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*

吴晓东[1)] 黄端[2)†] 黄鹏[3)‡] 郭迎[4)]

1) (福建工程学院管理学院, 福州 350118)

2) (中南大学计算机学院, 长沙 410083)

3) (上海交通大学区域光纤通信网与新型光通信系统国家重点实验室, 量子传感与信息处理中心, 上海 200240)

4) (中南大学自动化学院, 长沙 410083)

(2022 年 5 月 30 日收到; 2022 年 8 月 11 日收到修改稿)

由于离散调制连续变量测量设备无关量子密钥分发方案与高效纠错码具有良好的兼容性, 因此即使在低信噪比条件下, 也具备较高的协商效率, 并且其实现条件相比于高斯调制方案更加简单. 然而, 实验中常用的零差探测器的量子效率仅为 0.6, 这会严重影响离散调制连续变量测量设备无关量子密钥分发方案的实际应用性能. 鉴于此, 本文提出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, 即在该方案中对两条量子信道的输出端各采用一个相位敏感放大器用于补偿相对应的实际零差探测器. 仿真结果表明采用相位敏感放大器能够很好地补偿实际零差探测器的量子效率, 有效提升基于实际探测器的离散调制连续变量测量设备无关量子密钥分发方案的密钥率和安全传输距离, 为推动离散调制连续变量测量设备无关量子密钥分发方案的实用化发展提供了一个有效而实用的方法.

关键词: 离散调制, 连续变量, 测量设备无关量子密钥分发, 实际探测器补偿

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.71.20221072

1 引 言

量子密钥分发 (quantum key distribution, QKD)[1–4] 作为量子信息科学的一项重要应用, 允许相隔两地的合法通信双方 (Alice 和 Bob) 在不安全的量子及经典信道环境下建立一串安全密钥. 现阶段, QKD 主要可分为两大类, 即离散变量 (discrete-variable, DV)QKD[5–7] 与连续变量 (continuous-variable, CV)QKD[8–16]. DV-QKD 通常以单光子作为信息编码的载体, 在接收端需采用高效率的单光子探测器, 这种探测器造价高昂, 使得 DV-QKD 运行成本较高. 相比于 DV-QKD, CV-QKD 具备与现有光通信系统进行有效融合的潜力, 并且能够使用成本更低的光源及探测器.

在众多 CV-QKD 方案中, 高斯调制相干态 (Gaussian-modulated coherent state, GMCS) 方案因其理论安全性 [17–22] 和实用性 [23–27] 而备受关注. 然而, GMCS 方案的安全性分析通常基于设备完美且不被窃听的理想假设, 而这种假设在实验中很难实现 [28,29]. 实际上, 窃听者可能会利用不完美设备所造成的安全漏洞采取相应的量子攻击策略, 如校准攻击 [30]、本振光抖动攻击 [31]、本振光波长攻击 [32]、探测器饱和攻击 [33] 等. 上述这些针对实际设备的攻击策略严重影响了 CV-QKD 系统的实际安全性.

* 国家自然科学基金 (批准号: 61871407, 61872390, 61801522) 和福建工程学院科研启动基金 (批准号: GY-Z22042) 资助的课题.

† 通信作者. E-mail: duanhuang@csu.edu.cn

‡ 通信作者. E-mail: huang.peng@sjtu.edu.cn

为了有效地消除所有针对实际探测器的现有和潜在的攻击, 2012 年两个课题组各自独立提出测量设备无关 (measurement-device-independent, MDI) QKD 方案[34,35], 其中 Braunstein 和 Pirandola[34] 所提出的 MDI-QKD 方案全面解决了针对探测器的侧信道攻击问题, 而 Lo 等[35] 所提出的 MDI-QKD 方案则仅限于量子比特系统. 不久之后, MDI-QKD 方案不仅在理论安全性方面得到了很好的分析[36−39], 而且在实验方面也成功地进行了验证[40,41]. 目前, MDI-QKD 主要可分为离散变量 (discrete-variable, DV) MDI-QKD[35,42] 与连续变量 (continuous-variable, CV) MDI-QKD[43−47]. 在 CV-MDI-QKD 的框架下, Alice 和 Bob 均被视为发送方, 而不可信的第三方 Charlie 在接收到由 Alice 和 Bob 发送来的量子态时进行贝尔态检测 (Bell-state measurement, BSM), 并将所得到的测量结果向 Alice 和 Bob 进行公布以生成安全密钥. 由于方案的测量部分由不可信的第三方 Charlie 执行, 方案的安全性不再依赖于完美的探测器. 因此, CV-MDI-QKD 能够消除所有已知或未知的探测器侧信道攻击.

然而, 在实际应用中, CV-MDI-QKD 方案的最大传输距离却不尽如人意. 其中一个关键问题在于对高斯调制 CV-MDI-QKD 方案而言, 在低信噪比、长距离传输的情况下其协商效率非常低. 现阶段可使用的效果最好的纠错码, 如低密度奇偶校验 (low density parity check, LDPC) 码[48] 或 turbo 码, 在低信噪比的情况下可以很好处理离散 (如二进制) 值, 但在相同条件下处理连续 (如高斯调制) 值的性能较差.

为了解决上述问题, 常用的方法是编写低信噪比条件下具有高效率的纠错码. 该方法与解决点对点 QKD 方案中此类问题的方法一致, 通过适当优化和构造特定的 LDPC 码, 使其在低信噪比条件下具有良好的性能[49−51]. 然而, 此种类型的纠错码设计及实现具有较高的复杂度, 并且所需的硬件成本高. 不仅如此, 大部分此类纠错码能成功获得高协商效率的概率非常低. 最近, Ma 等[52] 提出离散调制 CV-MDI-QKD 方案, 该方案即使在极低的信噪比条件下, 也能与高效的协商纠错码进行良好的协作, 从而有效提高安全传输距离. 此外, 离散调制方案比高斯调制方案更便于实验实现和具体操作. 然而, Ma 等[52] 所提出的离散调制 CV-MDI-QKD 方案是基于这样一种理想化假设, 即 Charlie 采用完美的零差探测器 (量子效率为 1) 来进行量子态探测, 而这在实际应用中是无法实现的. 实验中常用的零差探测器其标准的量子效率仅为 0.6[53], 这会严重影响离散调制 CV-MDI-QKD 方案的性能.

