基于非理想量子态制备的实际连续变量量子秘密共享方案*

吴晓东[1)] 黄端[2)†]

1) (福建理工大学管理学院, 福州 350118)

2) (中南大学电子信息学院, 长沙 410083)

(2023 年 2 月 3 日收到; 2023 年 10 月 28 日收到修改稿)

连续变量量子秘密共享方案基于物理学基本定律, 能够保证密钥信息的无条件安全. 然而, 在实际连续变量量子秘密共享方案中, 量子态的制备往往并非是理想、完美的, 会引入额外的过噪声, 影响方案的安全性, 因此有必要对其进行分析. 本文提出基于非理想量子态制备的实际连续变量量子秘密共享方案. 具体而言, 在所提出的方案中假定有多个用户, 并且任意一个用户的非理想量子态制备, 可以描述为相对应的不可信第三方采用相位非敏感放大器, 对该用户的理想调制器与激光器进行放大操作. 每个用户由于非理想量子态制备所引入的等效过噪声, 可以通过相对应的相位非敏感放大器的增益参数进行全面与定量地计算. 研究结果表明, 连续变量量子秘密共享方案对非理想量子态制备所引入的过噪声非常敏感, 因此不可避免地会降低其性能和安全性. 幸运的是, 本文利用相位非敏感放大器特定的增益公式, 获得所提出方案对非理想量子态制备所引入的额外过噪声容忍度的上界限, 有效解决由非理想量子态制备所带来的安全隐患. 由于考虑了非理想量子态制备所引入的额外过噪声, 因此相比于理想连续变量量子秘密共享方案, 所提出的方案能够得到更紧的密钥率曲线. 这些结果表明, 本文所提出的方案能够对连续变量量子秘密共享方案的实际安全性进行改进与完善, 为其实用化发展提供理论依据.

关键词: 非理想量子态制备, 连续变量, 量子秘密共享

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20230138

1 引 言

量子密钥分发 (quantum key distribution, QKD) 以量子力学基本原理为基础, 从物理层面上提供一种能够在两个合法通信方 (Alice 与 Bob) 之间安全生成密钥的有效方法[1–4]. 和依赖于光子计数技术的离散变量 (discrete-variable, DV) QKD 不同[5–8], 连续变量 (continuous-variable, CV) QKD 是将密钥信息编码到光场的正则分量中, 并采用相干探测 (比如零差或外差探测) 技术进行解码[9–15]. CV-QKD 可以利用成熟的光学设备来实现, 并且所采用的基础通信设施与相干光通信类似, 这也意味着在现有光通信系统的基础上构建未来量子网络是有希望实现的. 不仅如此, CV-QKD 理论上的无条件安全性也得到严格证明[16–19].

在众多类型的 CV-QKD 方案中, 高斯调制相干态 (Gaussian modulated coherent state, GMCS) 方案[12] 由于具有较好的可行性而得到广泛的应用. 然而, GMCS CV-QKD 方案需要采用具有良好稳定性的高消光比调制器以实现高速调制, 这在实际条件下实现具有挑战性. 为了解决 GMCS CV-

* 国家自然科学基金 (批准号: 61972418, 61977062, 61801522) 和福建理工大学科研启动基金 (批准号: GY-Z22042) 资助的课题.

† 通信作者. E-mail: duanhuang@csu.edu.cn

QKD 中所存在的问题, 2018 年, Qi 等[20] 提出了基于被动态制备的 CV-QKD 方案, 采用热光源、分束器、光衰减器以及零差探测器来替代 GMCS CV-QKD 方案中的振幅与相位调制器以及随机数发生器. 2020 年, Qi 等[21] 在已有自发辐射放大光源的基础上开展实验, 验证了基于被动态制备的 CV-QKD 方案的可行性. 2021 年, Huang 等[22] 采用专门设计的帧同步算法在 Alice 和 Bob 的两组测量结果之间建立直接相关性, 并对系统过噪声进行控制, 通过真实的光纤信道实验实现了完整的基于被动态制备的 CV-QKD 方案. 同年, Wu 等[23] 提出本地本振被动 CV-QKD 方案, 解决了被动 CV-QKD 系统中本振光的安全漏洞问题, 从而能够提升被动 CV-QKD 的实际安全性. 被动态制备方案的发展使得 CV-QKD 更具实用性.

然而, 当用户数量较多时, 点对点 CV-QKD 系统难以满足其特定需求. 假设一个合法用户 (分发者 dealer) 打算通过一条不安全的量子通道与多个 (至少两个) 远程用户共享密钥, 分发者 dealer 知道其中一些用户并非是可信的, 因此决定将密钥分成若干份并分别单独发送给每个用户. 这也就意味着每个用户必须要相互合作才能获得完整的密钥. 这种情况广泛存在于商业、军事等领域. 为了满足多方用户对密钥共享日益增长的需求, 量子秘密共享方案 (quantum secret sharing, QSS) 被提出[24]. 通常而言, QSS 方案来源于一种被称为秘密共享的经典密码原语, 在该秘密共享中, 分发者 dealer 将秘密信息 W 分发给 M 个用户, 要求必须至少有 $k \leqslant M$ 个用户通过相互合作才能对秘密信息 W 进行解码. 这称为 (k, M)-阈值秘密共享方案. 在 QSS 方案中, 允许多个远程用户使用量子信息技术与分发者 dealer 共享一系列密钥. 在此种情况下, 每个用户都持有密钥不同的部分信息, 因此, 每个用户必须通过相互合作的方式才能对密钥信息进行解码.

一般来说, 相比于点对点两方 CV-QKD 方案, QSS 方案包含更多的通信用户, 并且可能会出现不可信的用户, 从而可能会引入额外的信息窃取方案. 因此, QSS 方案相比于 QKD 方案, 在安全性分析方面具有更高的要求. 最近, Kogias 等[25] 对基于纠缠模型的多方 QSS 方案的安全性进行证明, 其目的是从理论上证明基于高斯量子态和零差探测的 QSS 方案的可行性. 然而, 利用目前技术来实现此类 QSS 方案是很困难的, 尤其是当用户数量 M 比较大以及可容忍信道损耗非常小的时候.

为了实现更简单的 QSS 方案部署, 单量子比特顺序 QSS 方案被提出并进行了实验验证[26]. 虽然这些方案能够有效地简化 QSS 方案的实施, 但其安全性仍存在争议[27–29]. 不仅如此, 文献 [26] 中所提出的此类 QSS 方案的部署设计容易受到特洛伊木马攻击, 主要原因在于攻击者能够利用目标方拥有的偏振旋转装置发送多光子信号, 从而可以通过测量输出信号获得确定的对应偏振旋转. 为了解决这一问题, 2019 年, Grice 和 Qi[30] 提出了基于传统激光源和零差探测器的连续变量顺序 QSS 方案. 与单量子比特顺序 QSS 方案不同, 在该方案中, 每个用户采用高斯调制本地制备相干态, 并利用高度非对称分束器将所制备的相干态注入到循环光模式中. 这种方式可以防止窃听者访问或干扰量子态的准备过程, 并使 QSS 方案能够抵御特洛伊木马攻击. 随后, Wu 等[31] 和 Liao 等[32] 对该方案进行拓展, 分别提出了基于热态信源的被动 CV-QSS 方案与离散调制 CV-QSS 方案, 进一步推动了 CV-QSS 方案的发展.

