基于量子催化的离散调制连续变量量子密钥分发*

叶炜[1)] 郭迎[1)†] 夏莹[2)] 钟海[1)] 张欢[2)] 丁建枝[1)] 胡利云[2)‡]

1) (中南大学计算机学院, 长沙 410083)

2) (江西师范大学量子科学与技术中心, 南昌 330022)

(2019 年 11 月 4 日收到; 2019 年 11 月 30 日收到修改稿)

相比于离散变量量子密钥分发, 连续变量量子密钥分发虽然具备更高的安全码率等优势, 但是在安全传输距离上却略有不足. 尽管量子催化的运用对高斯调制连续变量量子密钥分发协议的性能, 尤其在安全传输距离方面有着显著的提升, 然而能否用来改善离散调制协议的性能却仍然未知. 鉴于上述分析, 本文提出了一种基于量子催化的离散调制协议的方案, 试图在安全密钥率、安全传输距离和最大可容忍过噪声方面进一步提升协议性能. 研究结果表明, 在相同参数下, 当优化量子催化引入的透射率 T, 相比于原始四态调制协议, 所提方案能够有效地提升量子密钥分发的性能. 特别是, 对于可容忍过噪声为 0.002, 量子催化可将安全通信距离突破 300 km, 密钥率为 10^{-8} bits/pulse, 而过大的可容忍噪声会抑制量子催化对协议性能的改善效果. 此外, 为了彰显量子催化的优势, 本文给出了点对点量子通信的最终极限 Pirandola-Laurenza-Ottaviani-Banchi 边界, 仿真结果表明, 虽然原始方案与所提方案都未能突破这种边界, 但是相比于前者, 后者能够在远距离通信上逼近于这种边界, 这为实现全球量子安全通信的最终目标提供理论依据.

关键词: 连续变量, 量子密钥分发, 离散调制, 量子催化

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20191689

1 引 言

量子密钥分发[1−4]旨在通过不安全信道建立起合法通信双方的密钥, 它的无条件安全源于海森伯不确定性关系和不可克隆原理, 使得它在商业金融、国防军事、外交通信等安全领域发挥着重要作用. 近几十年来, 量子密钥分发在量子信息领域中蓬勃发展, 它主要分为两大类: 离散变量量子密钥分发[1,2]和连续变量量子密钥分发[3,4]. 对于离散变量量子密钥分发, 单光子极化被常用来传输密钥比特信息, 使得它具有长距离安全通信的特征. 但是单光子探测器的使用造成了离散变量量子密钥分发的密钥率相对较低. 不同于前者, 在连续变量量子密钥分发中, 信息被发送端 Alice 编码到相干态或压缩态的正则坐标和正则动量上, 经信道传输后, 接收端 Bob 通过相干探测进行信息的解码. 虽然连续变量量子密钥分发具有高密钥率和易与传统光纤技术相容等优势, 但它的通信距离仍然存在局限性. 例如, 2002 年 Grosshans 和 Grangier[5] 提出的高斯调制“GG02”协议. 该协议虽然采用常见的相干态进行信息的编码, 使得它具有很好的实用价值, 但是其传输距离不超过 15 km. 同年, Silberhorn 等[6] 采用的逆向协商协议打破了这种安全距离的局限性, 进一步提升了该协议的实用性. 2007 年, Lodewyck 等[7] 实验上报道了在全光纤连续变

* 国家自然科学基金 (批准号: 61572529, 61821407, 11964013, 11664017)、江西省主要学科学术和技术带头人培养计划、湖南省研究生科研创新项目 (批准号: CX20190126) 和中南大学研究生自主探索创新项目 (批准号: 2019zzts070) 资助的课题.

† 通信作者. E-mail: yingguo@csu.edu.cn

‡ 通信作者. E-mail: hlyun2008@126.com

量系统下, 量子密钥在 25 km 的分布情况. 因此, 如何有效地提升量子密钥分发性能, 尤其是安全通信距离, 成为了连续变量量子通信的前沿热点之一.

为了实现长距离安全通信的目标, 人们提出了两种解决方案. 一种解决方案是通过引入非高斯操作[8–10]来提高量子态的抗噪能力, 使得信息保持稳定传输; 另一种方案则是采用离散调制协议[11–14], 如四态协议、八态协议等. 例如, 2013 年 Huang 等[15]将光子扣除操作运用到连续变量量子密钥分发系统. 研究表明, 这种操作的使用能够显著地提高安全传输距离和最大可容忍过噪声. 尤其是, 单光子扣除情况对协议性能改善最为明显. 不幸的是, 光子扣除操作需要多光子探测器, 加大了实验操作的复杂性. 为了解决这个问题, 2016 年 Li 等[16]指出了光子扣除操作可等效于一种虚拟后处理方案. 此外, 除了单路协议外, 光子扣除操作在双路协议[17]、测量设备无关协议[18]发挥着显著的性能优势. 另一方面, 由于存在一种对离散值甚至低信噪比都具有高效率的纠错码, 离散调制协议可以极大地提高安全距离[11,12]. 在安全性分析方面, 该协议也对应于低调制方差的高斯调制的连续变量量子密钥分发协议[13,14]. 最近, Liao 等[19]将光子扣除操作运用于四态离散调制协议进一步提升量子密钥分发的性能. 尽管光子扣除有上述优势, 但是在优化调制方差的情况下, 执行减光子操作的成功概率却低于 0.25, 这使得它在提升量子密钥分发性能方面也存在某种缺陷[20]. 为了克服这种缺陷, 量子催化操作[21,22]是一种可行的和较为成功的方案. 在催化过程中, 辅助模的光子似乎看起来没有变化, 但是却能够促进主通道模之间的量子态转换, 从而避免了通信双方的信息量丢失. 最近, 这种量子催化被应用于传统的高斯调制协议[20,23]. 特别是, 在零光子催化的情况下, 它不仅能展现出较高的成功概率, 还能在连续变量量子密钥分发性能上优于光子扣除操作的情况.

