引用本文：刘涛，王平平，房新新，等. 光放大器对空间量子通信系统性能的改进[J]. 光通信技术，2022，46(1)：49-56.

光放大器对空间量子通信系统性能的改进

刘 涛[1,2,3]，王平平[1*]，房新新[1]，李佳佳[1]，邱 佳[1]，王思佳[1]，刘舒宇[1]，张荣香[4]

（1. 华北电力大学 电子与通信工程系，河北 保定 071003；2. 华北电力大学 河北省电力物联网技术重点实验室，河北 保定 071003；
3. 华北电力大学 保定市光纤传感与光通信技术重点实验室，河北 保定 071003；4. 河北大学 物理科学与技术学院，河北 保定 071002）

摘要：为提升自由空间量子通信系统性能，以相敏放大器(PSA)和相位非敏感放大器(PIA)原理为基础，研究了在量子通信系统接收端分别加入PSA、PIA后的高斯调制连续变量量子密钥分发(CVQKD)模型，推导了相应的安全密钥率公式。当信号波长分别为810 nm、1550 nm和3800 nm时，仿真分析了系统受到集体攻击和个体攻击情况下接收端采用零差检测和外差检测时安全密钥率与距离的变化关系，对比了相同条件下PSA、PIA对系统性能的提升效果。仿真结果表明：当接收端分别采用零差检测、外差检测时，系统相应选择PSA、PIA时的性能更好。

关键词：连续变量量子密钥分发；自由空间量子通信；光放大器；安全密钥率

中图分类号：TN929.12　**文献标志码**：A　**文章编号**：1002-5561(2022)01-0049-08

DOI：10.13921/j.cnki.issn1002-5561.2022.01.011　开放科学(资源服务)标识码(OSID)：

Performance improvement of space quantum communication system by optical amplifier

LIU Tao[1,2,3], WANG Pingping[1*], FANG Xinxin[1], LI Jiajia[1], QIU Jia[1],
WANG Sijia[1], LIU Shuyu[1], ZHANG Rongxiang[4]

(1. Department of Electronic and Communication Engineering, North China Electric Power University, Baoding Hebei 071003, China;
2. Hebei Key Laboratory of Power Internet of Things Technology, North China Electric Power University, Baoding Hebei 071003, China;
3. Baoding Key Laboratory of Optical Fiber Sensing and Optical Communication Technology, North China Electric Power University, Baoding Hebei 071003, China; 4. College of Physics Science and Technology, Hebei University, Baoding Hebei 071002, China)

Abstract: In order to improve the performance of free space quantum communication system, based on the principles of phase sensitive amplifier(PSA) and phase insensitive amplifier(PIA), Gaussian modulated continuous variable quantum key distribution (CVQKD) with PSA and PIA at the receiver of quantum communication system is studied, deduces the corresponding security-key rate formula. When the signal wavelength is 810 nm, 1550 nm and 3800 nm respectively, the simulation analyzes the relationship between the security-key rate and the distance when the receiver adopts homodyne detection and heterodyne detection under the collective attack and individual attack, and compares the improvement effects of PSA and PIA on the system performance under the same conditions. The simulation results show that when the receiver adopts homodyne detection and heterodyne detection respectively in detection and heterodyne detection, the system has better performance when PSA and PIA are selected accordingly.

Key words: continuous variable quantum key distribution, free space quantum communication, optical amplifier, secret-key rate

收稿日期：2021-05-09。

基金项目：国家自然科学基金(批准号：62071180)资助；中央高校基本科研业务费专项基金(编号：2020MS099)资助。

作者简介：刘涛(1989—)，男，博士，副教授。2009年毕业于北京邮电大学做光子学与光通信研究所，长期从事光通信、量子通信和非线性光学等领域的科研和教学工作，发表了13篇EI论文、5篇SCI论文，发明专利多项。2015-2017年，以访问学者身份访问了美国亚利桑那大学。

*** 通信作者**：王平平(1996—)，女，硕士生，主要研究方向为量子通信。

0 引言

利用量子通信系统实现量子密钥分发的方式主要有2种：一种是离散变量量子密钥分发，另一种是连续变量量子密钥分发（CVQKD）。在CVQKD系统中，光量子的制备过程和探测过程使用的设备与传统光通信中所用设备基本一致，这使得CVQKD兼具安全性高和经济成本较低的优点，因此近年来受到了越来越多的关注。在量子通信时，较高的安全密钥率有助于支持更高速率的密钥使用；较长的通信距离有助

于更远的密钥分发，可以减少 CVQKD 系统的中继节点的个数；提高 CVQKD 的最大可容忍噪声容限能够使系统在比较复杂的通信环境下进行密钥分发过程，从而扩大了 CVQKD 的适用范围，提高其对实际通信环境的适应能力[1]。然而，量子通信系统的设计都是基于设备理想化的假设，实际设备中探测器的固有属性（检测效率低、引入电子噪声等）会使量子通信系统的安全密钥率降低、传输距离缩短。目前，相关研究表明，在通信系统中插入光学放大器可以改善这一问题。在光纤量子通信系统中使用的基本的光学放大器主要有掺铒光纤放大器、相敏放大器（PSA）和相位非敏感放大器（PIA）等。由于掺铒光纤放大器并不能改善色散效应，因此，研究者们提出利用 PIA 来解决此类问题。PSA 也同样能被用来改善自由空间量子通信系统的性能。

