基于非高斯态区分探测的往返式离散调制连续变量量子密钥分发方案*

吴晓东[1)] 黄端[2)†]

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)

(2022 年 11 月 25 日收到; 2022 年 12 月 23 日收到修改稿)

往返式离散调制连续变量量子密钥分发, 无需使用两台独立的激光器也能本地生成本振光, 并且信号光与本振光均来自于同一台激光器, 在有效保证系统实际安全性的同时, 具有较好的同频特性. 此外, 该方案与高效纠错码具有良好的兼容性, 即使在低信噪比情况下也能获得较高的协商效率. 然而, 基于非可信信源模型的往返式光路结构存在较大的过噪声, 严重限制离散调制方案的最大传输距离. 针对这个问题, 本文提出基于非高斯态区分探测的往返式离散调制连续变量量子密钥分发方案, 即在探测端部署非高斯态区分探测器, 采用自适应测量方法并结合贝叶斯推论, 可以在满足低于标准量子极限错误概率的情况下无条件区分出基于四态离散调制的四种非正交相干态. 本文详细分析了所提出的基于非高斯态区分探测的往返式离散调制连续变量量子密钥分发方案的安全性, 包括渐近情况与有限长效应情况. 仿真结果表明所提出的方案相比于原始方案, 即使在有信源噪声的情况下, 其密钥率与最大传输距离仍然有明显的提升. 这些结果表明本方案能够有效降低往返式离散调制连续变量量子密钥分发方案中非可信信源噪声对方案性能的负面影响, 在保证系统实际安全性的同时, 实现更高效、更远传输距离的量子密钥分发.

关键词: 往返式, 离散调制, 连续变量量子密钥分发, 非高斯态区分探测

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20222253

1 引 言

量子密钥分发 (quantum key distribution, QKD)[1−3] 作为最成熟的量子密码技术之一, 允许相隔两地的合法双方 Alice 与 Bob 在由攻击者 Eve 控制的不安全量子信道下生成安全密钥. 基于量子力学的基本定律, 理想化的 QKD 方案已被证明是无条件安全的[4,5]. 目前采用的 QKD 方案主要可分为两种: 离散变量 (discrete variable, DV)QKD[6−8] 与连续变量 (continuous variable, CV)QKD[9−12]. DV-QKD 主要依赖于造价高昂的单光子探测器技术, 而 CV-QKD 则是通过采用达到散粒噪声的相干探测器来提供安全性. 与 DV-QKD 相比, CV-QKD 由于具有较高的探测效率以及易融于现有的光通信系统而备受关注.

在众多类型的 CV-QKD 方案中, 高斯调制相干态 (Gaussian modulated coherent state, GMCS) 方案的应用最为广泛[13]. GMCS QKD 方案在实验室[14−17] 以及现场试验[18] 中均已被证明具有较好的可行性. 在传统的 GMCS QKD 实验方案中, 为了获得用于信号探测的固定相位基准, 发送方 Alice 将信号光与本振光安排在同一条量子信道中进行传输[13]. 然而, 这种传输方式会导致系统出现安全

* 国家自然科学基金 (批准号: 61972418, 61977062, 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

漏洞. 目前已报道的针对实际 CV-QKD 系统的攻击策略包括本振光抖动攻击[19]、波长攻击[20]、校准攻击[21]以及饱和攻击[22], 这些攻击策略均与 CV-QKD 系统中本振光的安全漏洞有关. 此外, 将光强度较高的本振光通过有损信道进行发送会大大降低 QKD 的效率.

为了解决这些问题, 2015 年, Qi 等[23]与 Soh 等[24]课题组各自独立提出单向本地本振 (local local-oscillator, LLO)CV-QKD 方案, 即在接收端用另外一台独立的激光器本地生成本振光. 之后, LLO CV-QKD 方案得到进一步的拓展研究[25–28]. 在单向 LLO CV-QKD 方案中无需将本振光与信号光一起进行传输, 因此能够有效抵御针对本振光的攻击策略. 然而, 单向 LLO CV-QKD 方案在实施过程中存在众多技术挑战, 比如需要保证所使用的两台独立激光器能够生成同频率的信号光与本振光, 对信号光进行相干探测时需要进行相位补偿等. 此外, 单向 LLO CV-QKD 系统中存在的由环境扰动引起的偏振漂移, 光纤长度波动以及两台独立激光器频率的不稳定性都会导致单向 LLO CV-QKD 方案性能及安全性降低.

为了解决单向 LLO CV-QKD 方案中存在的不足, 2016 年, Huang 等[29]提出本地本振往返式 CV-QKD 方案. 该方案无需采用两台独立的激光器来实现“本地本振”, 因此具有较好的同频特性. 不仅如此, 往返式的光路结构可以对系统的偏振变化进行自适应补偿, 从而更能够适应及满足实地应用的需求.

本地本振往返式 CV-QKD 方案虽然能够很好地解决 LLO CV-QKD 方案中所存在的不足, 保证系统的实际安全性, 但往返式 GMCS CV-QKD 方案相比于单向点对点 GMCS CV-QKD 方案, 其系统中存在有更大的过噪声, 并且在低信噪比远距离传输的情况下其协商效率非常低, 严重限制了往返式 GMCS CV-QKD 方案的最大传输距离. 解决这个问题的方法是设计一种比 LDPC 码更适用于低信噪比环境下的完美纠错码, 然而设计并实施这样的一种纠错码复杂度高, 并且所需的硬件成本也高. 而另外一种解决的方法是采用离散调制. 2002 年, Silberhorn 等[30]最早将离散调制用于 CV-QKD 方案中. 2009 年, Leverrier 和 Grangier[31]对离散调制 CV-QKD 的安全性进行证明并且发现离散调制 (如四态调制) 在低信噪比环境下可以获得更好的协商效率, 从而实现更远距离的量子密钥分发. 在离散调制 CV-QKD 方案中, 发送方准备一定数量的非正交相干态 (如四态调制, 非正交相干态的数量为 4), 并且利用所测量的每个相干态正则分量的符号来对密钥率比特进行编码. 所测量的正则分量的符号为离散值, 即使在低信噪比条件下, 也能够很好地与高效纠错码配合使用. 因此离散调制可以有效提高 CV-QKD 方案的最大传输距离.

虽然高性能零差或外差探测器能够有效测量所接收到的量子信号, 然而相干探测器中所固有的不确定性 (电噪声) 仍然会阻碍非正交相干态的精确分辨[32–34]. 即使所采用的探测器为理想探测器 (量子效率为 1), 接收方仍然无法获得精确的测量结果. 传统的理想探测器仅能达到标准量子极限 (standard quantum limit, SQL), SQL 的定义是可以通过直接测量信号光的物理性质来区分非正交相干态所获得的最小误差. 实际上, 量子力学允许存在一个被称为 Helstrom 界的误差下限, 这个下限可以通过设计一种优秀的态区分策略来获得[35]. 2013 年, Becerra 等[32]提出了一种性能良好的态区分探测器用于无条件区分正交相移键控 (quadrature phase-shift keying, QPSK) 调制中的 4 个非正交的相干态. 该探测器通过利用光子计数及以快速反馈的形式进行的自适应测量的方式, 从而接近或达到 Helstrom 界. 因此, 采用性能良好的态区分探测器能够有效提升 CV-QKD 方案的性能[36].

基于上述本地本振往返式光路结构、离散调制的使用优势, 并且针对往返式光路结构中所存在的非可信信源噪声对方案性能的负面影响, 本文提出基于非高斯态区分探测的往返式离散调制 CV-QKD 方案, 即在探测端部署非高斯态区分探测器. 所采用的态区分探测器可以满足在低于 SQL 错误概率的情况下无条件区分出基于 QPSK 调制的 4 种非正交相干态, 即使往返式光路结构中存在信源噪声的情况下, 相比于原始往返式离散调制 CV-QKD, 本文所提出的方案仍能够有效提升密钥率与最大传输距离, 从而能够获得更好的系统鲁棒性. 本文第 2 节详细描述了所提出的基于非高斯态区分探测的往返式离散调制 CV-QKD 方案; 第 3 节对所提出的方案的安全性进行分析, 包括渐近情况与有限长效应情况下方案的安全性; 第 4 节总结全文.