为了使离散调制 CV-MDI-QKD 方案在基于实际探测器的情况下依然保持较好的性能, 本文提出基于实际探测器补偿的离散调制 CV-MDI-QKD 方案, 即在 Alice 至 Charlie 以及 Bob 至 Charlie 这两条量子信道的输出端各采用一个相位敏感放大器 (phase-sensitive amplifiers, PSA) 来对相应的实际零差探测器 (量子效率为 0.6) 进行补偿. 仿真结果表明本文所提出的方案能够很好地补偿实际探测器的量子效率, 有效提升基于实际探测器的离散调制 CV-MDI-QKD 方案的性能, 为将来离散调制 CV-MDI-QKD 方案的实用化发展提供了一个很好的参考. 首先介绍了本文提出的基于实际探测器补偿的离散调制 CV-MDI-QKD 方案以及在集体攻击下方案的安全性分析, 然后对本文方案的性能分析和总结.

2 基于实际探测器补偿的离散调制 CV-MDI-QKD 方案

首先介绍基于实际探测器的离散调制 CV-MDI-QKD 方案, 特别是等效纠缠模型下的离散调制 CV-MDI-QKD 方案, 同时计算该方案在集体攻击下的渐近密钥率. 之后, 提出基于实际探测器补偿的离散调制 CV-MDI-QKD 方案.

2.1 基于实际探测器的离散调制 CV-MDI-QKD

在离散调制 CV-MDI-QKD 方案中, 发送方 Alice 和 Bob 同时进行离散调制操作. 为了简化分析, 此处主要考虑四态调制方案[54]. 该方案主要包括 4 种类型的调制相干态, 即$\left|\mu \mathrm{e}^{\mathrm{i}\pi/4}\right\rangle$, $\left|\mu \mathrm{e}^{3\ \mathrm{i}\pi/4}\right\rangle$, $\left|\mu \mathrm{e}^{-\mathrm{i}\pi/4}\right\rangle$和$\left|\mu \mathrm{e}^{-3\mathrm{i}\pi/4}\right\rangle$, 其中 μ 表示与相干态调制方差 V_{M} 有关的正数. 4 种类型的调制相干态如图 1 所示. 相干态的调制方差 $V_{\mathrm{M}}=2\mu^2$.

首先考虑 Alice 端的四态调制操作. 在制备-测量方案中, Alice 将混合量子态 Θ_4^A 经由量子信道发送给接收方 Charlie, 其表达式可写为

$$\Theta_4^A=\frac{1}{4}\sum_{m=0}^{3}\left|\mu_m^4\right\rangle\left\langle\mu_m^4\right|. \tag{1}$$

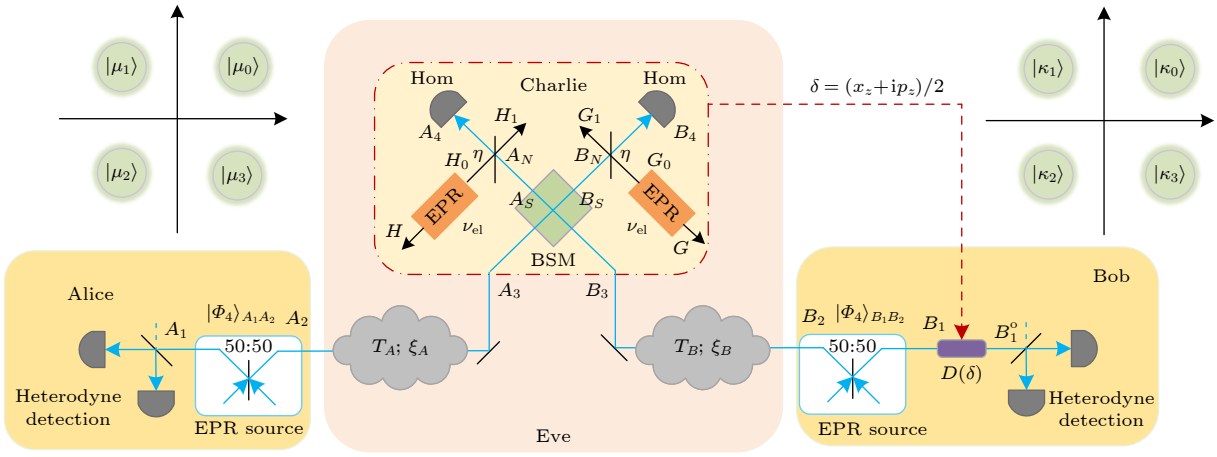

图 1 基于实际探测器的离散调制 CV-MDI-QKD 方案图, $D(\delta)$表示置换操作

Fig. 1. Schematic diagram of the discrete modulation CV-MDI-QKD based on realistic detector, $D(\delta)$ represents displacement operation.

在等效纠缠方案中, Alice 制备双模压缩态 $|\Phi_4\rangle_{A_1A_2}$, 其中模 A_1和 A_2的方差均为 V_A. Bob 制备双模压缩态$|\Phi_4\rangle_{B_1B_2}$, 其中模 B_1和 B_2 的方差均为 V_B, 并且 $V_A = V_B = V_{\rm M}+1$. Alice 和 Bob 所制备的双模压缩态 $|\Phi_4\rangle_{A_1A_2}$和$|\Phi_4\rangle_{B_1B_2}$如图 1 所示. Alice 所制备的双模压缩态$|\Phi_4\rangle_{A_1A_2}$表达式可写为

$$\begin{aligned}|\Phi_4\rangle_{A_1A_2} &= \sum_{m=0}^{3}\sqrt{\varpi_m}|\gamma_m^A\rangle|\gamma_m^A\rangle \\ &= \frac{1}{2}\sum_{m=0}^{3}|\varphi_m\rangle_{A_1}|\mu_m^4\rangle_{A_2},\end{aligned} \tag{2}$$