虽然, Grice 等所提出的 CV-QSS 方案能够有效抵御特洛伊木马攻击, 但对于其他操作, 比如量子态的制备, 在实际制备过程中往往并不是完美的. 在基于高斯调制量子态制备的 CV-QSS 方案的部署中, 通常采用波导电光振幅和相位调制器来进行高斯调制操作. 波导电光调制器具有高带宽、低驱动电压的特点, 正好可以满足系统的集成要求. 然而, 在实际中, 不可避免的是, 由于电气特性和环境扰动所引起的直流偏置电压漂移和实际激光器输入光信号的不完美到达[33], 使得量子态制备无法像理论假设那样理想. 这就意味着在实际的 CV-QSS 方案中, 非理想量子态的制备会引入额外的过噪声, 此类过噪声属于高斯噪声[34–36]. 非理想量子态的制备会导致错误的密钥率估计, 从而会给实际的 CV-QSS 方案带来安全性漏洞. 此外, 在 CV-QSS 方案中, 每个用户都需要制备量子态, 并且每个用户由于非理想量子态制备所引入的过噪声是相互独立的. 为了完善 CV-QSS 方案的实际安全性分析, 需要对每个用户非理想量子态制备进行系统的分析.

为了获得更紧的 CV-QSS 方案密钥率曲线, 本文提出基于非理想量子态制备的实际 CV-QSS

方案, 并且在实际量子信道条件下对所提出的 CV-QSS 方案进行安全性分析. 通过合理的建模, 能够对 CV-QSS 方案中每个用户在量子态制备过程中所存在的不完美进行描述刻画, 并得出由非理想量子态制备所引入的等效过噪声的计算公式. 以此为基础, 可以构建实际 CV-QSS 方案的综合安全性框架, 并且推导出了针对攻击者和不可信用户的更严格的方案安全界限. 仿真结果表明, 非理想量子态制备对 CV-QSS 方案的安全性具有显著影响, 但所提出的安全性分析框架模型能够定量分析非理想量子态制备对 CV-QSS 方案的影响, 有效地解决由非理想量子态制备所带来的安全隐患, 从而有效地改进与完善 CV-QSS 方案的实际安全性. 本文第 2 节详细描述所提出的基于非理想量子态制备的实际 CV-QSS 方案; 第 3 节对所提出方案的密钥率进行计算; 第 4 节给出本文方案的性能分析; 第 5 节总结全文.

2 基于非理想量子态制备的实际 CV-QSS 方案

图 1 展示了基于非理想量子态制备的实际 CV-QSS 方案. M 个用户 (user) 通过一条单通信信道与分发者 dealer 相连接, 此处通信信道可以是电信光纤. 该方案允许接收方与一群远程用户共享一串密钥. 在实际 CV-QSS 系统中, 每个用户所使用的振幅调制器、相位调制器以及激光器并不是完美的, 不可避免地会对所制备的相干态引入过噪声. 为了合理地描述此类过噪声, 采用将理想调制器与相位非敏感放大器 (phase-insensitive amplifier, PIA) 相结合的方式来对这种非理想量子态制备进行模拟. 所提出方案的具体流程如下.

步骤 1 对于每次量子传输, 离分发者 dealer 最远的用户, 即第一个用户 U_1 利用一对高斯随机数 $\{x_1,\ p_1\}$ 来制备相干态 $|x_1+\mathrm{i}p_1\rangle$. 此处将用户 U_1 处的 PIA 设为 Q_1, 由相对应的第三方 Fred_1 控制, 以此类推. 当经过 Q_1 的放大操作后, 原相干态 $|x_1+\mathrm{i}p_1\rangle$ 转化为相干态 $|x_1^{\mathrm{PI}}+\mathrm{i}p_1^{\mathrm{PI}}\rangle$, 并将此相干态发送给相邻的第二个用户 U_2.

步骤 2 与此同时, 用户 U_2 也制备独立相干态 $|x_2+\mathrm{i}p_2\rangle$, 并且经过 Q_2 (由相对应的第三方 Fred_2 控制) 的放大操作后, 原相干态 $|x_2+\mathrm{i}p_2\rangle$ 转化为相干态 $|x_2^{\mathrm{PI}}+\mathrm{i}p_2^{\mathrm{PI}}\rangle$. 通过高度非对称分束器 (highly asymmetric beam splitter, HABS) 的第二个输入口, 将相干态 $|x_2^{\mathrm{PI}}+\mathrm{i}p_2^{\mathrm{PI}}\rangle$ 耦合到与用户 U_1 所制备的输入信号相同的时空模式. 之后, 将混合信号发送给下一个用户.

步骤 3 其他每个用户沿着链路, 通过 HABS, 将各自所制备的经 PIA 放大后的高斯调制相干态注入到与用户 U_1 所制备的输入信号相同的时空模式.

步骤 4 由于第 s 个用户 U_s 能够通过仔细控制调制方差并了解不对称分束器的透过率来对经过 Q_s 放大操作后的高斯随机数 $\{x_s^{\mathrm{PI}},\ p_s^{\mathrm{PI}}\}$ ($s=1,\ 2,\ 3,\cdots,\ M$) 进行相空间位移操作, 因此最后到达分发者 dealer 处的相干态为 $\left|\sum_{s=1}^{M}\sqrt{T_s}x_s^{\mathrm{PI}}+\mathrm{i}\sum_{s=1}^{M}\sqrt{T_s}p_s^{\mathrm{PI}}\right\rangle$, 其中 T_s 表示来自第 s 个用户的量子信号所经受的总透过率 (包括由量子信道以及

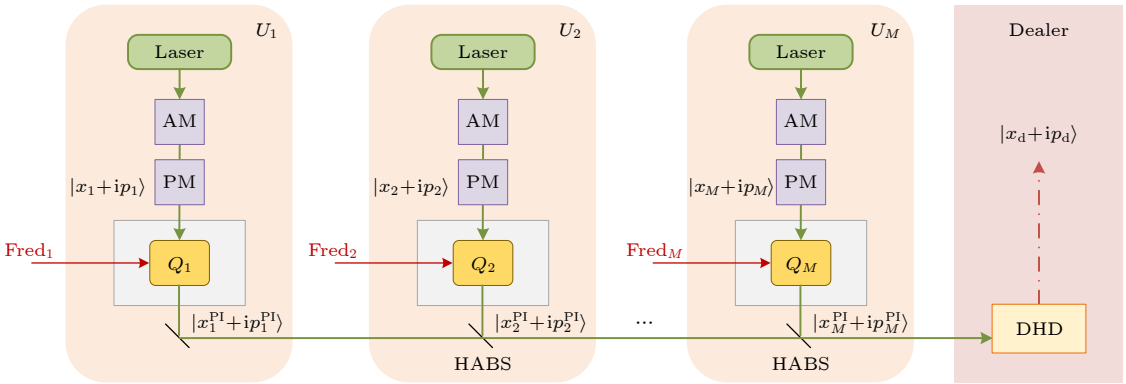

图 1 基于非理想量子态制备的实际 CV-QSS 方案. AM 为振幅调制器, PM 为相位调制器, DHD 为共扼零差探测, HABS 为高度非对称分束器, Q_s ($s=1,\ 2,\ \cdots,M$) 表示第 s 个用户 U_s 处的相位非敏感放大器

Fig. 1. Practical CV-QSS scheme based on imperfect quantum state preparation. AM, amplitude modulator; PM, phase modulator; DHD, double homodyne detection; HABS, highly asymmetric beam splitter; Q_s ($s=1,\ 2,\ \cdots,M$), phase insensitive amplifier at the s-th user.

