利用光放大器改进自参考连续变量量子密钥分发

龚峰, 杨鑫, 王天一*
贵州大学大数据与信息工程学院, 贵州 贵阳 550025

摘要 针对自参考连续变量量子密钥分发(SR-CV-QKD)协议传输距离还有待提升的问题,提出利用光放大器(OA)来改进系统,有效地补偿了由参考脉冲和探测器缺陷引起的相位噪声的衰减影响。通过安全性分析推导出改进后的安全码率,基于实际参数进行仿真,结果表明,利用放大器能够提升弱参考脉冲下的自参考连续变量量子密钥分发协议的性能,延长最大传输距离。

关键词 量子光学; 连续变量; 量子密钥分发; 光放大器; 参考脉冲; 相位噪声
中图分类号 O431.2 **文献标识码** A **doi**: 10.3788/LOP56.212702

Improvement of Self-Referenced Continuous Variable Quantum Key Distribution Using Optical Amplifier

Gong Feng, Yang Xin, Wang Tianyi*
College of Big Data and Information Engineering, Guizhou University, Guiyang, Guizhou 550025, *China*

Abstract The transmission distance of a self-referenced continuous variable quantum key distribution (SR-CV-QKD) protocol still needs to be improved. Therefore, this study proposes an optical amplifier to improve the system and effectively compensate for the attenuation of phase noise caused by reference pulse. The secret key rate is derived through security analysis. Simulation results based on practical parameters show that adding an amplifier can improve the performance of the SR-CV-QKD protocol with a weak reference pulse and extend the maximum transmission distance.

Key words quantum optics; continuous variable; quantum key distribution; optical amplifier; reference pulse; phase noise
OCIS codes 270.5565; 060.5525; 270.5568; 270.5585

1 引 言

量子密钥分发(QKD)[1]是一种新型密钥分发手段,它为通信双方 Alice 和 Bob 提供了一种在不安全量子信道中生成安全密钥的方法。QKD 经历了几个阶段的演化:首先是以单光子检测技术为基础的离散变量(DV)-QKD,其代表为 BB84 协议[2];其次是以光场正则分量为信息载体的连续变量(CV)-QKD,如 GG02 协议[3];而后又提出设备无关(DI)-类协议[4]等。由于实际情况中,单光子在制备和检测方面存在很大技术难题,而 CV-QKD 具有与目前光纤系统契合的特点,成了单光子类协议更有效的替代方案。

DV-QKD 研究取得了很多成果。朱卓丹等[5]提出了一种基于预报相干光子对的测量设备无关 QKD 协议改进方案,有效降低了密钥分发的误码率;唐鹏毅等[6]为解决中远距离悬空光缆 QKD 成码难的问题,设计了高速偏振反馈系统;何业锋等[7]研究了基于指示单光子源的非对称信道的测量设备无关 QKD 协议的性能;朱秋立等[8]利用离散相位编码构建了自由空间 QKD 分系统,通过偏振滤波抑制背景光,从而有效降低误码率;而 CV-QKD 相关理论研究也取得很多突破[9-11],但与此同时也暴露出了 CV-QKD 的一些重大缺陷[12-14]。特别是本振光(LO)的传输问题,这为 CV-QKD 的研究进展埋下了隐患。当前,一些

收稿日期: 2019-03-14; **修回日期**: 2019-04-29; **录用日期**: 2019-05-06
基金项目: 贵州省科技计划项目([2016]7431)
* **E-mail**: tywang@gzu.edu.cn

针对本振光传输的攻击已相继被提出，这些攻击一定程度上降低了 CV-QKD 的安全性，例如本振光强度攻击[15]、本振光校准攻击[16]等。所幸的是，研究者们提出了一种新的有效方案——SR-CV-QKD[17]，该方案利用参考脉冲建立起 Alice 和 Bob 之间的公共参考系，使用由参考系不匹配引入的相位差来估计双方之间数据的相关性，成功地消除了本振光传输的需求，提升了协议的整体安全性。此后，关于 CV-QKD 本振光的相关研究逐渐增多，其中大多数都倾向于协议性能的优化。如文献[18-19]提出了一种利用时分复用和极化复用技术改进 CV-QKD 的新方案，不仅保证了协议的安全性和易实现性，而且大大提高了密钥率和安全传输距离。

