第 57 卷 第 3 期 2008 年 3 月
1000-3290/2008/57(03)/1352-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.3,March,2008

1.55 μm 升频单光子探测量子密钥分配系统的性能研究*

焦荣珍† 冯晨旭 马海强

(北京邮电大学理学院,北京 100876)

(2007 年 5 月 31 日收到;2007 年 7 月 9 日收到修改稿)

分析了 1.55 μm 升频单光子探测量子密钥分配(QKD)系统的性能,讨论了升频单光子探测器的主要参数:量子效率和暗计数与抽运功率的关系.比较了 BB84 协议、BBM92 协议和 DPSK 协议的光纤 QKD 系统的性能:安全通信速率与距离的关系,通过比较得出升频探测器优于传统的 InGaAs/InP 雪崩二极管单光子探测器,用升频探测器后的通信距离能比传统的大两倍以上,能很好改善量子通信系统的性能.

关键词:量子效率,通信速率,暗计数

PACC:0367,4250

1. 引 言

量子保密通信是量子信息科学中的重要分支,量子保密通信以其优越的先天特点有可能改变未来的保密通信方式[1—3]. 量子密钥分配(QKD)是量子保密通信中不可或缺的一部分,它是保证通信安全性的重要环节,QKD 能让通信双方(发送端 Alice 和接收端 Bob)共享一个无条件安全密钥,密钥的安全性是基于量子力学原理:任何对未知状态量子系统的测量都会改变其状态. 当前,量子密码研究的核心内容,是如何利用量子技术在量子信道上安全可靠地分配密钥,利用各种协议来抵御外界的攻击[4]. 从国内外已经公布的公开文献来看,最常见的量子密钥分配协议有:BB84 协议,BBM92 协议,DPSK 协议[5—7].现今普遍采用的是把信息加载在通信波段(1.3 μm 和 1.55 μm)的单光子的相位或偏振态上,因此通信波段单光子探测就成为量子保密通信系统中的关键技术之一,其性能的好坏直接关系到密钥的生成率、系统的安全性、通信速率和通信距离等重要参数. 在国外,光通信三个波段(0.85 μm,1.3 μm 和 1.55 μm)的单光子探测器用于量子密钥系统已经有了相关的报道[8]. 在国内,中科院完成了 1.55 μm 单模光纤中的量子密钥分配,实际测量效果已经很接近于理论值[9]. 但在 1.3 μm 和 1.55 μm 波段的红外单光子探测国内还未见报道. 针对量子密钥系统的通信距离和安全通信速率决定于单光子源或纠缠光子的性质及系统单光子探测器的性能. 本文通过分析 1.55 μm 升频单光子探测器的性能,即量子效率和暗计数与抽运功率之间的关系,说明在光纤 QKD 系统中采用 1.55 μm 升频单光子探测器比采用 InGaAs/InP 雪崩光电二极管(APD)能获得更远的通信距离和更高的通信速率,同时,基于升频探测器,分析了在不同攻击条件下,BB84,BBM92 和 DPSK 协议中 QKD 系统对抗攻击的性能,计算得出通信速率和通信距离的关系.

2. 理论与计算公式

在 1.55 μm 升频单光子探测器中,1.55 μm 的单光子和 1.32 μm 的强抽运在周期极化的铌酸锂波导中相互作用,当在波导中达到相位匹配的条件,能够获得足够的抽运能量来达到 100% 的光子转换,这时就能达到最大的量子效率,升频探测器的量子效率 η_{up} 和暗计数率 D_{up} 随着抽运功率 p 变化的数学关系式为

* 国家自然科学基金(批准号:60544002)资助的课题.

† E-mail:jrz218@163.com

$$\eta_{\mathrm{up}}(p) = a_1 \sin^2(\sqrt{a_2 p}), \quad (1)$$

其中 $a_1 = 0.465$，$a_2 = 79.75$，p 以 mW 为单位.

$$D_{\mathrm{up}}(p) = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4, \quad (2)$$

其中 $b_0 = 50$，$b_1 = 826.4$，$b_2 = 110.3$，$b_3 = -0.403$，$b_4 = 0.00065$.