分束器引起的损耗). 此时, 分发者 dealer 采用外差探测对所接收到的量子信号的振幅与相位这两个正则分量进行测量, 得到测量结果 $\{x_{\rm d},\ p_{\rm d}\}$.

步骤 5 经过多轮上述步骤后, 分发者 dealer 和用户拥有足够数量的相关原始数据.

需要指出的是, 步骤 1—5 属于一种旨在利用量子光学产生相关数据的量子操作. 接下来的步骤则是采用经典后处理技术来对这些数据进行处理.

步骤 6 分发者 dealer 随机选择原始数据中的一个子集, 并且要求所有的用户公布相应的高斯随机数. 结合相应的测量结果, 可以得到信道透过率 $\{T_1,\ T_2,\ \cdots,T_M\}$ [30]. 所有用户将公布出去的数据进行舍弃.

步骤 7 分发者 dealer 假定第 1 个用户 U_1 为可信方, 并且其他 $M-1$ 个用户为不可信方. 之后随机选择原始数据中的一个子集, 并且要求除了用户 U_1 外其他用户公布相应的原始数据.

步骤 8 分发者 dealer 对步骤 7 中提到的子集的测量结果进行置换操作, 即 $x_{\rm W}=x_{\rm d}-\sum_{s=2}^{M}\sqrt{T_s}x_s^{\rm PI}$; $p_{\rm W}=p_{\rm d}-\sum_{s=2}^{M}\sqrt{T_s}p_s^{\rm PI}$. 基于 $\{x_{\rm W},p_{\rm W}\}$ 以及可信用户 U_1 原始数据两者相同的子集, 可以建立一条在分发者 dealer 与用户 U_1 之间点对点的 CV-QKD 链路. 因此, 通过采用高斯调制相干态 QKD 方案中的标准的安全性分析方法 [37], 可以估算出安全密钥率的下界限 K_1 (分发者 dealer 与可信用户 U_1 之间的密钥率). 所有用户舍弃公布出来的数据.

步骤 9 将步骤 7 和步骤 8 重复 M 次. 在每次运行过程中, 选择不同的用户作为可信方. 最后, 分发者 dealer 拥有 M 个密钥率 $\{K_1,\ K_2,\cdots,K_M\}$.

步骤 10 分发者 dealer 将密钥率集合 $\{K_1,\ K_2,\ \ldots,K_M\}$ 中的最小值确定为基于非理想量子态制备的实际 CV-QSS 方案的安全密钥率 K, 并且采用高斯调制 QKD 方案中的反向协商从那些未公布的数据中生成最终密钥 [15,38].

需要指出的是, 在反向协商过程中, 经典信息从分发者 dealer 传递给用户. 相应地, 这一过程可以在没有用户共同合作的情况下完成. 分发者 dealer 可以通过采用最终密钥对要共享的信息进行加密来实现 QSS 方案. 通过合作, M 个用户能够利用他们各自的高斯随机数以及由分发者 dealer 所公布的经典信息来恢复最终密钥, 从而恢复分发者 dealer 的信息. 但任意一组 $M-1$ 个用户只能获得关于最终密钥的极少量信息. 值得一提的是, 本方案所采用的数据协商算法与标准的高斯调制 QKD 方案中的数据协商算法是相同的 [38].

从上述介绍的基于非理想量子态制备的实际 CV-QSS 方案的运行流程可以看出, 直接对所提出的 CV-QSS 方案进行安全性分析是非常复杂的. 主要原因在于所提出的方案中有多个用户, 并且我们不知道有多少用户是不可信的以及在信息传输过程中会承受怎么样的信息攻击模式. 幸运的是, 通过巧妙利用已建立的高斯调制 CV-QKD 方案的安全性证明方法, 可以对所提出的基于非理想量子态制备的实际 CV-QSS 方案的安全性进行证明. 结合步骤 8 与步骤 9 可以发现, 上述问题可以利用点对点 QKD 方案的处理方式进行解决. 假定第 s 个用户 ($s=1,\ 2,\ 3,\cdots,\ M$) 是所有用户中唯一可以信任的, 则一条在分发者 dealer 与用户 U_s 之间点对点的 CV-QKD 链路就可以建立完成. 上述假定是最悲观的假定, 因为如果假定所有的用户都是不可信任的, 则 QSS 方案就无法成立. 因此, 这种两方通信链路可以被视为包含有两个合法通信方的 CV-QKD 模型, 即发送方 Alice (可信用户 U_s) 以及接收方 Bob (分发者 dealer). 现在需要考虑的主要问题是剩下的 $M-1$ 个不可信任的用户是否可以获得合法通信方 Alice 和 Bob 之间的信息并且用来恢复 Alice 和 Bob 的共享密钥. 由于分发者 dealer 要求除了可信用户 U_s 外所有的用户公布出相应的数据信息, 因此可信用户 U_s 能够全部掌握所有用户方的信息, 而剩余的 $M-1$ 个用户则无法根据所公布的数据信息去推导出用户 U_s 与分发者 dealer 之间的信息. 根据上述分析可知, 即使考虑最坏的情况 ($M-1$ 个用户是不可信的), Alice 和 Bob 仍然可以共享一串安全密钥. 基于此, 可以采用标准的高斯调制 QKD 方案的安全性证明方法来分析所提出的实际 QSS 方案的安全性 [30]. 考虑到分发者 dealer 无法区分哪个用户为可信任的, 他 (或她) 需要同每个用户进行合作来对方案的潜在密钥率进行估计, 并且从密钥率集合 $\{K_1,\ K_2,\cdots,K_M\}$ 中选出一个最小的密钥率值作为所提出的 QSS 方案的密钥率. 因此, 所提出的基于非理想量子态制备的实际 CV-QSS 方案能够有效地抵御攻击方与任意 $M-1$ 个不可信用户的协作攻击.

3 基于非理想量子态制备的实际 CV-QSS 方案的密钥率计算

在本节中, 首先介绍基于非理想量子态制备的实际 CV-QSS 方案的物理模型, 之后对所提出方案的密钥率进行计算.

3.1 基于非理想量子态制备的实际 CV-QSS 方案的物理模型

在第 2 节中对所提出的方案进行描述时, 采用将理想调制器与 PIA 相结合的方式来对此种非理想量子态的制备进行模拟描述. 之所以采用 PIA 来反映非理想量子态制备中的过噪声, 其主要原因在于此种放大器模型在光通信中存在许多匹配的实际应用. 在图 1 中, Q_1 表示在用户 U_1 处的 PIA, 其增益参数为 g_1, 由不可信的第三方 Fred_1 控制; Q_2 表示在用户 U_2 处的 PIA, 其增益参数为 g_2, 由不可信的第三方 Fred_2 控制; …; Q_M 表示在用户 U_M 处的 PIA, 其增益参数为 g_M, 由不可信的第三方 Fred_M 控制. 为了简化分析, 此处主要以用户 U_1 为例进行分析, 其他用户的分析方式与此类似. 需要指出的是, 此处只考虑最悲观的情况, 即只有一个用户是可信任的, 也就是将用户 U_1 对应为点对点 CV-QKD 中的发送方 Alice. 由于 Fred 与 Eve 的关系可表述为 Fred 受 Eve 控制, 因此其所产生的非可信信源过噪声可纳入到信道输入的总信道附加噪声 χ_{line} 中. 所提出的方案其制备-测量 (prepare-and-measure, PM) 模型如图 2 所示.