基于量子催化的使用优势, 本文提出了一种离散调制连续变量量子密钥分发方案, 主要关注量子催化用来改善离散调制协议的性能. 具体安排如下: 第 2 节阐述离散调制协议和量子催化, 其一是简要回顾离散调制协议的纠缠模型, 同时给出四态协议在集体攻击下的渐近密钥率, 其二是将量子催化运用于离散调制协议中, 导出零光子催化对输入-输出量子态之间的作用; 第 3 节详细地讨论和分析不同参数下量子催化对离散调制协议的性能影响; 最后, 第 4 节是本文的主要结论.

2 离散调制协议和量子催化

首先从纠缠型的视角来回顾离散调制协议, 尤其是传统的四态调制协议, 同时给出该协议在集体攻击下的渐近密钥率计算. 随后, 将量子催化运用于离散调制协议中, 具体地分析零光子催化对信息载体的贡献, 并导出量子态输入-输出的关系.

2.1 四态调制协议

在标准的制备-测量型四态调制协议中, Alice 通过采用高斯调制器制备和调制出一个四进制的相干态 $\{|\alpha_k\rangle = |\alpha \mathrm{e}^{\mathrm{i}\pi(2k+1)/4}\rangle,\ k=0,\ 1,\ 2,\ 3\}$, 并且通过高斯信道发送给 Bob. 当 Bob 接收量子态 $\{|\alpha_k\rangle,\ k=0,\ 1,\ 2,\ 3\}$后, 对其正交分量 ($x$ 和 p) 进行零差探测或者外差探测. 最后, 经过经典后处理, Alice 和 Bob 共享一串密钥.

虽然制备-测量型协议易于实际操作, 但是在安全性能分析方面却显得无能为力. 为此, Leverrier 和 Grangier[11]提出了一种纠缠型四态调制协议, 正如图 1 所示. Alice 制备一种双模纠缠态$|\varphi_{\mathrm{AB}}(\alpha)\rangle$, 对 A 模进行投影测量$\sum_{k=0}^{3}|\psi_k\rangle_{\mathrm{A}}\langle\psi_k|$, 则将待发送的量子态塌缩到相应的态$|\alpha_k\rangle_{\mathrm{B}}$上, 经高斯信道传输给 Bob 进行零差探测 (信道参数: 透射率 η 和可容忍过噪声 ξ). 利用 Schmidt 分解, Alice 所制备的纠缠态可表示为

$$\begin{aligned}|\varphi_{\mathrm{AB}}(\alpha)\rangle &= \frac{1}{2}\sum_{k=0}^{3}|\psi_k,\alpha_k\rangle_{\mathrm{AB}}\\ &= \sum_{k=0}^{3}\sqrt{\lambda_k}\,|\phi_k,\phi_k\rangle_{\mathrm{AB}},\end{aligned}\tag{1}$$

其中

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

$$|\phi_k\rangle = \frac{\mathrm{e}^{-\alpha^2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}\,|4n+k\rangle,\tag{2b}$$

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

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

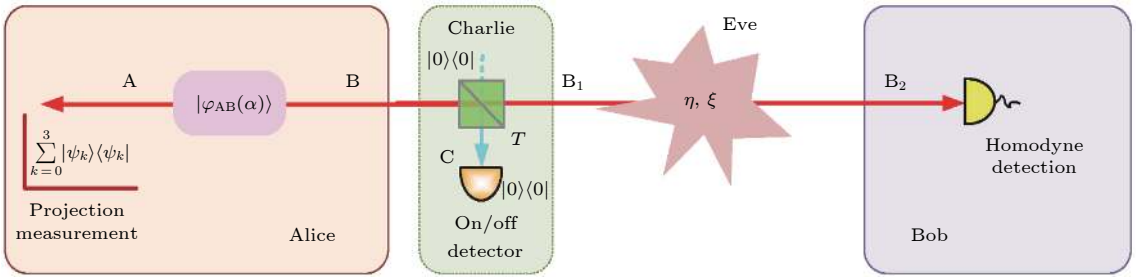

图 1 纠缠型的零光子催化四态调制协议原理图

Fig. 1. Schematic diagram of the entanglement-based (EB) model of the four-state modulation protocol using a zero-photon catalysis.

