基于态区分检测器的连续变量量子密钥分发

廖骏，唐冲，杨俊跃，李君浩
（湖南大学计算机学院，湖南 长沙 410082）

摘　要：针对连续变量量子密钥分发（CVQKD）协议中传统相干探测器受标准量子极限（SQL）限制的问题，提出了一种基于态区分检测器（SDD）的CVQKD协议，即SDD-CVQKD。该协议通过SDD替代传统相干探测器，利用多轮自适应测量与MAP准则，实现对离散调制相干态的高精度判别，降低检测错误概率。在反向协商与集体分束攻击的安全模型下推导了密钥率下界。数值模拟结果表明，所提协议在信道参数与密钥率方面均优于传统CVQKD协议，甚至超过PLOB界，展现出更高的安全性。

关键词：量子密钥分发；连续变量；态区分检测器；自适应测量
中图分类号：TN91
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026007

Continuous variable quantum key distribution based on state-discrimination detector

Liao Qin, Tang Chong, Yang Junyue, Li Junhao
College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

Abstract: Aiming at the problem that the traditional coherent detector was limited by the standard quantum limit (SQL) in the continuous variable quantum key distribution (CVQKD) protocol, a CVQKD protocol based on state-discrimination detector (SDD), namely SDD-CVQKD, was proposed. The protocol replaced the traditional coherent detector with SDD, and used multi-round adaptive measurement and MAP criterion to achieve high-precision discrimination of discrete modulated coherent states, which reduced the detection error probability. The security bounds were derived under the security model of reverse reconciliation and collective beam-splitting attack. Numerical simulation results show that the proposed protocol is superior to the traditional CVQKD protocol in terms of channel parameters and secret key rate, and even exceeds the PLOB bound, showing higher security.

Keywords: quantum key distribution, continuous variable, state-discrimination detector, adaptive measurement

0　引言

量子密钥分发（quantum key distribution, QKD）[1-3]允许远程合法通信方Alice和Bob共享随机安全的密钥序列，其依托量子力学原理建立安全框架，在窃听者（Eve）控制的不可信量子信道上也能保证无条件安全。通常来说，QKD主要包括离散变量量子密钥分发（discrete-variable QKD, DVQKD）[4]和连续变量量子密钥分发（continuous

收稿日期：2025–11–12；修回日期：2026–01–04
通信作者：廖骏，llqqlq@hnu.edu.cn
基金项目：国家自然科学基金资助项目（No.62101180）；湖南省重点研发计划基金资助项目（No.2025QK3011）；中国工程科技发展战略湖南研究院战略研究与咨询基金资助项目（No.2025WK1001）
Foundation Items: The National Natural Science Foundation of China (No.62101180), The Key Research and Development Program of Hunan Province (No.2025QK3011), The Monumental Consultation Project on the Development Strategy of Chinese Engineering and Technology (No.2025WK1001)

variable QKD, CVQKD）[5]。相比于DVQKD系统，CVQKD系统因其信号制备简单、与现有光通信网络兼容性强等优点，成为研究热点。其理念最早由Ralph[6]提出。随后，Hillery[7]基于离散调制压缩态提出了创新的CVQKD方案。Grosshans等[8]以高斯调制相干态为基础提出了全新的CVQKD协议，即GG02协议，该协议基于正向协商（direct reconciliation, DR）方案，受到了“3 dB极限”的限制[9]，使信道参数小于0.5时无法获得有效密钥。随后由Grosshans等[8]修正GG02协议并提出反向协商（reverse reconciliation, RR）方案，以突破“3 dB极限”的限制。至此CVQKD迅速发展，Weedbrook等[10]在GG02协议基础上提出了无开关协议，并由Navascués等[11]和García-Patrón等[12]完成集体攻击下的安全性证明。但高斯调制器通常受有限采样精度的限制，实现起来相当具有挑战性[13]。为了解决这个问题，Leverrier等[14]提出了一种离散调制（discrete modulation, DM）CVQKD方案，其中应用正交相移键控（quadrature phase shift keying, QPSK）调制代替高斯调制，降低了实现CVQKD系统的难度。随后文献[15-16]将QPSK调制CVQKD的渐近密钥率通过半定规划（semidefinite programming, SDP）方法求解，以此获得安全码率更精确的边界。Denys等[17]引入新的SDP方法计算了任意DM CVQKD系统的更精确安全码率下界。

以上所有工作有一个共同点，即由传统相干探测器测量调制相干态，这种广泛使用的策略受到了标准量子极限（standard quantum limit, SQL）的限制，这是高斯运算和经典通信中错误概率的下限[18]。通过协议改进可以一定程度上逼近SQL，例如，Liao等[19]通过优化调制方式，对相干态按概率进行不同幅度的离散调制，使其在空间中分布于若干幅度环上以增加相干态之间的距离，降低检测错误概率。值得注意的是，相干态的区分仅受Helstrom极限的限制，这为量子探测理论提供了超越SQL的理论可行性[20]。例如，态区分检测器（state-discrimination detector, SDD）采用非高斯测量结构，通过位移门与光子数检测器自适应测量未知相干态，并利用贝叶斯定理更新测量结果，实现比传统相干探测器更低的检测错误概率。Tsujino等[21]首先证实了可以使用近单位效率检测器来打破用于区分两个非正交态的SQL。之后，通过优化相干态事件的多元假设检验，成功超越了判别两个以上非正交态的SQL。Becerra等[22]随后证明了通过光子计数和快速反馈形式的自适应测量对QPSK调制相干态（QPSK modulation coherent state, QMCS）的无条件鉴别。因此，可以推测CVQKD协议通过适当地用某种优化的鉴别策略取代传统相干探测器有望得到性能的提升，这一思想在Liao等[23]的工作中得到了初步验证，并且在二进制调制的CVQKD[24]和QPSK调制的CVQKD[25]中表现出出色的性能改善，但采用的正向协商策略受到“3 dB极限”的限制，影响其性能改善效果。