经过理想调制器的相干态其正则分量表达式为

$$\begin{aligned} x_1^{\mathrm{h}} &= x_1 + \delta x, \\ p_1^{\mathrm{h}} &= p_1 + \delta p, \end{aligned} \tag{1}$$

其中 $\langle(\delta x)^2\rangle = \langle(\delta p)^2\rangle = 1$ 表示来源于散粒噪声的散粒噪声单位. 在经过相位非敏感放大器 Q_1 放大作用后, 用户 U_1 发送给分发者 dealer 的相干态其正则分量 $(x_1^{\mathrm{PI}},\ p_1^{\mathrm{PI}})$ 的表达式可写为

$$\begin{aligned} x_1^{\mathrm{PI}} &= \sqrt{g_1}x_1^{\mathrm{h}} + \sqrt{g_1-1}x_{Q_1}, \\ p_1^{\mathrm{PI}} &= \sqrt{g_1}p_1^{\mathrm{h}} + \sqrt{g_1-1}p_{Q_1}, \end{aligned} \tag{2}$$

其中 $(x_{Q_1},\ p_{Q_1})$ 表示方差为 V_{Q_1} 的相位非敏感放大器 Q_1 的真空输入模的正则分量. 之后, 经过进一步计算可得

$$\left\langle \left(x_1^{\mathrm{PI}}\right)^2 \right\rangle = \left\langle \left(p_1^{\mathrm{PI}}\right)^2 \right\rangle = g_1(V_{U_1}+1) + (g_1-1)V_{Q_1}, \tag{3}$$

其中 V_{U_1} 表示用户 U_1 的调制方差, $V_1 = V_{U_1}+1$, 并且由用户 U_1 处的非理想量子态制备所引入的额外过噪声为

$$\xi_1^{\mathrm{PI}} = (g_1-1)(V_{U_1}+1+V_{Q_1}). \tag{4}$$

之后 (3) 式可进一步写为

$$\left\langle \left(x_1^{\mathrm{PI}}\right)^2 \right\rangle = \left\langle \left(p_1^{\mathrm{PI}}\right)^2 \right\rangle = V_1 + \xi_1^{\mathrm{PI}}. \tag{5}$$

则条件方差 $V_{x_1^{\mathrm{PI}}|x_1} = V_{p_1^{\mathrm{PI}}|p_1}$ 可写为

$$V_{x_1^{\mathrm{PI}}|x_1} = V_{p_1^{\mathrm{PI}}|p_1} = \left\langle \left(x_1^{\mathrm{PI}}\right)^2 \right\rangle - \frac{\left\langle x_1^{\mathrm{PI}} x_1 \right\rangle^2}{\langle x_1^2 \rangle} = \xi_1^{\mathrm{PI}} + 1. \tag{6}$$

与上述分析方法类似, 在任一个用户 U_s 处 ($s = 1,\ 2,\ 3, \cdots,\ M$), 由非理想量子态制备所引入的额外过噪声 $\xi_s^{\mathrm{PI}} = (g_s-1)(V_{U_s}+1+V_{Q_s})$, 其中 g_s, V_{U_s} 与 V_{Q_s} 表示的含义和 g_1, V_{U_1} 及 V_{Q_1} 相似.

与上述 PM 模型等价的纠缠 (entanglement-based, EB) 模型如图 3 所示. 相比于 PM 模型, 采用 EB 模型更方便进行安全性分析[39]. 接下来将证明图 3 中所提出方案的 EB 模型与图 2 中所提出方案的 PM 模型等价. 值得一提的是, 由于考虑在最悲观的情况下进行安全性分析, 即只有一个用户为可信任的, 其余 $M-1$ 个用户为不可信的. 因此

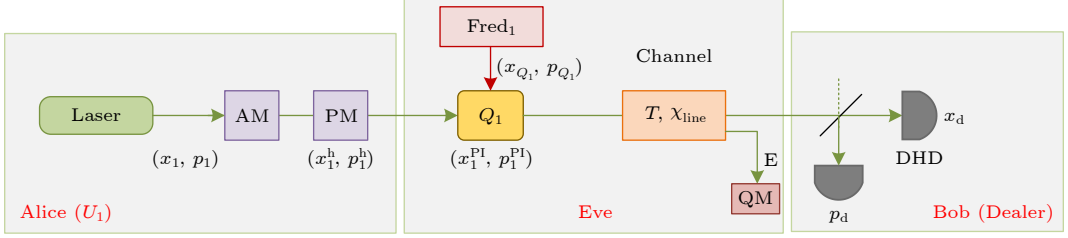

图 2 基于非理想量子态制备的 CV-QSS 制备-测量方案图. QM 为量子存储器, T 表示非可信信道的透过率, χ_{line} 表示信道附加噪声

Fig. 2. Schematic diagram of the prepare-and-measure (PM) model of the practical CV-QSS scheme based on imperfect quantum state preparation. QM, quantum memory; T, transmission efficiency; χ_{line}, channel-added noise.

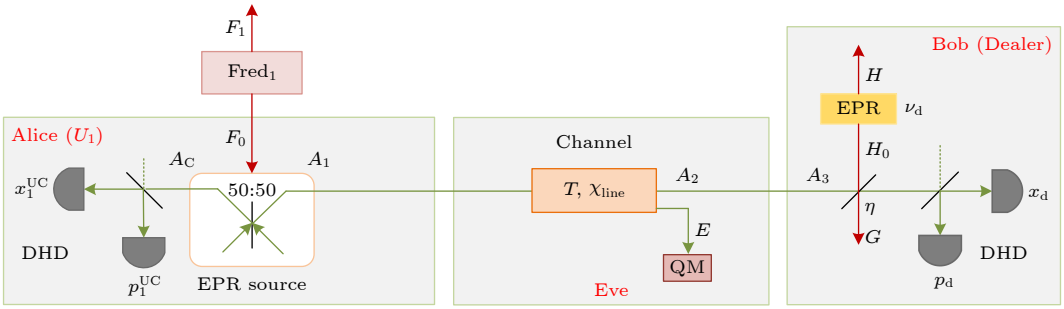

图 3 基于非理想量子态制备的 CV-QSS 纠缠模型方案图

Fig. 3. Schematic diagram of the entanglement-based (EB) model of the practical CV-QSS scheme based on imperfect quantum state preparation.

所提出的方案其 EB 模型可等效为点对点 CV-QKD 方案的 EB 模型. 在图 3 中唯一的可信用户记为 Alice, 分发者 dealer 记为 Bob, 此处同样以用户 U_1 为例进行说明, 即假定 U_1 为唯一可信用户 (Alice), 其余用户分析方法与此类似. 用户 U_1 制备双模压缩真空态 $\Phi_{A_C A_1}$, 并对其进行提纯. 用户 U_1 将其中一个正则分量为 $(x_1^{\rm PI},\ p_1^{\rm PI})$ 的模 A_1 发送给接收方 Bob, 保留另外一个正则分量为 $(x_1^{C},\ p_1^{C})$ 的模 A_C, 这些正则分量满足:

$$\begin{aligned}&\langle (x_1^C)^2\rangle = \langle (p_1^C)^2\rangle = V_1,\\ &\langle (x_1^{\rm PI})^2\rangle = \langle (p_1^{\rm PI})^2\rangle = V_1+\xi_1^{\rm PI}.\end{aligned}\tag{7}$$