近年来，PSA 具有无噪声放大的特性和含有固定噪声的 PIA 的放大能力已被研究者证实[2]，因此其在量子通信领域拥有很大的发挥空间。2017 年，张一辰[1]研究了相位敏感放大器和 PIA 对基于光纤信道的 CVQKD 双路协议的改善方案，并且当加入 PSA 时只研究了 Bob 采用零差检测方式下系统受到集体攻击时的安全密钥率随距离的变化关系；当加入 PIA 时只研究了 Bob 采用外差检测方式，系统受到集体攻击时的安全密钥率随距离的变化关系。2020 年，黄露雨[3]分析了 PSA 对基于光纤信道的高斯类协议和一维调制类协议的改进方法，只考虑了 Bob 采用零差检测方式下系统受到集体攻击时的安全密钥率随距离的变化关系。然而，在实际的量子通信过程中，系统遭受的不同攻击类型和 Bob 采用的不同检测方式都会对安全密钥率产生一定的影响。系统可能受到的攻击方式有 2 类：一类是集体攻击，另一类是个体攻击。Bob 端检测的方式也有 2 类：一类是零差检测，另一类是外差检测。虽然张一辰和黄露雨都利用放大器对基于光纤信道的 CVQKD 协议性能进行了改进，为本文研究光放大器对基于空间信道的 CVQKD 协议性能的改进提供了一定的参考，但他们未全面考虑系统可能遭受的攻击类型、Bob 采用的检测方式，也未比较不同放大器对同一量子通信系统的提升效果。此外，他们在关于光纤量子通信的研究中仅仅考虑了一种波长，然而，在自由空间量子通信中，不同波长的信号受到的空间信道特性的影响是不同的[4]。因此，本文研究 2 种不同攻击方式下 Bob 采用不同检测方式时，插入不同放大器对采用不同波长信号的空间量子通信系统的提升效果，为空间量子通信系统选择光放大器提供参考建议。

1 PSA 对空间量子通信系统性能的影响

1.1 PSA 原理

PSA 是一种简并光参量放大器，理想情况下允许对选定的正交分量进行无噪声放大[5-6]。信号的 2 个正交分量经放大倍数为 $g(g>1)$ 的 PSA 放大后，$x\rightarrow\sqrt{g}\,x$ 且 $p\rightarrow p/\sqrt{g}$（x 表示同相分量，p 表示与信号正交的分量），即放大过程对正交分量有不对称影响，同相的信号光分量被放大，而与之正交的信号光分量对应被衰减，如图 1 所示。

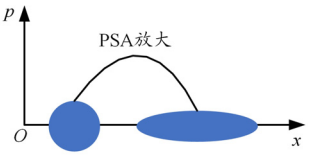
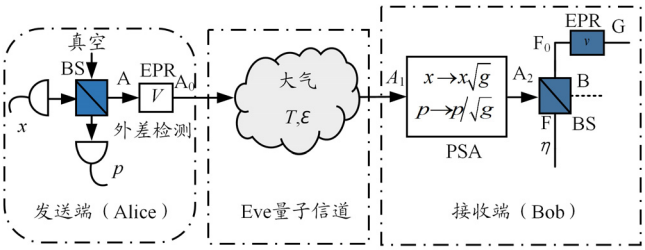


图 1 PSA 原理示意图

1.2 加入 PSA 后的高斯调制 CVQKD 模型

为研究 PSA 对空间量子通信系统性能的提升，本文建立了加入 PSA 后的系统模型（即在自由空间信道之后、Bob 检测设备的输入端之前插入 PSA），如图 2 所示。



注：A、A_0、A_1、A_2、F、F_0、B、G为模型中出现的各种模式

图 2 加入 PSA 后的高斯调制 CVQKD 模型

在发送端（Alice），EPR（Einstein-Podolsky-Rosen）纠缠源产生一对服从高斯分布且方差为 V_A、均值为 0 的双模压缩纠缠态，一个模式 A 留在本地进行外差检测，另一模式 A_0 经透射率为 T、额外噪声为 ε 的空间信道发送给接收端（Bob），此时 A_0 变成了 A_1。假设信道引入的额外噪声为 χ_{line}，则其表达式为 $\chi_{\text{line}}=1/T-1+\varepsilon$。其中，$T=e^{-\alpha(\lambda)L}$，$\lambda$ 为光信号波长，L 为传输距离，$\alpha(\lambda)$ 为总的衰减系数[4]。检测器的特性由检测效率 η 和电子噪声 v_{el} 来描述。实际上 Bob 检测器的检测效率由传输效率为 η_1 的分束器模拟（即 $\eta=\eta_1$），而其电子噪声 v_{el} 由方差为 V 的 EPR 纠缠态模拟，其中模式 F_0 被耦合进分束器的第二个输入端口。在接收端，不同的检测方式对应不同方差和检测器输入噪声 χ_{h}。设系统总噪声为 χ_{tot}，则其表达式为 $\chi_{\text{tot}}=\chi_{\text{line}}+\chi_{\text{h}}/T$。

在系统中不加入任何放大器情况下，当 Bob 采用零差检测时，$v_{hom}=\eta\chi_{hom}/(1-\eta)$且 $\chi_h=\chi_{hom}=[(1-\eta)+v_{el}]/\eta$；当采用外差检测方式时，$v_{het}=(\eta\chi_{het}-1)/(1-\eta)$且 $\chi_h=\chi_{het}=[1+(1-\eta)+2v_{el}]/\eta$。一旦信息传输阶段完成后，Alice 和 Bob 就开始进行纠错、保密增强等过程来获得最终的密钥。纠错协议分为 2 种：一种是 Bob 根据 Alice 发送的验证信息，修正数据使其与 Alice 的数据相一致，称为正向调节协议；另一种是 Alice 根据 Bob 发送过来的验证信息，对自身数据进行筛选，使其与 Bob 的数据一致，称为反向协调协议。