受近年来在量子态判别理论及CVQKD方面一系列突破性工作的启发，本文提出了一种全新的CVQKD协议架构——SDD-CVQKD，其核心创新在于将一种专门针对离散调制相干态（DM coherent state, DMCS）设计的高性能SDD引入接收端，以取代传统相干探测器，从而实现协议的性能提升。具体而言，该SDD基于多轮自适应最大后验概率（multi-round adaptive maximum-a-posteriori, MRA-MAP）准则，通过动态优化本振光相位与位移操作，在每一轮测量后实时更新后验概率分布，并据此调整下一轮测量基，最终能够在渐近极限下以低于SQL的错误概率准确判别接收到的相干态，有效提升信息提取效率。在此基础上，本文研究了采用反向协商机制的性能表现，从根本上突破了传统CVQKD协议面临的“3 dB极限”限制。在安全性分析方面，本文在Eve执行集体分束攻击（collective beam-splitting attack, CBSA）的假设框架下，严格推导了渐近情形下的密钥率表达式，并通过数值仿真系统评估了协议性能。结果表明，SDD-CVQKD协议在标准光纤信道参数下，无论是在最大安全传输距离上还是密钥生成速率上，均优于传统离散调制结合相干探测的CVQKD方案，其密钥率–信道参数曲线甚至能够突破PLOB（Pirandola-Laurenza-Ottaviani-Banchi）界[26]，展现出超越直接传输极限的潜力。进一步分析发现，由于SDD性能可以随着自适应测量次数提升，协议性能可通过增加SDD模块的自适应测量轮数实现持续优化。值得注意的是，在远距离传输场景下，探测器效率有限、电子噪声积累等因素导致的误判概率上升，会在一定程度上削弱SDD的优势，但本文提出的基于置信度阈值的后选择（post-selection, PS）方

案可有效筛选高置信度测量结果，从而补偿由设备非理想性引入的性能衰减，减小密钥率下降幅度，确保协议在实际部署中的鲁棒性与可行性，有助于长距离、高速率量子保密通信网络的构建。

1　态区分检测器

如图1所示，该方法由M个连续的自适应测量组成，分束器将初始信号分成M个等强度的分支，其反射率$R=\frac{1}{M-i}$，其中$i=(0,1,\cdots,M-1)$表示分支的索引，这样每个分支的信号能量强度都为$\frac{\beta_k}{\sqrt{M}}$。随后进行位移操作，对于$m\,(0\leqslant m\leqslant M)$次自适应测量，接收量子态通过透射率为$\zeta\to 1$分束器上的本振光对信号进行位移操作，本振光相干幅值设为$\sqrt{\frac{\zeta}{1-\zeta}}\gamma_{S_i}$，可以得到位移后的信号为

$$\hat{D}\left(\gamma_{S_i}\right)\left|\frac{\beta_k}{\sqrt{M}}\right\rangle=\left|\sqrt{\frac{\zeta}{M}}\beta_k+\sqrt{1-\zeta}\sqrt{\frac{\zeta}{1-\zeta}}\gamma_{S_m}\right\rangle=\left|\sqrt{\zeta}\left(\frac{\beta_k}{\sqrt{M}}+\gamma_{S_i}\right)\right\rangle \tag{1}$$

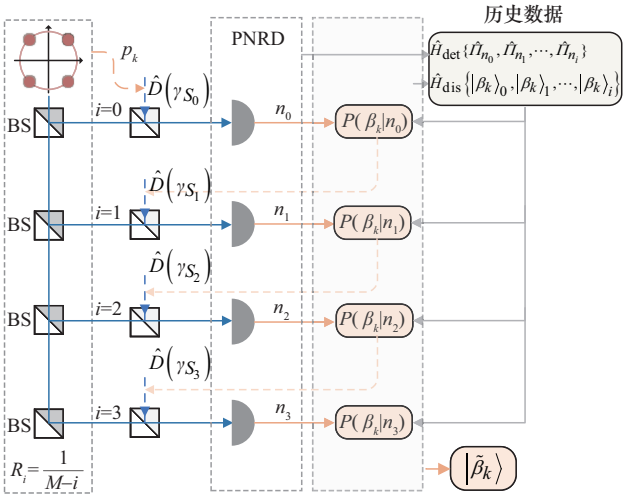

图1　SDD原理

考虑到SDD连续工作时负载电阻温度升高引起的热噪声的影响，位移后信号的密度算子可表示为

$$\hat{\rho}_{\mathrm{th}}\left(\beta_k,\gamma_{S_i}\right)=\frac{1}{\pi N_t}\int_{\mathbb{C}}\mathrm{e}^{-\frac{\left|\alpha-\sqrt{\zeta}\left(\frac{\beta_k}{\sqrt{M}}-\gamma_{S_i}\right)\right|^2}{N_t}}|\tau\rangle\langle\tau| \tag{2}$$

其中，N_t是平均热光子数。随后，采用光子数检测器（photon number resolving detector, PNRD）测量位移态。这种测量以正算子值测度（positive operator-valued measure, POVM）的形式给出了完整的量子力学描述，表示为

$$\hat{\Pi}_{n_i}=\sum_{j=n_i}^{\infty}\binom{j}{n_i}\eta_d^{n_i}(1-\eta_d)^{j-n_i}|j\rangle\langle j| \tag{3}$$

其中，η_d是PNRD的量子效率，n_i是第i分支上的检测光子数。显然，如果假设正确，$\hat{\Pi}_0$将响应，这意味着该分支的输入场将被位移至真空态，从而PNRD无法探测到任何光子。根据量子测量理论，在PNRD上探测光子数的条件概率可由式(4)求得。

$$P\left(n_i|\beta_k,\gamma_{S_i}\right)=\frac{(\eta_d N_t)^{n_i}}{(\eta_d N_t+1)^{n_i+1}}\mathrm{e}^{-\frac{\bar{N}}{N_t+\frac{1}{\eta_d}}}L_{n_i}\cdot\left(-\frac{\bar{N}}{N_t\left(\eta_d N_t+1\right)}\right) \tag{4}$$

其中，$L_{n_i}(\cdot)$是n_i阶Laguerre多项式，平均光子数$\bar{N}$可以通过式(5)计算得到。

$$\bar{N}=\zeta\left(\frac{|\beta_k|^2}{M}+|\gamma_{S_i}|^2-2\xi\left|\frac{\beta_k}{\sqrt{M}}\right||\gamma_{S_i}|\cos\left(\arg\left(\beta_k\right)-\arg\left(\gamma_{S_i}\right)\right)\right)+v \tag{5}$$

