

文章编号: 0253-2239(2007)08-1401-4

# 光纤耦合对量子密钥分配系统光子探测的影响

陈彦 邓科 胡渝

(电子科技大学物理电子学院, 成都 610054)

**摘要:** 借助量子密码术和卫星可以实现全球性的保密通信网络。但使用现有的单光子探测模块搭建星地量子密钥分配(QKD)系统,接收端就面临着空间光-多模光纤耦合的技术挑战。空间光-多模光纤耦合条件对星地量子密钥分配系统的跟瞄精度提出了严格要求。理论分析和定量计算表明,跟瞄精度  $\epsilon$  与光束发散角  $\theta_{\text{div}}$  的比值  $\epsilon/\theta_{\text{div}} \leq 0.5$  时,星地量子密钥分配系统的光子探测概率较高,系统可以正常工作;  $\epsilon/\theta_{\text{div}} \leq 0.1$  时,系统处于量子密钥产生速率为几 kb/s 的更理想状况。采用短波长更有利于满足空间光-多模光纤耦合条件,同时有利于系统获得更高的密钥产生速率。

**关键词:** 无线光通信技术; 光子探测概率; 星地量子密钥分配; 空间光-多模光纤耦合  
中图分类号: TN918.8 文献标识码: A

## Effect of Fiber Coupling on Photon-Detection Probability of Quantum Key Distribution Systems

Chen Yan Deng Ke Hu Yu

(Institution of Physics and Electronics, University of Electronic Science and Technology of China, Chengdu 610054)

**Abstract:** Global secure communication networks could become ture by use of quantum cryptography and satellite. However, satellite-to-ground quantum key distribution (QKD) systems by using of commercial single photon counting module (SPCM) are facing a challenge of spatial-light-to-multimode-fiber coupling on the receiver end. Spatial light-to-multimode-fiber coupling qualification puts strict restricts on pointing and tracking precision of satellite-to-ground QKD systems. It is indicated by theoretical analysis and quantificational calculation that QKD systems work normally with a high photon detection probability when the ratio of tracking error  $\epsilon$  to beam divergence  $\theta_{\text{div}}$  is below 0.5, and that QKD systems could work better when  $\epsilon/\theta_{\text{div}} \leq 0.1$  with a quantum key rate of a few kb/s. Light with shorter wavelength is more favorable to spatial-light-to-multimode-fiber coupling, and to achieve a higher quantum key production rate as well.

**Key words:** wireless optical communications; photon detection probability; satellite-to-ground quantum key distribution; spatial-light-to-multimode-fiber coupling

### 1 引 言

量子密码术是目前量子信息技术中最接近实际应用的一项技术。如何安全、有效、迅速地分发量子密钥是量子密码术的关键问题。在合法的通信用户之间产生、共享量子密钥的过程称为量子密钥分配(Quantum key distribution, QKD)。Bennett 等于 1992 年完成了第一个量子密钥分配的实验演示,实验是在 32 cm 的自由空间中进行的。Kurtsiefer 和美国洛斯·阿拉莫斯(Los Alamos)国家实验室

Hughes 的研究小组分别实现了距离为 23 km 和 10 km 的基于单光子源的自由空间量子密钥分配实验<sup>[1,2]</sup>。中国科技大学的彭承志等,在距离为 13 km 的自由空间中进行了基于纠缠光子对的量子密钥分配实验<sup>[3]</sup>。这些实验证明了将量子密码术应用于星-地通信链路,从而实现全球性量子保密通信的可行性。最近德国、奥地利、新加坡、荷兰和英国等多个国家的科学家,联合利用诱骗信号方法,在 144 km 的自由空间信道中演示了绝对安全的量子密钥分配<sup>[4]</sup>,这

作者简介: 陈彦(1978—),女,四川人,博士研究生,主要从事空间光通信技术、无线光传输技术以及量子密码术等方面的研究。E-mail: blastchen@163.com

导师简介: 胡渝(1939—),女,四川人,博士生导师,主要从事空间光通信技术、无线光传输技术等方面的研究。E-mail: huyu3919@sohu.com

收稿日期: 2006-11-14; 收到修改稿日期: 2007-01-14

项令人瞩目的进展进一步验证了星地量子密钥分配的可行性。

星地量子密钥分配能否成功关键在于,光子的成功发射,以及穿越湍流介质后,在强背景环境下对单光子的成功探测。单光子计数模块(Single photon counting module, SPCM)是对单光子进行探测的关键器件。星地量子密钥分配系统的光子传输信道是自由空间和随机大气信道,属于非导波信道。而现在商用的成熟单光子计数模块均是光纤器件。因此使用现有的单光子计数模块搭建星地量子密钥分配系统,则接收端就面临着空间光-光纤耦合的技术挑战<sup>[5]</sup>。