1.3 加入 PSA 后的安全密钥率计算

设通信双方根据反向协调协议进行纠错，则可计算插入 PSA 后基于空间信道的量子通信系统在 Eve 采用集体、个体攻击情况下的安全密钥率。

1.3.1 系统受集体攻击时的安全密钥

系统受到集体攻击时，安全密钥率 K_{col}^{PSA}[3]计算公式为：

$$K_{col}^{PSA}=\beta I_{AB}-\chi_{BE} \tag{1}$$

其中，β 为反向协调效率；χ_{BE} 为 Eve 从 Bob 处所能获得的信息量上限，即 Holevo 界；I_{AB} 为 Alice 和 Bob 之间的互信息量。当 Bob 采用零差检测时，$I_{AB}\Rightarrow I_{AB}^{hom+PSA}=\frac{1}{2}\times\log_2\left(\frac{V+\chi_{tot}^{PSA}}{1+\chi_{tot}^{PSA}}\right)$，$\chi_{tot}^{PSA}$ 为加入 PSA 后的系统总噪声；当 Bob 采用外差检测时，$I_{AB}\Rightarrow I_{AB}^{het+PSA}=\log_2\left(\sqrt{\frac{(V+\chi_{tot}^{x})(V+\chi_{tot}^{p})}{(1+\chi_{tot}^{x})(1+\chi_{tot}^{p})}}\right)$，其中，$\chi_{tot}^{x}$ 为系统总噪声的同相分量，χ_{tot}^{p} 为系统噪声的正交分量，V 表示纠缠态的方差。已有研究表明，高斯攻击是集体攻击的最佳选择，所以在此只需考虑高斯态，则 χ_{BE}[7-8]可以表示为：

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

其中，$G(y)=(y+1)\log_2(y+1)-y\log_2(y)$。$\lambda_i$ 为量子系统的协方差矩阵的第 i 个辛本征值。当 $i=5$ 时，$\lambda_5=1$；当 $i=1,2$ 时，有

$$\lambda_{1,2}^2=\frac{1}{2}(A\pm\sqrt{A^2-4B}) \tag{3}$$

其中，$A=V^2(1-2T)+2T+T^2(V+\chi_{line})^2$，$B=T^2(V\chi_{line}+1)^2$。

当 $i=3,4$ 时，有

$$\lambda_{3,4}^2=\frac{1}{2}(C\pm\sqrt{C^2-4D}) \tag{4}$$

①当 Bob 采用零差检测时，式(4)中的 C、D 分别表示为式(5)、式(6)中的 C_{hom}^{PSA}、D_{hom}^{PSA}。

$$C_{hom}^{PSA}=\frac{A\chi_{hom}^{PSA}+V\sqrt{B}+T(V+\chi_{line})}{T(V+\chi_{tot}^{PSA})} \tag{5}$$

$$D_{hom}^{PSA}=\sqrt{B}\,V+\frac{\sqrt{B}\,\chi_{hom}^{PSA}}{T(V+\chi_{tot}^{PSA})} \tag{6}$$

其中，χ_{hom}^{PSA} 为加入 PSA 后零差检测器的输入噪声，此时，$\chi_{hom}^{PSA}=((1-\eta)+v_{el})/(g\eta)$，$\chi_{tot}^{PSA}=\chi_{line}+\chi_{hom}^{PSA}/T$。

②当 Bob 采用外差检测时，式(4)中的 C_{het}^{PSA}、D_{het}^{PSA} 分别表示为式(7)、式(8)中的 C_{het}^{PSA}、D_{het}^{PSA}。

$$\begin{aligned}C_{het}^{PSA}=&\frac{1}{\left[T(V+\chi_{tot}^{x})\right]\left[T(V+\chi_{tot}^{p})\right]}\times\\&\{A\chi_{het}^{PSA+x}\chi_{het}^{PSA+p}+B+1+\left(\chi_{het}^{PSA+x}+\chi_{het}^{PSA+p}\right)\times\\&[V\sqrt{B}+T(V+\chi_{line})+2T(V^2-1)]\}\end{aligned} \tag{7}$$

$$D_{het}^{PSA}=\left[\frac{V+\sqrt{B}\,\chi_{het}^{PSA+x}}{T(V+\chi_{tot}^{x})}\right]\left[\frac{V+\sqrt{B}\,\chi_{het}^{PSA+p}}{T(V+\chi_{tot}^{p})}\right] \tag{8}$$

其中，χ_{het}^{PSA+x} 为系统加入 PSA 后外差检测器的输入噪声同相分量，$\chi_{het}^{PSA+x}=[1+(1-\eta)+2v_{el}]/(g\eta)$；$\chi_{het}^{PSA+p}$ 为系统加入 PSA 后外差检测器的输入噪声正向分量，$\chi_{het}^{PSA+p}=g[1+(1-\eta)+2v_{el}]/\eta$，$\chi_{tot}^{x,p}=\chi_{line}+\chi_{het}^{PSA+x,p}/T$，$g(g>1)$为放大器的放大倍数。

1.3.2 系统受个体攻击时的安全密钥

系统受到个体攻击时，密钥率计算公式为：

$$K_{ind}^{PSA}=\beta I_{AB}-I_{BE} \tag{9}$$

其中，I_{AB} 具有与集体攻击时零差检测和外差检测相同的表达式，I_{BE} 表示 Bob 和 Eve 之间的互信息量。

①当 Bob 采用零差检测时，$I_{BE}\Rightarrow I_{BE}^{hom+PSA}$ 的计算公式为：

$$I_{BE}^{hom+PSA}=\frac{1}{2}\log_2\left[\frac{T^2(V+\chi_{tot}^{PSA})(1/V+\chi_{line})}{1+T\chi_{hom}^{PSA}(1/V+\chi_{line})}\right] \tag{10}$$