对于任意的量子密钥分发协议, 安全性是衡量其性能优越性的重要体现. 这种纠缠型四态调制协议通过 Alice 和 Bob 未做测量前构建的协方差矩阵为安全性证明提供了便捷. 在上述情况下, Alice 所制备纠缠态$|\varphi_{\mathrm{AB}}(\alpha)\rangle$的协方差矩阵可表示为

$$\boldsymbol{\Gamma}_{\mathrm{AB}}=\begin{pmatrix} VI & Z_4\sigma_z \\ Z_4\sigma_z & VI \end{pmatrix}, \tag{3}$$

这里 $II=\mathrm{diag}(1,1)$, $\sigma_z=\mathrm{diag}(1,-1)$, $V=2\alpha^2+1$ 和 $Z_4=2\alpha^2\sum\limits_{k=0}^{3}\dfrac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}}$. 于是, 经过高斯信道后, 态 $\rho_{\mathrm{AB_1}}$的协方差矩阵则为

$$\boldsymbol{\Gamma}_{\mathrm{AB_1}}=\begin{pmatrix} VI & \sqrt{\eta}Z_4\sigma_z \\ \sqrt{\eta}Z_4\sigma_z & \eta(V+\chi)II \end{pmatrix}, \tag{4}$$

其中 η 表示信道的透射率, $\chi=(1-\eta)/\eta+\xi$ 表示高斯信道引入的过噪声.

2.2 安全密钥率

为了获取四态调制协议的安全码率, 这里首先假设敌手 Eve 采取集体攻击, 且 Alice 和 Bob 使用逆向协商 (协商效率为 β). 因此, 密钥率可表示为

$$K=\beta I(\mathrm{A}:\mathrm{B})-S(\mathrm{B}:\mathrm{E}), \tag{5}$$

这里的 $I(\mathrm{A}:\mathrm{B})$表示 Alice 和 Bob 之间的 Shannon 互信息, $S(\mathrm{B}:\mathrm{E})$表示 Bob 和 Eve 之间的互信息.

实际上, Bob 采取的零差探测对于密钥率有着显著的影响. 由 (5) 式可知, 对于零差探测, Alice 和 Bob 之间的 Shannon 互信息分别表示为

$$I_{\mathrm{Hom}}(\mathrm{A}:\mathrm{B})=\frac{1}{2}\log_2\frac{V+\chi}{1+\chi}, \tag{6}$$

为了计算出 Bob 和 Eve 之间的最大 Holevo 信息 $S(\mathrm{B}:\mathrm{E})$, 需借助于传统的高斯调制方案. 根据 (4) 式可知, 这种四态协议的离散调制协方差表达形式与常用的高斯调制情况相似, 即有

$$\boldsymbol{\Gamma}_{G\mathrm{AB_1}}=\begin{pmatrix} VII & \sqrt{\eta}Z_G\sigma_z \\ \sqrt{\eta}Z_G\sigma_z & \eta(V+\chi)II \end{pmatrix}, \tag{7}$$

其中 $Z_G=\sqrt{(V-1)^2+2(V-1)}$. 因此, 由 (3) 式和 (7) 式可得, Z_4和Z_G随 V的变化曲线图, 如图 2 所示. 显然, 当$V<1.5$时, Z_4与Z_G不可区分, 这意味着 $S_4(\mathrm{B}:\mathrm{E})\approx S_G(\mathrm{B}:\mathrm{E})$[11,12]. 于是,

$$S_4(\mathrm{B}:\mathrm{E})=\sum_{j=1}^{2}G\left(\frac{\lambda_j-1}{2}\right)-G\left(\frac{\lambda_3-1}{2}\right), \tag{8}$$

这里的 $G(x)=(x+1)\log_2(x+1)-x\log_2 x$. 此外, 辛本征值$\lambda_{1,2,3}$可由 (4) 式协方差矩阵获取, 即

$$\lambda_{1,2}^2=\frac{1}{2}\left(A\pm\sqrt{A^2-4B}\right), \tag{9a}$$

$$\lambda_3^2=V^2-\frac{V^2Z_4^2}{V+\chi}, \tag{9b}$$

其中

$$A=V^2+\eta^2(V+\chi)^2-2\eta Z_4^2, \tag{10a}$$

$$B=\left(\eta V^2+\eta V\chi-\eta Z_4^2\right)^2. \tag{10b}$$

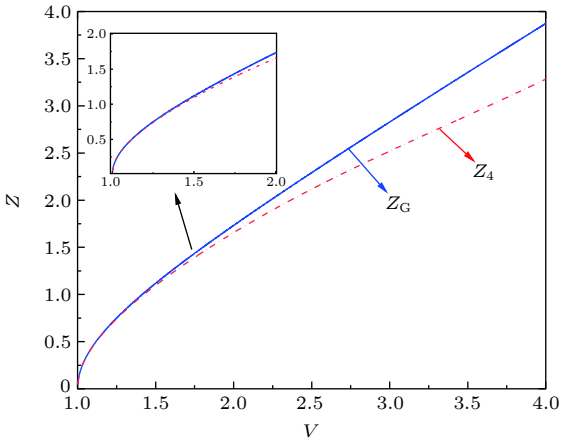

图 2 Z_4和Z_G随调制方差 V的变化

Fig. 2. Both Z_4 and Z_G as a function of the modulation variance V.