由于光纤芯径很小(标准多模光纤芯径为 50  $\mu\text{m}$  或 65  $\mu\text{m}$ ),因此空间光-光纤耦合模块对星地量子密钥分配系统的跟瞄精度提出了严格要求。现实中无法做到完美的跟瞄,残余跟瞄误差会影响空间光-光纤耦合的效率。而耦合效率直接与光子探测概率相关。维持一定的光子探测概率,是量子密钥分配系统产生有效密钥的前提。

本文将对使用单光子源的星地量子密钥分配系统中,空间光-多模光纤的耦合条件及其对光子探测概率的影响作出定量分析。

## 2 理论分析

### 2.1 空间光-多模光纤耦合条件

由于现有的成熟商用单光子计数模块均带多模光纤,且多模光纤的芯径更大,更容易进行空间光-多模光纤耦合,因此星地量子密钥分配系统接收端均针对多模光纤进行耦合。空间光-多模光纤耦合可以分为无源耦合和有源耦合两种方案。与单模光纤耦合不同,多模光纤不存在入射光场模式与光纤传输模式匹配的问题。无论采用哪种耦合方案,其实质均为:1)尽量使入射光束经过聚焦后,光斑处于多模光纤芯径端面范围内;2)入射方向必须进入多模光纤的数值孔径所规定的角度范围中。满足上述两个耦合条件的入射光经过聚焦后,才能在多模光纤中建立起稳定的传输光场。因此空间光-多模光纤耦合条件,对星地量子密钥分配系统的跟瞄(Acquisition, pointing and tracking, APT)子系统提出了严格要求。

原理上,对直接探测的光学接收系统,其接收机视场角  $\Omega_{\text{det}}$  与光电探测器的光敏面直径  $d_{\text{det}}$  和接收机光学系统的焦距  $f$  有关

$$\Omega_{\text{det}} = d_{\text{det}}/f, \quad (1)$$

这种系统对跟瞄子系统跟瞄精度  $\epsilon(3\sigma)$  的要求为

$$\epsilon \leq \Omega_{\text{det}}/k, \quad (2)$$

其中  $k$  为比例系数,与跟瞄子系统的伺服带宽有关。通信系统常用半导体雪崩光电二极管(APD)探测器的光敏面直径典型值为几百  $\mu\text{m}$  到 2 mm。若焦距  $f=30$  cm,  $d_{\text{det}}=300$   $\mu\text{m}$  (典型值),  $k=20$ , 则  $\Omega_{\text{det}}=1$  mrad,  $\epsilon \leq 50$   $\mu\text{rad}$ 。

对采用空间光-多模光纤耦合的星地量子密钥分配系统,耦合条件要求跟瞄子系统动态控制光束传输方向,使其不仅要处于由多模光纤芯径所决定的接收机的视场角  $\Omega_{\text{MMF}}$  内,还要始终处于多模光纤的数值孔径所决定的视场角  $\Omega_{\text{NA}}$  范围内。

$$\begin{cases} \Omega_{\text{mmf}} \approx d_{\text{mmf}}/f, \\ \Omega_{\text{NA}} = 2\varphi_{\text{max}} = 2\arcsin N_A. \end{cases} \quad (3)$$

这里,  $d_{\text{mmf}}$  为多模光纤的芯径,  $N_A$  为多模光纤的数值孔径。

空间光-多模光纤耦合条件对星地量子密钥分配系统跟瞄精度  $\epsilon(3\sigma)$  的要求为

$$\begin{aligned} \epsilon &\leq \Omega_{\text{fov}}/k, \\ \Omega_{\text{fov}} &= \min\{\Omega_{\text{NA}}, \Omega_{\text{MMF}}\}, \end{aligned} \quad (4)$$