2 基于非高斯态区分探测的往返式离散调制 CV-QKD 方案

首先介绍基于非高斯态区分探测的往返式离散调制 CV-QKD 的制备-测量方案, 之后介绍与之等价的基于非高斯态区分探测的往返式离散调制 CV-QKD 的纠缠模型方案, 最后介绍部署在探测端的非高斯态区分探测器原理.

2.1 基于非高斯态区分探测的往返式离散调制 CV-QKD 制备-测量方案描述

在基于非高斯态区分探测的往返式离散调制 CV-QKD 的制备-测量 (prepare-and-measure, PM) 方案中, Alice 将其中一束光强较高的经典光进行保留, 用作本振光, 而将另外一束光强较弱的经典光 (同一个激光器生成) 经过标准的光纤信道后发送给 Bob, 如图 1 所示. Bob 在接收到由 Alice 发送的经典光后, 对其进行离散调制. 为了简化分析, 此处主要分析离散调制中的四态方案 [31]. 在四态调制方案中, Bob 从 4 种类型的调制相干态 $\left\{\left|\alpha_k^4\right\rangle=\left|\alpha \mathrm{e}^{\mathrm{i}\pi(2k+1)/4}\right\rangle,\ k=0,\ 1,\ 2,\ 3\right\}$ 中随机选取其中一种, 然后借助于法拉第镜, 经过透过率为 T、过噪声为 ξ 的不可信信道反射回 Alice 端. 当经过非可信信道后, 探测方 Alice 利用分束器将发送过来的信号光一分为二, 其中光强较高的信号光束 (包含大多数光子) 用于进行零差探测, 而光强较低的信号光束 (包含少数光子) 则同步发送到态区分探测器中. 则 Alice 所接收到的混合量子态 $\gamma_4=\frac{1}{4}\sum_{k=0}^{3}\left|\alpha_k^4\right\rangle\left\langle\alpha_k^4\right|$ 并对其进行零差探测, 方案中 Bob 端的离散调制方差 $V_{\mathrm{B}}=2\alpha^2$, Alice 端实际零差探测器的量子效率为 η, 电噪声为 υ_{el}, 探测方 Alice 的输入噪声为 χ_{hom}. 最后, 经过经典后处理, Alice 和 Bob 共享一串密钥. 需要指出的是图 1 中所示的信源由不可信第三方 Fred 控制, 并且为了更好地量化往返式离散调制 CV-QKD 方案中的非可信信源过噪声, 图 1 中采用增益参数为 g 的相位非敏感放大器 (phase-insensitive amplifier, PIA) 来对方案中的非可信信源过噪声进行描述 [29]. 需要指出的是, 在实验环境中, 往返式结构 CV-QKD 方案中的非可信信源噪声包含攻击者 Eve 对信源进行窃听所引入的过噪声、Alice 进行脉冲调制所引入的噪声、Bob 端调制所引入的噪声以及激光器的相位噪声 [29]. 在往返式结构 CV-QKD 方案中, 由于本振光并不随着信号光一起在信道中传输, 而是可以直接在 Alice 端本地生成, 因此不会产生后向散射而引入系统过噪声. 与单向 CV-QKD 方案不同的是, 在往返式结构的 CV-QKD 方案中, Alice 端为探测端, Bob 主要负责信号调制, 即发送端.

2.2 基于非高斯态区分探测的往返式离散调制 CV-QKD 纠缠模型方案

由于 PM 方案不利于进行安全性分析, 因此介绍与之等价的纠缠模型 (entanglement-based, EB) 方案, 如图 2 所示. Fred 制备纠缠态 $|\Phi\rangle_{\mathrm{FB}A_0}$, 其中模 B 发送给 Bob, 模 A_0 则经过非可信信道发送给 Alice. 模 A_0 与 B 的正则分量分别为 $\langle X_{A_0}\rangle=\langle P_{A_0}\rangle=V+\xi_0$ 以及 $\langle X_B\rangle=\langle P_B\rangle=V$, 其中 $V=V_B+1$ 并且非可信信源过噪声 $\xi_0=(g-1)+(g-1)V_1$. 此处 V_1 表示

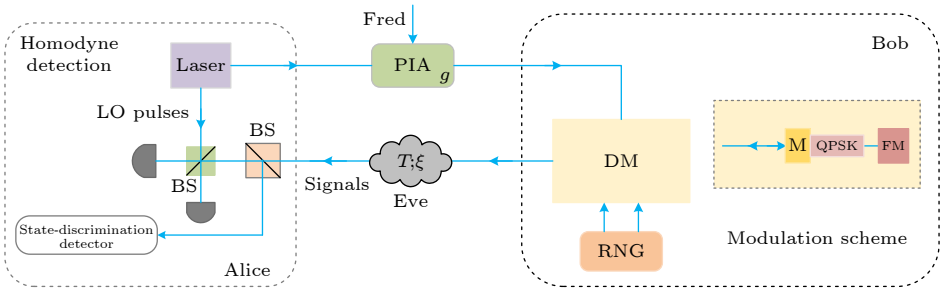

图 1 基于非高斯态区分探测的往返式离散调制 CV-QKD 制备-测量方案图. DM 为离散调制, RNG 为随机数发生器, M 为调制器, QPSK 为正交相移键控, PIA 为相位非敏感放大器, FM 为法拉第镜, BS 为分束器, LO 为本振光, T 表示非可信信道的透过率, ξ 表示信道过噪声, g 表示相位非敏感放大器的增益参数

Fig. 1. Prepare-and-measure version of plug-and-play discrete modulation CV-QKD protocol based on non-Gaussian state-discrimination detection. DM, discrete modulation; RNG, random number generator; M, modulator; QPSK, quadrature phase shift keying; PIA, phase insensitive amplifier; FM, Faraday mirror; BS, beam splitter; LO, local oscillator; T, transmission efficiency; ξ, channel excess noise; g, gain parameters of phase insensitive amplifier.

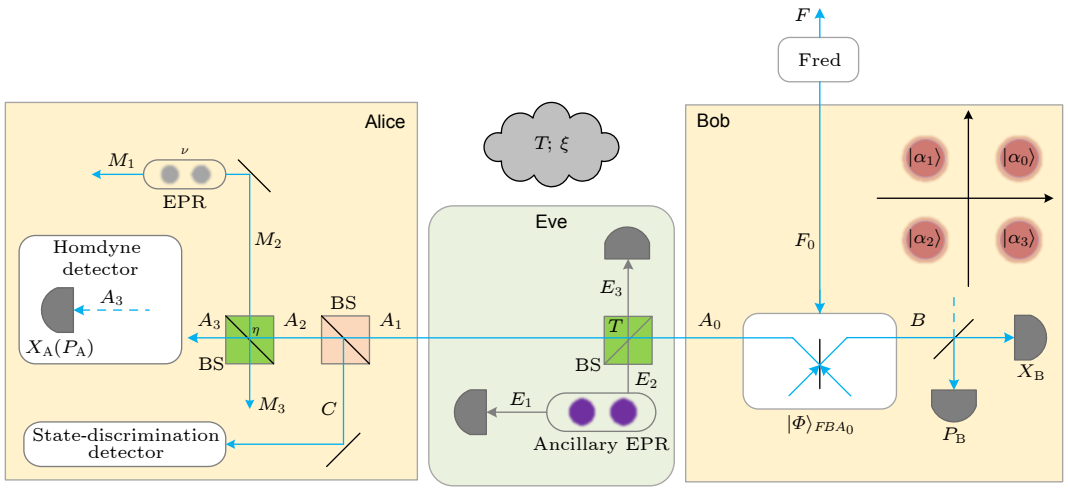

图 2 基于非高斯态区分探测的往返式离散调制 CV-QKD 纠缠模型原理图

Fig. 2. Schematic diagram of the entanglement-based (EB) model of plug-and-play discrete modulation CV-QKD protocol based on state-discrimination detection.