其中，$\xi\in[0,1]$是由输入功率不稳定性和输入信号与本振光之间的相对相位差引起的干扰可见度，具体数值可以从干扰测量中获得。

测量结束后，基于当前检测历史$\hat{H}_{\mathrm{det}}$和位移历史$\hat{H}_{\mathrm{dis}}$，利用贝叶斯推理可以得到所有可能态（即$\left\{\left|\beta_k\right\rangle\right\}$）的后验概率。对于第$i$次自适应测量中的各可能态$\left|\beta_k\right\rangle$，其后验概率可以表示为

$$P\left(\beta_k|n_0,\cdots,n_i\right)=\frac{P\left(\beta_k|n_{i-1}\right)P\left(n_i|\beta_k,\gamma_{S_i}\right)}{\sum_{k=0}^{3}P\left(\beta_k|n_{i-1}\right)P\left(n_i|\beta_k,\gamma_{S_i}\right)} \tag{6}$$

其中，$P\left(\beta_k|n_{i-1}\right)$是第$i-1$次自适应测量中的后验概率。根据MAP准则，后验概率最大的可能态$\left|\gamma_{S_{i+1}}\right\rangle=\arg\max_{|\beta_k\rangle}P\left(\beta_k|\gamma_{S_i},n_i\right)$被选中作为下一步适应性测量的输入假设。注意到，所有可能态的概率

是动态更新的，信号态的后验概率将成为下一次自适应测量中信号态的先验概率，并将最新的测量结果和自适应测量选择的信号态分别加入历史检测结果集$\hat{H}_{\mathrm{det}}$和历史预测状态集$\hat{H}_{\mathrm{dis}}$，作为之后自适应测量的计算参数加入运算。

通过递推运算，每个接收信号态经过M次自适应测量后的后验概率β_k可以表示为

$$P\left(\beta_k|n_0,\cdots,n_{M-1}\right)=\frac{p_kP\left(n_0|\beta_k,\gamma_0\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{S_i}\right)}{\sum_{k=0}^{3}p_kP\left(n_0|\beta_k,\gamma_0\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{S_i}\right)} \tag{7}$$

最后，SDD的估计态$\left|\tilde{\beta}_k\right\rangle$对应于$M$次自适应测量中后验概率最大的可能态，表示为$\left|\tilde{\beta}_k\right\rangle=\arg\max_{\left|\beta_k\right\rangle}p_kP\left(n_0|\beta_k,\gamma_0\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{S_i}\right)$。

SDD的装置性能可以由错误概率给出，由于在SDD检测到$(n_0,\cdots,n_{M-1})$个光子数时，信号以概率$P\left(\tilde{\beta}_k|n_0,\cdots,n_{M-1}\right)$被估计为$\left|\tilde{\beta}_k\right\rangle$，所有可能的检测结果的平均错误概率可以表示为

$$P_e=1-\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}p(n_0,\cdots,n_{M-1})P\left(\tilde{\beta}|n_0,\cdots,n_{M-1}\right) \tag{8}$$

其中，$p(n_0,\cdots,n_{M-1})=\sum_{k=0}^{3}p_kP\left(n_0,\cdots,n_{M-1}|\beta_k\right)$是测量结果为$(n_0,\cdots,n_{M-1})$时的错误概率，联立由贝叶斯定理推导出的计算式$P(\tilde{\beta}|n_0,\cdots,n_{M-1})=\frac{p_{|\tilde{\beta}\rangle}P(n_0,\cdots,n_{M-1}|\tilde{\beta})}{P(n_0,\cdots,n_{M-1})}$以及$P(n_0,\cdots,n_{M-1}|\tilde{\beta})=P(n_0|\tilde{\beta},\gamma_0)\prod_{m=1}^{M-1}P\left(n_m|\tilde{\beta},\gamma_{S_i}\right)$给定SDD平均误差概率为

$$P_e=1-\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}p_{|\tilde{\beta}_k\rangle}P\left(n_0|\tilde{\beta}_k,\gamma_0\right)\prod_{i=1}^{M-1}P\left(n_i|\tilde{\beta}_k,\gamma_{S_i}\right) \tag{9}$$

至此，得到了准确量化SDD性能的指标公式，为之后与SQL和Helstrom极限比较给出了理论基础。

2　安全性分析

如图2所示，在SDD-CVQKD协议中，Alice随机生成一个二进制序列，并将其映射到4个相干态$\left|\alpha_k\right\rangle=\left|\alpha\mathrm{e}^{\frac{\mathrm{i}\pi(2k+1)}{4}}\right\rangle,(k=0,1,2,3)$上，Bob利用SDD估计接收的信号，将其重新映射到原始二进制序列中，最后通信双方对序列执行纠错和秘密放大以提取最终密钥。

在此模型下，Eve可对经过不安全量子信道传输的信号态发动集体分束攻击，信号态经过集体分束攻击后被分裂为Bob态$\left|\beta_k\right\rangle$与Eve态$\left|\varepsilon_k\right\rangle$，表示为

$$\left|\alpha_k\right\rangle\rightarrow\sqrt{\eta}\left|\alpha_k\right\rangle_{\mathrm{B}}\otimes\left|\sqrt{1-\eta}\,\alpha_k\right\rangle_{\mathrm{E}} \tag{10}$$

随后Bob通过SDD估计接收的信号对$\left|\beta_k\right\rangle$进行估计，对于反向协商的情况，当Alice根据Bob透露的数据纠正自己的量子态时，集体分束攻击下的密钥率由式(11)限定。

$$G\geqslant I_{\mathrm{AB}}-\chi_{\mathrm{BE}} \tag{11}$$

其中，I_{AB}是通信方Alice和Bob之间的互信息，χ_{BE}是Eve态的Holevo量，其具体量化Eve可以从发送的信号中提取最大信息量。

2.1　Alice和Bob互信息

Alice和Bob之间的互信息表示为

$$I_{\mathrm{AB}}=H(A)-H\left(A|B\right) \tag{12}$$

其中，$H(A)=-\sum_{k=0}^{3}p_k\mathrm{lb}p_k$是Alice发送信号的熵，条件熵$H\left(A|B\right)$量化了发送信号$\left|\alpha_k\right\rangle$被Bob检测为$\left|\tilde{\beta}_k\right\rangle$的条件下的剩余不确定性，表示为

