41] Hajomer A A E, Bruynsteen C, Derkach I, Jain N, Bomhals A, Bastiaens S, Andersen U L, Yin X, Gehring T 2024 *Optica* **11** 1197
[42] Hajomer A A E, Derkach I, Filip R, Andersen U L, Usenko V C, Gehring T 2024 *Light Sci. Appl.* **13** 291
[43] Ji F Y, Huang P, Wang T, Jiang X Q, Zeng G H 2024 *Photonics Res.* **12** 1485
[44] Usenko V C, Grosshans F 2015 *Phys. Rev. A* **92** 062337
[45] Wang P, Wang X Y, Li J Q, Li Y M 2017 *Opt. Express* **25** 27995
[46] Wang X Y, Liu W Y, Wang P, Li Y M 2017 *Phys. Rev. A* **95** 062330
[47] Jacobsen C S, Madsen L S, Usenko V C, Filip R, Andersen U L 2018 *npj Quantum Inf.* **4** 32
[48] Liao Q, Guo Y, Xie C L, Huang D, Huang P, Zeng G H 2018 *Quantum Inf. Process.* **17** 113
[49] Usenko V C 2018 *Phys. Rev. A* **98** 032321
[50] Wang P, Wang X Y, Li Y M 2018 *Entropy* **20** 157
[51] Wang X Y, Cao Y X, Wang P, Li Y M 2018 *Quantum Inf. Process.* **17** 344
[52] Bai D Y, Huang P, Zhu Y Q, Ma H X, Xiao T L, Wang T, Zeng G H 2020 *Quantum Inf. Process.* **19** 53
[53] Shen S Y, Dai M W, Zheng X T, Sun Q Y, Guo G C, Han Z F 2019 *Phys. Rev. A* **100** 012325
[54] Zhang H, Ruan X C, Wu X D, Zhang L, Guo Y, Huang D 2019 *Quantum Inf. Process.* **18** 128
[55] Zhao W, Shi R H, Feng Y Y, Huang D 2020 *Phys. Lett. A* **384** 126061
[56] Zhou K L, Chen Z Y, Guo Y, Liao Q 2020 *Phys. Lett. A* **384** 126074
[57] Bian Y M, Huang L Y, Zhang Y C 2021 *Entropy* **23** 294
[58] Hu J K, Liao Q, Mao Y, Guo Y 2021 *Quantum Inf. Process.* **20** 31
[59] Zhao W, Shi R H, Wu X M, Wang F Q, Ruan X C 2023 *Opt. Express* **31** 17003
[60] Li Y Y, Wang T Y 2024 *J. Phys. B: At. Mol. Opt. Phys.* **57** 145502
[61] Zhao R B, Zhou J, Shi R H, Shi J J 2024 *Ann. Phys.* **536** 2300401
[62] Zheng Y, Huang P, Huang A Q, Peng J Y, Zeng G H 2019 *Opt. Express* **27** 27369
[63] Zheng Y, Huang P, Huang A Q, Peng J Y, Zeng G H 2019 *Phys. Rev. A* **100** 012313
[64] Wang P, Wang X Y, Li Y M 2020 *Phys. Rev. A* **102** 022609
[65] Li C Y, Qian L, Lo H K 2021 *npj Quantum Inf.* **7** 150
[66] Serafini A, Paris M G A, Illuminati F, Siena S D 2005 *J. Opt. B: Quantum Semiclassical Opt.* **7** R19

Influence of source intensity errors in unidimensional Gaussian modulation continuous-variable quantum key distribution*

WANG Pu† BAI Zengliang CHANG Liwei

(*School of Information, Shanxi University of Finance and Economics, Taiyuan* 030006, *China*)

(Received 7 January 2025; revised manuscript received 5 February 2025)

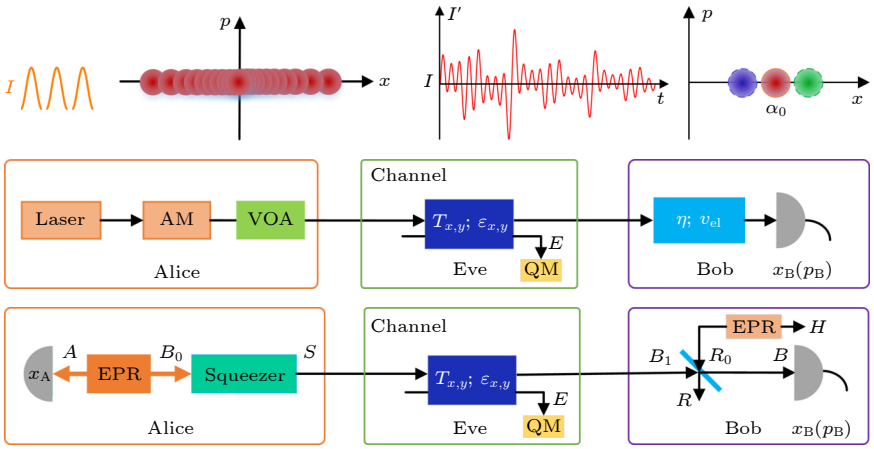
Abstract

Unidimensional Gaussian modulation continuous-variable quantum key distribution (UD CV-QKD) uses only one modulator to encode information. The UD CV-QKD has the advantages of low implementation cost and low random number consumption, making it attractive for the construction of future miniaturized and low-cost large-scale quantum communication networks. However, in the actual application of the protocol, the

* Project supported by the National Natural Science Foundation of China (Grant No. 62305198) and the Natural Science Foundation of Shanxi Province, China (Grant Nos. 202303021212168, 202103021224290).

† Corresponding author. E-mail: wangpu@sxufe.edu.cn

intensity fluctuation of the source pulsed light, device defects, and external environmental interference maybe lead to the generation of source intensity errors, thereby affecting the realistic security and performance of the protocol. To solve these problems, the security and performance of UD CV-QKD are studied in depth under source intensity errors in this work. The mechanism of source intensity errors influencing the protocol parameter estimation process is analyzed. To make it possible that the protocol can operate stably under various realistic conditions and ensure communication security, three practical assumptions about the sender's abilities are made in this work, and corresponding data optimization processing schemes for these assumptions are proposed to reduce the negative influence of source intensity errors. Additionally, both source errors and finite-size effect are comprehensively considered to ensure the realistic security of the system. The simulation results indicate that the source intensity errors cannot be neglected and the maximum transmission distance of the system will be reduced by approximately 20 km for significant intensity fluctuations. Therefore, in the practical implementation of the protocol, the influence of source intensity errors must be fully considered, and the corresponding countermeasures should be taken to reduce or even eliminate these errors. This study provides theoretical guidance for securely implementing the UD CV-QKD in real-world environments.



Keywords: continuous-variable quantum key distribution, unidimensional modulation, source errors, realistic security

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.74.20250025

CSTR: 32037.14.aps.74.20250025

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

一维高斯调制连续变量量子密钥分发现实源强度误差的影响

王普　白增亮　常利伟

Influence of source intensity errors in unidimensional Gaussian modulation continuous-variable quantum key distribution

WANG Pu　BAI Zengliang　CHANG Liwei

引用信息 Citation: Acta Physica Sinica, 74, 090302 (2025)　DOI: 10.7498/aps.74.20250025
CSTR: 32037.14.aps.74.20250025
在线阅读 View online: https://doi.org/10.7498/aps.74.20250025
当期内容 View table of contents: http://wulixb.iphy.ac.cn