本文中主要探究在 Bob 端加入的光放大器(OA)对 SR-CV-QKD 系统性能的影响，是否能够补偿由参考脉冲引入的相位噪声所带来的影响等问题。通过安全性分析，仿真结果表明，使用光放大器能够增大 SR-CV-QKD 系统安全传输距离。

2 SR-CV-QKD 协议

SR-CV-QKD 方案如图 1 所示。其中，A'、B_0、B_1、B_2、B_3、G、F、E 为相应端口的输入输出，V 和 v 表示对应 EPR(Einstein-Podolsky-Rosen paradox)态的调制方差，χ_{line} 指信道噪声，x_{A}、p_{A} 表示 Alice 测量的两个正交分量，x_{B}、p_{B} 表示 Bob 测量的两个正交分量。该方案消除了传输本振光的需要，从而简化了对硬件的要求，而且一定程度上加强了协议的安全性。协议开始时，Alice 会制备一个高斯调制相干态(信号脉冲)，发送给 Bob。接下来，Alice 还会将另一个相干态作为参考脉冲发送给 Bob，其中参考脉冲幅度 V_{R} 要比信号脉冲方差 V_{A} 大好几倍，但一般要比本振光小很多。

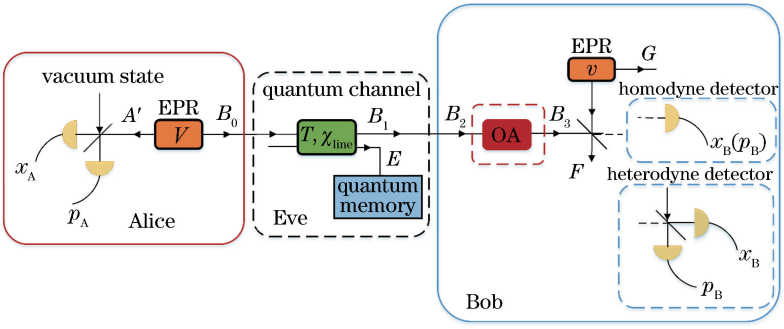

图 1 添加放大器的 SR-CV-QKD 协议纠缠等效方案

Fig. 1 Entangled equivalent scheme of SR-CV-QKD protocol with optical amplifier

与传统 CV-QKD 协议的区别在于 SR-CV-QKD 方案将进行两次测量：Bob 将对接收到的信号脉冲和参考脉冲正交分量进行零差或外差检测，以分别获取相应的测量值。Alice 和 Bob 参考系的相空间表示存在偏离，使得它们之间存在一个相位差 θ，考虑到量子不确定性影响，相位差估计 $\hat{\theta}=\theta+\varphi$，其中 φ 为估计存在的误差，$\hat{\theta}$ 为相位差估计。

在传统的 CV-QKD 协议中，测量前，Alice 和 Bob 的协方差矩阵为

$$\boldsymbol{\gamma}_{\text{AB}}=\begin{bmatrix} V\boldsymbol{H} & C\boldsymbol{\sigma}_z \\ C\boldsymbol{\sigma}_z & T(V+\chi_{\text{line}})\boldsymbol{H} \end{bmatrix}, \tag{1}$$

式中：$\boldsymbol{H}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$；$\boldsymbol{\sigma}_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$；$V=V_{\text{A}}+1$，$V_{\text{A}}$ 为 Alice 的调制方差；Alice 和 Bob 之间协方差的系数 $C=\sqrt{T(V^2-1)}$；信道透过率 $T=10^{-\alpha L/10}$，光纤衰减系数 $\alpha=0.2$ dB/km，L 为传输距离；信道噪声 $\chi_{\text{line}}=\dfrac{1-T}{T}+\varepsilon$，$\varepsilon$ 为信道过量噪声。