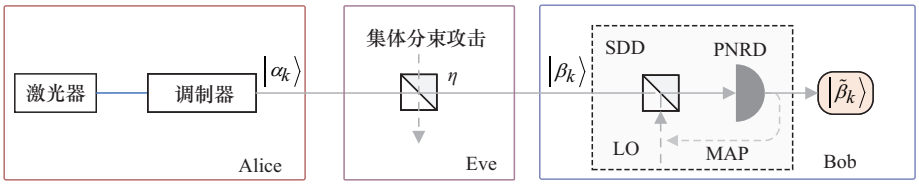

图2　SDD-CVQKD流程

$$H(A|B)=\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}p\left(n_0,\cdots,n_{M-1}\right)$$

$$H(A|n_0,\cdots,n_{M-1})=\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}p\left(n_0,\cdots,n_{M-1}\right)$$

$$\sum_{k=0}^{3}P(\alpha_k|n_0,\cdots,n_{M-1})\mathrm{lb}\frac{1}{P(\alpha_k|n_0,\cdots,n_{M-1})}\tag{13}$$

考虑到Alice发送的信号$|\alpha_k\rangle$与Bob接收的信号$|\beta_k\rangle$具有相同的概率分布，于是有$P\left(\beta_k|n_0,\cdots,n_{M-1}\right)=P(\alpha_k|n_0,\cdots,n_{M-1})$。将式(4)、式(5)、式(7)和式(13)代入式(12)可以得到Alice和Bob的互信息，表示为

$$I_{\mathrm{AB}}=-\sum_{k=0}^{3}p_k\mathrm{lb}p_k-\left(-\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}\sum_{k=0}^{3}p_kP\left(n_0|\beta_k,\gamma_{s_0}\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{s_i}\right)\mathrm{lb}P\left(\beta_k|n_{M-1}\right)\right)=$$

$$-\sum_{k=0}^{3}p_k\left(\mathrm{lb}p_k-\sum_{n_0=0}^{\infty}\cdots\sum_{n_{M-1}=0}^{\infty}P\left(n_0|\beta_k,\gamma_{s_0}\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{s_i}\right)\mathrm{lb}\frac{p_kP\left(n_0|\beta_k,\gamma_{s_0}\right)\sum_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{s_i}\right)}{\sum_{k=0}^{3}p_kP\left(n_0|\beta_k,\gamma_{s_0}\right)\prod_{i=1}^{M-1}P\left(n_i|\beta_k,\gamma_{s_i}\right)}\right)\tag{14}$$

2.2　Eve信息量

对于Eve，可以通过访问随机态来获取信息，该随机态以先验概率p_k从集合$\{\hat{\rho}_{\mathrm{E}|\beta_k}=|\varepsilon_k\rangle\langle\varepsilon_k|\}$取值。那么Eve窃听的混合态可以用密度算子表示为

$$\hat{\rho}_{\mathrm{E}}=\sum_{k=0}^{3}p_k\hat{\rho}_{\mathrm{E}|\beta_k}=\sum_{k=0}^{3}p_k|\varepsilon_k\rangle\langle\varepsilon_k|=\sum_{k=0}^{15}p_k|\sqrt{1-\eta}\,\alpha_k\rangle\langle\sqrt{1-\eta}\,\alpha_k|\tag{15}$$

Eve随后对混合态$\hat{\rho}_{\mathrm{E}}$执行POVM。对于反向协商机制，Eve关于Bob信号态的信息由Holevo量χ_{BE}限定为

$$\chi_{\mathrm{BE}}=S\left(\hat{\rho}_{\mathrm{E}}\right)-\sum_{k=0}^{3}P(k)S\left(\hat{\rho}_{\mathrm{E}|\tilde{\beta}_k}\right)\tag{16}$$

其中，$P(k)=\frac{1}{4}\sum_{k=0}^{3}p(\beta_k|n_{M-1})$是与输出结果$|\tilde{\beta}_k\rangle$相关的Bob的检测概率，$\hat{\rho}_{\mathrm{E}|\tilde{\beta}_k}$是Bob获得第$k$个结果时Eve的态，可以表示为

$$\hat{\rho}_{\mathrm{E}|\tilde{\beta}_k}=\frac{1}{4P(k)}\sum_{k=0}^{3}P\left(\beta_k|n_{M-1}\right)|\varepsilon_k\rangle\langle\varepsilon_k|\tag{17}$$

涉及χ_{BE}计算的冯诺依曼熵$S(\cdot)$计算方法如下[27]。注意到，以上量子态有相同的表示形式$\hat{\rho}=\sum_{k=0}^{3}c_k|\varepsilon_k\rangle\langle\varepsilon_k|$，系数$c_k$为常数。为了计算冯诺依曼熵，本文需要对角化量子态$\hat{\rho}$，若$|\psi\rangle$是与特征值$\lambda$相关联的$\hat{\rho}$的特征向量，则设方程的特征向量为$|\psi\rangle=\sum_{k=0}^{3}b_k|\varepsilon_k\rangle$，可以得到

$$\lambda|\psi\rangle=\hat{\rho}|\psi\rangle\tag{18}$$

将$\hat{\rho}$和$|\psi\rangle$代入式(18)表示为

$$\lambda\sum_{s=0}^{3}b_s|\varepsilon_s\rangle=\sum_{k=0}^{3}c_k|\varepsilon_k\rangle\langle\varepsilon_k|\sum_{m=0}^{3}b_m|\varepsilon_m\rangle=\sum_{k=0}^{3}c_k\left(\sum_{m=0}^{3}G_{km}b_m\right)|\varepsilon_k\rangle\tag{19}$$

其中，$G_{km}=\langle\beta_k|\beta_m\rangle=\exp\{-\frac{1}{2}|\beta_k-\beta_m|^2\}$，表示$|\beta_k\rangle$与$|\beta_m\rangle$的重叠。于是可得一组方程为

$$\lambda b_k=c_k\left(\sum_{m=0}^{3}G_{km}b_m\right),(k=0,1,2,3)\tag{20}$$

移项可得

$$\left(\frac{\lambda}{c_k}-1\right)b_k-\sum_{m\neq k}G_{km}b_{k_m}=0\tag{21}$$

式(21)定义了齐次线性系统$\boldsymbol{Wb}=0$，其中$\boldsymbol{b}=\left(b_0,b_1,b_2,b_3\right)$，$\boldsymbol{W}$可以表示为

$$\boldsymbol{W}=\begin{pmatrix}\frac{\lambda}{c_0}-1 & -G_{01} & -G_{02} & -G_{03}\\ -G_{10} & \frac{\lambda}{c_1}-1 & -G_{12} & -G_{13}\\ -G_{20} & -G_{21} & \frac{\lambda}{c_2}-1 & -G_{23}\\ -G_{30} & -G_{31} & -G_{32} & \frac{\lambda}{c_3}-1\end{pmatrix}\tag{22}$$