根据不确定性关系, 可以得到以下不等式:

$$\left\langle \left(x_1^{\rm PI}x_1^C\right)^2\right\rangle \leqslant V_1\left(V_1+\xi_1^{\rm PI}\right)-\frac{V_1}{V_1+\xi_1^{\rm PI}}.\tag{8}$$

由于在 EB 模型中, 系统 $\Phi_{A_C A_1 F_1}$ 无法达到最大的纠缠度, 因此可以假设:

$$\langle x_1^{\rm PI}x_1^C\rangle = \sqrt{V_1^2-1},\quad \langle p_1^{\rm PI}p_1^C\rangle = -\sqrt{V_1^2-1}.\tag{9}$$

用户 U_1 对所保留的正则分量为 $(x_1^{C},\ p_1^{C})$ 的模 A_C 进行外差探测, 可得

$$x_1^{UC}=x_1^C-\delta x_1^{UC},\quad p_1^{UC}=p_1^C-\delta p_1^{UC},\tag{10}$$

其中 $\langle(\delta x_1^{UC})^2\rangle=\langle(\delta p_1^{UC})^2\rangle=1$, 参数 $(x_1^{UC},\ p_1^{UC})$ 表示用户 U_1 对模 A_C 进行外差探测所得到的探测结果. 此处假定用户 U_1 对 $(x_1^{\rm PI},\ p_1^{\rm PI})$ 的估计值为 $(x_1,\ p_1)$, 则可得

$$x_1=\sqrt{\frac{V-1}{V+1}}x_1^{UC},\quad p_1=\sqrt{\frac{V-1}{V+1}}p_1^{UC}.\tag{11}$$

之后容易通过计算得到

$$\begin{aligned}&\langle x_1^2\rangle=\langle p_1^2\rangle=V_1-1=V_{U_1},\\ &V_{x_1^{\rm PI}|x_1}=V_{p_1^{\rm PI}|p_1}=1+\xi_1^{\rm PI}.\end{aligned}\tag{12}$$

(12) 式所给出的结果与 PM 模型所推导出的结果等价, 这表明所提出的基于非理想量子态制备的实际 CV-QSS 方案其 EB 模型等价于其 PM 模型. 值得一提的是, 图 2 与图 3 中量子存储器的作用在于对 Eve 额外的输出模 E 进行存储, Eve 在最后对存储在量子存储器的模进行集体测量. 一般而言, 在 PM 模型中, 分发者 dealer 由于不完美外差探测器所引入的探测器附加噪声 $\chi_{\rm het}$ 其表达式为 $\chi_{\rm het}=[(2-\eta)+2\upsilon_{\rm el}]/\eta$, 其中 η 表示探测器的量子效率, $\upsilon_{\rm el}$ 表示探测器的电噪声. 在 EB 模型中, 分发者 dealer 的不完美探测器可利用透过率为 η 的分束器以及方差为 $\upsilon_{\rm d}$ 的 Einstein-Podolsky-Rosen (EPR) 纠缠态 ρ_{HH_0} 来进行模拟表示. 值得一提的是, 方差 $\upsilon_{\rm d}$ 的选取应能够保证探测器的总噪声在 EB 模型中同样为 $\eta\chi_{\rm het}$, 则方差 $\upsilon_{\rm d}$ 的表达式可写为 $\upsilon_{\rm d}=(\eta\chi_{\rm het}-1)/(1-\eta)$. 因此, 当假定 EPR 信源与 Alice 的探测器都隐藏在黑盒子中时, 攻击方将无法鉴别所采用的是 PM 模型还是 EB 模型.

综上所述, 图 2 (PM 方案) 与图 3 (EB 方案) 两者具体等价的地方体现在以下两个方面.

1) 在图 2 中, Alice 利用一对高斯随机数 $\{x_1,\ p_1\}$ 经由振幅和相位调制器来制备相干态 $|x_1+{\rm i}p_1\rangle$. 当经过 Q_1 的放大操作后, 原相干态 $|x_1+{\rm i}p_1\rangle$ 转化为相干态 $|x_1^{\rm PI}+{\rm i}p_1^{\rm PI}\rangle$, 此为 Alice 非理想量子态的制备, 之后经不可信信道发送给 Bob. 该过程等效为图 3 中 Fred$_1$ 制备纠缠态 $\Phi_{A_C A_1 F_1}$, 并对其中一个正则分量为 $(x_1^{\rm PI},\ p_1^{\rm PI})$ 的模 A_C 进行外差探测, 而另一个模 A_1 则经不可信信道发送给 Bob.

2) 图 2 中, 在探测方 Bob 处实际探测器的量子效率 η 等效为图 3 中透过率为 η 的分束器, 图 2 中实际探测器的电噪声 $\upsilon_{\rm el}$ 则等效于图 3 中方差为 $\upsilon_{\rm d}$ 的辅助 EPR 纠缠态 ρ_{HH_0} 其中一模式 H_0 经分

束器后所引入的过噪声.

3.2 密钥率计算

基于上述所建立的物理模型, 现在对所提出的基于非理想量子态制备的实际 CV-QSS 方案的密钥率进行计算. 此处假定分发者 dealer 与相离最远的用户 (Alice) 距离为 L, 其他所有 M–1 个用户都分布在这两者之间, 并且每个用户之间相隔的距离相同. 根据步骤 10 可知, 所提出的 QSS 方案其密钥率为分发者 dealer 与每个用户之间点对点 QKD 的最小密钥率. 为了简化分析, 此处假定每个用户引入相同的过噪声 ξ_0, 并且每个用户由非理想量子态制备所引入的额外过噪声相同, 即 $\xi_1^{\rm PI}=\xi_2^{\rm PI}=\cdots=\xi_M^{\rm PI}$. 为了方便分析, 令 $\xi^{\rm PI}=\xi_1^{\rm PI}=\xi_2^{\rm PI}=\cdots=\xi_M^{\rm PI}$. 则在正常情况下, 最小的 QKD 密钥率为分发者 dealer 与 Alice 之间的密钥率. 需要指出的是方案最终密钥率的计算应基于实际数据, 并且选取最小值作为所提出的 QSS 方案的密钥率. 由上述分析可知, 所提出的 CV-QSS 方案密钥率的计算可以采用高斯调制 CV-QKD 方案密钥率的计算方法. 则在反向协商下, 所提出的 CV-QSS 方案其密钥率下界限的表达式可写为 [37,39]

$$K=\beta I_{\rm AB}-\chi_{\rm BE}, \tag{13}$$

其中 $I_{\rm AB}$ 表示 Alice 与 Bob 之间的互信息量; β 表示方案的协商效率; $\chi_{\rm BE}$ 表示 Eve (包括外部攻击者以及其余 $M-1$ 个用户) 与接收方 Bob 之间的 Holevo 界. 第 s 个用户的信道透过率 T_s 可写为

$$T_s=10^{\frac{-\omega l_s}{10}}, \tag{14}$$

其中 ω 表示光纤损耗系数; $l_s=[(M-s+1)/M]L$ 表示接收方 Bob (分发者 dealer) 与第 s 个用户的距离. 第 s 个用户所引入的归结于信道输入的过噪声其表达式可写为

$$\xi_s=\frac{T_s}{T_1}\left(\xi_0+\xi^{\rm PI}\right). \tag{15}$$

因此归结于信道输入的总信道附加噪声 $\chi_{\rm line}$ 其表达式可写为

$$\chi_{\rm line}=\frac{1}{T_1}-1+\sum_{s=1}^{M}\xi_s. \tag{16}$$

则归结为信道输入的总噪声为

$$\chi_{\rm tot}=\chi_{\rm line}+\chi_{\rm het}/T_1. \tag{17}$$

接下来计算 Alice 和 Bob 之间的互信息量 $I_{\rm AB}$. 当接收方 Bob (分发者 dealer) 采用外差探测时, 互信息量 $I_{\rm AB}$ 的表达式可写为

$$I_{\rm AB}=\log_2\frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}, \tag{18}$$

其中 $V=V_{\rm A}+1$, $V_{\rm A}$ 为 Alice 的调制方差. 当用户 U_1 为离分发者 dealer 最远的可信用户时, 有 $V=V_1$ 并且 $V_{\rm A}=V_{U_1}$.