②当 Bob 采用外差检测时，$I_{BE}\Rightarrow I_{BE}^{het+PSA}$ 的计算公式为：

$$I_{BE}^{het+PSA}=\log_2\left[\frac{T(V+\chi_{tot}^{x})(V+\chi_{tot}^{p})}{\sqrt{\left(\frac{V\chi_E+1}{V+\chi_E}+\chi_{het}^{PSA+x}\right)\left(\frac{V\chi_E+1}{V+\chi_E}+\chi_{het}^{PSA+p}\right)}}\right] \tag{11}$$

其中，$\chi_E=\frac{T(2-\varepsilon)^2}{(\sqrt{2-2T+T\varepsilon}+\sqrt{\varepsilon})^2}+1$。

2 PIA 对空间量子通信系统性能的影响

2.1 PIA 原理与加入 PSA 后的高斯调制 CVQKD 模型

PIA 是一种非简并光学放大器，允许对 2 个正交分量同时同等程度进行放大，如图 3 所示。其放大原理是信号模式和 PIA 内的闲置模式进行相互作用，使得 $x_S \to \sqrt{g}\,x_S + \sqrt{g-1}\,x_I$，$p_S \to \sqrt{g}\,p_S - \sqrt{g-1}\,p_I$。S、I 分别表示信号模式和闲置模式。在理想状态下，闲置模式为一个真空态，而现实中其包含了一定的噪音，这里噪音用一个方差为 N 的 EPR 态表征[9-11]。同样地，为研究 PIA 对自由空间量子通信系统性能的提升，本文建立了加入 PIA 后的系统模型，即在自由空间信道的输出端和 Bob 检测设备的输入端之间插入 PIA，如图 4 所示。

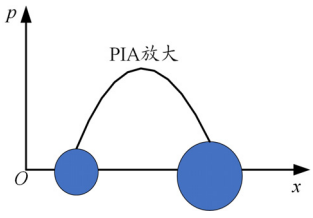


图 3 PIA 原理示意图

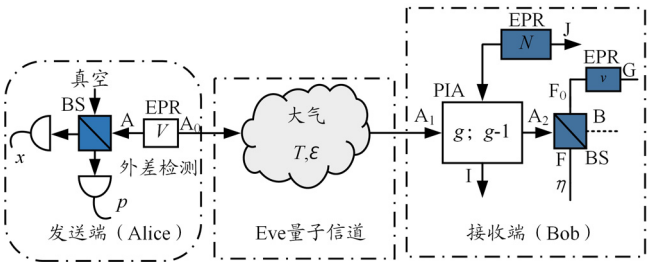


图 4 加入 PIA 后的高斯调制 CVQKD 模型

2.2 加入 PIA 后的安全密钥率计算

当系统中加入 PIA 时，安全密钥率的计算方法与第 1 节类似。

2.2.1 系统受集体攻击时的安全密钥

系统受到集体攻击时，式(1)中的 I_{AB} 分别为：当 Bob 采用零差检测时，$I_{AB} \Rightarrow I_{AB}^{\text{hom+PIA}} = \frac{1}{2}\log_2\left(\frac{V+\chi_{tot}^{PIA}}{1+\chi_{tot}^{PIA}}\right)$，其中，$\chi_{tot} \Rightarrow \chi_{tot}^{PIA} = \chi_{line} + \chi_{hom}^{PIA}/T$，$\chi_{tot}^{PIA}$ 为加入 PIA 后零差检测器的输入噪声；当 Bob 采用外差检测时，$I_{AB} \Rightarrow I_{AB}^{\text{het+PIA}} = \log_2\left(\frac{V+\chi_{tot}^{PIA}}{1+\chi_{tot}^{PIA}}\right)$，其中，$\chi_{tot} \Rightarrow \chi_{tot}^{PIA} = \chi_{line} + \chi_{het}^{PIA}/T$，$\chi_{het}^{PIA}$ 为加入 PIA 后外差检测器的输入噪声。

加入 PIA 后，需要考虑放大器噪声的影响，在计算 Eve 从 Bob 处获得信息量 χ_{BE} 时，需要将 I 和 J 这 2 个模式考虑在内，计算方法与式(2)相同，此时，λ_i 定义如下：$\lambda_{1,2}$ 的表达式和式(3)相同，$\lambda_{5,6,7}=1$，$\lambda_{3,4}$ 的表达式与式(4)相同。

①当 Bob 采用零差检测时，式(4)中的 C、D 分别表示为式(12)、式(13)中的 C_{hom}^{PIA}、D_{hom}^{PIA}。

$$C_{hom}^{PIA} = \frac{A\chi_{hom}^{PIA} + V\sqrt{B} + T(V+\chi_{line})}{T(V+\chi_{tot}^{PIA})} \tag{12}$$

$$D_{hom}^{PIA} = \sqrt{B}\,\frac{V+\sqrt{B}\,\chi_{hom}^{PIA}}{T(V+\chi_{tot}^{PIA})} \tag{13}$$

此时，$\chi_{hom}^{PIA} = [(1-\eta)v_{el} + N(g-1)\eta\,]/(g\eta)$，$\chi_{tot}^{PIA} = \chi_{line} + \chi_{hom}^{PIA}/T$。