真空态的噪声方差, $g(g \geqslant 1)$表示 PIA 的增益参数, 用于衡量往返式离散调制 CV-QKD 方案中的非可信信源过噪声 ξ_0的大小[29]. Bob 利用外差探测器对模 B进行测量, 而模 A_0经过非可信信道后转换为模 A_1, Alice 对所接收到的模进行零差探测. 值得一提的是, 在图 2 中, 采用透过率为 η的分束器以及方差为 ν的辅助 EPR 纠缠态来分别模拟 Alice 端实际探测器的量子效率与电噪声. 图 2 中 M_1和 M_2表示辅助 EPR 纠缠态的一对纠缠模, 并且 M_2与 A_2经分束器相互作用后得到模 M_3与 A_3. 当经过非可信信道后, 探测方 Alice 利用分束器将发送过来的模 A_1一分为二, 即模 A_2和模 C. 其中模 A_2(包含大多数光子) 用于进行零差探测, 而模 C(包含少数光子) 则同步发送到态区分探测器中用于提升系统性能. 当 Alice 和 Bob 收集到足够多相关联的数据时, 就可以利用经过认证的公共信道进行参数估计. 最后, 经过信息协商和保密增强, Alice 和 Bob 就可以获得一串共享密钥. 归结于信道输入端的总附加噪声 $\chi_{\text{line}} = 1/T - 1 + \xi$, 其中 T表示信道透过率, ξ表示信道过噪声.

需要指出的是在往返式 CV-QKD 方案中, Fred 由攻击者 Eve 控制, 属于不可信的第三方. 在 EB 方案中采用纠缠态 $|\Phi\rangle_{\text{FB}A_0}$来等价描述 PM 方案中的带噪信源, 纠缠态 $|\Phi\rangle_{\text{FB}A_0}$在往返式 CV-QKD 方案中本质上是双模纠缠态, 其计算方式与传统的双模压缩真空态的计算方式一样. 而当 Fred 是中立的第三方时, 由于 Fred 不受 Eve 控制, 即与 Eve 没有关联, 在这样情况下可认为 Fred 是与 Alice 及 Bob 等价的合法通信方, 则此时纠缠态 $|\Phi\rangle_{\text{FB}A_0}$就变成三模纠缠态[37–39].

基于上述分析, 在 EB 方案中 Fred 制备的纠缠态 $|\Phi\rangle_{\text{FB}A_0}$(为简化分析此处将 $|\Phi\rangle_{\text{FB}A_0}$记为 $|\Phi\rangle$) 其表达式可写为

$$|\Phi\rangle = \sum_{k=0}^{3} \sqrt{\mu_k}\,|\psi_k\rangle\,|\psi_k\rangle = \frac{1}{2}\sum_{k=0}^{3} |\phi_k\rangle\,|\alpha_k^4\rangle\,, \tag{1}$$

其中量子态

$$|\phi_k\rangle = \frac{1}{2}\sum_{n=0}^{3} \mathrm{e}^{\mathrm{i}(1+2k)n\pi/4}|\psi_n\rangle \tag{2}$$

为非高斯态, 其中 $n \in \{0,\ 1,\ 2,\ 3\}$, 并且

$$|\psi_k\rangle = \frac{\mathrm{e}^{-\alpha^2/2}}{\sqrt{\mu_k}} \sum_{m=0}^{\infty} (-1)^m \frac{\alpha^{4m+k}}{\sqrt{(4m+k)!}}|4m+k\rangle, \tag{3}$$

其中 $k \in \{0,\ 1,\ 2,\ 3\}$, 并且

$$\mu_{0,2} = \frac{1}{2\mathrm{e}^{\alpha^2}}\left[\cosh(\alpha^2) \pm \cos(\alpha^2)\right],$$

$$\mu_{1,3} = \frac{1}{2\mathrm{e}^{\alpha^2}}\left[\sinh(\alpha^2) \pm \sin(\alpha^2)\right]. \tag{4}$$

因此, PM 方案中的混合量子态 γ_4的表达式可进一步写成:

$$\gamma_4 = \mathrm{Tr}\left(|\Phi\rangle\langle\Phi|\right) = \sum_{k=0}^{3} \mu_k\,|\psi_k\rangle\langle\psi_k|\,. \tag{5}$$

量子态 $|\Phi\rangle$的协方差矩阵 $\boldsymbol{\Gamma}_4$其表达式可写为

$$\boldsymbol{\Gamma}_4 = \begin{pmatrix} P\boldsymbol{I}_2 & U_4\sigma_z \\ U_4\sigma_z & S\boldsymbol{I}_2 \end{pmatrix}. \tag{6}$$

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

$$P=\langle\Phi|\,1+a_1^{\dagger}a_1\,|\Phi\rangle=1+2\alpha^2,$$

$$S=\langle\Phi|\,1+a_2^{\dagger}a_2\,|\Phi\rangle=1+2\alpha^2,$$

$$U_4=\langle\Phi|\,a_1a_2+a_1^{\dagger}a_2^{\dagger}\,|\Phi\rangle=2\alpha^2\sum_{k=0}^{3}\mu_{k-1}^{3/2}\mu_k^{-1/2}. \quad (7)$$

值得一提的是, 在纠缠模型中, Eve 能够对量子信道进行替换从而可以进行纠缠克隆攻击[40−42]. 在该攻击策略中, Eve 制备方差为 R 的辅助态 $|E\rangle$ 来进行信息窃取, 所替换的量子信道透过率为 T, 并且 Eve 可以通过调整 R 的值来对应匹配真实信道的噪声 $\chi_{\mathrm{line}}=(1-T)/T+\xi$. Eve 将辅助纠缠态 $|E\rangle$ 其中一个模 E_2 注入到分束器其中一个未使用端口, 从而获得模 E_3, 而对另一个模 E_1 进行保留. 当有脉冲经过信道时, Eve 都会重复上述过程, 并将所收集到的辅助模 E_1 和 E_3 用量子存储器进行存储. 最后, 基于 Alice 和 Bob 所公布的经典通信信息, Eve 能够精确测量 E_1 和 E_3 的正交值.

图 1 中制备-测量方案与图 2 中纠缠模型方案两者等价处如下.

1) 图 1 制备-测量方案中, 由于往返式结构 CV-QKD 信源是从 Alice 发送给 Bob, 第三方 Fred 可以对该经典信源进行控制. Bob 在接收到由 Alice 发送的经典光后, 对其进行离散调制, 即从 4 种类型的调制相干态 $\{|\alpha_k^4\rangle=|\alpha\mathrm{e}^{\mathrm{i}\pi(2k+1)/4}\rangle,\ k=0,\ 1,\ 2,\ 3\}$ 中随机选取其中一种, 然后借助于法拉第镜, 经过透过率为 T 并且过噪声为 ξ 的不可信信道反射回 Alice, 这个过程等效为图 2 中 Fred 制备一个方差为 $V=V_B+1$ 的纠缠态 $|\Phi\rangle_{\mathrm{FB}A_0}$(记为 $|\Phi\rangle$), 其中模 B 发送给 Bob, 模 A_0 则经过非可信信道发送给 Alice. Bob 对模 B 进行保留, 并用外差探测进行投影测量 $|\Phi\rangle\langle\Phi|$, 如果 Bob 得到的测量结果为 k, 这就相当于制备了相干态 $|\alpha_k^4\rangle$, 从而实现了往返式离散调制. 此处 $V_B=2\alpha^2$ 即为图 1中制备-测量模型的调制方差.