而在 SR-CV-QKD 协议过程中，需要考虑参考系失衡所导致的相空间旋转的影响，这包括随机变量 θ 和 φ 的分布。测量前，Alice 和 Bob 共享态的密度矩阵[17]为

$$\bar{\boldsymbol{\rho}}_{\text{AB}}=\overline{\boldsymbol{\rho}}_{\text{AB}}(\hat{\theta},\theta)=\int_{-\pi}^{\pi}\mathcal{P}(\varphi)\mathrm{d}\varphi\int_{-\pi}^{\pi}\frac{\boldsymbol{\rho}_{\text{AB}}(\hat{\theta},\theta)}{2\pi}\mathrm{d}\theta, \tag{2}$$

$$\boldsymbol{\rho}_{\text{AB}}(\hat{\theta},\theta)=\boldsymbol{U}_{\text{A}}(-\hat{\theta})\boldsymbol{U}_{\text{B}}(\theta)\boldsymbol{\rho}_{\text{AB}}\boldsymbol{U}_{\text{A}}^{\dagger}(-\hat{\theta})\boldsymbol{U}_{\text{B}}^{\dagger}(\theta), \tag{3}$$

式中：$\boldsymbol{U}_{\text{A}}$ 和 $\boldsymbol{U}_{\text{B}}$ 表示相空间旋转算符；$\mathcal{P}(\varphi)$ 为随机变量 φ 的概率分布函数；$\boldsymbol{\rho}_{\text{AB}}$ 为量子态；$\boldsymbol{U}_{\text{A}}^{\dagger}$ 和 $\boldsymbol{U}_{\text{B}}^{\dagger}$ 为 $\boldsymbol{U}_{\text{A}}$ 和 $\boldsymbol{U}_{\text{B}}$ 的厄米共轭；态 $\bar{\boldsymbol{\rho}}_{\text{AB}}$ 也是高斯的，其协方差矩阵[17]可表示为

$$\bar{\boldsymbol{\gamma}}_{AB}=\overline{\boldsymbol{\gamma}}_{AB}(\hat{\theta},\theta)=\int_{-\pi}^{\pi}\mathscr{P}(\varphi)\mathrm{d}\varphi\int_{-\pi}^{\pi}\frac{\boldsymbol{\gamma}_{AB}(\hat{\theta},\theta)}{2\pi}\mathrm{d}\theta,\tag{4}$$

$$\boldsymbol{\gamma}_{AB}(\hat{\theta},\theta)=[\boldsymbol{U}'_{A}(-\hat{\theta})\oplus\boldsymbol{U}'_{B}(\theta)]\,\boldsymbol{\gamma}_{AB}\,[\boldsymbol{U}'^{T}_{A}(-\hat{\theta})\oplus\boldsymbol{U}'^{T}_{B}(\theta)],\tag{5}$$

式中：$\boldsymbol{U}'_{A}$和$\boldsymbol{U}'_{B}$是相空间旋转算符$\boldsymbol{U}_{A}$和$\boldsymbol{U}_{B}$的辛表示；$\boldsymbol{U}'^{T}_{A}$和$\boldsymbol{U}'^{T}_{B}$表示$\boldsymbol{U}'_{A}$和$\boldsymbol{U}'_{B}$的转置矩阵；⊕表示直和。

通过计算上述积分可得到 SR-CV-QKD 的初始协方差矩阵为

$$\bar{\boldsymbol{\gamma}}_{AB}=\begin{bmatrix}V\boldsymbol{H} & C\sqrt{1-\xi}\boldsymbol{\sigma}_{z}\\ C\sqrt{1-\xi}\boldsymbol{\sigma}_{z} & T(V+\chi)\boldsymbol{H}\end{bmatrix},\tag{6}$$

式中：$\xi=1-\overline{(\cos\varphi)}^{2}$。不难看出，引入参考脉冲所带来的影响其实是对传统 CV-QKD 协议的初始协方差矩阵的相关系数进行一定调整。