式中非高斯态$|\varphi_m\rangle_{A_1}$的表示式可写为

$$|\varphi_m\rangle_{A_1} = \frac{1}{2}\sum_{n=0}^{3}{\rm e}^{{\rm i}(2m+1)n\pi/4}\left|\gamma_n^A\right\rangle, \tag{3}$$

$$n\in\{0,\ 1,\ 2,\ 3\};$$

$$\left|\gamma_m^A\right\rangle = \frac{1}{{\rm e}^{\mu^2/2}\sqrt{\varpi_m}}\sum_{j=0}^{\infty}(-1)^j\frac{\mu^{4j+m}}{\sqrt{(4j+m)!}}|4j+m\rangle, \tag{4}$$

$$m\in\{0,\ 1,\ 2,\ 3\};$$

$$\begin{aligned}\varpi_{0,2} &= \frac{1}{2{\rm e}^{\mu^2}}\left[\cosh(\mu^2)\pm\cos(\mu^2)\right], \\ \varpi_{1,3} &= \frac{1}{2{\rm e}^{\mu^2}}\left[\sinh(\mu^2)\pm\sin(\mu^2)\right].\end{aligned} \tag{5}$$

Alice 将模 A_2发送给不可信第三方 Charlie, 保留模 A_1. 同样地, Bob 将模 B_2发送给 Charlie, 保留模 B_1. Alice 至 Charlie 之间的量子信道长度设为 L_{AC}, Bob 至 Charlie 之间的量子信道长度设为 L_{BC}.

当 Charlie 接收到模 A_3和 B_3时, 利用分束比为 50∶50 的分束器对其进行干涉得到输出模 A_S和 B_S. 随后, 这两个输出模进一步转化为 A_4和 B_4. 之后, Charlie 利用共扼零差探测器同时对模 A_4的 X 正则分量以及模 B_4的 P 正则分量进行测量. 经过探测后, Charlie 获得了探测结果, 此处记为 $\{X_Z, P_Z\}$. 随后, Charlie 将 $\{X_Z, P_Z\}$向 Alice 和 Bob 进行公布. 值得一提的是, 在图 1 中, 采用透过率均为η的两个分束器来模拟 Charlie 两个实际探测器的量子效率, 而其电噪声则用两个方差均为$\upsilon_{\rm el}$的辅助 EPR 纠缠态来模拟. 需要指出的是, 图 1 中 H 和 H_0 以及 G 和 G_0 分别表示左侧辅助 EPR 纠缠态的纠缠模以及右侧辅助 EPR 纠缠态的纠缠模, 并且 H_0 与 A_N 经分束器相互作用后得到模 A_4 与 H_1, G_0 与 B_N 经分束器相互作用后得到模 B_4 与 G_1.

Bob 根据 Charlie 所公布的探测结果采用置换操作 $D(\delta)$ 对模 B_1进行修正, 即:

$$\boldsymbol{\chi}_{B_1^{\rm o}} = D(\delta)\boldsymbol{\chi}_{B_1}D^{\dagger}(\delta), \tag{6}$$

其中 $\boldsymbol{\chi}_{B_1}$表示模 B_1的密度矩阵, 并且 $\delta = g(X_Z+{\rm i}P_Z)$, g表示置换操作的增益参数. 利用外差探测器, Bob 对经过修正后的模 $B_1^{\rm o}$进行探测, 得到$\{X_B, P_B\}$, 而 Alice 对模 A_1进行探测, 得到$\{X_A,\ P_A\}$.

Alice 和 Bob 在经过参数估计、信息协商以及保密增强这些步骤后, 最终得到一串安全密钥. 经过贝尔基测量 (Bell-state measurement, BSM) 以及 Bob 的置换操作后, 模 A_1和 $B_1^{\rm o}$具有纠缠效应[55], 并且$\{X_B,\ P_B\}$和$\{X_A,\ P_A\}$是相关联的.

而在制备-测量方案中, Alice 随机制备 4 个非正交的相干态并且将其中一个发送给 Charlie, Bob 随机制备另外 4 个非正交的相干态并将其中一个发送给 Charlie. 当 Charlie 对所接收到的两个相干态进行 BSM 之后, 对所得到测量结果向 Alice 和 Bob 进行公布, Bob 根据所公布的测量结果对自己的数据进行修正, 而 Alice 则保持自己的数据不变. 值得一提的是, 在制备-测量方案中, Bob 并没有进行置换操作. Alice 和 Bob 在经过参数估计、信息协商以及保密增强这些步骤后, 最终得到一串安全密钥.

由于离散调制 CV-MDI-QKD 的制备-测量方案等价于其纠缠模型方案, 因此混合量子态:

$$\Theta_4^A = \mathrm{tr}\left(|\Phi_4\rangle_{A_1A_2}\langle\Phi_4|_{A_1A_2}\right) = \sum_{m=0}^{3} \varpi_m \left|\gamma_m^A\right\rangle\left\langle\gamma_m^A\right|. \tag{7}$$

二分态$|\Phi_4\rangle_{A_1A_2}$其协方差矩阵$\Gamma_{A_1A_2}$可写为

$$\Gamma_{A_1A_2} = \begin{pmatrix} U\boldsymbol{I}_2 & W_4\sigma_z \\ W_4\sigma_z & H\boldsymbol{I}_2 \end{pmatrix}, \tag{8}$$

其中$\boldsymbol{I}_2$表示 2 × 2 的单位矩阵, $\sigma_z = \mathrm{diag}(1, -1)$,

$$\begin{aligned} U &= \langle\Phi_4|\, 1 + a_1^\dagger a_1 \,|\Phi_4\rangle = 1 + 2\mu^2, \\ H &= \langle\Phi_4|\, 1 + a_2^\dagger a_2 \,|\Phi_4\rangle = 1 + 2\mu^2, \\ W_4 &= \langle\Phi_4|\, a_1 a_2 + a_1^\dagger a_2^\dagger \,|\Phi_4\rangle \\ &= 2\mu^2 \sum_{m=0}^{3} \varpi_{m-1}^{3/2} \varpi_m^{-1/2}. \end{aligned} \tag{9}$$

需要指出的是, Bob 端的调制方差仍然设置为$V_{\mathrm{M}} = 2\kappa^2 = 2\mu^2$, 其中参数$\kappa$表示与 Bob 端相干态调制方差相关的正数, 并且$|\kappa_0\rangle = \left|\kappa \mathrm{e}^{\mathrm{i}\pi/4}\right\rangle$, $|\kappa_1\rangle = \left|\kappa \mathrm{e}^{3\,\mathrm{i}\pi/4}\right\rangle$, $|\kappa_2\rangle = \left|\kappa \mathrm{e}^{-\mathrm{i}\pi/4}\right\rangle$和$|\kappa_3\rangle = \left|\kappa \mathrm{e}^{-3\mathrm{i}\pi/4}\right\rangle$表示 Bob 所调制四种不同类型的相干态. 并且二分态$|\Phi_4\rangle_{B_1B_2}$的两个输出模分别为B_1和B_2. 由于 Alice 和 Bob 执行相同的离散调制操作, 因此$|\Phi_4\rangle_{B_1B_2}$的协方差矩阵$\Gamma_{B_1B_2}$与$|\Phi_4\rangle_{A_1A_2}$的协方差矩阵$\Gamma_{A_1A_2}$相同. Bob 端所执行的置换操作并不对其协方差矩阵产生影响.