攻击者 Eve 以及其他 $M-1$ 个不可信用户能够从接收方 Bob 的密钥中获得的最大信息量 $\chi_{\rm BE}$ 其表达式为

$$\chi_{\rm BE}=S(\rho_{\rm E})-\int {\rm d}\phi_{\rm B}p(\phi_{\rm B})S(\rho_E^{\phi_{\rm B}}), \tag{19}$$

其中 $\phi_{\rm B}$ 表示 Bob 采用外差探测所获得的探测结果, 并且有 $\phi_{\rm B}=\{x_{\rm B},\ p_{\rm B}\}=\{x_{\rm d},\ p_{\rm d}\}$, $S(\cdot)$ 表示量子态 ρ 的冯·诺依曼熵, $p(\phi_{\rm B})$ 表示接收方测量结果的概率密度, 并且 $\rho_{\rm E}^{\phi_{\rm B}}$ 表示 Eve 基于接收方 Bob 测量结果的量子态. 考虑到在实际中无法对 Eve 通过利用光源所获得的最大信息量进行限制, 为了解决这个问题, 可以假设 $\rho_{A_{\rm C}FEA_1}$ 是纯量子态, 当 Alice 所制备的量子态 ($\rho_{A_{\rm C}FA_1}$) 为高斯态时, 仍可以获得所提出方案密钥率的下界限 [40,41]. 因此 (19) 式可进一步写为

$$\chi_{\rm BE}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right), \tag{20}$$

其中 $G(x)=(x+1)\log_2(x+1)-x\log_2 x$, 并且

$$\lambda_{1,2}^2=\frac{1}{2}\left[\Delta\pm\sqrt{\Delta^2-4D}\right], \tag{21}$$

其中

$$\begin{aligned}&\Delta=V^2+{T_1}^2(V+\chi_{\rm line})^2+2T_1\left(1-V^2\right),\\&D={T_1}^2(1+V\chi_{\rm line})^2.\end{aligned} \tag{22}$$

$\lambda_{3,4}$ 其表达式可写为

$$\lambda_{3,4}^2=\frac{1}{2}\left[A\pm\sqrt{A^2-4B}\right], \tag{23}$$

其中

$$\begin{aligned}A=&\frac{1}{[T_1(V+\chi_{\rm tot})]^2}\Big\{\Delta\chi_{\rm het}^2+1+D+2\chi_{\rm het}[V\sqrt{D}\\&+T_1(V+\chi_{\rm line})]+2T_1(V^2-1)\Big\},\\B=&\left[\frac{\sqrt{D}\chi_{\rm het}+V}{T_1(V+\chi_{\rm tot})}\right]^2,\end{aligned} \tag{24}$$

$$\lambda_5=1. \tag{25}$$

根据 (18) 式, (20) 式, (21) 式, (22) 式, (23) 式以及 (24) 式, (25) 式可以计算出所提出方案渐近密钥率的下界限.

4 性能分析

本节采用实际系统参数来对基于非理想量子态制备的实际 CV-QSS 方案的性能进行分析, 并与基于理想量子态制备的 CV-QSS 方案 (以下记为理想方案) 的性能进行比较. 涉及全局仿真参数设定如下: 光纤信道损耗系数 $\omega = 0.2$ dB/km, 接收端探测器量子效率和电噪声分别为 $\eta = 0.6$, $\upsilon_{\rm el} = 0.05$ [42], 过噪声 $\xi_0 = 0.001$, 协商效率 $\beta = 0.95$. 由于在上述分析中, 假定非理想量子态制备所引入的额外过噪声每个用户均为 $\xi^{\rm PI}$, 因此每个用户 PIA 的增益参数相等, 则有 $g_1 = g_2 = \cdots = g_M$. 为了方便分析, 令 $g = g_1 = g_2 = \cdots = g_M$. 当增益参数 $g = 1$ 时, 即 $\xi^{\rm PI} = 0$, 表明量子态制备是完美的, 不存在额外过噪声.

图 4 给出了所提方案的密钥率与调制方差的关系, 增益参数 $g = 1.001$, 其中图 4(a) 考虑在不同传输距离的情况下, 而图 4(b) 则考虑在不同的用户数量的情况下. 在图 4(a) 中传输距离 $L = 5,\ 10,\ 20,\ 30$ km, 并且用户数量 $M = 5$. 在图 4(b) 中用户数量 $M = 3,\ 5,\ 7,\ 10$, 并且传输距离 $L = 10$ km. 从图 4(a) 与图 4(b) 可以发现, 随着传输距离以及用户数量的增加, 调制方差 $V_{\rm A}$ 的可选择区域被逐渐压缩, 并且方案的密钥率也显著降低. 此外, 密钥率曲线在调制方差 $V_{\rm A}$ 趋于 0 和趋于某个上界的时候都向 0 截断. 此种情况其主要原因在于当调制方差 $V_{\rm A}$ 趋于 0 时, 根据 (18) 式, Alice 与 Bob 的互信息量 $I_{\rm AB}$ 也趋于 0, 从而导致方案密钥率趋于 0, 因此密钥率曲线向 0 截断; 当调制方差 $V_{\rm A}$ 趋于某个上界时, 根据 (13) 式, 会出现 $\beta I_{\rm AB} = \chi_{\rm BE}$, 从而使得密钥率 $K = 0$, 因此密钥率曲线同样会向 0 截断. 而当调制方差 $V_{\rm A} = 3$ 时, 在图 4(a) 和图 4(b) 中密钥率总是存在一个峰值, 并且该峰值对应的调制方差 $V_{\rm A}$ 几乎不随传输距离 L 和用户数量 M 的变化而变化. 这表明所提出的方案中的调制方差 $V_{\rm A}$ 存在一个最优值, 即 $V_{\rm A} = 3$. 当 $V_{\rm A}$ 取到这个最优值 3 的时候, 无论传输距离和用户数量如何变化, 相对应的密钥率曲线都会出现一个峰值. 因此在下面的仿真中, 调制方差的取值设定为 3.