整个 SR-CV-QKD 协议中，相位差估计在安全码率的计算中起着至关重要的作用，有关它的一系列推导在此不详细赘述[17]。SR-CV-QKD 协议的剩余部分与传统的 CV-QKD 协议相同，包括参数估计、误差校正、保密增强等。

3 改进后的安全码率

3.1 无限码长下的安全性分析

本文主要考虑两种类型的光放大器[20]：相位敏感光放大器（PSA）和相位非敏感光放大器（PIA），其结构模型图如图 2 所示，N 为放大器噪声。PSA 是一种简并的光参量放大器，它能够对单个正交分量进行无噪放大。这个放大过程是非对称的，即同相的放大，正交的压缩。PIA 是一种非简并的光参量放大器，它能够同时放大两个正交分量，但是放大过程中，信号态要与该放大器内的闲置模式相互作用，因而会引入额外的噪声，也就是说信号态的两个正交分量能够同等程度放大，但是自身的不确定性也会增加。

考虑到两种放大器和零差、外差两种检测方式的特性，本文主要分析零差检测与 PSA 组合以及外差检测与 PIA 组合后的系统性能。

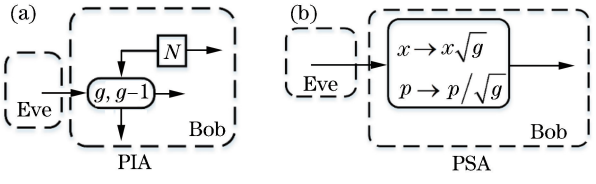

图 2 两种放大器的结构模型图。(a) PIA；(b) PSA

Fig. 2 Structural models of two types of amplifiers. (a) PIA; (b) PSA

集体攻击反向协调下的安全码率公式[21]为

$$R=\beta I_{AB}-\chi_{BE},\tag{7}$$

式中：I_{AB}是 Alice 和 Bob 之间的互信息；β 为协调效率；χ_{BE}是 Eve 和 Bob 之间互信息的 Holevo 界。

在计算两个互信息之前，先定义如下系统参数：信道输入的总噪声 $\chi_{tot}=\chi_{line}+\chi_{h}/T$，其中 χ_{h} 为不同检测方式引入的噪声。考虑到放大器的影响，Bob 探测结果的总噪声[20]分别为零差检测方式中加入 PSA 后的探测噪声 $\chi_{hom}^{PSA}=\dfrac{1-\eta+v_{el}}{g\eta}$，以及外差检测方式中加入 PIA 后的探测噪声 $\chi_{het}^{PIA}=\dfrac{1+(1-\eta)+2v_{el}+N(g-1)\eta}{g\eta}$。其中 η 为检测效率，v_{el}为电子噪声，g 为放大器增益。

通过(6)式并考虑到放大器的影响，互信息 I_{AB} 即可得到。

相干态零差检测的互信息为

$$I_{AB}=\frac{1}{2}\mathrm{lb}\frac{V+\chi_{tot}}{1+\chi_{tot}+(V-1)\xi}。\tag{8}$$

相干态外差检测的互信息为

$$I_{AB}=\mathrm{lb}\frac{V+\chi_{tot}}{1+\chi_{tot}+(V-1)\xi}。\tag{9}$$

其中 ξ 可转化为

$$\xi\lessapprox V_{\hat{\theta}}=\frac{\chi_{tot}+1}{V_{R}}+\frac{\delta_{R}}{TV_{R}},\tag{10}$$

式中：V_{R} 为参考脉冲幅度；$V_{\hat{\theta}}$ 表示相位差估计的方差；δ_{R} 对应采用不同检测方式的系数，外差检测$\delta_{R}=1$，零差检测 $\delta_{R}=0$。不难看出，加入放大器其实是通过直接影响信道总噪声 χ_{tot}来间接影响相位噪声的。