2) 图 1 中, 在探测方 Alice 处实际探测器的量子效率 η 等效为图 2 中透率为 η 的分束器, 图 1 中实际探测器的电噪声 υ_{el} 则对应于图 2 中方差为 ν 的辅助 EPR 纠缠态其中一模式 M_2 通过分束器后所引入的过噪声. 对于图 1 中制备-测量方案, 探测方 Alice 的输入噪声为 χ_{hom}, 则图 2 中辅助 EPR 纠缠态方差 ν 的选择应满足探测器的总噪声在纠缠模型中同样为 $\eta\chi_{\mathrm{hom}}$, 因此在图 2 纠缠模型中, $\nu=\eta\chi_{\mathrm{hom}}/(1-\eta)=1+\upsilon_{\mathrm{el}}/(1-\eta)$.

综上所述, 图 1 中的制备-测量方案等价于图 2 中纠缠模型方案.

2.3 部署在探测方 Alice 处的非高斯态区分探测器原理

部署在探测方 Alice 处的非高斯态区分探测器原理如图 3 所示. 该量子探测器可以满足在低于标准量子极限 (standard quantum limit, SQL) 错误概率的情况下无条件区分出基于四态离散调制的 4 种非正交相干态. 由图 3 可知, 本方案所采用的态区分探测器能够对相干态 $|\alpha\rangle$ 进行 W 次自适应测量. 对于每次探测 i ($i\in\{0,\ 1,\ \cdots,\ W\}$), 态区分探测器以当前经典寄存器中的数据为基准, 制备一个具有最高概率的预测量子态 $|\delta_i\rangle$, 之后利用位移算符 $D(\delta_i)$ 对相干态 $|\alpha\rangle$ 进行位移变换, 使得 $|\alpha\rangle$ 位移至 $|\alpha-\delta_i\rangle$, 随后采用一个光子数分辨探测器 (photon number resolving detector, PNRD) 对位移场的光子数量进行探测. 假如探测得到 $|\delta_i\rangle=|\alpha\rangle$, 表明预测态是正确的, Λ_0 发生响应, 主要原因是输入场在位移置换的作用下被位移至真空, 因此 PNRD 无法探测到任何光子[32]. 需要指出的是, 此处 Λ_0 响应意味着态区分策略对所输入的量子态进行正确的预测, 预测成功则给定类别标记为 $h_i=0$, 而预测失败类别标记则为 $h_i=1$. 经过 i 次自适应测量后, 该策略根据当前标记集 Ξ_{Hist} 以及预测集 $\hat{\mathrm{X}}_{\mathrm{Hist}}$ 采用贝叶斯推论, 就能计算出所有可能态 $\{|\alpha_{i0}\rangle,\ |\alpha_{i1}\rangle,\ |\alpha_{i2}\rangle,\ |\alpha_{i3}\rangle\}$ 的后验概率. 在下一轮中, 指定具有最高概率的量子态 $|\delta_{i+1}\rangle$ 作为反馈的输入态. 需要指出的是, 在本轮中 δ_i 已被加入到预测集 $\hat{\mathrm{X}}_{\mathrm{Hist}}$, 同其他历史数据一起进行迭代以计算可能态的后验概率. 因此, 根据上述分析可知, 所有可能态的概率在每一个反馈阶段都在进行动态更新, 并且第 i 次反馈的后验概率则会转换为第 $i+1$ 次反馈的先验概率. 贝叶斯推论的规则其表达式可写为

$$P_{\mathrm{po}}(\{|\alpha\rangle\}|\delta_i,\ h_i)=\vartheta\Upsilon(h_i|\delta_i,\ \{|\alpha\rangle\})P_{\mathrm{pr}}(\{|\alpha\rangle\}), \quad (8)$$

其中, $P_{\mathrm{po}}(\{|\alpha\rangle\}|\delta_i,\ h_i)$ 表示后验概率, $P_{\mathrm{pr}}(\{|\alpha\rangle\})$ 表示先验概率, $\Upsilon(h_i|\delta_i,\ \{|\alpha\rangle\})$ 表示对量子态 $|\alpha\rangle$ 进行位移操作后所观测到的结果 h_i 的条件泊松概率, 参数 ϑ 表示标准归一化因子. 由于贝叶斯推论采用

贝叶斯定理来对假设的概率进行更新, 属于统计推论的一种方法, 所给的信息越充分, 推论也就越准确. 因此, 输入态$|\alpha\rangle$在经过W次自适应测量后, 能够由第$W+1$的预测态$|\delta_{W+1}\rangle$所决定[34].

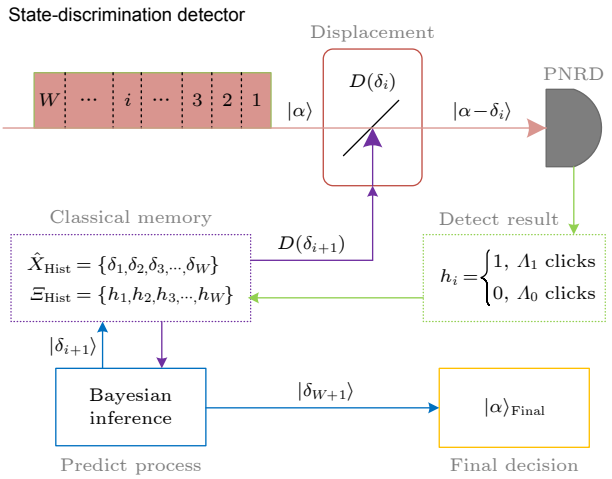

图 3 非高斯态区分探测器原理图. PNRD 为光子数分辨探测器

Fig. 3. Schematic diagram of non-Gaussian state discrimination detector. PNRD, photon-number-resolving detector.

从数学的角度考虑, 标准量子极限区分采用QPSK 调制的非正交相干态, 其失败概率的表达式可写为

$$P_{\rm SQL}=1-\left[1-\frac{1}{2}\mathrm{erfc}\left(\sqrt{|\alpha|^2/2}\right)\right]^2, \tag{9}$$

其中$\mathrm{erfc}(x)=\dfrac{2}{\sqrt{\pi}}\displaystyle\int_x^{\infty}\mathrm{e}^{-t^2}\mathrm{d}t$. 对基于 QPSK 调制的信号而言, 可以采用平方根 (SRM) 测量来对 Helstrom 界进行估算, 其表达式可写为

$$P_{\rm Hel}=1-\frac{1}{16}\left(\sum_{n=1}^{4}\sqrt{\kappa_n}\right)^2, \tag{10}$$

其中

$$\kappa_n=\mathrm{e}^{-\alpha^2}\sum_{s=1}^{4}\exp\left[(1-n)\frac{2\pi\,\mathrm{i}s}{4}+\alpha^2\exp\left(\frac{2\pi\,\mathrm{i}s}{4}\right)\right], \tag{11}$$

表示 QPSK 信号 Gram 矩阵的特征值. 由于在往返式方案中, Alice 为探测方, 并且执行零差探测, 因此在所提出的方案中将非高斯态区分探测器与零差探测器并行部署在探测方 Alice 处. 基于此, 量子态的探测结果由零差探测器与非高斯态区分探测器共同决定. 此处, 为了更好地描述态区分探测器对往返式离散调制 CV-QKD 方案性能的提升效果, 可定义一个参数, 即提升因子Ω, 其表达式可写为[36]

$$\Omega=\frac{1-P_{\rm r}^{W}}{1-P_{\rm SQL}}, \tag{12}$$

其中, $P_{\rm r}^{W}$表示W次自适应测量下非高斯态区分探测器测量错误的概率. 从理论角度来分析, 当自适应测量的次数W足够大时, 态区分探测器能够达到 Helstrom 界. 由上述分析可知, 在量子力学所允许的最小错误概率下, 我们可以通过计算得到最优的提升因子$\Omega_{\rm opt}$, 即

$$\Omega_{\rm opt}=\frac{1-P_{\rm Hel}}{1-P_{\rm SQL}}. \tag{13}$$

3 方案安全性分析

本节在渐近情况[43]以及有限长效应情况[44]下对基于非高斯态区分探测器的往返式离散调制 CV-QKD 方案进行安全性分析.