2.2 基于实际探测器的离散调制 CV-MDI-QKD 安全密钥率

需要指出的是, 在离散调制 CV-MDI-QKD 方案中共有两条量子信道, 即 Alice 至 Charlie 以及 Bob 至 Charlie 之间的信道. 目前已报道的针对 CV-MDI-QKD 方案的攻击策略主要有两种, 分别是单模攻击与双模攻击. 单模攻击指的是攻击者 Eve 分别对每条量子信道采取相互独立的纠缠克隆攻击, 而双模攻击指的是 Eve 通过利用两条量子信道之间的相互作用来进行相关联的双模相干高斯攻击[47]. 从实际角度考虑, Eve 想要在两条量子信道之间进行双模攻击, 需要解决许多技术上的难题, 具有诸多挑战. 不仅如此, 当两条量子信道来自不同的方向时, 这两条量子信道各自的过噪声关联性非常弱, 因此双模攻击策略的实施在实际上存在许多困难[52]. 根据上述分析, 此处主要考虑两个互不影响的马尔可夫无记忆高斯量子通道. 则此时 CV-MDI-QKD 的量子信道退化为单模信道, 而双模攻击则退化为单模攻击[56].

为了计算方案的安全密钥率, 此处将 Alice 至 Charlie 以及 Bob 至 Charlie 量子信道中的过噪声分别设为ξ_A和ξ_B, 两者的信道透过率分别设为T_A和T_B. 两条量子信道的损耗量均设置为0.2 dB/km, 则透过率$T_A = 10^{-0.2L_{AC}/10}$, $T_B = 10^{-0.2L_{BC}/10}$. 等效单模量子信道下的等效过噪声ξ表达式可写为

$$\begin{aligned} \xi = {} & \frac{T_B}{T_A}\left(\sqrt{\frac{2}{g^2 T_B}}\sqrt{V_B - 1} - \sqrt{V_B + 1}\right)^2 \\ & + 1 + \psi_A + \frac{T_B}{T_A}\left(\psi_B - 1\right), \end{aligned} \tag{10}$$

其中$\psi_A = 1/T_A - 1 + \xi_A$, $\psi_B = 1/T_B - 1 + \xi_B$, g表示 Bob 执行置换操作时的增益参数. 为了最小化等效过噪声ξ, 此处取$g^2 = \dfrac{2(V_B - 1)}{T_B(V_B + 1)}$, 则$\xi$的表达式可写为

$$\begin{aligned} \xi &= \frac{T_B}{T_A}\left(\psi_B - 1\right) + \psi_A + 1 \\ &= \frac{T_B}{T_A}\left(\xi_B - 2\right) + \xi_A + \frac{2}{T_A}. \end{aligned} \tag{11}$$

值得一提的是, 为了使离散调制 CV-MDI-QKD 方案更加符合实际, 本文中 Charlie 所使用的零差探测器为非完美探测器, 则探测器附加噪声χ_{hom}表达式可写为$\chi_{\mathrm{hom}} = [(1-\eta) + \upsilon_{\mathrm{el}}]/\eta$, 其中$\eta$表示零差探测器的量子效率, υ_{el}表示零差探测器的电噪声. 归结为信道输入端的总噪声$\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + 2\chi_{\mathrm{hom}}/T_A$, 其中$\chi_{\mathrm{line}}$表示归结到输入端的信道加性噪声, 其表达式为$\chi_{\mathrm{line}} = (1-T)/T + \xi$, 并且$T = T_A g^2/2$表示与等效单模信道相关联的透过率参数[43].

离散调制 CV-MDI-QKD 在反向协商下安全密钥率的计算式为

$$K_{\rm D} = \beta I_{AB} - \chi_{BE} \tag{12}$$

其中$\beta \in [0,\ 1]$表示协商效率, I_{AB}表示 Alice 和 Bob 的互信息量, χ_{BE}表示 Bob 和 Eve 的 Holevo 界.

经过 BSM 以及 Bob 的置换操作后, 量子态$\gamma_{A_1B_1^{\rm o}}$协方差矩阵其表达式可写为

$$\begin{aligned} \varGamma_{A_1B_1^{\rm o}} &= \begin{pmatrix} a\boldsymbol{I}_2 & c\sigma_z \\ c\sigma_z & b\boldsymbol{I}_2 \end{pmatrix} \\ &= \begin{pmatrix} U\boldsymbol{I}_2 & \sqrt{T}W_4\sigma_z \\ \sqrt{T}W_4\sigma_z & T(H+\chi_{\rm tot})\boldsymbol{I}_2 \end{pmatrix}, \end{aligned} \tag{13}$$

其中参数U, H以及W_4的表达式在 (9) 式中已给出, $\boldsymbol{I}_2$表示 2 × 2 的单位矩阵, $\sigma_z = {\rm diag}(1,\ -1)$. 根据 (13) 式可以发现, 当关联系数$W_4$被双模压缩真空态中的关联系数$W_{\rm EPR} = \sqrt{(V_{\rm M}+1)^2 - 1}$替换时, 协方差矩阵$\varGamma_{A_1B_1^{\rm o}}$将转变成与高斯调制方案中的协方差矩阵相同的形式. 关联系数W_4和$W_{\rm EPR}$与调制方差$V_{\rm M}$的关系如图 2 所示. 从图 2 可以发现, 当调制方差$V_{\rm M}$足够小时, 代表W_4与$W_{\rm EPR}$的两条曲线几乎重合, 即W_4与$W_{\rm EPR}$几乎是等价的. 在这种情况下, 离散调制 CV-MDI-QKD 方案中 Bob 与 Eve 的互信息量与高斯调制 CV-MDI-QKD 方案中 Bob 与 Eve 的互信息量几乎相等.