方程$\boldsymbol{Wb}=0$总有平凡解$\boldsymbol{b}=0$，于是为了获得非零特征向量，将施加条件$\det\boldsymbol{W}=0$，这为本文提供了本征值λ_k和相应的冯诺依曼熵$S[\rho]=-\sum_{k=0}^{3}\lambda_k\mathrm{lb}\lambda_k$。

3　性能分析和讨论

本节对SDD-CVQKD协议的性能进行定量分析。数值模拟将噪声和器件缺陷作为全局影响参数，包括SDD检测效率、热噪声、相位噪声、暗计

数噪声和分束器透射率。这些仿真参数如表1所示，其值源于现实的实验环境[28-30]，具有可实现性。

表1　　仿真参数

参数	取值
SDD检测效率η_d	0.72
热噪声N_t	0.01
相位噪声ξ	0.998
暗计数噪声v	0.001
分束器透射率ζ	0.99

图3展示了SDD-CVQKD协议在四分支自适应测量结构下的渐近密钥率性能表现。为突出SDD面对不同调制量子态的兼容性和有效性，不仅展示了SDD-CVQKD协议在QPSK和16QAM两种不同调制方式下的性能，还对比了在QPSK调制下传统CVQKD协议的密钥率曲线，同时为突显SDD-CVQKD协议的性能优势，绘制了正向协商下非高斯探测器在CVQKD中的密钥率表现作为对比[25]。通过对比分析发现，SDD-CVQKD协议在最小信道透射率和密钥生成率两个关键性能指标上均展现出明显的优势，这一优势主要得益于SDD较低的检测错误概率和数据协商策略。具体而言，SDD的部署使本文协议以低于SQL的错误概率判别出接收量子态类别，使密钥率对比传统CVQKD协议展现出了显著的提升，说明SDD在提高CVQKD密钥率方面的优势。在数据协商策略方面，对比正向协商下非高斯探测器在CVQKD中的表现，反向协商策略在密钥率和信道参数上均有提升。具体而言，密钥率在信道参数较低（$\eta < 0.5$）时仍为正，而在正向协商下总呈现负密钥率的现象，这说明本文协议能突破“3 dB极限”的限制，从而大幅提高协议性能。

进一步分析表明，在16QAM调制下，SDD-CVQKD协议的密钥生成率明显优于QPSK调制下SDD-CVQKD协议的密钥生成率。这是因为16QAM调制相较于QPSK调制能够传输更多的信息量。为更清晰地解释这一点，本文定义调制增益因子$\Gamma = \dfrac{\mathrm{lb}(N)}{1+P_e}$量化调制方式在信息承载能力与错误概率之间综合效率的核心指标，其中N表示调制态数目，P_e表示SDD对不同调制方式的错误概率。图4给出了调制增益因子关于平均光子数的函数。从图4可以看出，16QAM调制增益因子优于QPSK调制，表明信息承载量的提升幅度超过了错误概率增加带来的损耗，因此在16QAM调制下的密钥生成率自然更高。此外，所有基于SDD技术的协议均能够突破PLOB界，这一突破源于SDD技术的工作机制，它能够准确地识别和恢复发送方传输的量子态。具体地说，若$\left|\tilde{\beta}_k\right\rangle = \left|\beta_k\right\rangle$推断正确，这在概念上类似于在Bob端入口前部署无噪放大器[31]，以补偿信道损耗和噪声引起的负面影响，为传统CVQKD协议超过PLOB界提供了一种可行的方法。

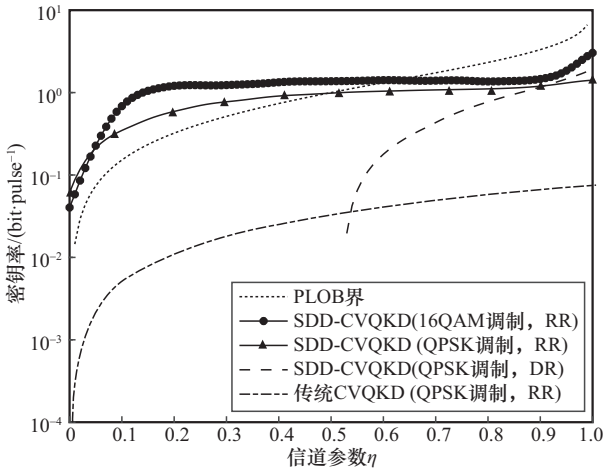

图3　密钥率曲线

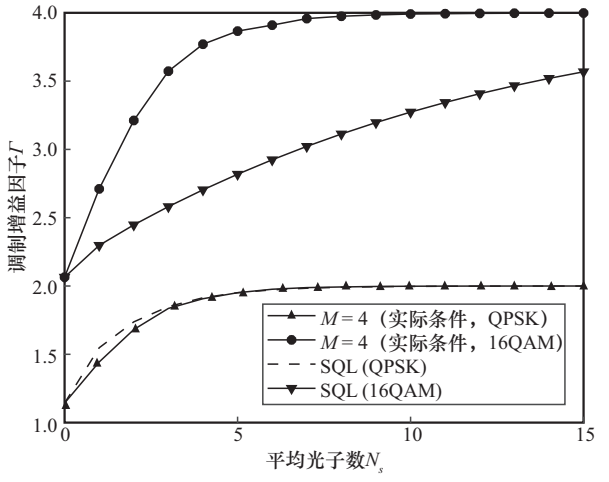

图4　调制增益因子

为深入探究SDD在提高CVQKD协议密钥率方面的机理，绘制了如图5所示的错误概率曲线。此外，图5中还包含SQL和Helstrom极限作为对比的分析，它们都是作为平均光子数（N_s）的函数来表示的。不难看出，采用四轮自适应测量的SDD在