②当 Bob 采用外差检测时，式(4)中的 C、D 分别表示为式(14)、式(15)中的 C_{het}^{PIA}、D_{het}^{PIA}。

$$C_{het}^{PIA} = \frac{1}{\left[T\left(V+\chi_{tot}^{PIA}\right)\right]^2} \times \left\{A(\chi_{het}^{PIA})^2 + B + 1 + 2\chi_{het}^{PIA}\left[V\sqrt{B} + T(V+\chi_{line})\right] + 2T(V^2-1)\right\} \tag{14}$$

$$D_{het}^{PIA} = \left[\frac{V+\sqrt{B}\,\chi_{het}^{PIA}}{T(V+\chi_{tot}^{PIA})}\right]^2 \tag{15}$$

此时，$\chi_{het}^{PIA} = [1+(1-\eta)+2v_{el}+N(g-1)\eta\,]/(g\eta)$，$\chi_{tot}^{PIA} = \chi_{line} + \chi_{het}^{PIA}/T$。

2.2.2 系统受个体攻击时的安全密钥

系统受到个体攻击时，Alice 和 Bob 间的互信息量 I_{AB} 具有与集体攻击下零差检测和外差检测时相同的表达式，式(9)中的 I_{BE} 如式(16)、式(17)所示。

①当 Bob 采用零差检测时，$I_{BE}^{\text{hom+PIA}}$ 的计算公式为：

$$I_{BE}^{\text{hom+PIA}} = \frac{1}{2}\log_2\left[\frac{T^2(V+\chi_{tot}^{PIA})(1/V+\chi_{line})}{1+T\chi_{hom}^{PIA}(1/V+\chi_{line})}\right] \tag{16}$$

②当 Bob 采用外差检测时，$I_{BE}^{\text{het+PIA}}$ 的计算公式为：

$$I_{BE}^{\text{het+PIA}} = \log_2\left[\frac{T\left(V+\chi_{tot}^{PIA}\right)(V+x_E)}{Vx_E+1+\chi_{het}^{PIA}(V+x_E)}\right] \tag{17}$$

3 仿真结果与分析

根据上文推导的加入不同放大器后的安全密钥率公式，本文应用 Matlab 软件对采用 810 nm、1550 nm 和 3800 nm 波长的空间量子通信系统在分别遭受个体攻击和集体攻击的情况下、Bob 采用零差检测和外差检

测时的性能进行了仿真。此外，PIA 对系统的提升性能与其固有噪声有关，因此以 1550 nm 波长信号为例仿真分析了 PIA 的固有噪声对安全密钥率的影响。由于目前研究中使用的 PSA 和 PIA 一般都是针对光纤通信 C 波段的信号进行放大，为了进行对比分析，本文假设在接收端先将 810 nm、3800 nm 波长的信号通过波长转换技术转换到 1550 nm 附近后再进行探测（即在接收端对它们采用了频率转换单光子探测技术进行探测[12]）。当系统采用实际探测器时（即系统不加入任何光放大器时的情况），自由空间量子通信系统密钥率的仿真参数设置如表 1 所示。

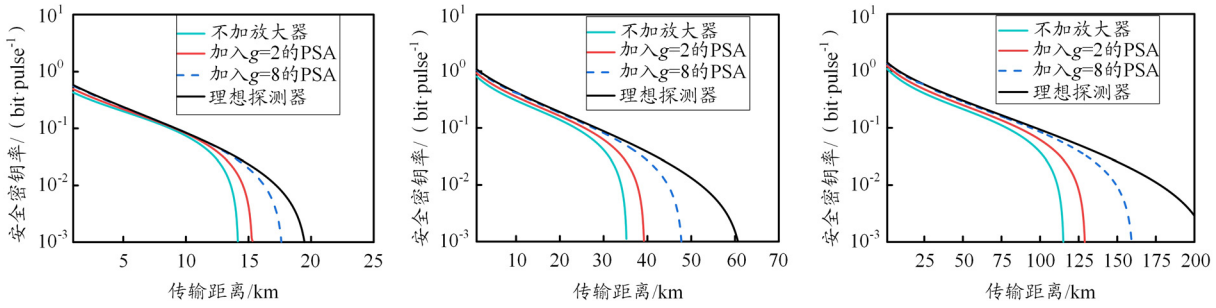
表 1　不同波长下安全密钥率的仿真参数

参数名称	数值
光波长 λ/nm	810、1550、3800
电子噪声 v_{el}/SNU	0.01
调制方差 V_A/SNU	10
反向协调效率 β	90%
探测器的探测效率 η	60%
额外噪声 ε/SNU	0.15、0.04、0.00683
PIA 的固有噪声 N/SNU	1

3 种不同波长信号在零差检测、个体攻击情况下，加入不同放大倍数的 PSA 后安全密钥率随距离的变化关系如图 5 所示。可以看出，放大倍数 g 越大，通信系统的安全密钥率越高，传输距离越远，越接近完美探测器时的系统性能，即 Bob 采用零差检测时，通过选择合适的 PSA 可以完全弥补探测器的非理想性造成的影响，从而提高自由空间量子通信系统性能；另外，3800 nm 波长信号比 810 nm、1550 nm 波长信号具有更远的传输距离和更高的密钥率。相同增益下，长波长信号传输距离增加得更多，因此长波长信号在空间量子通信中更具有优势。

