文章编号：0253-2239(2008)supplement2-0167-03

量子密钥分配系统中的通信速率和误码率

焦荣珍 冯晨旭 唐少杰
（北京邮电大学理学院，北京 100876）

摘要 基于通信速率和误码率在量子保密通信研究中的重要性，采用 1.55 μm 上转换单光子探测器，分析其量子效率随抽运功率的变化关系，得出 1.55 μm 上转换单光子探测器较传统的铟镓砷二极管具有较高的量子效率和较低暗计数的优势，并根据通信距离、上转换单光子探测器的量子效率和暗计数之间建立一种平衡，得出每种距离上探测器的优化方案；在考虑个体攻击无量子记忆的条件下，比较 BB84 协议，BBM92 协议和差分相移协议的量子密钥分配(QKD)系统的安全通信速率和误码率随通信距离的变化关系，得出了差分相移键控协议的量子密钥分配系统是一个非常实用的，通信距离大于 200 km 的很有吸引力的长距离量子密钥分配系统。

关键词 量子光学；单光子探测器；通信速率；误码率
中图分类号 O431.2 **文献标识码** A **doi**：10.3788/AOS200828s2.0167

Communication Rate and Error Rate in the Quantum-Key-Distribution System

Jiao Rongzhen Feng Chenxu Tang Shaojie
(*Science School*, *Beijing University of Post and Telecommunication*, *Beijing* 100876, *China*)

Abstract The performance of various quantum-key-distribution systems is analyzed using 1.55-μm up-conversion single-photon detector. Important parameters such as communication rate, error rate, quantum efficiency and dark count rate are discussed. It is shown that quantum efficiency depends on the pump power, and that 1.55-μm up-conversion single-photon detector has great advantage over the InGaAs avalanche photodiodes detector. The analysis is based on the secure communication rate and error rate as a function of distance for three quantum-key-distribution (QKD) protocols: the Bennett-Brassard 1984, the Bennett-Brassard-Mermin 1992, and the differential-phase-shift-keying protocols. We consider that the secure communication rate of the three protocols against an arbitrary individual attack, including the most commonly considered intercept-resend and photon-number splitting attacks, and concluded that the simple and efficient differential-phase-shift-keying protocol allows for more than 200 km of secure communication distance with high communication rate.

Key words quantum optics; single-photon detector; communication rate; error rate

1 引 言

信息时代的到来，一方面对信息传输速度的要求越来越高，另一方面，对信息安全性的要求也日益增加。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成为改变未来的保密通信方式，近年来已成为国内外的热门研究领域[1~3]。量子保密通信的关键 在于量子密钥分配(QKD)，QKD 能让通信双方(假定 Alice 和 Bob)共享一个无条件安全密钥，因为量子机制就能保证安全，密钥能用来一次性地加密和解密消息。因此，研究低误码率和长距离稳定的量子密钥分配系统已成为量子保密通信走向实用化的关键。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，并利用各种协议来抵御外界的攻击。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 协议和相关粒子协仪[4~6]。1992 年，Bennett 等人基于 BB84 协议，以强烈衰减

基金项目：北京市共建基金(XK100130837)资助项目。
作者简介：焦荣珍(1970—)，女，博士，副教授，主要从事量子光学和量子通信方面的研究。E-mail：jrz218@163.com

的激光脉冲做单光子源，信息加载在单光子的偏振上，第一次成功地在自由空间完成了演示性实验，从而掀起了量子密钥分配实验研究的高潮。2002 年，瑞士日内瓦大学的研究组在 67 km 光纤中实现了往复光路的长时间稳定的量子密钥分配实验。2004 年，世界上第一个量子密码通信网络在美国剑桥城正式投入运行，2006 年，多个研究小组合作实现了在自由空间 144 km 的量子密钥分配实验；在国内中国科学研究院和华东师范大学等单位也相继实现了远距离的 QKD 实验[7]。针对现今普遍采用的是把信息加载在通信波段(1.31 μm 和 1.55 μm)的单光子的相位或偏振态上，通过分析 1.55 μm 上转换单光子探测器的性能，即量子效率和暗计数与抽运能量之间的关系，说明在光纤 QKD 系统采用 1.55 μm 上转换单光子探测器较传统的雪崩二极管探测器的优势，并在此基础上，采用差分相移键控(DPSK)协议[8~10]分析 QKD 系统的性能，比较了 BB84，BBM92 和 DPSK 协议在截断-重发和光子数分裂攻击条件下，安全通信速率和误码率随通信距离的变化关系。