3.1 方案的渐近安全性

此处主要考虑反向协商下方案的渐近密钥率, 并且为了简化分析, 主要考虑探测端 Alice 执行零差探测的情况. 为了获得更加紧的安全界限, 本方案假定第三方 Fred 由攻击者 Eve 控制, 则所提出方案的渐近密钥率其表达式可写为

$$K_{\rm asy}=\beta I^{o}(A:B)-\chi(A:E), \tag{14}$$

其中$I^{o}(A:B)=\Omega_{\rm opt}I(A:B)$表示引入非高斯态区分探测器的往返式离散调制 CV-QKD 方案中 Alice 与 Bob 的互信息量, $I(A:B)$表示未引入非高斯态区分探测器的原始方案中 Alice 与 Bob 的互信息量, 参数β表示方案的协商效率, $\Omega_{\rm opt}$表示所采用的非高斯态区分探测器的最优提升因子, $\chi(A:E)$表示 Eve 从 Alice 密钥中所窃取的信息量 Holevo 界. 此处将光纤的衰减系数设为ς, 则光纤透过率的表达式$T=10^{-\varsigma L/10}$, 其中L表示光纤长度. 原始方案中 Alice 与 Bob 的互信息量$I(A:B)$的表达式可写为

$$\begin{aligned}I(A:B)&=\frac{1}{2}\log_2\left(\frac{V+\chi_{\rm tot}+\xi_0}{1+\chi_{\rm tot}+\xi_0}\right)\\&=\frac{1}{2}\log_2\left(1+\frac{V_B}{1+\chi_{\rm tot}+\xi_0}\right)\\&=\frac{1}{2}\log_2(1+R_{\rm SN}),\end{aligned} \tag{15}$$

其中$V=V_B+1$, $R_{\rm SN}$表示原始方案信噪比 (SNR). 在所提出的方案中, 由于引入了非高斯态区分探测器, 则互信息量$I^o(A:B)=\Omega_{\rm opt}I(A:B)=\dfrac{1}{2}\log_2(1+R^o_{\rm SN})$, 其中$R^o_{\rm SN}$表示所提出方案的信噪比 (SNR^o), 经过进一步推导可得

$$1+R^o_{\rm SN}=2^{2I^o(A:B)}, \tag{16}$$

则所提出方案的信噪比$R^o_{\rm SN}$的表达式可写为

$$R^o_{\rm SN}=2^{2I^o(A:B)}-1=2^{2\Omega_{\rm opt}I(A:B)}-1. \tag{17}$$

接下来计算 Alice 共扼零差探测器的加性噪声归结到信道输入端, 其表达式可写为

$$\chi_{\rm hom}=[(1-\eta)+\upsilon_{\rm el}]/\eta, \tag{18}$$

其中, 参数η和$\upsilon_{\rm el}$分别表示 Alice 探测器的量子效率以及探测器电噪声方差.

由于信道加性噪声归结到输入端$\chi_{\rm line}=1/T-1+\xi$, 其中$\xi$表示非可信信道的过噪声[25]. 则归结到信道输入端的总噪声其表达式可写为

$$\chi_{\rm tot}=\chi_{\rm line}+\chi_{\rm hom}/T. \tag{19}$$

为了计算参数$\chi(A:E)$, 此处假定 Eve 无法对 Alice 系统中的不完美器件进行攻击. 该噪声评估模型已经被广泛应用于 CV-QKD 实验中[15,19,28,29]. 基于此种噪声评估模型, Eve 和 Alice 之间互信息量的 Holevo 界$\chi(A:E)$的表达式可写为

$$\chi(A:E)=\sum_{j=1}^{2}G\left(\frac{\lambda_j-1}{2}\right)-\sum_{j=3}^{5}G\left(\frac{\lambda_j-1}{2}\right), \tag{20}$$

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

$$\lambda^2_{1,2}=\frac{1}{2}\left(\Delta\pm\sqrt{\Delta^2-4D}\right), \tag{21}$$

其中

$$\begin{aligned}\Delta&=V^2+T^2(V+\chi_{\rm line}+\xi_0)^2-2TU_4^2,\\ D&=\left[TV^2+TV\left(\chi_{\rm line}+\xi_0\right)-TU_4^2\right]^2.\end{aligned} \tag{22}$$

而$\lambda_{3,4}$表达式可写为

$$\lambda^2_{3,4}=\frac{1}{2}\left(A\pm\sqrt{A^2-4B}\right), \tag{23}$$

其中

$$\begin{aligned}A=&\frac{1}{T(V+\chi_{\rm tot}+\xi_0)}[\Delta\chi_{\rm hom}+V\sqrt{D}\\&+T\left(V+\chi_{\rm line}+\xi_0\right)],\\ B=&\frac{\sqrt{D}V+D\chi_{\rm hom}}{T(V+\chi_{\rm tot}+\xi_0)},\quad \lambda_5=1.\end{aligned} \tag{24}$$

接下来分析基于非高斯态区分探测的往返式离散调制 CV-QKD 方案在渐近情况下的方案性能. 涉及的仿真系统参数分别设定为$V_B=0.35$, $\eta=0.6$, $\upsilon_{\rm el}=0.05$. 所提出方案的渐近密钥率与传输距离在不同增益参数$g=1,1.003,1.005,1.01$下的关系如图 4 所示, 其中协商效率$\beta=0.8$. 此处g值的大小用于衡量非可信信源噪声的强弱, 即g值越大, 方案的非可信信源噪声强度越高. 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[45]. 图 4 中实线表示原始往返式离散调制 CV-QKD 方案的性能曲线, 而虚线则表示所提出的基于非高斯态区分探测的往返式离散调制 CV-QKD 方案的性能曲线. 由图 4 可以观察到, 无论是在理想信源的情况 ($g=1$, 不存在信源噪声) 还是在实际信源的情况 ($g>1$, 存在非可信信源噪声) 下, 所提出的方案性能始终优于原始方案的性能. 即使在实际信源的情况下 ($g>1$), 所提出的方案其渐近密钥率与安全传输距离仍然显著优于原始方案的渐近密钥率与安全传输距离, 并且所提出方案的性能更接近 PLOB 界. 比如当$g=1.005$时, 所提出方案的安全传输距离为 90.8 km(绿色虚线), 而原始方案的最大传输距离则不足 50 km(绿色实线). 这表明所提出的方案能够有效抵御往返式系统中非可信信源噪声对其性能产生的负面影响, 相比于原始方案, 受非可信信源噪声的影响更小.

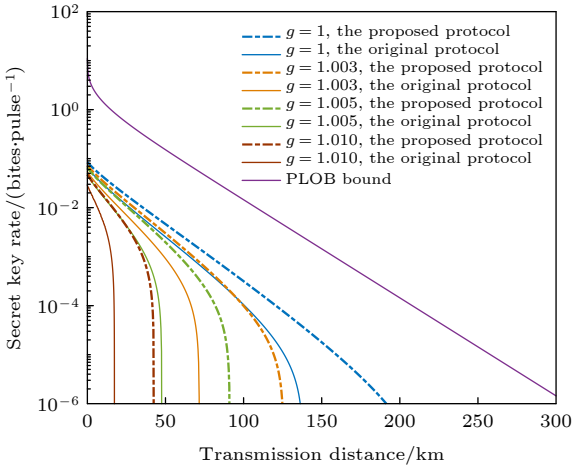

图 4 不同增益参数g下基于非高斯态区分探测的往返式离散调制 CV-QKD 方案的渐近密钥率和传输距离的关系

Fig. 4. The relationship between the asymptotic secret key rate of plug-and-play discrete modulation CV-QKD protocol based on non-Gaussian state-discrimination detection and the transmission distance under different gain g.