2.3 量子催化的离散调制协议

将量子催化 (浅绿色框) 运用于四态调制协议, 如图 1 所示. 值得注意的是, 为了减少发送端 Alice 的实验器材成本, 量子催化操作受不可信任方 Charlie 操控. 此外, 为了便于安全性分析, 这里假设 Eve 意识到 Charlie 的存在. 量子催化的概念首次被文献 [22] 提出. 例如, 对于零光子催化过程, 辅助模 C 的输入端口注入零光子, 经过透射率为 T 的分束器后, 开关探测器在输出端口仅探测零光子. 注意, 开关光子探测器的无响应意味着探测到零光子. 于是, 输入的真空态 $|0\rangle_{\rm C}$ 在辅助模 C 与模 B 的待输入量子态 $|\varphi\rangle_{\rm in}$ 进行分束器干涉; 随后, 开关光子探测器在模 C 的输出端进行无响应探测. 可见, 尽管在辅助模输入端输入真空态, 输出端探测真空态, 看上去模 C 没有变化, 但是这种催化效果确实能够促进输入-输出的量子态之间的转换. 为了表述量子态输入-输出的关系, 这里引入一种量子催化等效算符:

$$\hat{O}_0 = (T)^{b^\dagger b/2}. \tag{11}$$

关于更详细的量子催化等效算符的推导可参考文献 [9, 20, 21, 23]. 因此, 输入-输出量子态的关系式可表示为

$$|\psi\rangle_{\rm out} = \frac{\hat{O}_0}{\sqrt{P_{\rm d}}}|\varphi\rangle_{\rm in}, \tag{12}$$

这里 $P_{\rm d}$ 表示量子态 $|\psi\rangle_{\rm out}$ 的归一化系数. 如图 1 所示, 对于四态调制协议, 传输给 Bob 的是相干态 $|\alpha_k\rangle$. 于是, 催化后的量子态为

$$|\tilde{\alpha}_k\rangle = \frac{{\rm e}^{\frac{1}{2}(T-1)|\alpha_k|^2}}{\sqrt{P_{\rm d}}}|\sqrt{T}\alpha_k\rangle, \tag{13}$$

其中

$$P_{\rm d} = {\rm e}^{(T-1)|\alpha_k|^2}. \tag{14}$$

根据 (13) 式可知, 经过零光子催化后, 量子态的振幅变化关系可写成 $\tilde{\alpha}_k = \sqrt{T}\alpha_k$. 因此, 只要将 2.2 节的符号"$\alpha$"替换成"$\sqrt{T}\alpha$". 特别注意的是, 当 $T = 1$, 输出态简化成输入态形式, 即 $|\tilde{\alpha}_k\rangle = |\alpha_k\rangle$, 这暗示着不存在任何量子催化效应. 此外, 由于执行零光子催化是一种概率性事件, 使得相应的密钥率公式应改写成:

$$K_0 = P_{\rm d}\left(\beta I\left({\rm A}:{\rm B}\right) - S\left({\rm B}:{\rm E}\right)\right). \tag{15}$$

由 (15) 式可知, 量子催化的成功概率 $P_{\rm d}$ 是与密钥率安全性边界 ($K_0 = 0$) 密切相关. 若 $P_{\rm d} = 0$, 则 $K_0 = 0$. 若 $0 < P_{\rm d} \leqslant 1$, 则成功概率 $P_{\rm d}$ 不会影响密钥率的安全性边界. 此外, 根据 (14) 式, 图 3 给出了不同的调制方差 $V = 1.2, 1.3, 1.4, 1.5$ 下量子催化的成功概率 $P_{\rm d}$ 随透射率 T 的变化. 显然, 在固定透射率 T 下, $P_{\rm d}$ 随着调制方差 V 减小而增大. 当给定调制方差 V 时, $P_{\rm d}$ 随着透射率 T 的增加而增大. 这意味着零光子催化易于实现, 极大地促进了输入-输出量子态之间的转换, 从而避免通信双方量子信息的丢失.

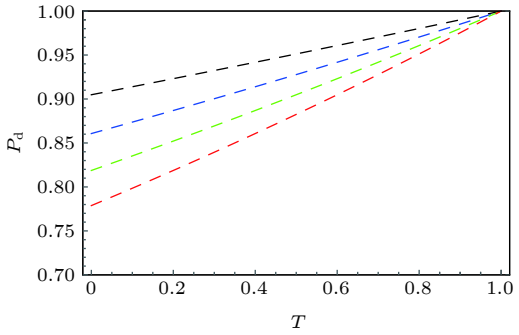

图 3 对于不同的调制方差 V 下量子催化的成功概率 $P_{\rm d}$ 随透射率 T 的变化 (图中从上往下的虚线分别表示 $V = 1.2, 1.3, 1.4, 1.5$)

Fig. 3. Success probability of implementing such a zero-photon catalysis as a function of the transmittance T for several different V. The dashed lines from bottom to top correspond to $V = 1.2, 1.3, 1.4, 1.5$, respectively.

3 性能分析与讨论

一般而言, 量子密钥分发协议的性能评估有 3 个重要指标: 安全密钥率 (secret key rate)、最大安全传输距离 (transmission distance) 以及最大可容忍过噪声 (tolerable excess noise). 本文基于以上 3 个指标对所提的协议进行性能分析和讨论.