2 理论和计算公式

在 1.55 μm 上转换单光子探测器中，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，在波导结构干涉长度上产生的准相位匹配和紧密模式限制，转换光子然后被一个硅雪崩二极管(Si-APD)探测到，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

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

其中 $a_1 = 0.465$，$a_2 = 79.75$，p 以毫瓦为单位。

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

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

DPSK 协议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，其组成图如图 1 所示。

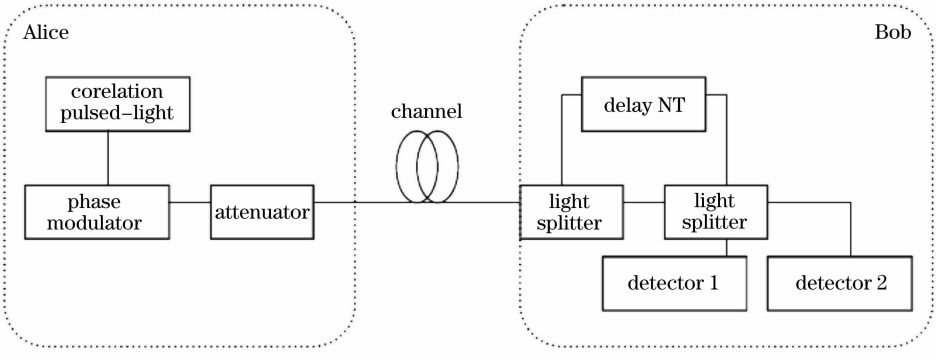

图 1 DPSK 协议组成图

Fig. 1 Configuration of the DPSK protocol

基于 DPSK 协议的安全性，在分析中考虑了光子数分裂和截断-重发攻击，DPSK 协议对抗多种复合攻击时的通信速率为

$$R_{DPSK} = \upsilon p_{click}\{\tau(e,\gamma) + f(e)[e\mathrm{lb}_2 e + (1-e)\mathrm{lb}_2(1-e)]\}, \tag{3}$$

误码率为：

$$e = \frac{\frac{1}{2}p_{dark} + bp_{signal}}{p_{click}} \tag{4}$$

其中 p_{click} 为 Bob 探测到的光子概率，其表达式为

$$p_{click} = \mu\eta 10^{-(aL+L_r)/10} + 2d$$

$$p_{signal} = \mu\eta 10^{-(aL+L_r)/10}, p_{dark} = 2d$$

这里，υ 为传输的重复速率，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，b 为系统本身的误码率，d 为系统每个测量时间窗内的暗计数；BB84 和 BBM92 协议在截断-重发和光子数分裂攻击条件下，通信速率和误码率的计算公式参见文献[8]。

3 结果与讨论

1.55 μm 上转换探测器的量子效率 η_{up} 随抽运的功率 p 的变化关系如图 2 所示。计算得出上转换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

它受到被捕获带电载流子的后向脉冲影响，这导致了在相当一段长的时间里有暗计数。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 $D_{\mathrm{up}}=6.4\times10^{3}\mathrm{s}^{-1}$。

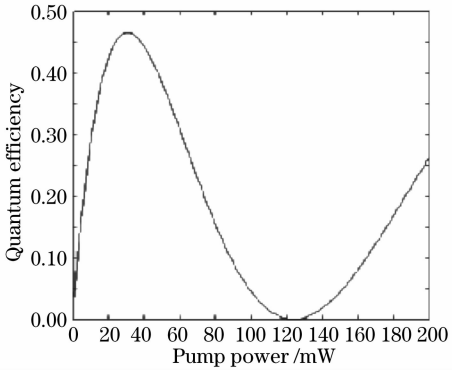

图 2　1.55 μm 升频探测器量子效率随抽运功率的变化关系

Fig. 2　Quantum efficiency of the 1.55 μm up-conversion single-photon detector as a function of pump power

利用 1.55 μm 上转换探测器，计算 BB84，BBM92 和 DPSK 协议下 QKD 系统的安全通信速率和误码率与通信距离的关系如图 3 和图 4 所示，其中 BB84 协议只限定在理想条件下，而 BBM92 协议在计算过程中只考虑确定纠缠光子源；信道衰减在 1.55 μm 的时候 $\alpha=0.2$ dB/km，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。