将(10)式分别代入(8)式和(9)式可求出互信息 I_{AB}的下界。

接下来，就要求出两种组合情况下 Eve 和 Bob 的互信息 χ_{BE}。对于零差检测和 PSA 组合情况，其 Holevo 界可表示为

$$\chi_{BE}=\sum_{i=1}^{2}G\left(\frac{\lambda_{i}-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_{i}-1}{2}\right),\tag{11}$$

式中：$G(x)=(x+1)\mathrm{lb}(x+1)-x\mathrm{lb}\,x$，为热场态的冯·诺依曼熵；$\lambda_{i}$ 为不同辛特征值，i 用于区分多

个辛特征值。辛特征值 $\lambda_{1,2}$ 可用下式求解：

$$\lambda_{1,2}^2=\frac{1}{2}(A\pm\sqrt{A^2-4B}),\tag{12}$$

其中：

$$\begin{cases}A=V^2(1-2T)+2T[1+(V^2-1)\xi]+\\ \quad T^2(V+\chi_{\text{line}})^2\\ B=T^2[V\chi+1+(V^2-1)\xi]^2\end{cases}。\tag{13}$$

联立(12)式和(13)式可求出辛特征值 $\lambda_{1,2}$，进而求出(11)式右边第一部分的熵。

而求解 $\lambda_{3,4,5}$ 需要先求解一个三模协方差矩阵[20]，通过该三模协方差矩阵求出辛特征值 $\lambda_{3,4}$，而 $\lambda_5=1$，进而可以求出 χ_{BE}。

对于外差检测和 PIA 组合的情况，由于 PIA 自身会引入噪声，因此需要把两个附加模式考虑进去，也就相当于比 PSA 多了两个模式，这时，互信息 χ_{BE} 可表示为

$$\chi_{\text{BE}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{7}G\left(\frac{\lambda_i-1}{2}\right)。\tag{14}$$

(14)式右边第一部分与(11)式一样，不同点在于第二部分，这里需要求解一个五模协方差矩阵[20]。同样，根据求出的五模协方差矩阵可求出辛特征值 $\lambda_{3,4}$，且 $\lambda_{5,6,7}=1$。通过(14)式即可求出互信息 χ_{BE}，最后求出安全码率 R。

3.2 有限码长下的简要分析

有限码长[22]对 CV-QKD 协议安全性有很大影响，与无限码长方案相比，其安全码率相对受限，传输距离也较短。具体而言，当数据长度有限时，抽样估计的波动会变差，这将导致对信道中 Eve 窃听行为的评估准确度下降。而为了获取更高的安全性，只能放宽估计的波动空间以包含更多可能的情况，对窃听行为作最坏估计，否则会面临高估安全码率的风险，正是这种放宽估计导致了协议性能的下降。由于篇幅有限，此部分内容在本次分析中相关公式不作详细推导，在分析部分将展示有限码长条件下零差检测的结果图。

对于有限码长情况，安全码率[22]为

$$R=\frac{n}{N'}[\beta I_{\text{AB}}^{\text{hom}}-S_{\text{BE}}^{\epsilon_{\text{PE}}}-\Delta(n)],\tag{15}$$

式中：N' 表示 Alice 和 Bob 之间交换数据的总长度；$I_{\text{AB}}^{\text{hom}}$ 为零差检测方式下 Alice 和 Bob 之间的互信息；n 表示总长度 N' 中只有 n 个数据用于生产密钥；ϵ_{PE} 为参数估计出错的概率；$S_{\text{BE}}^{\epsilon_{\text{PE}}}$ 为有限码长下 Bob 和 Eve 之间的互信息；β 为协调效率。剩余的 $m(m=N-n)$ 个数据用于参数估计。

$\Delta(n)$ 和保密增强安全性有关，其表达式[18]为

$$\Delta(n)=7\sqrt{\frac{\text{lb}(2/\bar{\epsilon})}{n}}+\frac{2}{n}\text{lb}(1/\epsilon_{\text{PA}}),\tag{16}$$