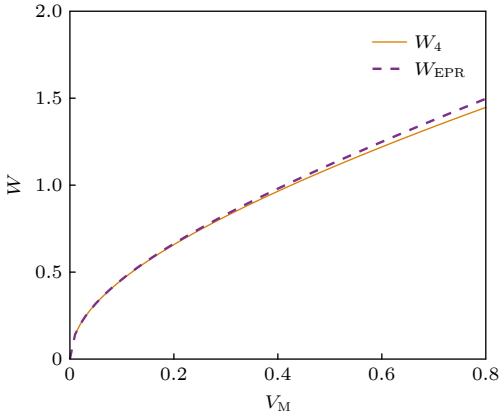

图 2 W (W_4 和 $W_{\rm EPR}$) 与调制方差 $V_{\rm M}$ 的关系

Fig. 2. Relationship between W (W_4 and $W_{\rm EPR}$) and the modulation variance $V_{\rm M}$.

基于上述分析, χ_{BE}的表达式可以写为

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \tag{14}$$

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

辛特征值$\lambda_{1,2}$可通过下式进行计算:

$$\lambda_{1,2}^2 = \frac{1}{2}\left(\varDelta \pm \sqrt{\varDelta^2 - 4D^2}\right), \tag{15}$$

其中

$$\begin{aligned} \varDelta &= a^2 + b^2 - 2c^2, \\ D &= ab - c^2. \end{aligned} \tag{16}$$

而另外一个辛特征值:

$$\lambda_3 = a - c^2/(b+1), \tag{17}$$

其中$a = U$, $b = T(H + \chi_{\rm tot})$, $c = \sqrt{T}W_4$. Alice 与 Bob 之间的互信息量I_{AB}表达式可写为

$$I_{AB} = \log_2\left[\frac{a+1}{a+1-c^2/(b+1)}\right]. \tag{18}$$

2.3 基于实际探测器补偿的离散调制 CV-MDI-QKD

由于第三方 Charlie 所采用的实际探测器并非是完美的 (量子效率$0 < \eta < 1$), 会对离散调制 CV-MDI-QKD 方案的性能产生重要影响, 因此有必要对该方案所使用的实际探测器进行补偿. 此处采用相位敏感放大器 (phase-sensitive amplifiers, PSA) 对 Charlie 所使用的实际探测器进行补偿, 如图 3 所示. 在图 3 中, 模A_S与B_S对应图 1 中的A_S与B_S, 表示分束比为 50∶50的分束器对模A_3和B_3进行干涉后所得到输出模, 模A_N与B_N则分别表示模A_S与B_S经 PSA 作用后所得到的输出模. PSA 可被视为一种简并光放大器, 其变换公式如下[57]:

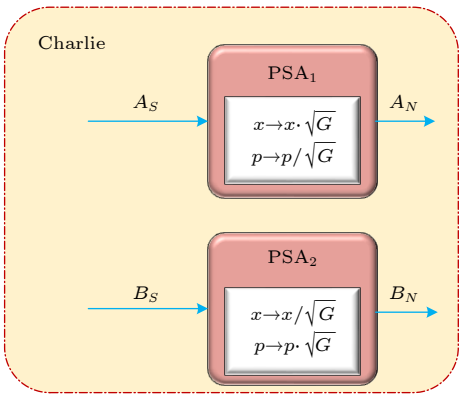

图 3 基于 PSA 的离散调制 CV-MDI-QKD 实际探测器补偿方案图, PSA 为相位敏感放大器

Fig. 3. Schematic diagram of discrete modulation CV-MDI-QKD with realistic detector compensation based on PSA, where PSA is the phase-sensitive amplifier.

$$\begin{pmatrix} x_{A_N} \\ p_{A_N} \end{pmatrix} = \Omega_{\mathrm{PSA_1}} \begin{pmatrix} x_{A_S} \\ p_{A_S} \end{pmatrix} = \begin{pmatrix} \sqrt{G} & 0 \\ 0 & 1/\sqrt{G} \end{pmatrix} \begin{pmatrix} x_{A_S} \\ p_{A_S} \end{pmatrix}, \tag{19}$$

并且

$$\begin{pmatrix} x_{B_N} \\ p_{B_N} \end{pmatrix} = \Omega_{\mathrm{PSA_2}} \begin{pmatrix} x_{B_S} \\ p_{B_S} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{G} & 0 \\ 0 & \sqrt{G} \end{pmatrix} \begin{pmatrix} x_{B_S} \\ p_{B_S} \end{pmatrix}, \tag{20}$$

其中, G表示 PSA$_{1,2}$的增益参数, $\{x_{A_N}, p_{A_N}\}$与$\{x_{A_S}, p_{A_S}\}$分别表示模A_N与A_S的正则分量, $\{x_{B_N}, p_{B_N}\}$与$\{x_{B_S}, p_{B_S}\}$分别表示模B_N与B_S的正则分量. 基于 2.2 节中对离散调制 CV-MDI-QKD 方案安全密钥率的计算, 当采用 PSA$_{1,2}$对方案的实际探测器进行补偿时, χ_{hom}可修正为$\chi_{\mathrm{hom}}^{\mathrm{PSA}}$, 其表达式如下:

$$\chi_{\mathrm{hom}}^{\mathrm{PSA}} = \frac{(1-\eta)+\upsilon_{\mathrm{el}}}{G\eta}. \tag{21}$$

则 2.2 节中所计算的安全密钥率K_{D}可以修正为$K_{\mathrm{D}}^{\mathrm{PSA}}$.

3 基于实际探测器补偿的离散调制 CV-MDI-QKD 方案性能分析

本节从安全密钥率和传输距离的角度对基于实际探测器补偿的离散调制 CV-MDI-QKD 方案的性能进行分析, 并与基于完美探测器的离散调制 CV-MDI-QKD 方案 (简记为理想方案, 即$\eta=1$及$\upsilon_{\mathrm{el}}=0$)[52] 进行性能比较. 涉及全局的仿真参数以及设定如下: Charlie 所使用的实际探测器的性能参数为量子效率$\eta=0.6$, 探测器电噪声$\upsilon_{\mathrm{el}}=0.05$, 这也是实验中标准的探测器性能参数[53]. Alice 至 Charlie 以及 Bob 至 Charlie 量子信道中的过噪声$\xi_A=\xi_B=0.002$.