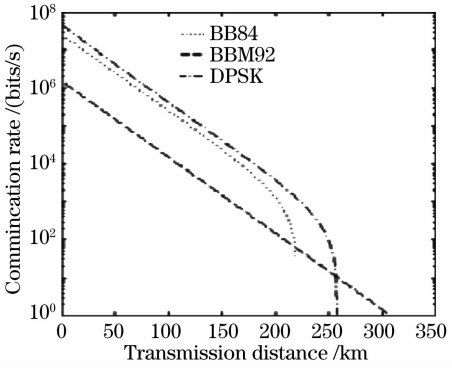

图 3　BB84，BBM92 和 DPSK 协议安全通信速率随距离的变化关系

Fig. 3　Secure communication rate as a function of distance for the BB84, BBM92 and DPSK protocols

对于任何 QKD 协议而言，如果用的不是 1.55 μm上转换探测器而是 InGaAs/InP APD，它的 $\nu_{\mathrm{APD}}=10$ MHz，其他的参数 $\eta_{\mathrm{APD}}=0.1$，$d_{\mathrm{APD}}=10^{-5}$/门，可见这样的通信距离只是应用 1.55 μm 上转换探测器系统的一半，通信速率却大了大概两个数量级，这是由于 InGaAs/InP APD 的门模式效应引起的。所以，1.55 μm 上转换探测器比起普通的探测器的在通信速率和通信距离上有很大的优势；通过比较三种协议通信速率和误码率随通信距离的变化，得出 DPSK 是一个非常实用的长距离 QKD 系统，密钥生成率大于 1 kHz，传输距离超过 200 km。

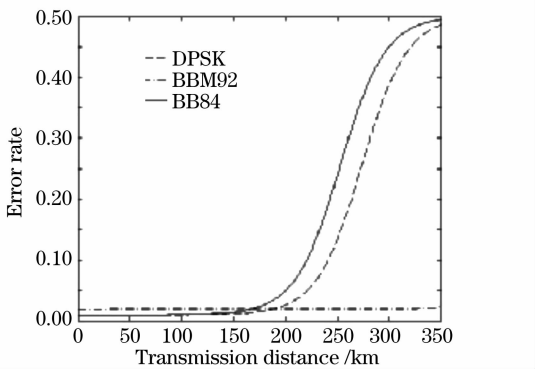

图 4　BB84，BBM92 和 DPSK 协议误码率随距离的变化关系

Fig. 4　Error rate as a function of distance for the BB84, BBM92 and DPSK protocols

参　考　文　献

1 Gui Youzhen, Mo Xiaofan, Han Zhengfu *et al*.. Quantum key distribution in optical fiber at wavelength of 1150nm[J]. *Acta Sinica Quantum Optica*, 2004, **10**(3): 131～134
桂有珍，莫小范，韩正甫 等. 1550 nm单模光纤的量子密钥分配[J]. 量子光学学报，2004，**10**(3)：131～134

2 Wang Xiangbin. Beat the photon-number-splitting attack in practical quantum cryptography[J]. *Phys. Rev. Lett.*, 2005, **94**: 230503

3 Kumar R, Lucamarini M, Giuseppe G D *et al*.. Two-way quantum key distribution at telecommunication wavelength [J]. *Phys. Rev. A*, 2008, **77**: 022304

4 Bennett C H, Brassard G. Computers, systems and signal processing Bangalore[C]. *Proc. of IEEE*, New York, 1984, 175～179

5 Bennett C H. Quantum cryptography using any two nonorthogonal states [J]. *Phys. Rev. Lett.*, 1992, **68**(21): 3121～3124

6 Ekert K. Quantum cryptography based on Bell′s theorem [J]. *Phys. Rev. Lett.*, 1991, **67**(6): 661～664

7 Wu Guang, Zhou Chunyuan, Chen Xiuliang *et al*.. A stable long-distance quantum key distribution system [J]. *Acta Physica Sinica*, 2005, **54**(8): 3622～3625
吴　光，周春源，陈修亮 等. 长距离长期稳定的量子密钥分配系统[J]. 物理学报，2005，**54**(8)：3622～3625

8 Diamanti E, Takesue H, Honjo T *et al*.. Performance of various quantum-key-distribution systems using 1.55 μm up- conversion single-photon detectors [J]. *Phys. Rev. A*, 2005, **72**: 052311

9 Inoue K, Waks E, Yamamoto Y. Differential-phase-shift quantum key distribution using coherent light[J]. *Phys. Rev. A*, 2003, **68**: 022317

10 Tsurumaru T. Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol [J]. *Phys. Rev. A*, 2007, **75**: 062319