式中：$\bar{\epsilon}$ 为平滑参数；ϵ_{PA} 为保密增强过程失败概率。

分析过程中，对于参数估计阶段，主要考虑了过量噪声 ε 和透过率 T 的统计波动影响，表达式[18]为

$$\begin{cases}T_{\min}=\dfrac{(t-\Delta T)^2}{\eta}\\ \varepsilon_{\max}=\dfrac{\sigma^2+\Delta\sigma_0^2-1-v_{\text{el}}}{\eta T}\end{cases},\tag{17}$$

式中：$t=\sqrt{\eta T}$；$\sigma^2=\eta T+1+v_{\text{el}}$；$\Delta T=Z_{\epsilon_{\text{PE}}/2}\times\sqrt{\dfrac{\sigma^2}{mV_{\text{A}}}}$；$\Delta\sigma_0^2=Z_{\epsilon_{\text{PE}}/2}\dfrac{\sigma^2\sqrt{2}}{\sqrt{m}}$；$Z_{\epsilon_{\text{PE}}/2}$ 表示置信系数。

Bob 使用零差检测时，Alice 和 Bob 之间的互信息依然可以用(8)式表示。不同在于 Bob 和 Eve 之间的互信息计算，由于篇幅原因，这部分互信息在此不作详细阐述，具体分析详见文献[18]。

4 实际参数仿真分析

基于第 3 节推导出的安全码率表达式，利用 Matlab 软件对其进行仿真分析，来比较这两种组合(PSA＋零差探测和 PIA＋外差探测)在不同参数设定下的性能表现。本文主要绘制了集体攻击反向协调下基于光纤的高斯调制相干态 SR-CV-QKD 协议的安全码率曲线图。整个仿真过程中，系统主要参数设定如下：Alice 调制方差 $V_{\text{A}}=4$，参考脉冲 $V_{\text{R}}=100$，协调效率 $\beta=0.96$，额外噪声 $\varepsilon=0.01$，探测效率 $\eta=0.6$，电子噪声 $v_{\text{el}}=0.01$，$\bar{\epsilon}=\epsilon_{\text{PA}}=\epsilon_{\text{PE}}=10^{-10}$。

图 3 所示为渐进情况下，零差检测和 PSA 组合

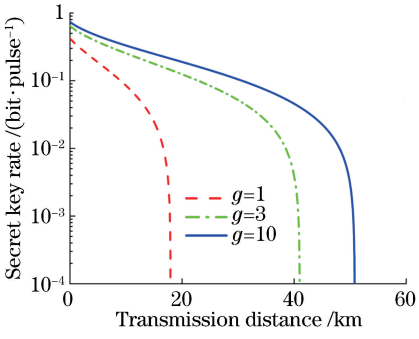

图 3 渐进情况下零差检测与 PSA 组合时的渐进安全码率

Fig. 3 Asymptotic secret key rate of homodyne detection combined with PSA under asymptotic case

的安全码率与传输距离关系曲线图。从图 3 可看出，SR-CV-QKD 协议传输距离随着放大器增益的增加有明显的提升，但提升效果逐渐减弱，这说明此类放大器的放大效果有限。

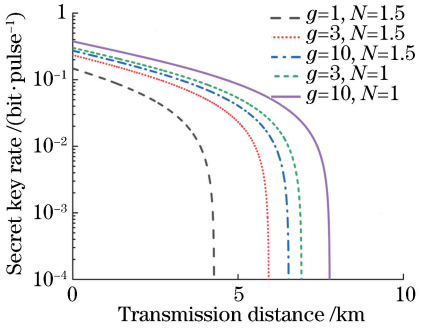

图 4 渐进情况下外差检测与 PIA 组合安全码率

Fig. 4 Secret key rate of heterodyne detection combined with PIA under asymptotic case