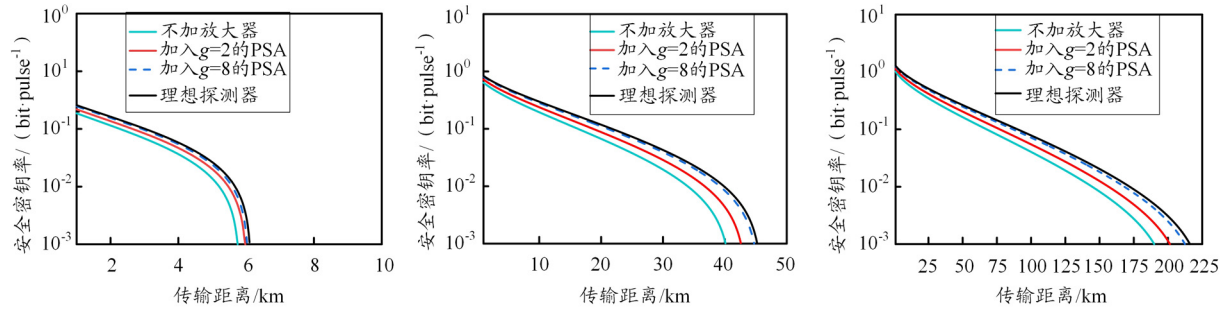
3 种不同波长信号在零差检测、集体攻击情况下加入不同放大倍数的 PSA 后安全密钥率随距离的变化关系如图 6 所示。可以看出，集体攻击时可以得到与个体攻击相同的结论，即只要选择合适放大倍数 g 的 PSA，则可以完全弥补探测器的非理想性造成的影响。对比图 5 与图 6 可知，对于同一波长来说，采用相同增益的 PSA 时，集体攻击下的系统性能比个体攻击下的系统性能更接近采用理想探测器时的性能。

3 种不同波长信号在外差检测情况下、系统分别遭受个体攻击和集体攻击时及加入不同放大倍数的 PSA 后安全密钥率随距离的变化关系如图 7 和图 8 所示。可以看出，当 Bob 采用外差检测时，系统内加入放大器后，无论系统遭受集体攻击还是个体攻击，随着放大倍数的增加，系统性能均得到了改善，增加了传输距离，提高了安全密钥率。但是，此时并不能得到理想探测器时的安全密钥率，即当 Bob 进行外差检测时，加入 PSA 并不能完全补偿探测器的非理想性。同



（a）810 nm　（b）1550 nm　（c）3800 nm

图 5　零差检测下、个体攻击时，加入不同放器倍数的 PSA 后不同波长安全密钥率随距离的变化关系

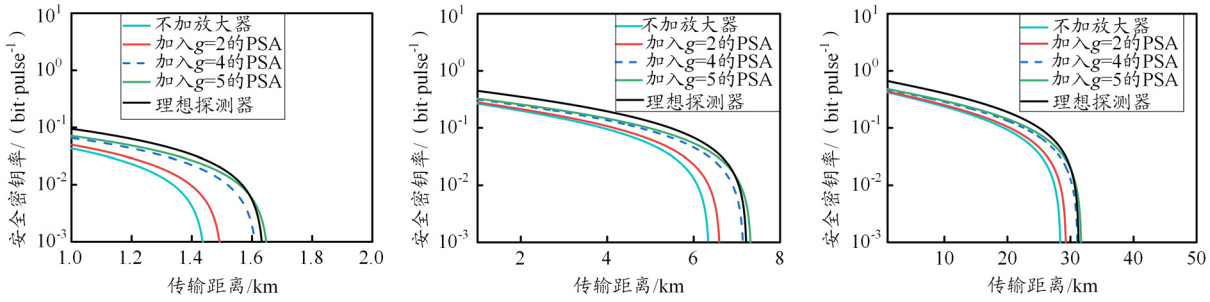


（a）810 nm　（b）1550 nm　（c）3800 nm

图 6　零差检测下、集体攻击时，加入不同放器倍数的 PSA 后不同波长安全密钥率随距离的变化关系

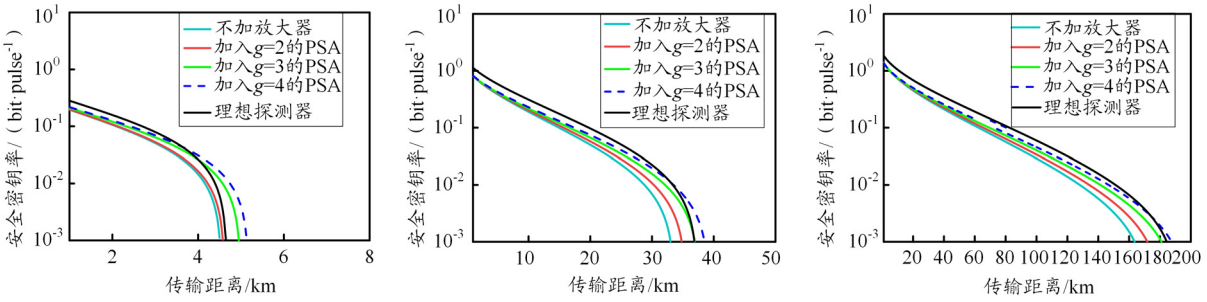
样地，对比图 7 和图 8 还可以得到与零差检测时相同的结论，即对同一波长而言，采用相同增益的 PSA 时，集体攻击下系统性能的提升效果更好。

3 种不同波长信号在零差检测情况下、系统分别遭受个体攻击和集体攻击时加入不同放大倍数的 PIA 后的安全密钥率随距离的变化关系如图 9 和图 10 所示。可以看出，在零差检测时，无论系统受到集体攻击还是个体攻击，随着放大倍数 g 的增加，系统性能却越来越差，即若 Bob 采用零差检测方式，在系统中加入 PIA 并不能使得系统性能得到提升。