其中  $\Omega_{\text{fov}}$  为采用空间光-多模光纤耦合后接收机视场角。对采用单光子计数模块(带标准 62.5/125  $\mu\text{m}$  多模光纤,  $N_A=0.275$ )的量子密钥分配系统的接收端:若  $f=30$  cm,  $k=20$ , 则  $\Omega_{\text{mmf}}=0.2$  mrad,  $\Omega_{\text{NA}}=560$  mrad,  $\Omega_{\text{fov}}=0.2$  mrad,  $\epsilon \leq 10$   $\mu\text{rad}$ 。

对比(1)式和(4)式可知,空间光-多模光纤耦合条件对星地量子密钥分配系统的跟瞄精度提出了更严格的要求。随着空间光通信系统技术的发展,跟瞄子系统技术已经基本被突破,目前国际先进水平的跟瞄精度可以达到  $\epsilon \leq 10$   $\mu\text{rad}(3\sigma)$  的水平<sup>[6]</sup>。因此现有的空间光通信技术和跟瞄子系统技术,可以部分满足空间光-多模光纤耦合条件对星地量子密钥分配系统的跟瞄精度的要求。

### 2.2 耦合效率

理想信道中(如真空),跟瞄子系统跟瞄精度满足  $\epsilon \leq \Omega_{\text{fov}}/k$ , 则空间光-多模光纤耦合模块以 99.8%(3 $\sigma$ )的概率,达到 100%的耦合效率(即  $\eta_c=1$ )。实际上,由于系统平台的振动以及大气湍流的影响,  $\eta_c < 1$ , 且  $\eta_c$  是一个随机变量。大气湍流引起的波前畸变中,波前倾斜分量占绝大部分,该部分畸变可通过跟瞄子系统纠正,残余误差可放在跟瞄误差  $\epsilon$  中考虑。假设  $\epsilon$  在  $x$  和  $y$  方向的跟踪误差分量  $\epsilon_x$ 、 $\epsilon_y$  为零均值、等标准差的正态分布随机变量,且  $\epsilon_x$ 、 $\epsilon_y$  互相独立<sup>[7]</sup>, 则由跟瞄误差对应的总角度误差  $\epsilon$

的二维分布为瑞利分布。

对高斯光束,由跟瞄误差引起的损耗因子为<sup>[8]</sup>

$$L(\epsilon) = \exp[-G_T \epsilon^2], \quad (5)$$

其中  $G_T$  为发射天线增益,通常采用  $G_T = 16/\theta_{\text{div}}^2$  计算<sup>[9]</sup>,  $\theta_{\text{div}}$  为光束发散角。因此,受跟瞄误差影响,空间光-多模光纤耦合效率为

$$\eta_c = \eta_0 \cdot L(\epsilon) = \exp\left(-\frac{16\epsilon^2}{\theta_{\text{div}}^2}\right), \quad (6)$$

$\eta_0$  为理想情况下的耦合效率,  $\eta_0 = 1$ 。

### 2.3 耦合效率对单光子探测概率的影响

采用单光子光源的量子密钥分配系统的光源为高度衰减的激光脉冲,脉冲中含有的光子数  $n$  服从泊松分布:

$$P(n) = \frac{\mu^n}{n!} \exp(-\mu), \quad (7)$$

其中  $\mu$  为每个脉冲所包含的平均光子数,  $0 < \mu < 1$ , 则接收端(Bob)至少探测到一个光子的概率为

$$P_B = P\{n \geq 1\} = \exp(-\mu\eta) \sum_{n=1}^{\infty} \frac{(\mu\eta)^n}{n!} = 1 - \exp(-\mu\eta), \quad (8)$$

$$\eta = T_{\text{Am}} \eta_r \eta_c \eta_D \eta_Q, \quad (9)$$

其中  $\eta$  为量子密钥分配系统的光子传输效率。 $T_{\text{Am}}$  为从发射端 Alice 到接收端 Bob 的大气光学透射率,它与系统工作波长有关; $\eta_r$  为 Bob 接收机的光学透射率,包括光学接收天线、分光镜、滤波器等光学器件的光学透射率; $\eta_c$  为空间光-多模光纤耦合效率;

$\eta_D$  为探测器的量子效率; $\eta_Q$  为系统所使用的密钥分配协议所决定的光子探测概率:

$$\eta_Q = \begin{cases} 50\%, & (\text{BB84}) \\ 25\%. & (\text{B92}) \end{cases} \quad (10)$$