从图 4 容易看出，放大器的使用能增加这种情况下的传输距离，不过 PIA 自身存在噪声，这不可避免会使安全码率降低。总的来说，无论是零差检测与 PSA 组合，还是外差检测与 PIA 组合的情况，使用放大器都能提升系统的传输距离，其原因在于，随着放大器增益 g 的增加，总噪声 χ_{tot} 会减小，这无疑相当于增加了安全码率。此外，值得注意的是，实际情况中，放大器的使用起到的是积极还是消极的作用，这取决于放大器自身的固有噪声，对于本文的仿真参数，该阈值约为 2.37。即当 $N>2.37$ 时，使用放大器反而会降低系统性能，如图 5 所示，协议的最大传输距离随着放大器自身噪声的增加线性降低，当 $N>2.37$ 时，传输距离反而降低。原因在于有噪放大器引入的噪声本质上会同时降低 Alice 和 Bob 之间的互信息 I_{AB}，以及 Eve 所窃取的最大信息 χ_{BE}。但两者的下降程度并不一致，从而使安全码率和放大器噪声之间呈现出非线性的关系。在噪

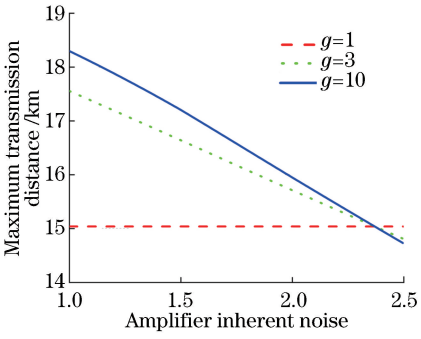

图 5 不同放大器噪声下的最大传输距离

Fig. 5 Maximum transmission distance under different amplifier noise

声容限内，噪声引起的 I_{AB} 的减少量小于的 χ_{BE} 减少量，因而可以达到提升性能的目的。而一旦超出该噪声容限，过多的噪声则会造成互信息 I_{AB} 的减少量大于 χ_{BE} 的减少量，这将导致安全码率和传输距离大幅下降。

图 6 是有限码长下零差检测与 PSA 组合时安全码率与距离的关系曲线图。从图 6 可看出，在有限码长下，协议性能相对无限码长而言受到限制，表现为码率下降，传输距离缩短，与图 3 对比来说，无限码长情况下，放大倍数分别为 1 和 3 时，传输距离分别为 17.94 km 和 40.98 km，而码长为 10^7 时，传输距离分别为 14.77 km 和 38.89 km。总体而言，随着码长的增加，其性能将不断提升。此外，受到低参考脉冲幅度的影响，SR-CV-QKD 性能与传统本振光传输的 CV-QKD 性能有着明显差距。

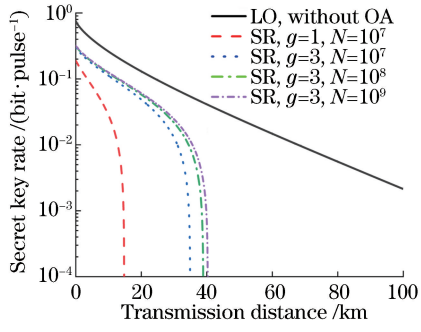

图 6 有限码长情况下零差检测与 PSA 组合时的安全码率

Fig. 6 Secret key rate of homodyne detection combined with PSA under finite code length

5 结论

本文研究了光放大器的使用对 SR-CV-QKD 协议性能的影响情况。将两种类型的光放大器置于 Bob 端，通过安全性分析分别计算了它们的安全码率。基于实际参数的仿真的结果表明，放大器的使用能够较好地补偿由参考脉冲引入的相位噪声带来的影响，从而使协议的最大传输距离延长。本文着重于 SR-CV-QKD 协议在有噪情况下的性能提升，而对于实际情况，CV-QKD 的理论分析还受到多方面因素的影响。接下来，将对所提改进方案在有限码长效应下更多参数统计波动进行具体分析。

参 考 文 献

[1] Ekert A K. Quantum cryptography based on Bell′s theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.

[2] Bennet C H, Brassard G. Quantum cryptography:

public key distribution and coin tossing[C]// IEEE International Conference on Computers, Systems, and Signal processing, December 9-12, 1984, Bangalore, India. New York: IEEE, 1984: 175-179.