图 4 给出了在对称情况 ($L_{AC}=L_{BC}$) 以及不同的 PSA 增益参数G下所提出方案的安全密钥率与传输距离的关系, 其中协商效率$\beta=0.95$, 调制方差$V_{\mathrm{M}}=0.5$[52], 并且增益参数$G=200,\ 300,\ 400,\ 500,\ 800$. 在图 4 中也仿真出了 Pirandola-Laurenza-Ottaviani-Banchi (PLOB) 界, 该界限表示点对点量子通信性能的最终极限[58]. 从图 4 可以发现 PSA 的增益参数G越大, 基于实际探测器的离散调制 CV-MDI-QKD 方案的性能越好. 此外随着G的增大, 基于实际探测器的离散调制 CV-MDI-QKD 方案的性能曲线越来越接近理想方案的性能曲线以及 PLOB 界限.

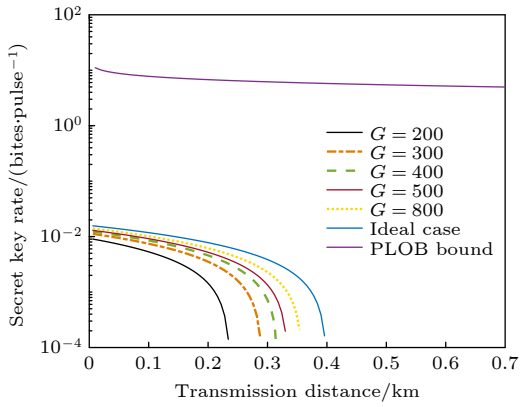

图 4 在对称情况以及不同的 PSA 增益参数G下所提出方案的安全密钥率与传输距离的关系

Fig. 4. Relationship between the security key rate and transmission distance of the proposed scheme in the symmetric case with different PSA gain G.

需要指出的是, 最优的 CV-MDI-QKD 框架配置是极端非对称情况, 即不可信第三方 Charlie 与其中一个合法通信方非常接近的情况, 此时 Charlie 充当该合法通信方的代理服务器[47]. 因此此处设定 Charlie 与合法通信方 Bob 非常接近, 即$L_{BC}=0$, 则此时方案的有效传输距离就等价为L_{AC}. 图 5 给出了极端非对称情况下 ($L_{BC}=0$) 所提出方案的安全密钥率与 PSA 增益参数G和传输距离L_{AC}的关系, 其中协商效率$\beta=0.95$, 调制方差$V_{\mathrm{M}}=0.4$[52]. 此外, 在图 5 中也给出了理想方案 ($\eta=1$, $\upsilon_{\mathrm{el}}=0$) 的性能曲面, 用于和所提出的方案进行性能比较. 由图 5 可知, 在极端不对称情况下, 所提出的基于实际探测器补偿的离散调制 CV-MDI-QKD 方案的性能随着 PSA 增益参数G的增大而稳步提升, 并且越来越接近理想方案的性能曲面.

图 6 给出了在极端非对称情况 ($L_{BC}=0$) 以及不同的 PSA 增益参数G下所提出方案的安全密钥率与传输距离的关系, 其中协商效率$\beta=0.95$, 调制方差$V_{\mathrm{M}}=0.4$, 并且增益参数$G=100,\ 200,\ 300,\ 400,\ 500,\ 800$. 从图 6 可以发现, 在极端非对称情况下, 通过增大 PSA 增益参数G, 可以使所提出的方案其性能得到有效提升, 并且随着G的增大, 所

提出方案的性能曲线越来越接近理想方案的性能曲线以及 PLOB 界限.

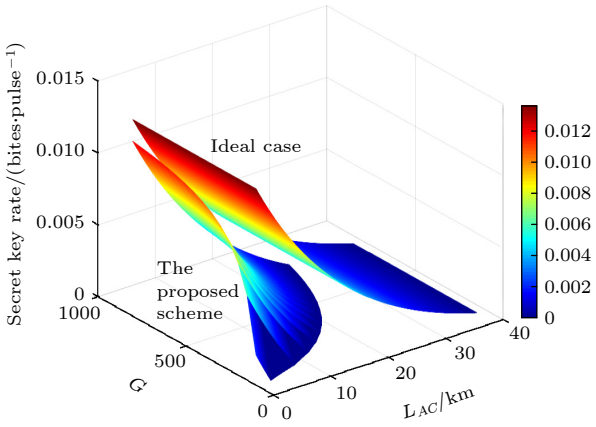

图 5 极端非对称情况下所提出方案的安全密钥率与 PSA 增益参数 G 及传输距离 L_{AC} 的关系

Fig. 5. Relationship between the secret key rate and the PSA gain G, transmission distance L_{AC} of the proposed scheme in the extreme asymmetric case.

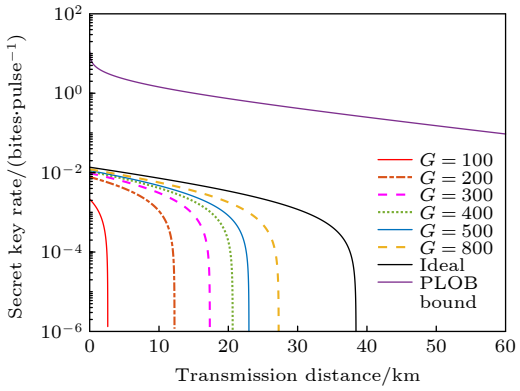

图 6 极端非对称情况以及不同的 PSA 增益参数 G 下所提出方案的安全密钥率与传输距离的关系

Fig. 6. Relationship between the secret key rate and the transmission distance of the proposed scheme in the extreme asymmetric case with different PSA gain G.