图 5 给出了所提出方案的密钥率与传输距离的关系, 其中图 5(a) 表示增益参数 $g = 1$ (理想方案), 图 5(b) 表示增益参数 $g = 1.001$, 图 5(c) 表示增益参数 $g = 1.002$, 图 5(d) 表示增益参数 $g = 1.003$. 在图 5 中用户数量 $M = 2,\ 5,\ 8,\ 10,\ 15$, 并且也仿真出了 Pirandola–Laurenza–Ottaviani–Banchi (简记为 PLOB) 界, 该界限表示点对点量子通信性能的最终极限 [43]. 从图 5 中可以观察到, 在拥有相同用户数量的情况下, 理想方案 ($g = 1$) 的性能总是优于所提出方案的性能 ($g > 1$). 随着增益参数 g 的增大, 即由非理想量子态制备所引入的额外过噪声 $\xi^{\rm PI}$ 增大, 所提出的基于非理想量子态制备的 CV-QSS 方案其性能也显著降低. 这表明非理想量子态的制备会对 CV-QSS 方案的安全性产生显著影响. 而从另一方面看, 相比于理想方案, 所提出的方案由于考虑了非理想量子态制备所引入的额外过噪声, 因此能够得到更紧的密钥率曲

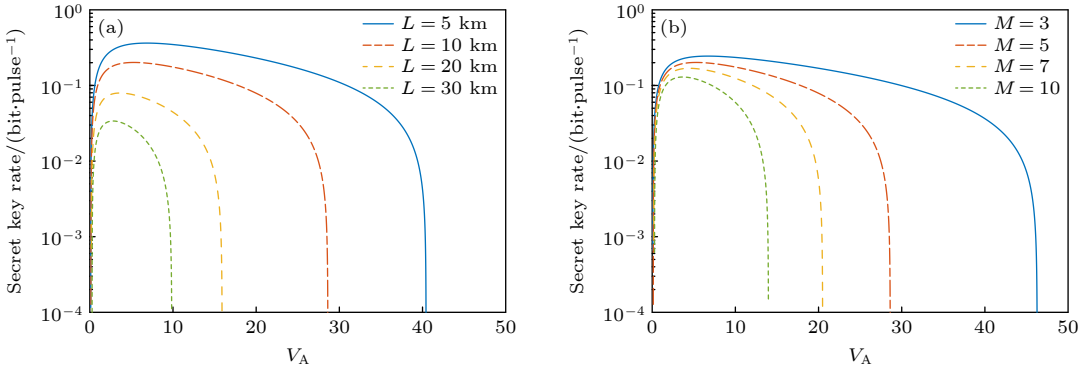

图 4 所提出方案的密钥率与调制方差的关系 (a) 不同传输距离 L; (b) 不同用户数量 M

Fig. 4. The relationship between the secret key rate of the proposed scheme and the modulation variance under: (a) Different transmission distance L; (b) different numbers of users M.

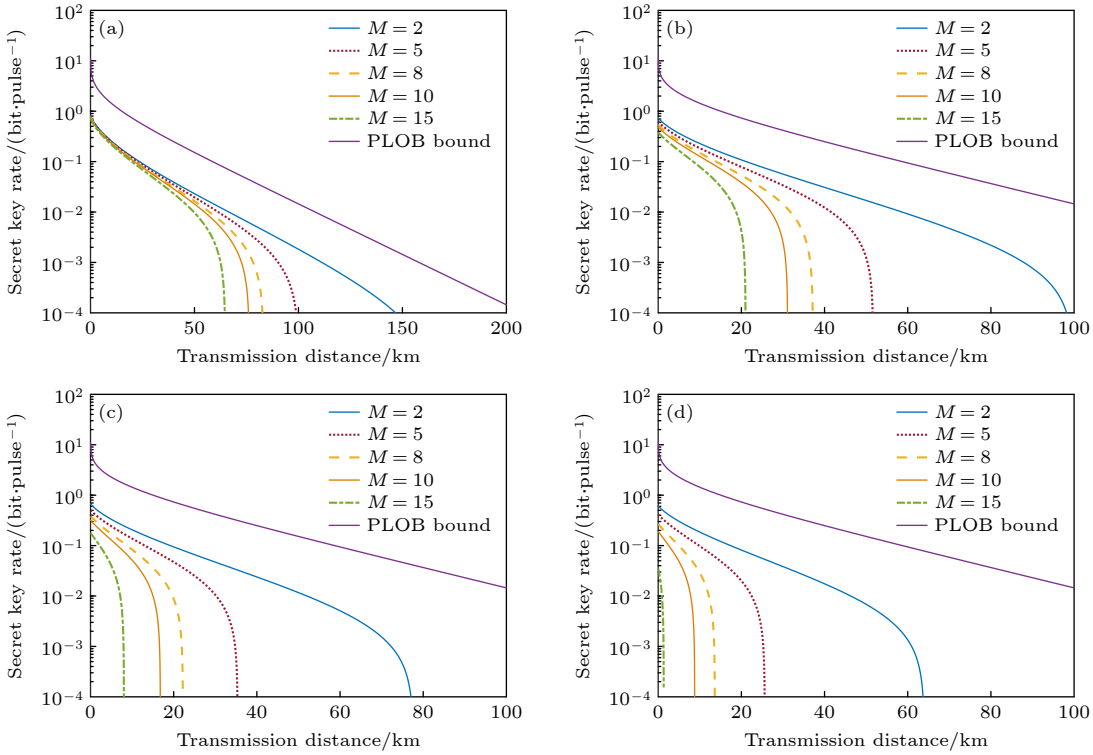

图 5 所提出方案的密钥率与传输距离的关系 (a) $g=1$; (b) $g=1.001$; (c) $g=1.002$; (d) $g=1.003$

Fig. 5. The relationship between the secret key rate of the proposed scheme and the transmission distance: (a) $g=1$; (b) $g=1.001$; (c) $g=1.002$; (d) $g=1.003$.

线. 此外, 随着用户数量 M 的增加, 所提出的基于非理想量子态制备的 CV-QSS 方案与理想 CV-QSS 方案的性能都随之降低.

图 6 给出了在不同传输距离 L 下, 方案密钥率与增益参数 g 的关系, 其中用户数量 $M=5$. 若要获得当用户数量 $M=5$ 时所提出的 CV-QSS 方案对增益参数 g 的容忍度阈值上界, 可令传输距离 $L=0$. 在图 6 中, $L=0$ 时的情形用蓝色曲线表示. 从图 6 可以发现, 随着传输距离 L 的增加, 所提出的方案对增益参数 g 的容忍度降低, 即对非理想量子态制备所引入的额外过噪声 ξ^{PI} 的容忍度降低. 此外, 蓝色性能曲线截止于 1.01026, 即增益参数 g 的容忍度阈值上界 $\hat{g}_{\mathrm{th}}=1.01026$. 这表明当 PIA 的增益参数超过 1.01026 时, 所提出的 CV-QSS 方案在用户数量 $M=5$ 的情形下无法提取任何密钥. 因此, 从非理想量子态制备所引入的额外过噪声的角度上考虑, 在 $M=5$ 的情形下, 所提出的 CV-QSS 方案对额外过噪声 ξ^{PI} 的容忍度阈值上界为 0.0513.

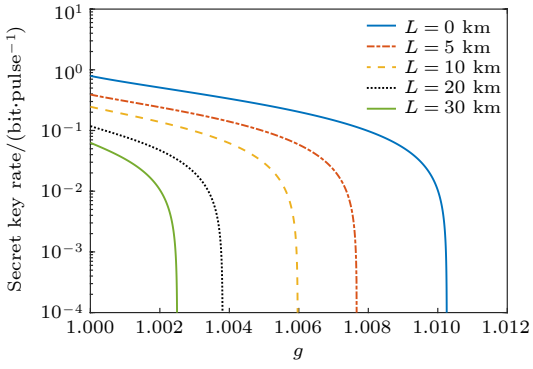

图 6 在不同传输距离 L 下, 所提出方案的密钥率与增益参数 g 的关系

Fig. 6. The relationship between the secret key rate of the proposed scheme and the gain g under different transmission distances L.