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

[4] Acín A, Massar S, Pironio S. Efficient quantum key distribution secure against no-signalling eavesdroppers[J]. New Journal of Physics, 2006, 8(8): 126.

[5] Zhu Z D, Zhang X, Zhao S H, *et al*. Measurement-device-independent quantum key distribution protocols for heralded pair coherent state[J]. Laser & Optoelectronics Progress, 2017, 54(12): 122703.
朱卓丹, 张茜, 赵尚弘, 等. 预报相干光子对的测量设备无关量子密钥分发协议[J]. 激光与光电子学进展, 2017, 54(12): 122703.

[6] Tang P Y, Li G C, Gao S, *et al*. Fast polarization feedback algorithm for quantum key distribution with aerial fiber for power grid[J]. Acta Optica Sinica, 2018, 38(1): 0106005.
唐鹏毅, 李国春, 高松, 等. 针对电力悬空光缆量子密钥分发的高速偏振反馈算法[J]. 光学学报, 2018, 38(1): 0106005.

[7] He Y F, Song C, Li D Q, *et al*. Asymmetric-channel quantum key distribution based on heralded single-photon sources[J]. Acta Optica Sinica, 2018, 38(3): 0327001.
何业锋, 宋畅, 李东琪, 等. 基于指示单光子源的非对称信道量子密钥分配[J]. 光学学报, 2018, 38(3): 0327001.

[8] Zhu Q L, Shi L, Wei J H, *et al*. Quantum key distribution system based on polarization filtering for background light suppression[J]. Acta Optica Sinica, 2018, 38(12): 1227001.
朱秋立, 石磊, 魏家华, 等. 基于偏振滤波抑制背景光的量子密钥分配系统[J]. 光学学报, 2018, 38(12): 1227001.

[9] Huang D, Huang P, Lin D K, *et al*. Long-distance continuous-variable quantum key distribution by controlling excess noise[J]. Scientific Reports, 2016, 6: 19201.

[10] Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de finetti reduction[J]. Physical Review Letters, 2017, 118(20): 200501.

[11] Wang X Y, Zhang Y C, Yu S, *et al*. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code[J]. Scientific Reports, 2018, 8: 10543.

[12] Huang J Z, Weedbrook C, Yin Z Q, *et al*. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack[J]. Physical Review A, 2013, 87(6): 062329.

[13] Ma X C, Sun S H, Jiang M S, *et al*. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol[J]. Physical Review A, 2013, 87(5): 052309.

[14] Qin H, Kumar R, Alléaume R. Saturation attack on continuous-variable quantum key distribution system[J]. Proceedings of SPIE, 2013, 8899: 88990N.

[15] Ma X C, Sun S H, Jiang M S, *et al*. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems[J]. Physical Review A, 2013, 88(2): 022339.

[16] Jouguet P, Kunz-Jacques S, Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution[J]. Physical Review A, 2013, 87(6): 062313.

[17] Soh D B S, Brif C, Coles P J, *et al*. Self-referenced continuous-variable quantum key distribution protocol[J]. Physical Review X, 2015, 5(4): 041010.

[18] Wang T, Huang P, Zhou Y M, *et al*. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator[J]. Physical Review A, 2018, 97(1): 012310.

[19] Wang T, Huang P, Zhou Y M, *et al*. High key rate continuous-variable quantum key distribution with a real local oscillator[J]. Optics Express, 2018, 26(3): 2794-2806.

[20] Fossier S, Diamanti E, Debuisschert T, *et al*. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers[J]. Journal of Physics B: Atomic, Molecular and Optical Physics, 2009, 42(11): 114014.

[21] Scarani V, Bechmann-Pasquinucci H, Cerf N J, *et al*. The security of practical quantum key distribution[J]. Reviews of Modern Physics, 2009, 81(3): 1301-1350.

[22] Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution[J]. Physical Review A, 2010, 81(6): 062343.