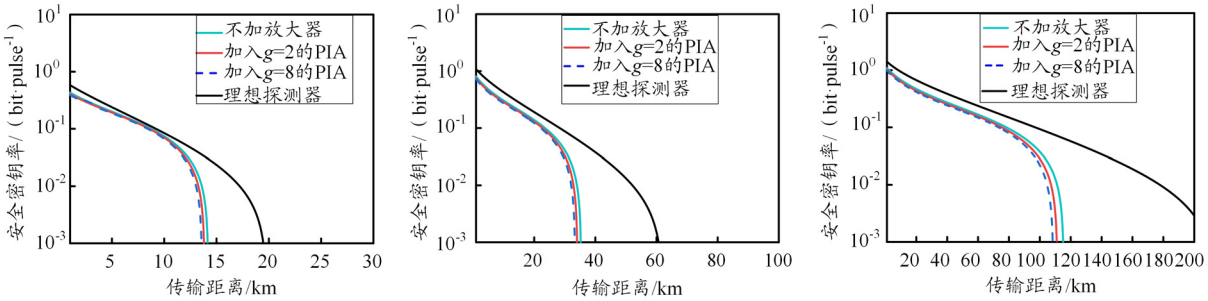
（a） 810 nm　　（b） 1550 nm　　（c） 3800 nm

图 7　外差检测下、个体攻击时，加入不同放器倍数的 PSA 后不同波长安全密钥率随距离的变化关系



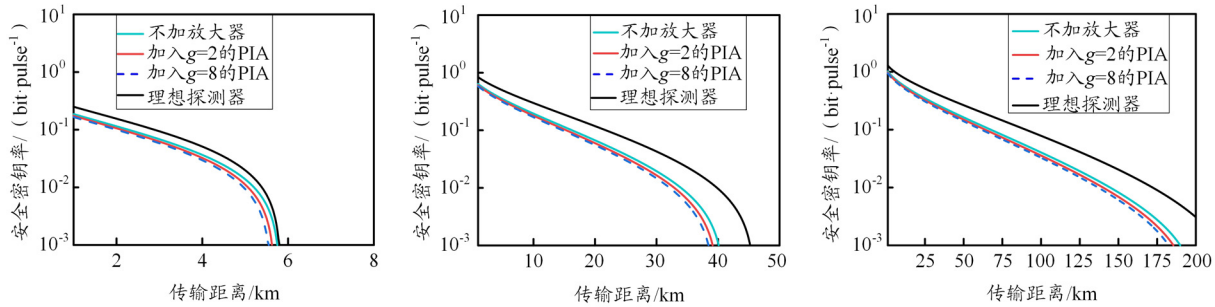
（a） 810 nm　　（b） 1550 nm　　（c） 3800 nm

图 8　外差检测下、集体攻击时，加入不同放器倍数的 PSA 后不同波长安全密钥率随距离的变化关系



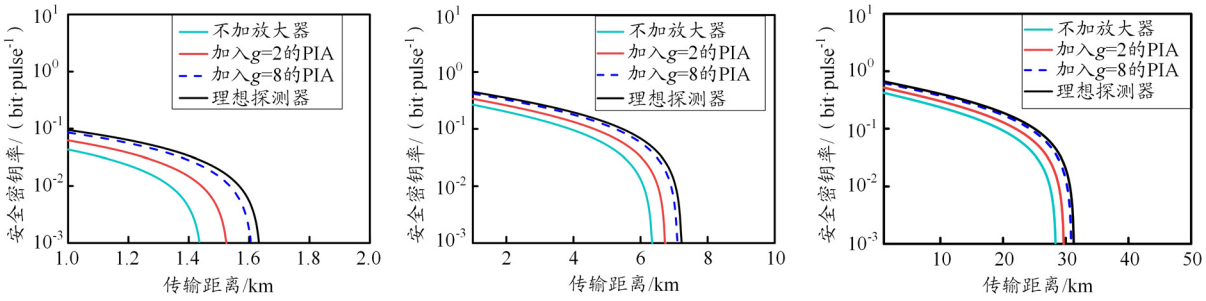
（a） 810 nm　　（b） 1550 nm　　（c） 3800 nm

图 9　零差检测下、个体攻击时，加入不同放器倍数的 PIA 后不同波长安全密钥率随距离的变化关系



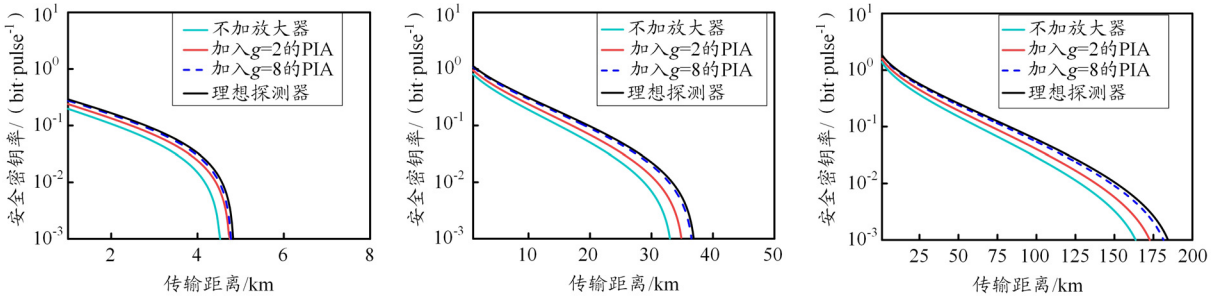
（a） 810 nm　　（b） 1550 nm　　（c） 3800 nm

图 10　零差检测下、集体攻击时，加入不同放器倍数的 PIA 后不同波长安全密钥率随距离的变化关系



（a）810 nm　（b）1550 nm　（c）3800 nm

图 11　外差检测下、个体攻击时，加入不同放器倍数的 PIA 后不同波长安全密钥率随距离的变化关系



（a）810 nm　（b）1550 nm　（c）3800 nm

图 12　外差检测下、集体攻击时，加入不同放器倍数的 PIA 后不同波长安全密钥率随距离的变化关系

3 种不同波长信号在外差检测情况下、系统分别受到个体攻击、集体攻击时以及加入不同放大倍数 g 的 PIA 后安全密钥率随距离的变化关系如图 11 和图 12 所示。可以看出，在外差检测情况下，对于不同波长信号，不管系统受到集体攻击还是个体攻击，加入 PIA 都对量子通信性能有显著提高效果，放大倍数 g 越大，系统性能越接近系统采用理想探测器时的性能，即在外差检测时，加入 PIA 可以弥补探测器的非理想性。此外，相同放大倍数 g 的 PIA 对集体攻击和个体攻击下的系统具有相同的提升效果。