由图 2 可知, 在离散调制协议下, 调制方差 V 需控制在 $V \in [1,\ 1.5)$ 范围内该方案才能与高斯调制的连续变量量子密钥分发协议等价, 这使得求解 Holevo 信息问题大大简化. 在信道损耗为 0.2 dB/km 下, 假设 $\beta = 0.95, \xi = 0.005$, 对于不同的调制方差 $V = 1.2, 1.3, 1.4$, 当优化透射率 T, 图 4(a) 为基于量子催化的四态协议在不同距离下的安全码率. 图中黑色线为原始四态协议 (original four-state modulation protocol, original protocol). 当调制方差取某些值 (如 1.3, 1.4), 本文的零光子催化四态协议 (zero-photon catalysis-based four-state modulation protocol, ZPC protocol)能够在

最大安全传输距离及安全密钥率性能方面优于原始四态协议. 这是源于零光子催化实际是一种无噪衰减过程, 而无噪声衰减已在参考文献 [24]证实了可以提升量子密钥分发系统的性能. 另一方面, 通过优化量子催化引入的透射率 T 来调控和获取最优调制方差, 使得进一步提高量子密钥分发协议的性能. 同时, 这里也给出了透射率 T 在不同距离下的曲线图, 如图 4(b) 所示. 值得注意的是, 当 $T=1$ 时, 不存在任何量子催化效果. 正是如此, 一方面, 导致了在短距离安全通信下, 本方案与原始方案的性能保持一致. 另一方面, 如图 4(a)所示, 这也使得对于 $V=1.2$ 的所提方案 (蓝色虚线) 与原始方案 (黑色实线) 的性能曲线重合. 这意味当调制方差低于某个值, 量子催化不能用来提高离散调制协议的性能. 此外, 从图 4(a)可知, 对于原始四态协议 (黑色线) 而言, 调制方差的减小, 可以提高安全传输距离. 有趣的是, 量子催化的引入可进一步提升原始四态协议的安全传输距离.

此外, 可容忍过噪声是影响性能的另一项重要指标. 为了清晰理解可容忍过噪声对性能的影响, 这里适当选取固定参数 $\beta=0.95, V=1.3$, 当优化透射率 T 时, 对于不同可容忍过噪声 $\xi=$ 0.002, 0.005, 0.008, 图 5(a) 显示了安全密钥率随传输距离的变化. 显然, 可容忍噪声过噪声越低, 量子密钥分发协议的性能越好. 此外, 仿真结果表明, 量子催化可以用来有效地改善量子密钥分发的性能. 尤其对于较小的可容忍过噪声, 改善效果比较明显. 这正如图 5(a) 所示, 对于可容忍过噪声取 0.002

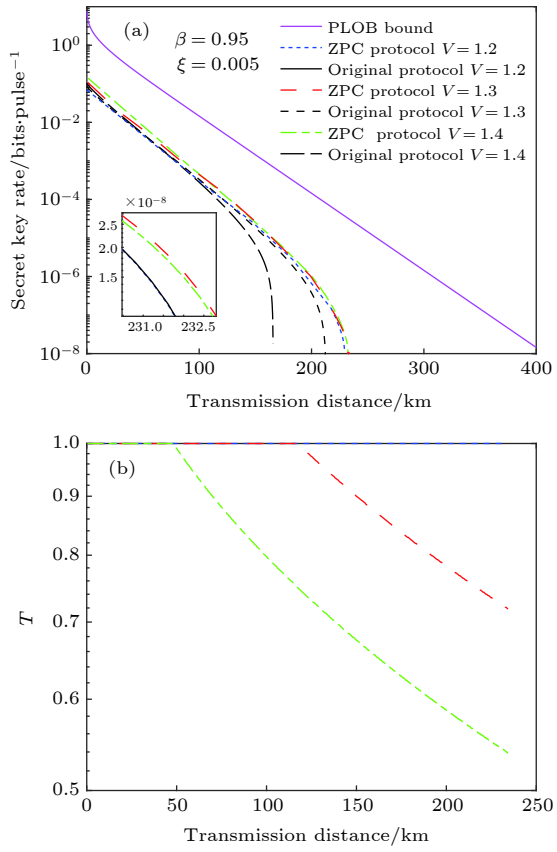

图 4 离散调制量子密钥分发系统的性能比较 (a) 固定参数 $\beta=0.95, \xi=0.005$ 下, 当优化透射率 T 时, 密钥率在不同调制方差随传输距离的变化; (b) 对应 (a) 情况下, 透射率 T 随传输距离的变化

Fig. 4. Comparison of the performances between the original protocol and the ZPC-based four-state modulation protocol: (a) At a fixed $\beta=0.95, \xi=0.005$, the secret key rate as a function of the transmission distance with different $V=1.2$, 1.3, 1.4, when optimized over the transmittance T; (b) the transmittance T as a function of the transmission distance corresponding to panel (a).