考虑跟瞄误差对空间光-多模光纤耦合效率  $\eta_c$  的影响时, Bob 至少探测到一个光子的概率为

$$P_B = 1 - \exp\left[-\mu T_{\text{Am}} \eta_r \exp\left(-\frac{16\epsilon^2}{\theta_{\text{div}}^2}\right) \eta_D \eta_Q\right]. \quad (11)$$

## 3 仿真和讨论

根据上一节的理论分析,我们对采用空间光-多模光纤耦合的星地量子密钥分配系统的光子探测概率进行了计算。计算以跟瞄误差与光束发散角的比值  $\epsilon/\theta_{\text{div}}$  的归一化参量为横坐标。

图 1 显示,量子密钥分配系统的光子探测概率  $P_B$  强烈地依赖于跟瞄误差与光束发散角的比值  $\epsilon/\theta_{\text{div}}$ 。为了保持相对较高的光子探测概率,系统设计和运行必须维持在  $\epsilon/\theta_{\text{div}} \leq 0.5$  的范围内。这种情况下,假设 Alice 的脉冲产生频率为 10 MHz,平均光子数  $\mu=0.1$ ,在 BB84 协议下, Bob 在 1 s 内至少可以探测到 7700 个光子,即原始密钥产生率(Raw Key Rate)  $\geq 7.7$  kb/s。再经过一系列纠错和保密加强措施后,系统在 1 s 可以提取得到几百个比特的量子密钥。

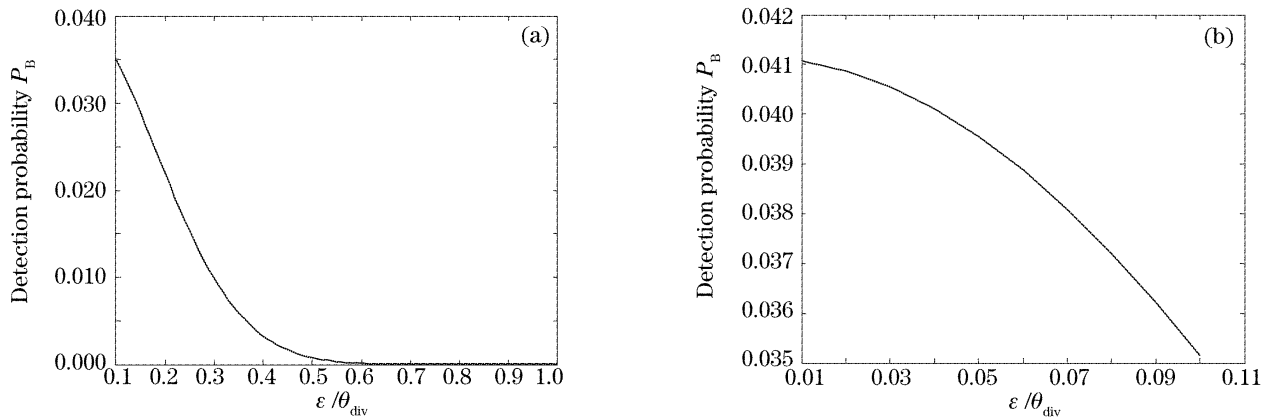


图 1 空间光-多模光纤耦合对星地量子密钥分配系统光子探测概率的影响。(a)  $0.1 \leq \epsilon/\theta_{\text{div}} \leq 1$ , (b)  $0.01 \leq \epsilon/\theta_{\text{div}} \leq 0.1$

Fig. 1 Effect of coupling efficiency of spatial-light-to-multimode fiber on satellite-to-ground quantum key distribution system. (a)  $0.1 \leq \epsilon/\theta_{\text{div}} \leq 1$ , (b)  $0.01 \leq \epsilon/\theta_{\text{div}} \leq 0.1$

$\epsilon/\theta_{\text{div}} > 0.5$  的区域,  $P_B$  急剧下降。如  $\epsilon/\theta_{\text{div}} = 1$  时,  $P_B = 4.7 \times 10^{-9}$ , 此时相同情况下, 1 s 内 Bob 只能探测到  $4.7 \times 10^{-2}$  个光子, 系统无法进行密钥提取。

从图 1 还可以看出, 当  $\epsilon/\theta_{\text{div}} \leq 0.1$  时, 系统的光子探测概率  $P_B > 0.035$ 。假设 Alice 的脉冲产生频