在 BB84 协议中，考虑个体攻击时，对抗任意个体攻击的通信速率由下面的等式给出：

$$R_{\mathrm{BB84}} = \frac{1}{2}\nu p_{\mathrm{click}} \{\tau(e,\beta) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}, \quad (3)$$

其中，因数 1/2 为筛选参数，ν 为传输重复速率，$\tau(e,\beta)$为保密放大阶段的主要衰减因子，如窃听者(Eve)在有限长的相关时间内有量子记忆，其关系式如下：

$$\tau(e,\beta) = -\beta\log_2\left[\frac{1}{2} + 2\frac{e}{\beta} - 2\left(\frac{e}{\beta}\right)^2\right];$$

如 Eve 无量子记忆，其关系式为

$$\tau(e,\beta) = -\frac{1+\beta}{2}\log_2\left[\frac{1}{2} + 4\frac{e}{1+\beta} - 8\left(\frac{e}{1+\beta}\right)^2\right],$$

其中

$$\beta = \frac{p_{\mathrm{click}} - p_m}{p_{\mathrm{click}}},$$

p_m 为光源发射多光子态的概率，对于一个理想的单光子源，$p_m = 0$(即 $\beta = 1$)，然而对于泊松光源

$$p_m = 1 - (1+\mu)\mathrm{e}^{-\mu},$$

p_{click}为 Bob 探测到一个光子的概率，其表达式为

$$p_{\mathrm{click}} = \mu\eta 10^{-(\alpha L + L_r)/10} + 4d,$$

这里 μ 为每脉冲的平均光子数，η 为探测器的量子效率，α 为光纤的损耗因数，L_r 为接收机的损耗，d 为系统每个测量时间窗内的暗计数.

BBM92 协议是 BB84 协议双光子派生出来的协议. 对抗个体攻击的通信速率由下式给出：

$$R_{\mathrm{BBM92}} = \frac{1}{2}\nu p_{\mathrm{coin}} \{\tau(e) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}. \quad (4)$$

通信速率对确定性纠缠光子源和泊松纠缠光子源是不同的，其中参数的表达式参见文献[8].

DPSK 协议与 BB84 协议，BBM92 协议不同，它用很多含有脉冲的非正交基，其原理为所有的脉冲都经过强烈衰减，并在(0，π)之间随机进行相位调制. 考虑 DPSK 协议的安全性，我们在分析中考虑到了复合攻击. 含有分光和截断-重发攻击的复合攻击时，保密放大衰减参数为

$$\tau(e,\gamma) = \gamma - \frac{e}{N(1-1/2N)},$$

这里

$$\gamma = \begin{cases} 1 - \dfrac{\mu(1-\eta_{\mathrm{BS}})}{N} = 1 - \dfrac{\mu}{N} + \dfrac{p_{\mathrm{signal}}}{N}, \\ 1 - 2\mu(1-\eta_{\mathrm{BS}}) = 1 - 2\mu + 2p_{\mathrm{signal}}, \end{cases}$$

其中

$$p_{\mathrm{signal}} = \mu\eta 10^{-(\alpha L + L_r)/10},$$

传输效率为

$$\eta_{\mathrm{BS}} = \eta 10^{-(\alpha L + L_r)/10},$$

DPSK 协议对抗多种复合攻击时的通信速率为

$$R_{\mathrm{DPSK}} = \nu p_{\mathrm{click}} \{\tau(e,\gamma) + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}, \quad (5)$$

其中，ν 为传输的重复速率. p_{click}为 Bob 探测到光子的概率，即

$$p_{\mathrm{click}} = \mu\eta 10^{-(\alpha L + L_r)/10} + 2d,$$

其他参数与上文相同.

3. 结果与讨论

升频探测器的量子效率 η_{up}随抽运功率 p 的变化关系如图 1 所示，计算得出升频探测器的量子效率最大能达到 0.46，且受后向脉冲的影响不严重，而传统的 InGaAs/InP APD 的量子效率很低(通常在 0.1 数量级上)，而且最严重的是它受到被俘获带电载流子的后向脉冲影响，这导致了在相当一段的长时间里有暗计数. 对于 InGaAs/InP APD 说，通常 $D_{\mathrm{APD}} = 10^4\,\mathrm{s}^{-1}$，而对于 1.55 μm 升频探测器来说 $D_{\mathrm{up}} = 6.4\times10^3\,\mathrm{s}^{-1}$.