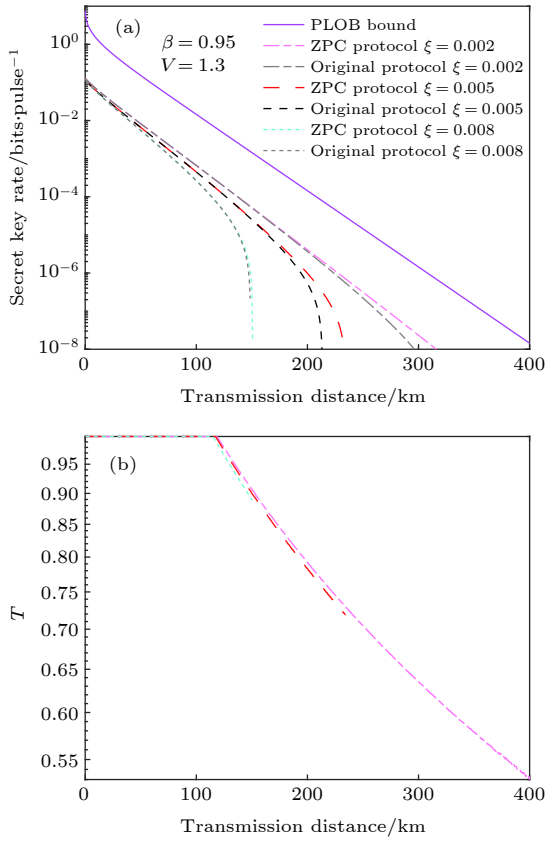

图 5 离散调制量子密钥分发系统的性能比较 (a) 固定参数 $\beta=0.95, V=1.3$ 下, 当优化透射率 T 时, 密钥率在不同可容忍过噪声随传输距离的变化; (b) 对应 (a) 情况下, 透射率 T 随传输距离的变化曲线

Fig. 5. Comparison of the performances between the original protocol and the ZPC-based four-state modulation protocol: (a) At a fixed $\beta=0.95, V=1.3$, the secret key rate as a function of the transmission distance with different $\xi=0.002, 0.005, 0.008$, when optimized over the transmittance T; (b) the transmittance T as a function of the transmission distance corresponding to panel (a).

(点划线) 和 0.005 (划线) 时, 零光子催化四态协议在传输距离和安全密钥率方面都能优越于原始方案. 而对于$\xi = 0.008$的情况, 性能改善不明显. 这是因为透射率 T 随可容忍过噪声的增加而在安全传输距离上缩短 (如图 5(b) 所示). 同时, 这也暗含着可容忍过噪声的增加可以抑制量子催化的效果.

为了进一步研究协商效率对量子密钥分发性能的影响, 这里假定$V = 1.3, \xi = 0.005$, 对于优化透射率 T 的情况下, 图 6(a) 表示不同的协商效率$\beta = 0.90, 0.95, 1.0$的安全密钥率随传输距离的变化. 显然地, 协商效率越高, 则量子密钥分发的性能表现越好. 特别是, 对于更为实际的协商效率为 0.90 (点划线) 时, 采用量子催化操作能够提升原始方案的传输距离约至 210 km, 密钥率为 10^{-8} bits/pulse.

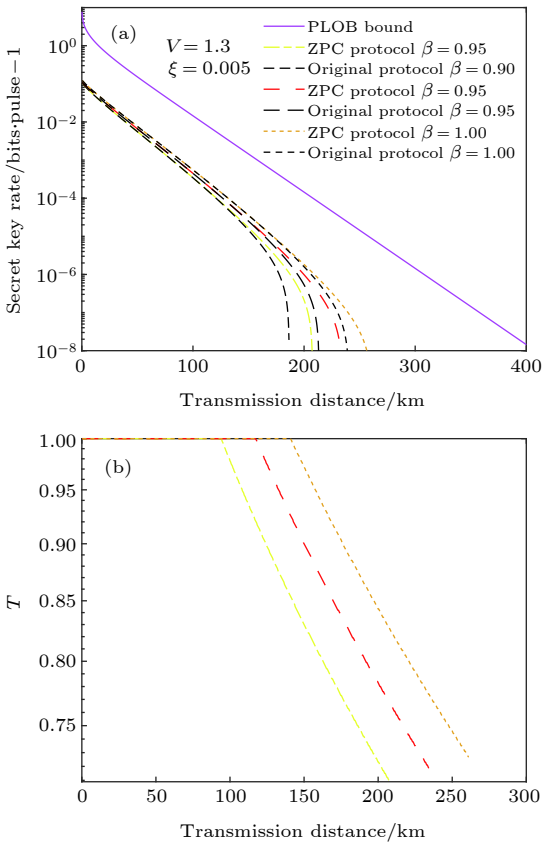

图 6 离散调制量子密钥分发系统的性能比较 (a) 固定参数$V = 1.3, \xi = 0.005$下, 当优化透射率 T时, 密钥率在不同协商效率随传输距离的变化; (b) 对应 (a) 情况下, 透射率 T随传输距离的变化曲线

Fig. 6. Comparison of the performances between the original protocol and the ZPC-based four-state modulation protocol: (a) At a fixed $V = 1.3, \xi = 0.005$, the secret key rate as a function of the transmission distance with different $\beta = 0.90, 0.95, 1.0$, when optimized over the transmittance T; (b) the transmittance T as a function of the transmission distance corresponding to panel (a).