5 结 论

CV-QSS 方案能够有效地解决多个远程用户之间秘密共享的安全性问题. 然而, 在实际 CV-QSS 方案中, 量子态的制备通常无法达到理论上的理想状态, 因而会引入额外的过噪声. 这无疑会给 CV-QSS 系统带来安全风险. 本文提出基于非理想量子态制备的实际 CV-QSS 方案, 研究分析了实际 CV-QSS 方案中导致量子态的制备出现非理想的原因, 即在实际 CV-QSS 方案中, 实际激光器、波导电光调幅器和相位调制器的工作状态无法达到

理论水平. 不仅如此, 为了能够对非理想量子态制备所引入的额外过噪声进行定量分析, 本方案采用将理想调制器与 PIA 相结合的方式来对这种非理想量子态的制备进行描述. 基于此, 通过利用 PIA 的增益参数 g, 可以对实际 CV-QSS 方案中非理想量子态的制备所引入的额外过噪声进行完整定量地计算, 并且能够获得密钥率的下界限. 此外, 基于每个用户 PIA 的增益参数 g, 能够得到实际 CV-QSS 方案对非理想量子态制备所引入的额外过噪声容忍度的上界限. 因此, 本文提出的方案可以在不改变 CV-QSS 框架结构的前提下, 有效地解决由非理想量子态制备所带来的安全隐患, 为 CV-QSS 方案在复杂环境下的实际应用奠定基础.

参考文献

[1] Liu H, Jiang C, Zhu H T, Zou M, Yu Z W, Hu X L, Xu H, Ma S, Han Z, Chen J P, Dai Y, Tang S B, Zhang W, Li H, You L, Wang Z, Hua Y, Hu H, Zhang H, Zhou F, Zhang Q, Wang X B, Chen T Y, Pan J W 2021 *Phys. Rev. Lett.* **126** 250502

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

[3] 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

[4] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C, Han Z F 2022 *Nat. Photon.* **16** 154

[5] Yin J, Li Y H, Liao S K, Yang M, Cao Y, Zhang L, Ren J G, Cai W Q, Liu W Y, Li S L, Shu R, Huang Y M, Deng L, Li L, Zhang Q, Liu N L, Chen Y A, Lu C Y, Wang X B, Xu F H, Wang J Y, Peng C Z, Ekert A K, Pan J W 2020 *Nature* **582** 501

[6] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W J, Han Z Y, Ma S Z, Hu X L, Li Y H, Liu H, Zhou F, Jiang H F, Chen T Y, Li H, You L X, Wang Z, Wang X B, Zhang Q, Pan J W 2021 *Nat. Photon.* **15** 570

[7] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C, Han Z F 2019 *Phys. Rev. X* **9** 021046

[8] Liu W Z, Zhang Y Z, Zhen Y Z, Li M H, Liu Y, Fan J , Xu F, Zhang Q, Pan J W 2022 *Phys. Rev. Lett.* **129** 050502

[9] 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]

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

[11] Zhong H, Ye W, Wu X D, Guo Y 2021 *Acta Phys. Sin.* **70** 020301 (in Chinese) [钟海, 叶炜, 吴晓东, 郭迎 2021 物理学报 **70** 020301]

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

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

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

[15] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature (London)* **421** 238

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

[17] Laudenbach F, Pacher C, Fung C H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011

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

[19] Chen Z, Zhang Y, Wang G, Li Z, Guo H 2018 *Phys. Rev. A* **98** 012314

[20] Qi B, Evans P G, Grice W P 2018 *Phys. Rev. A* **97** 012317

[21] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M, Peters N A 2020 *Phys. Rev. Appl.* **13** 054065

[22] Huang P, Wang T, Chen R, Wang P, Zhou Y, Zeng G 2021 *New J. Phys.* **23** 113028

[23] Wu X, Wang Y, Guo Y, Zhong H, Huang D 2021 *Phys. Rev. A* **103** 032604

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

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

[26] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Zukowski M, Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505

[27] He G P 2007 *Phys. Rev. Lett.* **98** 028901

[28] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Zukowski M, Weinfurter H 2007 *Phys. Rev. Lett.* **98** 028902

[29] He G P, Wang Z D 2010 *Quantum Inf. Comput.* **10** 28

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

[31] Wu X , Wang Y, Huang D 2020 *Phys. Rev. A* **101** 022301

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

[33] Liu W, Wang X, Wang N, Du S, Li Y 2017 *Phys. Rev. A* **96** 042312

[34] Shen Y, Yang J, Guo H 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 235506

[35] Usenko V C, Filip R 2010 *Phys. Rev. A* **81** 022318

[36] Jouguet P, Kunz J S, Diamanti E, Leverrier A 2012 *Phys. Rev. A* **86** 032309

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

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

[39] 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

[40] Huang P, He G Q, Zeng G H 2013 *Int. J. Theor. Phys.* **52** 1572

[41] Huang D, Huang P, Wang T, Li H, Zhou Y, Zeng G 2016 *Phys. Rev. A* **94** 032305

[42] Zhang H, Fang J, He G 2012 *Phys. Rev. A* **86** 022338

[43] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043

Practical continuous variable quantum secret sharing scheme based on non-ideal quantum state preparation*

Wu Xiao-Dong [1)] Huang Duan [2)†]

1) (*School of Management, Fujian University of Technology, Fuzhou* 350118 , *China*)

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

(Received 3 February 2023; revised manuscript received 28 October 2023)

Abstract

Continuous variable quantum secret sharing protocol can guarantee the unconditional security of secret key information based on the fundamental laws of physics. However, the state preparation operation may become non-ideal and imperfect in practical continuous variable quantum secret sharing scheme, which will introduce additional excess noise and affect the security of the scheme. Therefore, it is necessary to analyze it. We propose a practical continuous variable quantum secret sharing protocol based on imperfect state preparation. Specifically, in the proposed scheme, we assume that there are multiple users, and the imperfect state preparation performed by any user is equivalent to the corresponding untrusted third party using a phase insensitive amplifier to amplify the ideal modulator and laser owned by the user. The equivalent excess noise introduced by the imperfect state preparation can be calculated comprehensively and quantitatively through the gain of the corresponding phase insensitive amplifier. The results show that the continuous variable quantum secret sharing scheme is sensitive to the excess noise introduced by the imperfect state preparation operation, which will inevitably reduce its performance and security. Fortunately, the upper bound of the additional excess noise tolerance for the imperfect state preparation is achieved by using the specific gain formula of the phase insensitive amplifier, thus the security risks caused by the imperfect state preparation can be effectively solved. Due to considering the additional excess noise introduced by imperfect state preparation, tighter secret key rate curves can be obtained by the proposed scheme than those by the ideal continuous variable quantum secret sharing protocol. These results indicate that the proposed scheme can improve the practical security of continuous variable quantum secret sharing scheme, and provide a theoretical basis for its practical applications.

Keywords: imperfect state preparation, continuous variable, quantum secret sharing

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.73.20230138

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61972418, 61977062, 61801522) and the Scientific Research Initiation Fund of Fujian University of Technology, China (Grant No. GY-Z22042).

† Corresponding author. E-mail: duanhuang@csu.edu.cn

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

基于非理想量子态制备的实际连续变量量子秘密共享方案

吴晓东　黄端

Practical continuous variable quantum secret sharing scheme based on non-ideal quantum state preparation

Wu Xiao-Dong　Huang Duan

引用信息 Citation: Acta Physica Sinica, 73, 020304 (2024)　DOI: 10.7498/aps.73.20230138
在线阅读 View online: https://doi.org/10.7498/aps.73.20230138
当期内容 View table of contents: http://wulixb.iphy.ac.cn