图 5 给出了所提出方案的渐近密钥率与协商效率β在实际信源($g=1.005$)以及不同的传输距离L=40, 50, 60, 70 km 下的关系. 图中虚线表示所提出方案的性能曲线, 实线表示原始方案的性能曲线. 从图 5 可以观察到, 对于所提出的方案, 协商效率β的可使用范围随着传输距离的增大而减小. 相比于原始方案, 本文所提出的方案在相同的传输距离以及协商效率下, 其渐近密钥率始终高于原始方案的渐近密钥率. 比如当传输距离L=40 km 以及协商效率$\beta=0.8$, 所提出方案的渐近密钥率为 0.004 bit/pulse, 而原始方案的渐近密钥率仅为 0.00066 bit/pulse. 不仅如此, 所提出方案其协商效率β的可使用范围显著大于原始方案中协商效率β的可使用范围. 比如在L=40 km 的情况下, 所提出方案的协商效率β的可使用范围为 [0.65, 1], 而原始方案协商效率β的可使用范围仅为 [0.775, 1].

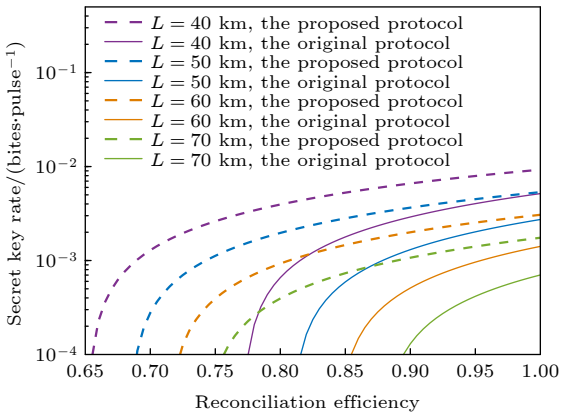

图 5 在实际信源($g=1.005$)与不同传输距离L下, 基于非高斯态区分探测的往返式离散调制 CV-QKD 方案的渐近密钥率与协商效率的关系

Fig. 5. The relationship between the asymptotic secret key rate of plug-and-play discrete modulation CV-QKD protocol based on non-Gaussian state-discrimination detection and the reconciliation efficiency under practical source($g=1.005$) and different transmission distance L.

图 6 给出了有无态区分探测器时, 信噪比随不同信源条件 (增益参数 g 的不同) 的变化曲线. 从图 6 中可以发现在相同传输距离下, 是否采用态区分探测, 信噪比是存在差异的, 即引入非高斯态区分探测器的方案 (本文所提出的方案), 其信噪比 (实线) 高于没有引入非高斯态区分探测器的方案 (称为原始方案) 的信噪比 (虚线), 并且随着增益参数 g 的增大, 信噪比逐渐降低. 而由图 5 可知, 所提出方案其协商效率的可使用范围显著大于原始方案中协商效率的可使用范围. 主要原因在于所提出的方案的互信息量 $I^o(A:B)$要大于原始方案的互信息量$I(A:B)$, 而根据 (17) 式可知, 互信息量的增大使得本文所提出方案的信噪比SNR^{o}大于原始方案的信噪比 SNR , 因此信噪比的变化使得所提出方案的协商效率与原始方案的协商效率适用范围不同.

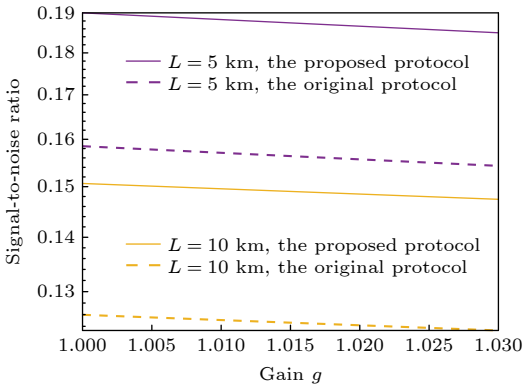

图 6 不同传输距离下 L, 基于非高斯态区分探测的往返式离散调制 CV-QKD 方案的信噪比与增益参数 g (不同的信源条件) 的关系

Fig. 6. The relationship between the signal-to-noise ratio of plug-and-play discrete modulation CV-QKD protocol based on non-Gaussian state-discrimination detection and the gain g (different source conditions) under different transmission distance L.

3.2 有限长效应情况下方案的安全性

在上述渐近安全性分析中, 对所提出的基于非高斯态区分探测的往返式离散调制 CV-QKD 方案渐近密钥率计算的前提是假定 Alice 和 Bob 可以采用无限多的信号进行互换交流. 然而这在实验中是无法实现的, 主要原因是实际安全密钥的长度是有限的. 因此有必要考虑有限长效应情况下所提出方案的安全性. 则反向协商下所提出方案的有限长密钥率计算公式为[44]

$$K_{\rm fin}=\frac{f}{F}\left[\beta\Omega_{\rm opt}I(A:B)-\chi_{\varepsilon_{\rm PE}}(A:E)-\Delta(f)\right], \quad (25)$$

其中$I(A:B)$, β以及$\Omega_{\rm opt}$的定义在上述分析中已给出. F表示所采集到的有效数据总长度, f表示 Alice 和 Bob 生成最终密钥所需的数据量长度, $Q=F-f$表示方案参数估计所需的数据量长度, $\varepsilon_{\rm PE}$表示参数估计失败的概率, $\Delta(f)$则和保密增强相关联, 其表达式可写为

$$\Delta(f)=(2\dim H_{\rm A}+3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{f}}+\frac{2}{f}\log_2\frac{1}{\varepsilon_{\rm PB}}, \quad (26)$$

其中 $H_{\rm A}$ 表示与 Alice 原始密钥相对应的 Hilbert 空间, $\bar{\varepsilon}$ 表示平滑参数, $\varepsilon_{\rm PB}$ 表示保密增强失败的概率. 由于原始密钥是基于二进制比特来进行编码, 因此 $\dim H_{\rm A}=2$.

在有限长效应情形下, $\chi_{\varepsilon_{\rm PE}}(A:E)$ 需要在参数估计过程中进行计算得到. 为了得到 $\chi_{\varepsilon_{\rm PE}}(A:E)$, 可以在该过程中寻找一个能够使所提出方案密钥率最小化的协方差矩阵 $\boldsymbol{\Theta}_{\varepsilon_{\rm PE}}$, 最小化成功的概率为 $1-\varepsilon_{\rm PE}$. 值得一提的是, 协方差矩阵 $\boldsymbol{\Theta}_{\varepsilon_{\rm PE}}$ 可由 Q 对相关联的变量对 $(x_i,\,y_i)_{i=1,2,\cdots,Q}$ 计算得到. 可以采用如下线性模型对这些相关联的变量对进行分析, 即

$$y=tx+z, \tag{27}$$

其中参数 $t=\sqrt{T}$ 并且 z 服从均值为 0, 方差为 $\varpi^2=1+T(\xi+\xi_0)$ 的正态分布. 则协方差矩阵 $\boldsymbol{\Theta}_{\varepsilon_{\rm PE}}$ 的表达式为

$$\boldsymbol{\Theta}_{\varepsilon_{\rm PE}}=\begin{bmatrix}(V_{\rm B}+1)I_2 & t_{\min}U_4\sigma_z\\ t_{\min}U_4\sigma_z & \left(t_{\min}^2V_B+\varpi_{\max}^2\right)I_2\end{bmatrix}, \tag{28}$$

此处 $t_{\min}$ 与 $\varpi_{\max}^2$ 分别表示参数 t 与 ϖ^2 的最小值与最大值. (28) 式中极大似然估计 $\hat{t}$ 与 $\hat{\varpi}^2$ 分别为

$$\hat{t}=\frac{\sum_{i=1}^{Q}x_iy_i}{\sum_{i=1}^{Q}x_i^2},\quad \hat{\varpi}^2=\frac{1}{Q}\sum_{i=1}^{Q}\left(y_i-\hat{t}x_i\right)^2. \tag{29}$$