图 6(b) 给出对应量子催化四态调制协议的透射率 T 随传输距离的变化. 此外, 比较图 6(a) 与图 5(a) 可以看出, 可容忍过噪声对量子密钥分发的性能影响程度要大于协商效率的情况.

可容忍过噪声是影响量子密钥分发性能的关键因素. 为了看清量子催化能否提升最大可容忍过噪声, 对于不同的协商效率$\beta = 0.90, 0.95, 1.0$, 图 7 给出了最大可容忍过噪声随传输距离的变化. 本方案的性能提升随着协商效率的降低而呈现得更为明显. 例如, 对于给定可容忍过噪声为$\xi = 0.003$, 原始协议的传输距离可达到 240 km 附近; 而相同参数下, 本方案的传输距离大约达到 320 km. 这些研究结果表明, 零光子催化可提升离散调制协议的可容忍过噪声. 此外, 需要注意的是, 图中优化透射率 T指的是在可取范围$T \in [0, 1]$内找到某个透射率使得密钥率最大 (图 4—图 6) 或者密钥率为零 (图 7).

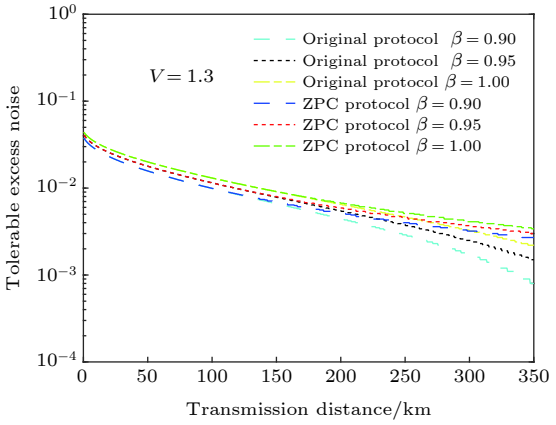

图 7 在固定参数$V = 1.3$下, 当优化透射率 T时, 可容忍过噪声在不同协商效率随传输距离的变化

Fig. 7. At a fixed $V = 1.3$, the tolerable excess noise between the original protocol and the ZPC-based four-state modulation protocol as a function of a transmission distance for several different $\beta = 0.90, 0.95, 1.0$, when optimized over T.

为了突出量子催化的优势, 图 4(a)、图 5(a)、图 6(a) 均给出了 Pirandola-Laurenza-Ottaviani-Banchi (PLOB) 边界 (bound)[25] (品红实线), 它是点对点量子通信的最终极限, 并为量子中继器提供了精确和通用的基准. 由图 3(a) 和图 5(a) 可知, 虽然量子催化的离散调制协议和原始方案都无法突破 PLOB bound, 但是相比后者, 前者的远距离传输更能接近这种边界. 这也表明量子催化确实在远距离安全密钥通信上发挥着显著优势.

4 结 论

本文提出了一种基于量子催化离散调制协议的方案, 并给出了零光子催化的等效算符. 研究发现, 这种量子催化实际就是一种无噪声衰减, 它使得传输给 Bob 的相干态振幅 α 衰减成 $\sqrt{T}\alpha$. 随后, 本文对所提方案进行渐近安全性分析. 研究表明, 当固定参数 $\beta=0.95, \xi=0.005$ 下, 对于不同的调制方差 $V=1.3$, 1.4, 本方案能够进一步提高量子密钥分发协议的性能. 而对于较小的 $V=1.2$, 本方案在性能改善方面不能显示出量子催化的优势. 此外, 当适当选取固定参数 $\beta=0.95, V=1.3$, 对于不同可容忍过噪声 $\xi=0.002$, 0.005, 所提方案在较小的可容忍过噪声中性能改善比较明显. 而对于较大可容忍过噪声 $\xi=0.008$, 它较与原始四态协议方案性能改善不明显. 而对于不同的协商效率 $\beta=0.90$, 0.95, 1.0, 当给定参数 $V=1.3$, $\xi=0.005$, 协商效率越高, 则量子密钥分发的性能表现越好. 特别是, 对于更为实际的协商效率 0.90, 利用量子催化操作能够进一步提升原始方案的传输距离约至 210 km, 密钥率为 10^{-8} bits/pulse. 值得注意的是, 虽然两种方案都未能突破点对点量子通信的最终极限 PLOB 边界, 但是量子催化的运用确实能够在远距离传输进一步逼近这种边界. 因此, 为了试图突破这种边界, 在今后的研究工作中, 可将量子催化运用于测量设备无关离散调制协议[26].