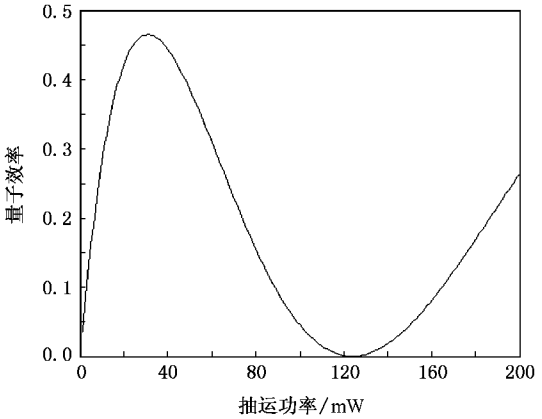

图 1　1.55 μm 升频探测器量子效率随抽运功率的变化关系

利用升频探测器，计算 BB84，BBM92 和 DPSK

协议下 QKD 系统的安全通信速率与通信距离的关系如图 2—4 所示，在 BB84 和 BBM92 协议中，考虑了理想和实际情况的单光子光源和纠缠光子光源. 信道衰减在 1.55 μm 时 $\alpha = 0.2$ dB/km，基线系统误码率定为 $b = 0.01$，除了光纤损耗，考虑了在接收端有附加的损耗 $L_r = 1$ dB. 在利用泊松光源的 BB84 协议中，从图 2 中观察到 Eve 无量子记忆并没有对系统的性能产生很大的影响，而由 PNS 攻击产生的通信速率和光纤长度呈二次方关系衰减是一个主要的因素，使得标准的 BB84 协议不适合长距离量子通信. 相反，用理想单光子光源可以在较长的距离用比较高的通信速率.

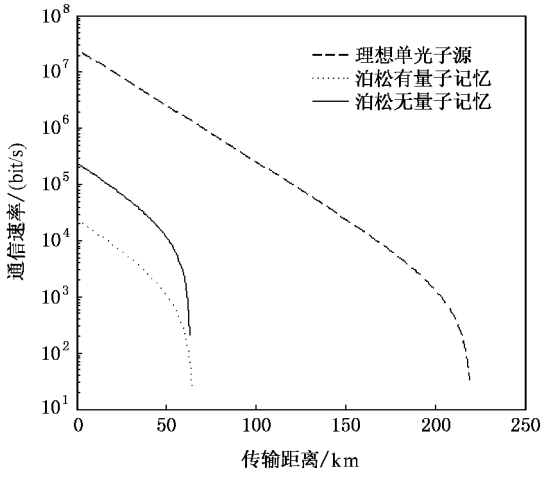

图 2 BB84 协议安全通信速率与通信距离的关系

由图 3 可知，有较强防御性的 BBM92 协议能传输更远的距离.

DPSK 协议的特点和 BB84 有相似之处，Eve 有量子记忆时，由图 4 可知，引入时间延迟参数 N 并不能对系统的性能产生很大的影响，因为和 N 无关的分光攻击在此时起主要作用，而当实际过程中，如 Eve 无量子记忆时，在这种情况下引入大于 1 的时间延迟参数 N 将很可观地增大安全通信速率和通信距离. 当 N 大于 10 时，此优势变弱. 这个结果表明 DPSK 是一个非常实用的，很有吸引力的长距离 QKD 系统的替代者，密钥生成率大于 1 kHz，通信距离大于 200 km.