通过上述分析可以发现, PSA 的使用能够有效降低离散调制 CV-MDI-QKD 方案对实际探测器量子效率的需求. 即使采用实验中常用的传统探测器 ($\eta = 0.6$, $\upsilon_{\mathrm{el}} = 0.05$), 通过利用 PSA 对其进行补偿后, 依然能够获得较为合理的离散调制 CV-MDI-QKD 的方案性能, 并且随着 PSA 增益参数的增大, 其性能越来越接近理想方案的性能以及 PLOB 界. 这表明 PSA 能够有效克服由于实际探测器不完美所导致的离散调制 CV-MDI-QKD 方案性能的局限.

图 7 给出了在极端非对称情况以及不同增益参数 G 下所提出方案的安全密钥率与协商效率 β 的关系, 其中调制方差 $V_{\mathrm{M}} = 0.4$, 传输距离 $L_{AC} = 10$ km, 并且 $G = 200$, 300, 400, 500, 800. 由图 7 可以观察到协商效率 β 的可用范围随着 PSA 增益参数 G 的增大而增大. 比如当 $G = 200$ 时, 所提出方案的协商效率 β 的可用范围为 [0.92, 1]; 而当 $G = 800$ 时, 所提出方案其协商效率 β 的可用范围则扩展至 [0.76, 1]. 此外, 随着增益参数 G 的增大, 所提出方案其协商效率 β 的可用范围越来越接近理想方案协商效率 β 的可用范围. 这表明所提出的基于实际探测器补偿的离散调制 CV-MDI-QKD 能够有效提高方案对协商效率 β 的容忍度.

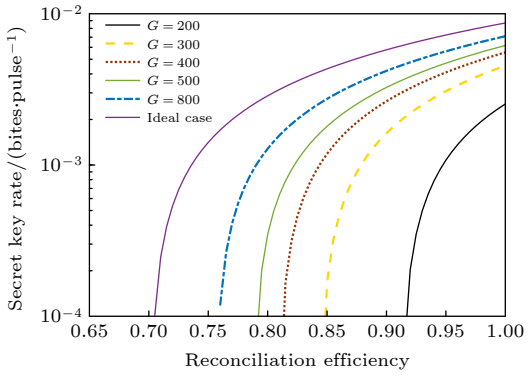

图 7 极端非对称情况以及不同 PSA 增益参数 G 下所提出方案的安全密钥率与协商效率 β 的关系

Fig. 7. Relationship between the secret key rate and the reconciliation efficiency β of the proposed scheme in the extreme asymmetric case with different PSA gain G.

需要指出的是, 在上述分析中, 我们并没有给出当增益参数 $G = 1$ (即没有经过 PSA 补偿) 时基于实际探测器的离散调制 CV-MDI-QKD 的性能曲线. 原因在于当采用量子效率 $\eta = 0.6$ 的传统零差探测器时, 离散调制 CV-MDI-QKD 方案会出现非物理特性的负密钥率性能曲线, 即无法正常生成密钥. 这种情况表明 Charlie 端不完美的实际零差探测器对离散调制 CV-MDI-QKD 方案的性能影响很大. 由于归结为信道输入端的总噪声 $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + 2\chi_{\mathrm{hom}}/T_{\mathrm{A}}$, 显然不完美的实际零差探测器的附加噪声 χ_{hom} 能够使得总噪声 χ_{tot} 显著增大. 再者, 离散调制 CV-MDI-QKD 方案中量子信号的强度远低于高斯调制 CV-MDI-QKD 方案中量子信号的强度, 因此离散调制 CV-MDI-QKD 方案对总噪声 χ_{tot}, 特别是不完美探测器的附加噪声 χ_{hom}, 相比于高斯调制 CV-MDI-QKD 方案更加敏感 [52]. 这也进一步说明了本文所提出的针对 Charlie 端实

际零差探测器的补偿方案对保证离散调制 CV-MDI-QKD 在实际条件下的正常运行具有十分重要的作用.

在上述分析中可以发现, 所提出的基于实际探测器补偿的离散调制 CV-MDI-QKD 方案的性能随着 PSA 增益参数的增大, 越来越接近理想方案的性能, 但无法达到理想方案的性能水平. 主要原因在于理想方案中假定量子效率 $\eta=1$, 电噪声 $\upsilon_{\rm el}=0$, 因此其探测器附加噪声 $\chi_{\rm hom}=0$. 而在本文所提出的方案中, 其修正后的探测器附加噪声为 $\chi_{\rm hom}^{\rm PSA}=[(1-\eta)+\upsilon_{\rm el}]/(G\eta)$, 其中 $\eta=0.6$, $\upsilon_{\rm el}=0.05$. 若要使得所提出的基于实际探测器补偿的离散调制 CV-MDI-QKD 方案的性能达到理想方案的性能, 即 $\chi_{\rm hom}^{\rm PSA}=0$, 则 PSA 的增益参数 G 必须为无穷大 (∞), 然而这在实际情况下是无法实现的, 因此所提出的方案其性能无法达到理想方案的性能水平.

4 结 论

本文提出基于实际探测器补偿的离散调制 CV-MDI-QKD 方案, 通过在 Alice 至 Charlie 以及 Bob 至 Charlie 这两条量子信道的输出端各采用一个 PSA 来对相应的实际零差探测器进行补偿. 在进行方案性能分析时考虑两种常见的 CV-MDI-QKD 框架, 即对称情况 ($L_{AC}=L_{BC}$) 与极端非对称情况 ($L_{BC}=0$). 仿真结果表明无论是在对称情况还是极端非对称情况, 本文所提出的方案能够很好地对实际探测器的量子效率进行补偿, 并且通过增大 PSA 的增益参数 G 可以有效提高离散调制 CV-MDI-QKD 方案在实际情况下的密钥率和安全传输距离, 使其越来越接近理想方案的性能以及 PLOB 界限. 此外, 随着增益参数 G 的增大, 所提出方案的协商效率 β 的可用范围越来越接近理想方案协商效率 β 的可用范围, 这表明所提出的方案能够有效提高基于实际探测器的离散调制 CV-MDI-QKD 方案对协商效率 β 的容忍度. 因此本文提出的方案有力地推动离散调制 CV-MDI-QKD方案的实用化发展, 使得该方案具有更强的实用性.