对比图 9~图 12 可知，当系统中加入 PIA 时，Bob 只能采用外差检测方式进行测量。综合对比图 5~图 8 以及图 9~图 12 可知，当 Bob 采用零差检测时，无论系统受到集体攻击还是个体攻击，都应选择 PSA 来补偿探测器的非理想性；采用外差检测时，无论系统受到集体攻击还是个体攻击，都应选择 PIA 来补偿探测器的非理想性，并且在长距离通信中，选用长波长更具优势。

安全密钥率与 PIA 固有噪声 N 的变化关系如图 13 所示。可以看出，安全密钥率是噪声的单调递减函数。红色虚线以上表示性能改善区，红色虚线以下表示性能下降区。由图 13 可知，红色虚线和蓝色实线的交点对应的横坐标就是 PIA 的最大可容忍噪声，只有当

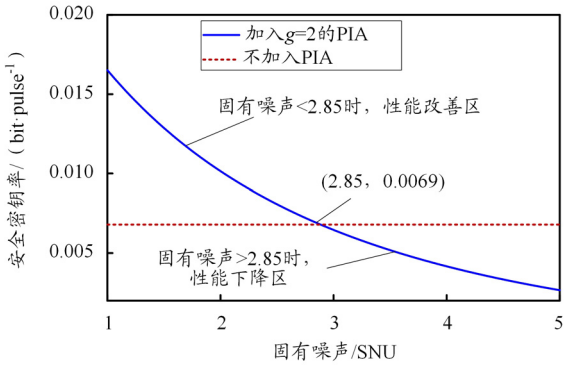


图 13　安全密钥率随 PIA 固有噪声 N 的变化曲线

实际 PIA 噪声小于最大可容忍噪声时，系统性能才可以得到提升。自由空间量子通信系统采用 1550 nm 波长信号进行信息传输 30 km 时，要想使用 PIA 提升量子通信系统性能，则 N 必须要小于 2.85 SNU。因此，实际的量子通信系统可以根据 PIA 最大可容忍噪声来判断是否要加入 PIA。

4 结束语

本文利用 PSA 和 PIA 对自由空间量子通信系统的性能进行了改善，仿真分析了加入不同放大倍数 g 的 PIA、PSA 后，系统分别受到集体攻击和个体攻击、Bob 采用零差检测和外差检测时，不同波长量子信号的安全密钥率随传输距离的变化关系。仿真结果表

明:与短波长量子信号相比,长波长量子信号在自由空间量子通信系统中具有一定的优势;当 Bob 采用零差检测时,只要选择合适的 PSA 就能完全补偿零差探测器固有属性导致的量子通信系统性能下降,而使用 PIA 不仅不能提升系统性能,反而会使系统性能下降;相同增益的 PSA 对集体攻击时的系统性能提升效果比个体攻击时的好;当 Bob 采用外差检测方式时,系统中加入 PSA 后,虽然随着放大倍数 g 的增加系统性能提升效果越好,但是其提升效果并不能完全补偿探测器的非理想性;而当系统中加入 PIA 后,通过选取合适的增益能够完全补偿探测器的非理想性,但是,在选择 PIA 时需要考虑 PIA 的最大可容忍噪声,否则可能导致系统性能不升反降。本文的研究成果为实际的自由空间量子通信系统选择光放大器时提供了参考性的建议。

参考文献:

[1] 张一辰. 连续变量量子密钥分发协议的安全性证明及协议改进[D]. 北京:北京邮电大学,2017.

[2] 谢博娅. 光探测和光放大中的额外量子噪声研究[D]. 武汉:华中科技大学,2018.

[3] 黄露雨. 相敏光放大器对连续变量量子密钥分发协议的改进研究[D]. 北京:北京邮电大学,2020.

[4] LIU T, ZHU C, SUN C, et al. Performance analysis of free space quantum key distribution with different wavelengths [C]//AOPC 2019: Quantum Information Technology. International Society for Optics and Photonics, 2019:1133909-1–1133909-6.

[5] 杨维利. 相敏放大及其应用研究[D]. 武汉:华中科技大学,2017.

[6] 龚峰. 基于光纤通信的连续变量量子密钥分发改进研究[D]. 贵阳:贵州大学,2019.

[7] 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, 2009, 42 (11): 114014-1 – 114014-11.

[8] GARCÍA-PATRÓN R, CELF N J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution[J]. Physical Review Letters, 2006, 97(19): 190503-1–190503-4.

[9] CAVES C M. Quantum limits on noise in linear amplifiers[J]. Physical Review D, 1982, 26(8): 1817–1839.

[10] OU Z Y, PEREIRA S F, KIMBLE H J. Quantum noise reduction in optical amplification [J]. Physical Review Letters, 1993, 70 (21): 3239–3242.

[11] ZHANG H, FANG J, HE G. Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers[J]. Physical Review A, 2012, 86(2): 022338-1–022338-7.

[12] SHENTU G L, XIA X X, SUN Q C, et al. Upconversion detection near 2 μm at the single photon level [J]. Optics Letters, 2013, 38(23): 4985–4987.