率为 10 MHz, 平均光子数  $\mu = 0.1$ , 在 BB84 协议下, Bob 在 1 s 内至少可以探测到 35000 个光子, 即原始密钥产生率大于 35 kb/s。再经过一系列纠错和保密加强措施后, 系统在 1 s 可以提取得到几千个量子密钥。这种数量级的量子密钥产生速率更加理想。

另外,2.1节的分析指出,空间光-多模光纤耦合条件要求量子密钥分配系统跟瞄误差处于  $\epsilon \leq 10 \mu\text{rad}$  的量级。为保证系统有较高的光子探测效率,即  $\epsilon/\theta_{\text{div}} \leq 0.5$ ,则 Alice 发射的信号光发散角必须维持在  $\theta_{\text{div}} \leq 20 \mu\text{rad}$  的范围内。由于光束的衍射极限角度与波长成正比,因此,采用短波长更有利于满足空间光-多模光纤耦合条件,同时有利于系统获得更高的密钥产生速率。目前的空间光通信系统中,光束发散角度典型值为  $10 \sim 60 \mu\text{rad}$ <sup>[6]</sup>。因此,目前的光学设计和加工能力尚无法完全满足星地量子密钥分配系统的要求。

## 4 结 论

空间光-多模光纤耦合条件对星地量子密钥分配系统的跟瞄精度提出了严格要求,不完美的跟瞄使得空间光-多模光纤耦合效率下降。耦合效率的降低导致星地量子密钥分配系统的光子探测概率下降,进而影响系统的密钥产生速率。本文的定量分析表明,系统跟瞄精度与光束发散角度的比值  $\epsilon/\theta_{\text{div}} \leq 0.5$  时,量子密钥分配系统可以进行正常的工作。而  $\epsilon/\theta_{\text{div}} \leq 0.1$  时,系统的密钥产生速率可以达到几 kb/s 的较理想状况。另外空间光-多模光纤耦合条件对星地量子密钥分配系统的信号光发散角也提出了严格要求。由于光束的衍射极限角与波长成正比,因此采用短波长更有利于满足空间光-多模光纤耦合条件,同时有利于系统维持更高的密钥产

生速率。

## 参 考 文 献

- 1 C. Kurtsiefer, P. Zarda, P. M. Gorman *et al.*. Long distance free space quantum cryptography[C]. *Proc. SPIE*, 2002, **4917**: 25~31
- 2 R. J. Hughes, J. E. Nordholt, D. Derkacs *et al.*. Practical free-space quantum key distribution over 10 km in daylight and at night[J]. *New J. Phys.*, 2002, **4**: 43.1~43.14
- 3 Chenzhi Peng, Tao Yang, Xiaohui Bao *et al.*. Experimental free space distribution of entangled photon pairs over 13 km; towards satellite-based global quantum communications[J]. *Phys. Rev. Lett.*, 2005, **94**(15): 150501-1~150501-4
- 4 S. M. Tobias, W. Henning, F. Martin *et al.*. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km[J]. *Phys. Rev. Lett.*, 2007, **98**(1): 010504-1~010504-4
- 5 W. T. Buttler, R. J. Hughes, P. G. Kwiat *et al.*. Practical free-space quantum key distribution over 1 km[J]. *Phys. Rev. Lett.*, 1998, **81**(15): 3283~3286
- 6 J. Romba, Z. Sodnik, M. Reyes *et al.*. ESA's bidirectional space-to-ground laser communication experiments [C]. *Proc. SPIE*, 2004, **5550**: 287~298
- 7 K. Kiasaleh. On the probability density function of signal intensity in free-space optical communications systems impaired by pointing jitter and turbulence [J]. *Opt. Engng.*, 1994, **33**(11): 3748~3757
- 8 A. Polishuk, S. Arnon. Impact of the random jitter on laser satellite communication system with an optical preamplifier[C]. *Proc. SPIE*, 2004, **5160**: 319~328
- 9 R. M. Gagliardi, S. Karp. *Optical Telecommunications* [M]. , Chen Genxiang, Qin Yuwen, Zhao Yucheng *et al.* transl., Beijing: Publishing House of Electronics Industry, 1998. 10~11 (in Chinese)  
R. M. Gagliardi, S. Karp. 光通信技术与应用[M]. 陈根祥,秦玉文,赵玉成 等译. 北京: 电子工业出版社, 1998. 10~11