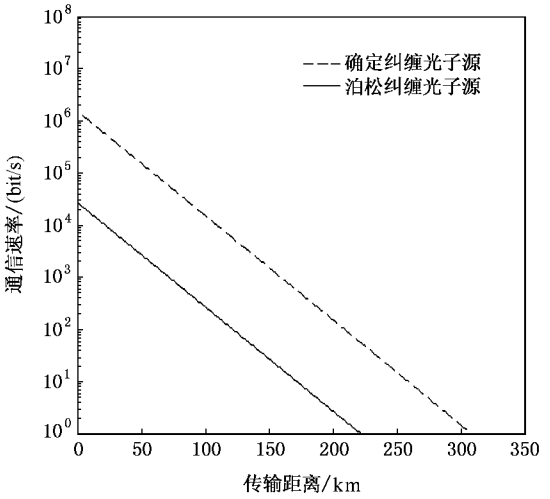

图 3 BBM92 协议下安全通信速率与通信距离的关系

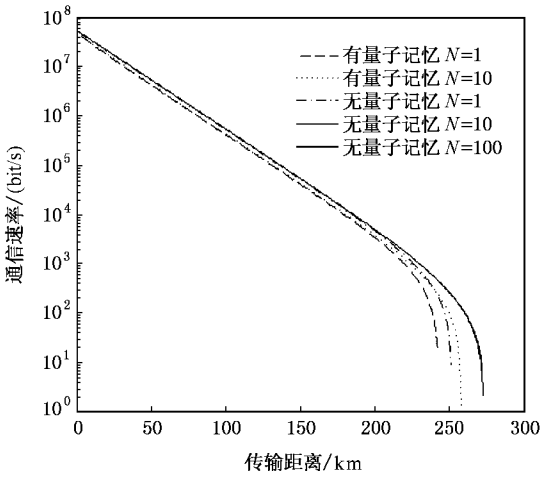

图 4 DPSK 协议安全通信速率与通信距离的关系

对于任何 QKD 协议，如采用的不是升频探测器而是 InGaAs/InP APD，它的 $\nu_{APD} = 10$ MHz[10]，通常 $\eta_{APD} = 0.1$，$d_{APD} = 10^{-5}$/门[11]，此时最大的通信距离为用升频探测器的一半，而通信速率则比后者大约小了两个数量级，这是由于 InGaAs/InP APD 的门模式操作引起的. 由此可得出，采用升频探测器要比 InGaAs/InP APD 在通信速率和通信距离上有很大优势，将 1.55 μm 升频单光子探测器应用于 QKD 系统中能很好地改善量子通信系统的性能.

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

[2] Mao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2126 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2126]

[3] Ma H Q, Li Y L, Zhao H, Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强、李亚玲、赵　环、吴令安 2005 物理学报 **54** 5014]

[4] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese) [杨宇光、温巧燕、朱甫臣 2005 物理学报 **54** 5544]

[5] Bennet C H, Brassard G 1984 *Proc. IEEE Interna. Conf. Computers, Systems, and Signal Processing* (Bangalore, New York, IEEE)

[6] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[7] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev.* A **68** 22317

[8] Diamanti E, Takesue H, Honjo T, Inoue K, Yamamoto Y 2005 *Phys. Rev.* A **72** 052311

[9] Gui Y Z,, Mo X F, Han Z P, Guo G C 2004 *Acta Sinica Quantum Optica* **10** 131 (in Chinese) [桂有珍、莫小范、韩正甫、郭光灿 2004 量子光学学报 **10** 131]

[10] Yoshizawa A, Kaji R Tsuchida H 2004 *Jpn. J. Appl. Phys.* **43** 735

[11] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N, Scarani V e-print quant-ph/0411022

Performance of various quantum-key-distribution systems using 1.55 μm up-conversion single-photon detector*

Jiao Rong-Zhen　Feng Chen-Xu　Ma Hai-Qiang

(*Science School, Beijing University of Post and Telecommunication, Beijing* 100876, *China*)

(Received 31 May 2007; revised manuscript received 9 July 2007)

Abstract

The performance of various quantum-key-distribution (QKD) systems is analyzed using 1.55 μm up-conversion single-photon detector. The dependence of quantum efficiency and dark count rate change on the pump power was also discussed. The comparison is based on the secure communication rate as a function of distance for three QKD protocols: the Bennett-Brassard 1984, the Bennett-Brassard-Mermin 1992, and the coherent differential-phase-shift keying protocols. We show that the up-conversion detector allows for higher communication rate and longer communication distance than the commonly used InGaAs/InP APD for all three QKD protocols, and the properties of quantum key distribution system can be greatly improved by this detector.

Keywords: quantum efficiency, communication rate, dark count rate

PACC: 0367, 4250

* Project supported by the National Natural Science Foundation of China (Grant No. 60544002).