错误概率方面始终保持在SQL以下。这些定量结果不仅验证了本文提出的SDD能够超越SQL的假设，而且随着自适应测量次数的增加，SDD的错误概率进一步降低。可以预见，随着自适应测量次数的增加，SDD的错误概率将进一步趋近Helstrom极限。理论上，当自适应测量次数达到一定量时，其错误概率将趋近Helstrom极限。同时，SDD装置的理想程度也影响着错误概率性能，理想条件（无噪声、设备无损耗）下SDD展现的错误概率始终低于实际条件下的错误概率，因此优化SDD设备硬件也是降低其错误概率的一个方向。值得注意的是，SDD在判别16QAM调制相干态时表现出相对较高的错误概率。这是因为16QAM调制涉及的相干态数量更多，从而增加了判别难度。然而，尽管16QAM调制下的错误概率较高，但其展示出的密钥率却高于QPSK调制。针对这一现象，一方面，由于16QAM调制下每个脉冲能够传输更多的信息量，从而在整体上提高了密钥率。另一方面，如图5子图所示，即使SDD在判别16QAM调制相干态的错误概率高于判别QPSK调制相干态，但相对于16QAM调制的SQL仍表现出一定的优势，且其提升明显优于QPSK调制时SDD相比于传统相干探测器的错误概率提升。此外，调制方式在信息承载能力与错误概率之间的综合效率已在上述分析中给出，16QAM调制效率始终高于QPSK调制。综合表明，尽管16QAM调制下的判别难度增加，但其在信息传输效率上的优势仍然能够为CVQKD系统带来更高的密钥率。

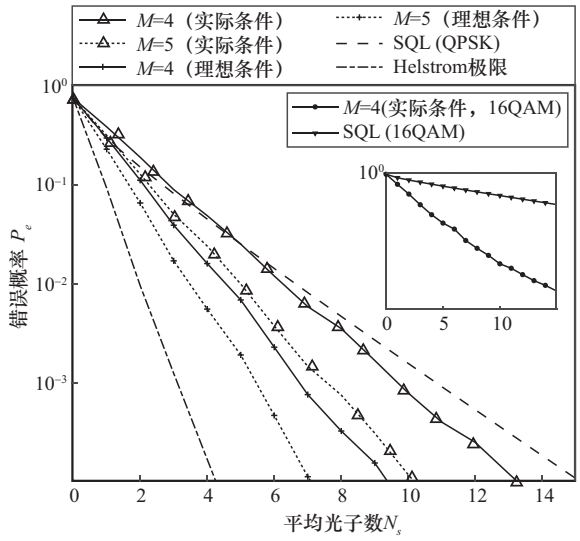

图5　错误概率曲线

针对信道参数η较小时SDD-CVQKD协议密钥率快速下降的问题，采用PS方案进行补偿，其是一种有效的策略，用于增强安全密钥生成的效率[32]。具体而言，该方案允许通信双方Alice和Bob仅保留那些具有正密钥率的测量结果，而舍弃密钥率为负的事件。图6展示了在不同信道参数η下，PS方案对SDD-CVQKD协议在QPSK和16QAM调制方案下性能的影响。当信道参数η较大$(\eta > 0.1)$时，PS方案对SDD-CVQKD协议性能的提升作用有限。这是因为在信道损耗较小的范围内，几乎所有Alice和Bob之间的相关事件均表现为正密钥率，因此PS方案的筛选作用并不显著。然而，当信道参数η较小，即信道噪声较大时，SDD检测的准确性会受到影响，导致Alice和Bob之间的相关事件数量减少。在这种情况下，PS方案的选择性保留可以有效地补偿信道噪声与设备条件不理想而造成的信息损失。此外，在16QAM调制方案下，PS方案对SDD-CVQKD协议性能的提升幅度明显大于QPSK调制方案。这一现象可以归因于16QAM调制方案下SDD的错误概率高于QPSK调制方案。由于16QAM调制方案的相干态预测更加困难，因此更容易出现密钥率为负的信号。在这种情况下，PS方案的补偿效果尤为明显，提高了密钥生成的效率和安全性。总的来说，PS方案在信道条件不理想时，尤其是在16QAM调制方案下，对于提高SDD-CVQKD协议的性能具有重要作用。PS方案通过选择性地保留具有正密钥率的事件，能够有效地补偿由于信道噪声和设备条件不理想带来的信息损失，增强了量子密钥分发的安全性和可靠性。

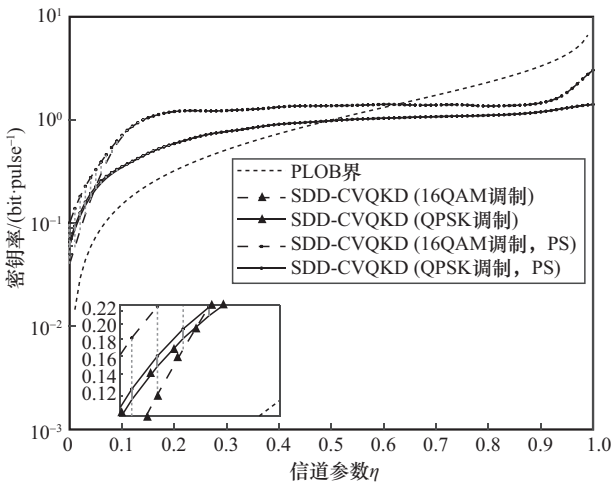

图6　后选择补偿

上述所有的性能分析均基于SDD-CVQKD协议受到Eve发动集体分束攻击的情形。但这类攻击限制了Eve的能力，实际上Eve可以执行比集体分束攻击更强大的一般攻击，即相干攻击。因此，本文通过广义熵累积定理（GEAT）进一步研究了有限长密钥下SDD-CVQKD协议对相干攻击的组合安全性，详细推导见附录1。图7给出了SDD-CVQKD的组合密钥率表现。为方便对比，也给出了其在集体分束攻击下的渐近性能曲线。可以看出，随着密钥块长度的减小，SDD-CVQKD的组合密钥率减小。特别地，当密钥块长度n=10^4时，SDD-CVQKD的组合密钥速率保持为正，这相对于传统CVQKD的有限长密钥率有明显改进，这种改进的主要原因是SDD-CVQKD不再需要牺牲部分信号数据进行专门的参数估计，这是因为信道参数的影响已实时反映在SDD的测量结果中，从而直接改变了基于历史数据的概率计算。