参考文献

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

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

[3] 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

[4] 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

[5] 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. Photonics* **15** 570

[6] 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

[7] Fang X T, Zeng P, Liu H, Zou M, Wu W J, Tang Y L, Sheng Y J, Xiang Y, Zhang W, Li H, Wang Z, You L, Li M J, Chen H, Chen Y A, Zhang Q, Peng C Z, Ma X, Chen T Y, Pan J W 2020 *Nat. Photonics* **14** 422

[8] 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

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

[10] 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]

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

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

[13] Wang T, Zuo Z, Li L, Huang P, Guo Y, Zeng G 2022 *Phys. Rev. Appl.* **18** 014064

[14] Liu C, Zhu C, Nie M, Yang H, Pei C 2022 *Opt. Express* **30** 14798

[15] Jing F, Liu X, Wang X, Lu Y, Wu T, Li K, Dong C 2022 *Opt. Express* **30** 8075

[16] Sarmiento S, Etcheverry S, Aldama J, López I H, Vidarte L T, Xavier G B, Nolan D A, Stone J S, Li M J, Loeber D, Pruneri V 2022 *New J. Phys.* **24** 063011

[17] García-Patrón R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[18] Navascués M, Grosshans F, Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[19] Pirandola S, Braunstein S L, Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504

[20] Renner R, Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504

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

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

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

[24] 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

[25] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E 2013 *Nat. Photonics* **7** 378

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

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

[28] Filip R 2008 *Phys. Rev. A* **77** 022310

[29] Yuan Z L, Dynes J F, Shields A J 2010 *Nat. Photonics* **4** 800
[30] Jouguet P, Kunz-Jacques S, Diamanti E 2013 *Phys. Rev. A* **87** 062313
[31] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **88** 022339
[32] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **87** 052309
[33] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325
[34] Braunstein S L, Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[35] Lo H K, Curty M, Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[36] Wang X B 2013 *Phys. Rev. A* **87** 012320
[37] Xu F, Curty M, Qi B, Lo H K 2013 *New J. Phys.* **15** 113007
[38] Curty M, Xu F, Cui W, Lim C C W, Tamaki K, Lo H K 2014 *Nat. Commun.* **5** 3732
[39] Lupo C, Ottaviani C, Papanastasiou P, Pirandola S 2018 *Phys. Rev. Lett.* **120** 220505
[40] Ferreira da S T, Vitoreti D, Xavier G B, do Amaral G C, Temporao G P, von derWeid J P 2013 *Phys. Rev. A* **88** 052303
[41] Cao Y, Li Y H, Yang K X, Jiang Y F, Li S L, Hu X L, Abulizi M, Li C L, Zhang W, Sun Q C, Liu W Y, Jiang X, Liao S K, Ren J G, Li H, You L, Wang Z, Yin J, Lu C Y, Wang X B, Zhang Q, Peng C Z, Pan J W 2020 *Phys. Rev. Lett.* **125** 260503
[42] Xu F, Qi B, Liao Z, Lo H K 2013 *Appl. Phys. Lett.* **103** 061101
[43] Li Z, Zhang Y C, Xu F, Peng X, Guo H 2014 *Phys. Rev. A* **89** 052301
[44] Ma X C, Sun S H, Jiang M S, Gui M, Liang L M 2014 *Phys. Rev. A* **89** 042335
[45] Zhang Y C, Li Z, Yu S, Gu W, Peng X, Guo H 2014 *Phys. Rev. A* **90** 052325
[46] Wu X D, Wang Y J, Huang D, Guo Y 2020 *Front. Phys.* **15** 31601
[47] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S, Andersen U L 2015 *Nat. Photonics* **9** 397
[48] Richardson T J, Shokrollahi M A, Urbanke R 2001 *IEEE Trans. Inf. Theory* **47** 619
[49] Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P 2008 *Phys. Rev. A* **77** 042325
[50] Jouguet P, Kunz-Jacques S, Leverrier A 2011 *Phys. Rev. A* **84** 062317
[51] Milicevic M, Chen F, Zhang L M, Gulak P. G 2018 *npj Quantum Inf.* **4** 21
[52] Ma H X, Huang P, Bai D Y, Wang T, Wang S Y, Bao W S, Zeng G H 2019 *Phys. Rev. A* **99** 022322
[53] 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
[54] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[55] Polkinghorne R E S, Ralph T C 1999 *Phys. Rev. Lett.* **83** 2095
[56] Pirandola S 2013 *New J. Phys.* **15** 113046
[57] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P 2009 *J. Phys. B* **42** 114014
[58] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043

Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation*

Wu Xiao-Dong [1)] Huang Duan [2)†] Huang Peng [3)‡] Guo Ying [4)]

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

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

3) (*State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai* 200240, *China*)

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

(Received 30 May 2022; revised manuscript received 11 August 2022)

Abstract

Discrete modulation continuous variable measurement device independent quantum key distribution scheme has good compatibility with efficient error correction codes, which leads to high reconciliation efficiency even at low signal-to-noise ratio. Besides, the implementation of this protocol is simpler than that of Gaussian modulation scheme. However, the quantum efficiency of homodyne detector commonly used in the experiment is only 0.6, which will seriously affect the practical application performance of discrete modulation continuous variable measurement device independent quantum key distribution scheme. To solve this problem, we propose a discrete modulation continuous variable measurement device independent quantum key distribution scheme based on realistic detector compensation. In our scheme, for the outputs of two quantum channels, each adopts a phase sensitive amplifier to compensate for the corresponding realistic homodyne detector. The simulation results show that the phase sensitive amplifier can well compensate for the quantum efficiency of the realistic detector and effectively improve the performance of the discrete modulation continuous variable measurement device independent quantum key distribution scheme with realistic detector in terms of secret key rate and secure transmission distance. The proposed protocol provides an effective method for promoting the practical development of the discrete modulation continuous variable measurement device independent quantum key distribution scheme.

Keywords: discrete modulation, continuous variable, measurement device independent quantum key distribution, realistic detector compensation

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.71.20221072

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61872390, 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

‡ Corresponding author. E-mail: huang.peng@sjtu.edu.cn

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

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

吴晓东　黄端　黄鹏　郭迎

Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation

Wu Xiao-Dong　Huang Duan　Huang Peng　Guo Ying

引用信息 Citation: Acta Physica Sinica, 71, 240304 (2022)　DOI: 10.7498/aps.71.20221072
在线阅读 View online: https://doi.org/10.7498/aps.71.20221072
当期内容 View table of contents: http://wulixb.iphy.ac.cn