并且极大似然估计 $\hat{t}$ 与 $\hat{\varpi}^2$ 分别服从如下分布:

$$\hat{t}\sim N\left(t,\ \frac{\varpi^2}{\sum_{i=1}^{Q}x_i^2}\right),\quad \frac{Q\hat{\varpi}^2}{\varpi^2}\sim\chi^2(Q-1). \tag{30}$$

由 (27) 式可知, $\hat{t}$ 与 $\hat{\varpi}^2$ 相互独立. 则 $t_{\min}$ 与 $\varpi_{\max}^2$ 的表达式分别为

$$\begin{aligned}t_{\min}&\approx\hat{t}-z_{\varepsilon_{\rm PE}/2}\sqrt{\frac{\hat{\varpi}^2}{QV_{\rm B}}},\\ \varpi_{\max}^2&\approx\hat{\varpi}^2+z_{\varepsilon_{\rm PE}/2}\frac{\sqrt{2}\hat{\varpi}^2}{\sqrt{Q}}.\end{aligned} \tag{31}$$

其中借助于 $1-{\rm erf}\left(z_{\varepsilon_{\rm PE}/2}/\sqrt{2}\right)/2=\varepsilon_{\rm PE}/2$ 可推导出 $z_{\varepsilon_{\rm PE}/2}$, ${\rm erf}(x)=\dfrac{2}{\sqrt{\pi}}\displaystyle\int_0^x{\rm e}^{-t^2}{\rm d}t$ 表示误差函数. $\hat{t}$ 与 $\hat{\varpi}^2$ 的数学期望表达式分别为 $E\left[\hat{t}\right]=\sqrt{T}$, $E\left[\hat{\varpi}^2\right]=1+T(\xi+\xi_0)$, 则 $t_{\min}$ 与 $\varpi_{\max}^2$ 可分别通过下式进行计算:

$$\begin{aligned}t_{\min}&\approx\sqrt{T}-z_{\varepsilon_{\rm PE}/2}\sqrt{\frac{1+T(\xi+\xi_0)}{QV_{\rm B}}},\\ \varpi_{\max}^2&\approx1+T(\xi+\xi_0)+z_{\varepsilon_{\rm PE}/2}\frac{\sqrt{2}\left[1+T(\xi+\xi_0)\right]}{\sqrt{Q}}.\end{aligned} \tag{32}$$

对于参数 $\bar{\varepsilon}$, $\varepsilon_{\rm PE}$ 以及 $\varepsilon_{\rm PB}$, 三者的值可设定为[44]

$$\bar{\varepsilon}=\varepsilon_{\rm PE}=\varepsilon_{\rm PB}=10^{-10}. \tag{33}$$

由 (32) 式可计算 (25) 式中有限长效应影响下所提出方案的密钥率.

接下来分析所提出的基于非高斯态区分探测的往返式离散调制 CV-QKD 在有限长效应情况下方案的性能. 涉及全局的仿真系统参数与渐近情情况下所采用的仿真系统参数一致. 图 7 给出了在不同的有效数据总长度 $F=10^8,10^9,10^{10}$ 下所提出方案的有限长密钥率与传输距离的关系, 并且也给出 PLOB 界. 图 7(a)—(d) 分别对应不同强度的非可信信源噪声, 即 $g=1,1.003,1.005,1.01$. 在图 7(a)—(d) 中也给出了渐近密钥率曲线以及 PLOB 界, 用于参照对比. 结合图 7(a)—(d) 可以发现, 所提出方案的渐近密钥率 (蓝色虚线) 总是高于其有限长密钥率, 然而随着 F 的增大, 所提出方案的有限长密钥率曲线逐渐趋近于渐近密钥率曲线以及 PLOB 界. 此外, 即使考虑有限长效应情况, 所提出的方案其性能 (虚线) 无论是在理想信源的情况 ($g=1$, 图 7(a)) 还是在实际信源的情况 ($g>1$, 图 7(b)—(d)) 始终都要优于原始方案的性能 (实线). 这表明所提出的基于非高斯态区分探测往返式离散调制 CV-QKD 能有效降低有限长效应, 以及系统信源噪声对方案性能的负面影响.

4 结 论

本文提出了一种基于非高斯态区分探测的往返式离散调制 CV-QKD 方案, 通过在探测方 Alice 处部署非高斯态区分探测器, 在满足低于标准量子极限错误概率的情况下无条件区分出基于四态离散调制的 4 种非正交相干态, 从而能够有效弥补往返式光路结构中非可信信源噪声对方案性能的负面影响. 此外, 对所提出的方案进行安全性分析, 不仅考虑了其渐近安全性, 同时也对有限长效应情况下方案的安全性进行分析, 使得所获得的结果更符合实际情况. 仿真结果表明本文所提出的基于非高斯态区分探测的往返式离散调制 CV-

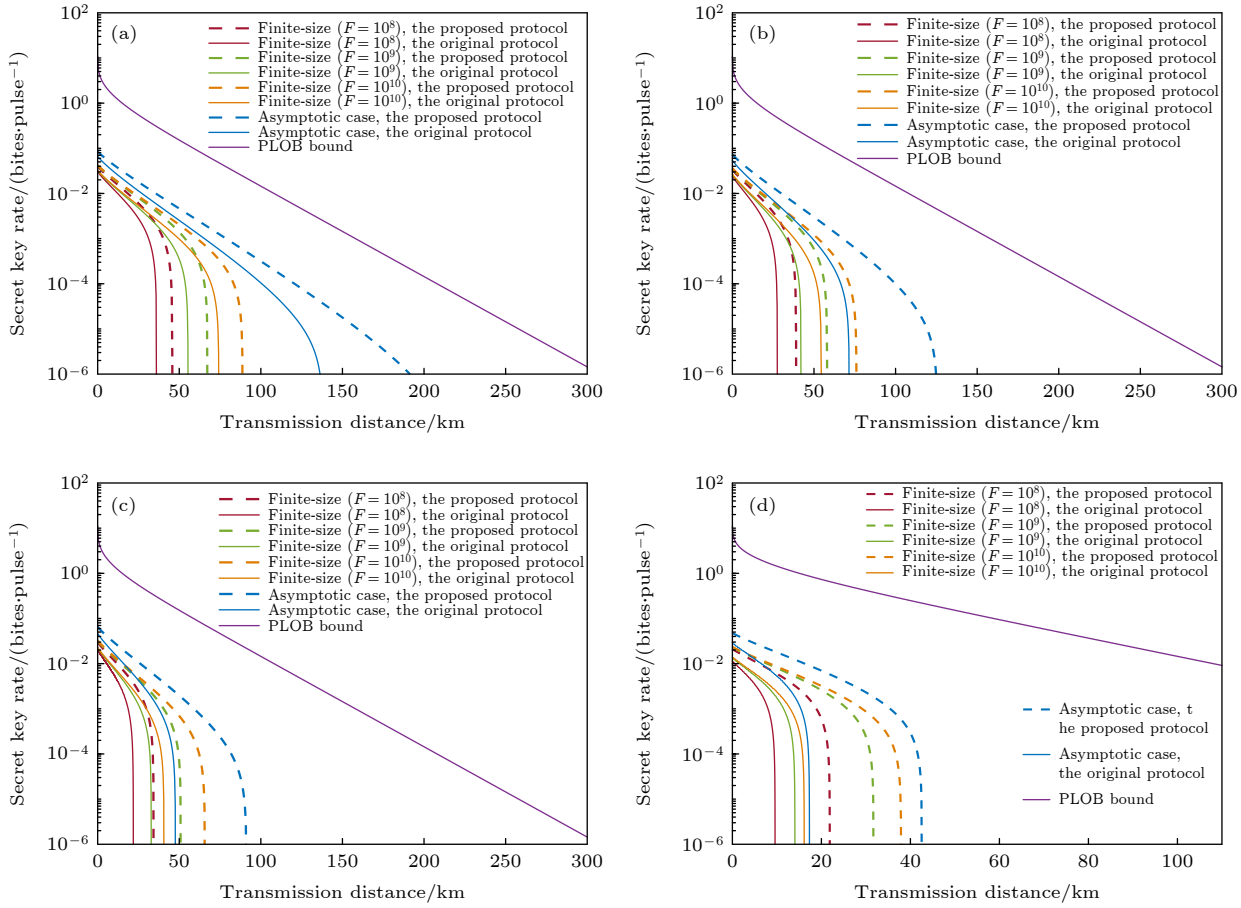

图 7 在不同的有效数据总长度 F 下基于非高斯态区分探测的往返式离散调制 CV-QKD 方案有限长密钥率与传输距离的关系 (a) $g=1$; (b) $g=1.003$; (c) $g=1.005$; (d) $g=1.01$