参考文献

[1] Li J, Chen Y H, Pan Z S, Sun F Q, Li N, Li L L 2016 *Acta Phys. Sin.* **3** 030302 (in Chinese) [李剑, 陈彦桦, 潘泽世, 孙风琪, 李娜, 黎蕾蕾 2016 物理学报 **3** 030302]

[2] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙, 莫小范, 桂有珍, 韩正甫, 郭光灿 2004 物理学报 **53** 2123]

[3] Cao Z W, Zhang S H, Peng X Y, Zhao G, Chai G, Li D W 2017 *Acta Phys. Sin.* **66** 020301 (in Chinese) [曹正文, 张爽浩, 冯晓毅, 赵光, 柴庚, 李东伟 2017 物理学报 **66** 020301]

[4] Braunstein S L, Loock P V 2005 *Rev. Mod. Phys.* **77** 513

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

[6] Silberhorn C, Ralph T C, Lütkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[7] Lodewyck J, Bloch M, GarciaPatron 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

[8] Hu L Y, Liao Z Y, Zubairy M S 2017 *Phys. Rev. A* **95** 012310

[9] Hu L Y, Wu J N, Liao Z Y, Zubairy M S 2016 *J. Phys. B: At. Mol. Phys.* **49** 175504

[10] Zhang H, Ye W, Zhou W D, Hu L Y 2019 *Journal of Liaocheng University* 32 1672 (in Chinese) [张欢, 叶炜, 周维东, 胡利云 2019 聊城大学学报 32 21]

[11] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504

[12] Leverrier A, Grangier P 2011 *Phys. Rev. A* **83** 042312

[13] Huang P, Fang J, Zeng G H 2014 *Phys. Rev. A* **89** 042330

[14] Huang P, Huang J Z, Zhang Z S, Zeng G H 2018 *Phys. Rev. A* **97** 042311

[15] Huang P, He G Q, Fang J, Zeng G H 2013 *Phys. Rev. A* **87** 012317

[16] Li Z Y, Zhang Y C, Wang X Y, Xu B J, Peng X, Guo H 2016 *Phys. Rev. A* **93** 012310

[17] Zhao Y J, Zhang Y C, Li Z Y, Yu S, Guo H 2017 *Quantum Inf. Process.* **16** 184

[18] Ma H X, Huang P, Bai D Y, Wang S Y, Bao W S, Zeng G H 2018 *Phys. Rev. A* **97** 042329

[19] Liao Q, Guo Y, Huang D, Huang P, Zeng G H 2018 *New J. Phys.* **20** 023015

[20] Guo Y, Ye W, Zhong H, Liao Q 2019 *Phys. Rev. A* **99** 032327

[21] Zhou W D, Ye W, Liu C J, Hu L Y, Liu S Q 2018 *Laser Phys. Lett.* **15** 065203

[22] Lvovsky A I, Mlynek J 2002 *Phys. Rev. Lett.* **88** 250401

[23] Ye W, Zhong H, Liao Q, Huang D, Hu L Y, Guo Y 2019 *Opt. Express* **27** 17186

[24] Fiurasek J, Cerf N J 2012 *Phys. Rev. A* **86** 060302(R)

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

[26] 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

Discrete modulation continuous-variable quantum key distribution based on quantum catalysis*

Ye Wei [1)] Guo Ying [1)†] Xia Ying [2)] Zhong Hai [1)]
Zhang Huan [2)] Ding Jian-Zhi [1)] Hu Li-Yun [2)‡]

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

2) (*Center for Quantum Science and Technology, Jiangxi Normal University, Nanchang* 330022, *China*)

(Received 4 November 2019; revised manuscript received 30 November 2019)

Abstract

Compared with discrete variable quantum key distribution (DVQKD), continuous variable (CV) QKD has high security bit rate and other advantages, which, however, are slightly insufficient in secure transmission distance. In addition, the application of quantum catalysis has significantly improved the performance of Gaussian modulated (GM) CVQKD, especially in secure transmission distance. Recently, the application of quantum catalysis has significantly improved the performance of GM-CVQKD. However, whether it can be used to improve the performance of discrete modulated (DM) CVQKD protocol is still ambiguous. Therefore, a scheme of DM CVQKD protocol based on quantum catalysis is proposed in this paper to further improve the performance of the proposed protocol in terms of secure key rate, secure transmission distance and maximum tolerable noise. Our results show that under the same parameters, when the transmittance T introduced by quantum catalysis is optimized, the proposed scheme can effectively further improve the performance of QKD system compared with the original four-state modulation CVQKD scheme. In particular, when the tolerable excess noise is 0.002, the use of quantum catalysis can break the safe communication distance of 300 km with a key rate of 10^{-8} bits/pulse. However, if this noise is too large, the improvement in the effect of quantum catalysis on protocol performance will be restrained. In addition, in order to highlight the advantages of the use of quantum catalysis, the ultimate limit PLOB (Pirandola-Laurenza-Ottaviani-Banchi) bound of point-to-point quantum communication is given in this paper. The simulation results indicate that although neither the original scheme nor the proposed scheme can break the bound, compared with the former, the latter can be close to the boundary in long-distance transmission. These results provide theoretical basis for achieving the ultimate goal of global quantum security communication.

Keywords: continuous variable, quantum key distribution, discrete modulation, quantum catalysis

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.7498/aps.69.20191689

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61572529, 61821407, 11964013, 11664017), the Training Program for Academic and Technical Leaders of Major Disciplines in Jiangxi Province, the Postgraduate Scientific Research Innovation Project of Hunan Province, China (Grant No. CX20190126), and the Postgraduate Independent Exploration and Innovation Project of Central South University, China (Grant No. 2019zzts070).

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

‡ Corresponding author. E-mail: hlyun2008@126.com