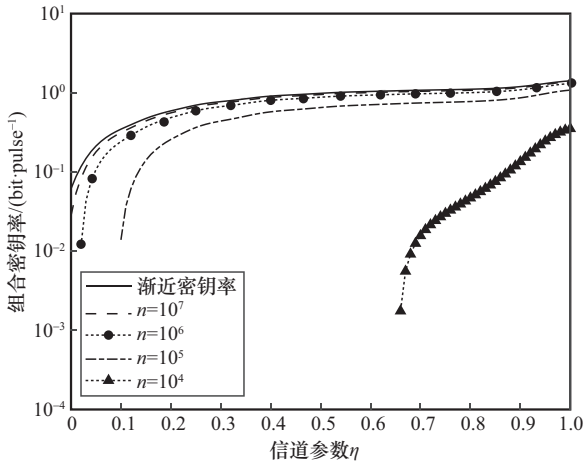

图7　组合密钥率

4　结束语

针对CVQKD系统中传统相干探测器受SQL的限制问题，本文提出了一种基于SDD的改进协议SDD-CVQKD。该协议通过多轮自适应测量与MAP准则判断，实现对离散调制相干态的高精度识别，降低了检测错误概率，并在反向协商与集体分束攻击条件下推导出密钥率表达式。数值仿真结果表明，在相同条件下，SDD-CVQKD协议在信道参数与密钥率性能方面均优于传统CVQKD协议，甚至突破了PLOB界。研究观察到，SDD通过非高斯测量结构和贝叶斯推理机制，能够以低于SQL的错误概率区分非正交相干态，且错误概率随自适应测量轮次的增加而进一步降低并逼近Helstrom极限。值得注意的是，尽管SDD-CVQKD在多进制调制（如16QAM）下因相干态数增加导致判别难度上升，但其每个脉冲携带更多信息以及检测错误概率仍低于16QAM下的SQL，因此能实现更高的密钥率。此外，本文提出了一种PS方案，以补偿SDD-CVQKD在长距离传输情况下设备非理想性以及信道噪声增加导致的性能下降。结论表明，SDD-CVQKD协议通过提升态识别精度和优化检测策略，有效提升了传统CVQKD协议的性能，为远距离、高安全性量子密钥分发提供了可行方案。

值得注意的是，PLOB界代表了两方量子通信在纯损量子信道与局域操作和经典通信条件下的性能极限。而SDD-CVQKD协议采用了非高斯测量操作、后选择方法等额外资源，从而获得性能上的显著提升。虽然本文协议并不违背基本的量子力学原理，但其性能的提升确实源于对额外资源的利用，这超出了PLOB界的假设条件。因此，本文对PLOB界的突破仅基于数值仿真下的“表观”超越，而非严格意义上的物理极限突破。

未来工作将进一步探索SDD在多用户量子通信、高维调制系统以及实际网络环境中的集成应用，同时将利用量子算法等优化自适应测量策略降低计算复杂度，在同样算力资源下实现更多的自适应测量次数，提高检测准确率，推动该技术向实用化方向发展。

附录1　SDD-CVQKD在相干攻击下的组合密钥速率推导

相干攻击是指最普遍和最强大的一类窃听策略，其中Eve利用整个量子系统的量子相干性对所有传输的量子态进行全局联合操纵。本文利用GEAT推导了SDD-CVQKD在相干攻击下的组合密钥率，该方法可以直接应用于制备–测量协议，而不依赖于虚拟层析成像，提供了改进的有限大小密钥速率[33]。

假设Alice发送n轮脉冲，Eve的条件熵在单轮中给定Bob的测量结果，计算式为

$$H(B|E)=H(B)-I(B,E)=I_{\mathrm{AB}}+H(B|A)-I(B,E) \tag{23}$$

其中，$H(B|A)$可以通过纠错来最小化，$I(B,E)$是Bob和Eve之间的互信息，其可以由式(16)给出。由于集体分束攻击已被证明在纯损无噪信道时是最佳的[32]。因此，本文有$H(B|E)\geqslant I_{\mathrm{AB}}-\chi_{\mathrm{BE}}$，根据定义，最小折中函数$f_{\mathrm{const}}$=

$\min\left(H\left(B|A\right)\right)$，使$f_{\text{const}}=I_{\text{AB}}-\chi_{\text{BE}}$。有限长$n$轮下最小光滑熵的下界为

$$H_{\min}>nf_{\text{const}}-n\left[\frac{a-1}{2-a}\frac{\ln 2}{2}V^2+\left(\frac{a-1}{2-a}\right)^2K_a\right]-\frac{\Xi(\varepsilon)}{a-1} \quad (24)$$

其中，$\frac{a-1}{2-a}\frac{\ln 2}{2}V^2$是GEAT的二阶项，它量化了样本有限时熵累积的误差，其规模为$O\left(\sqrt{n}\right)$；$V=\sqrt{2}+\text{lb}\left(2d^2+1\right)$，其中$d$表示系统维数；$\left(\frac{a-1}{2-a}\right)^2K_a$是GEAT的高阶项，它可以对二阶项进行边界控制，从而防止其在n较低时掩盖一阶项引起的边界失效；$\frac{\Xi(\varepsilon)}{a-1}$是最小平滑熵的校正项，其反映了在有限尺寸范围内实现安全性的成本，且$\Xi(x)=-\text{lb}(1-\sqrt{1-x^2})$。因此有

$$K_\alpha=\frac{(2-\alpha)^3}{6(3-2\alpha)^3\ln 2}2^{\frac{2(\alpha-1)}{2-\alpha}\text{lb}d}\ln^3\left(2^{2\text{lb}d}+\text{e}^2\right) \quad (25)$$

纠错期间泄漏的信息量为$\frac{1}{n}\text{leak}_{\text{EC}}\leqslant(1+f)H\left(B\middle|A\right)$，其中$f\geqslant 0$表示错误校正的无效性（$f=0$表示完美纠错）。$2\text{lb}\frac{1}{\varepsilon_{\text{PA}}}$表示秘密放大的成本，其中，$\varepsilon_{\text{PA}}$表示秘密放大的失败概率。然后，SDD-CVQKD抵抗相干攻击的组合密钥速率可以通过式(26)计算。

$$R_{\text{comp}}\geqslant\frac{l}{n} \quad (26)$$

其中，密钥长度$l=H_{\min}-\text{leak}_{\text{EC}}-2\text{lb}\frac{1}{\varepsilon_{\text{PA}}}$，因此有

$$R_{\text{comp}}\geqslant f_{\text{const}}-\frac{a-1}{2-a}\frac{\ln 2}{2}V^2+\left(\frac{a-1}{2-a}\right)^2K_a-\frac{1}{n}\left[\frac{\Xi(\varepsilon)}{a-1}+\text{leak}_{\text{EC}}+2\text{lb}\frac{1}{\varepsilon_{\text{PA}}}\right] \quad (27)$$

在仿真实验中，本文设置了$\varepsilon=\varepsilon_{\text{PA}}=10^{-10}$，参数$a\in\left(1,1+O(\sqrt{n})\right)$。

参考文献：

[1] Kok P, Lovett B W. Introduction to optical quantum information processing[M]. Cambridge: Cambridge University Press, 2010.