Fig. 7. The relationship between the finite-size secret key rate of plug-and-play discrete modulation CV-QKD protocol based on non-Gaussian state-discrimination detection and the transmission distance under different total exchanged signals F: (a) $g=1$; (b) $g=1.003$; (c) $g=1.005$; (d) $g=1.01$.

QKD 方案相比原始方案, 无论是在理相信源情况 ($g=1$)、实际信源情况 ($g>1$) 还是有限长效应情况, 其性能都有明显的提升. 不仅如此, 本文所提出的方案其协商效率 β 的可使用范围显著大于原始方案中协商效率 β 的可使用范围. 这表明所提出的基于非高斯态区分探测往返式离散调制 CV-QKD 方案能够有效降低有限长效应以及系统信源噪声对方案性能的负面影响. 因此本文所提出的方案在保证系统实际安全性的同时能够实现更高效、更远传输距离的量子密钥分发.

参考文献

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

[2] Pirandola S, Andersen U L, Banchi L, et al. 2020 *Adv. Opt. Photon.* **12** 1012

[3] Liu H, Jiang C, Zhu H T, et al. 2021 *Phys. Rev. Lett.* **126** 250502

[4] Lo H K, Chau H F 1999 *Science* **283** 2050

[5] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[6] Yin J, Li Y H, Liao S K, et al. 2020 *Nature* **582** 501

[7] Fang X T, Zeng P, Liu H, et al. 2020 *Nat. Photonics* **14** 422

[8] Chen J P, Zhang C, Liu Y, et al. 2021 *Nat. Photonics* **15** 570

[9] 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

[10] Wu X D, Wang Y J, Huang D, Guo Y 2020 *Front. Phys.* **15** 31601

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

[12] 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]

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

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

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

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

[17] 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

[18] Huang D, Huang P, Li H, Wang T, Zhou Y, Zeng G 2016 *Opt. Lett.* **41** 3511
[19] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **88** 022339
[20] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **87** 052309
[21] Jouguet P, Kunz-Jacques S, Diamanti E 2013 *Phys. Rev. A* **87** 062313
[22] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325
[23] Qi B, Lougovski P, Pooser R, Grice W, Bobrek M 2015 *Phys. Rev. X* **5** 041009
[24] Soh D B S, Brif C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J, Sarovar M 2015 *Phys. Rev. X* **5** 041010
[25] Huang D, Lin D K, Huang P, Zeng G H 2015 *Opt. Lett.* **40** 3695
[26] Marie A, Alléaume R 2017 *Phys. Rev. A* **95** 012316
[27] Wang T, Huang P, Zhou Y, Liu W, Zeng G 2018 *Phys. Rev. A* **97** 012310
[28] Wu X, Wang Y, Guo Y, Zhong H, Huang D 2021 *Phys. Rev. A* **103** 032604
[29] Huang D, Huang P, Wang T, Li H, Zhou Y, Zeng G 2016 *Phys. Rev. A* **94** 032305
[30] Silberhorn C, Ralph T C, Lütkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
[31] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[32] Becerra F E, Fan J, Baumgartner G, Goldhar J, Kosloski J T, Migdall A 2013 *Nat. Photonics* **7** 147
[33] Becerra F E, Fan J, Migdall A 2013 *Nat. Commun.* **4** 2028
[34] Becerra F E, Fan J, Baumgartner G, Polyakov S V, Goldhar J, Kosloski J T, Migdall A 2011 *Phys. Rev. A* **84** 062324
[35] Helstrom C W 1976 *Quantum Detection and Estimation Theory (Mathematics in Science and Engineering)* (Vol. 123) (New York: Academic)
[36] Liao Q, Guo Y, Huang D, Huang P, Zeng G 2018 *New J. Phys.* **20** 023015
[37] Shen Y, Peng X, Yang J, Guo H 2011 *Phys. Rev. A* **83** 052304
[38] Wu X D, Wang Y J, Zhong H, Liao Q, Guo Y 2019 *Front. Phys.* **14** 41501
[39] Wu X, Wang Y, Zhong H, Ye W, Huang D, Guo Y 2020 *Quantum Inf. Process.* **19** 234
[40] Navascués M, Acín A 2005 *Phys. Rev. Lett.* **94** 020505
[41] García-Patrón R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[42] Pirandola S, Braunstein S L, Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504
[43] Renner R, Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[44] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343
[45] Pirandola S, Laurenza R, Ottaviani C, Banchi L 2017 *Nat. Commun.* **8** 15043

Plug-and-play discrete modulation continuous variable quantum key distribution based on non-Gaussian state-discrimination detection*

Wu Xiao-Dong [1)] Huang Duan [2)†]

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

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

(Received 25 November 2022; revised manuscript received 23 December 2022)

Abstract

Plug-and-play discrete modulation continuous variable quantum key distribution can generate local oscillator light locally without using two independent lasers, and both signal light and local oscillator are generated from the same laser, which can effectively ensure the practical security of the system and have a completely identical frequency characteristic. In addition, this scheme has good compatibility with efficient error correction codes, and can achieve high reconciliation efficiency even at low signal-to-noise ratio. However, there exists large excess noise in the plug-and-play configuration based on the untrusted source model, which seriously limits the maximum transmission distance of the discrete modulation scheme. To solve this problem, we propose a plug-and-play discrete modulation continuous variable quantum key distribution based on non-Gaussian state-discrimination detection. That is to say, a non-Gaussian state-discrimination detector is deployed at the receiver. With adaptive measurement method and Bayesian inference, four non-orthogonal coherent states which are based on four-state discrete modulation can be unconditionally distinguished on condition that the error probability is lower than the standard quantum limit. We analyze the security of the proposed protocol by considering both asymptotic limit and finite-size effect. Simulation results show that the secret key rate and maximum transmission distance are significantly enhanced by using no-Gaussian state-discrimination detection even under the influence of the untrusted source noise compared with the original plug-and-play discrete modulation continuous variable quantum key distribution. These results indicate that the proposed scheme can effectively reduce the negative influence of the untrust source noise on the performance of the plug-and-play discrete modulation continuous variable quantum key distribution protocol. The proposed protocol can not only ensure the practical security of the system, but also achieve more efficient and longer transmission distance quantum key distribution.

Keywords: plug-and-play, discrete modulation, continuous variable quantum key distribution, non-Gaussian state-discrimination detection

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.72.20222253

* 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

基于非高斯态区分探测的往返式离散调制连续变量量子密钥分发方案

吴晓东　黄端

Plug-and-play discrete modulation continuous variable quantum key distribution based on non-Gaussian state-discrimination detection

Wu Xiao-Dong　Huang Duan

引用信息 Citation: Acta Physica Sinica, 72, 050303 (2023)　DOI: 10.7498/aps.72.20222253
在线阅读 View online: https://doi.org/10.7498/aps.72.20222253
当期内容 View table of contents: http://wulixb.iphy.ac.cn