[2] Braunstein S L, Loock P V. Quantum information with continuous variables[J]. Reviews of Modern Physics, 2005, 77(2): 513-577.

[3] Lo H K, Curty M, Tamaki K. Secure quantum key distribution[J]. Nature Photonics, 2014, 8(8): 595-604.

[4] Bennett C H, Bessette F, Brassard G, et al. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

[5] Weedbrook C. Continuous-variable quantum key distribution with entanglement in the middle[J]. Physical Review A, 2013, 87(2): 022308.

[6] Ralph T C. Continuous variable quantum cryptography[J]. Physical Review A, 1999, 61: 010303.

[7] Hillery M. Quantum cryptography with squeezed states[J]. Physical Review A, 2000, 61(2): 022309.

[8] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states[J]. Physical Review Letters, 2002, 88(5): 057902.

[9] Silberhorn C, Ralph T C, Lütkenhaus N, et al. Continuous variable quantum cryptography: beating the 3 dB loss limit[J]. Physical Review Letters, 2002, 89(16): 167901.

[10] Weedbrook C, Lance A M, Bowen W P, et al. Quantum cryptography without switching[J]. Physical Review Letters, 2004, 93(17): 170504.

[11] Navascués M, Grosshans F, Acín A. Optimality of Gaussian attacks in continuous-variable quantum cryptography[J]. Physical Review Letters, 2006, 97(19): 190502.

[12] García-Patrón R, Cerf N J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution[J]. Physical Review Letters, 2006, 97(19): 190503.

[13] Jouguet P, Kunz-Jacques S, Diamanti E, et al. Analysis of imperfections in practical continuous-variable quantum key distribution[J]. Physical Review A, 2012, 86(3): 032309.

[14] Leverrier A, Grangier P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation[J]. Physical Review A, 2011, 83(4): 042312.

[15] Ghorai S, Grangier P, Diamanti E, et al. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation[J]. Physical Review X, 2019, 9(2): 021059.

[16] Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution[J]. Physical Review X, 2019, 9(4): 041064.

[17] Denys A, Brown P, Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation[J]. Quantum, 2021, 5: 540.

[18] Takeoka M, Sasaki M. Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers[J]. Physical Review A, 2008, 78(2): 022320.

[19] Liao Q, Liu X Q, Ou B, et al. Continuous-variable quantum secret sharing based on multi-ring discrete modulation[J]. IEEE Transactions on Communications, 2023, 71(10): 6051-6060.

[20] Helstrom C W. Quantum detection and estimation theory[J]. Journal of Statistical Physics, 1969, 1(2): 231-252.

[21] Tsujino K, Fukuda D, Fujii G, et al. Quantum receiver beyond the standard quantum limit of coherent optical communication[J]. Physical Review Letters, 2011, 106(25): 250503.

[22] Becerra F E, Fan J, Baumgartner G, et al. M-ary-state phase-shift-keying discrimination below the homodyne limit[J]. Physical Review A, 2011, 84(6): 062324.

[23] Liao Q, Guo Y, Huang D, et al. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection[J]. New Journal of Physics, 2018, 20(2): 023015.

[24] Zhao M F, Yuan R Z, Cheng J L, et al. Security of binary modulated continuous variable quantum key distribution using optimally displaced threshold detection[J]. IEEE Communications Letters, 2021, 25(4): 1089-1093.

[25] Zhao M F, Yuan R Z, Feng C, et al. Security of coherent-state quantum key distribution using displacement receiver[J]. IEEE Journal on Selected Areas in Communications, 2024, 42(7): 1871-1884.

[26] Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications[J]. Nature Communications, 2017, 8: 15043.

[27] Notarnicola M N, Jarzyna M, Olivares S, et al. Optimizing state-discrimination receivers for continuous-variable quantum key distribution over a wiretap channel[J]. New Journal of Physics, 2023, 25(10): 103014.

[28] Becerra F E, Fan J, Baumgartner G, et al. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination[J]. Nature Photonics, 2013, 7(2): 147-152.

[29] Wittmann C, Andersen U L, Takeoka M, et al. Demonstration of coherent-state discrimination using a displacement-controlled photon-number-resolving detector[J]. Physical Review Letters, 2010, 104(10): 100505.

[30] Becerra F E, Fan J, Migdall A. Photon number resolution enables quantum receiver for realistic coherent optical communications[J]. Nature Photonics, 2015, 9(1): 48-53.

[31] Blandino R, Leverrier A, Barbieri M, et al. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier[J]. Physical Review A, 2012, 86: 012327.

[32] Heid M, Lütkenhaus N. Efficiency of coherent-state quantum cryptography in the presence of loss: influence of realistic error correction[J]. Physical Review A, 2006, 73(5): 052316.

[33] Pascual-García C, Bäuml S, Araújo M, et al. Improved finite-size key rates for discrete-modulated continuous-variable quantum key distribution under coherent attacks[J]. Physical Review A, 2025, 111(2): 022610.

[作者简介]

廖骁（1990– ），男，湖南长沙人，博士，湖南大学副教授，主要研究方向为量子保密通信、智能量子计算、网络安全。

唐冲（2001– ），男，湖南益阳人，湖南大学硕士生，主要研究方向为量子保密通信。

杨俊跃（2002– ），男，安徽六安人，湖南大学硕士生，主要研究方向为量子保密通信。

李君浩（2000– ），男，湖南娄底人，湖南大学硕士生，主要研究方向为量子保密通信。