第 29 卷 第 11 期
2009 年 11 月

光 学 学 报
ACTA OPTICA SINICA

Vol. 29, No. 11
November, 2009

文章编号：0253-2239(2009)11-2989-05

# 光子数分束攻击对星地量子密钥分配系统安全的影响

陈 彦[1] 杨红宇[2] 邓 科[1]

([1] 电子科技大学空天科学技术研究院，四川 成都 610054；[2] 电子科技大学自动化工程学院，四川 成都 610054)

**摘要** 由于仪器设备性能的不完美和信道传输损耗的存在，光子数分束(PNS)攻击对采用弱相干脉冲（WCP）光源的量子密钥分配(QKD)系统的安全性构成重大威胁。以基于 WCP 光源的星地 QKD 系统为研究对象，推导了在 PNS 攻击者采用最佳窃听策略进行窃听时，保证密钥绝对安全的最大天顶角和可采用的平均光子数之间的关系。理论分析和计算结果表明，星地 QKD 系统的最大安全传输天顶角和可使用的平均光子数等重要系统参数的取值上限均受 PNS 攻击的限制，最终系统的密钥交换速率和系统容量受到限制。对星地 QKD 系统的传输容量来说，天顶角和平均光子数是一对矛盾的影响因素。提供了一种对实际星地 QKD 系统的天顶角和平均光子数参数进行估算的方法。

**关键词** 光通信；参数估算；统计分析；光子数分束攻击；星地量子密钥分配；安全性；天顶角；平均光子数

**中图分类号** TN929.1 **文献标识码** A **doi**：10.3788/AOS20092911.2989

# Effects of Photon-Number-Splitting Attacks on the Security of Satellite-to-Ground Quantum Key Distribution Systems

Chen Yan[1] Yang Hongyu[2] Deng Ke[1]

([1] *Institute of Astronautics and Aeronautics, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*

[2] *College of Automation, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

**Abstract** The security of practical quantum key distribution (QKD) systems based on weak coherent pulse (WCP) sources is imperiled by photon number splitting (PNS) attacks due to imperfectness of devices and channel loss. The relation between the zenith angle and the mean photon number for security of a satellite-to-ground QKD system based on the WCP source against PNS attacks which operates with the optimal eavesdropping strategy is provided. The theoretical and calculation results shows the upper limits of key parameters for satellite-to-ground QKD systems, such as the zenith angle and the mean photon number, are limited by PNS attacks, and eventually the key exchange rate and the capacity of QKD systems are limited as well. The zenith angle and the mean photon number have an incompatible effect on the capacity of a satellite-to-ground QKD system. At the same time a method of parameter estimation of the zenith angle and the mean photon number for security of practical satellite-to-ground QKD systems against PNS attacks is provided.

**Key words** optical communications; parameter estimation; statistical analysis; photon number splitting attacks; satellite-to-ground quantum key distribution; security; zenith angle; mean photon number

## 1 引 言

基于弱相干脉冲（WCP）光源的量子密钥分配(QKD)技术是目前研究最广泛、最接近实用水平的量子密码术。理论上量子密码术提供了前所未有的安全性。但在实际应用中仪器设备性能的不完美和传输信道损耗的存在，给窃听者(Eve)留下了攻击

**收稿日期**：2008-12-20；**收到修改稿日期**：2009-02-23

**基金项目**：电子科技大学青年基金(L08047401JX0782)资助项目。

**作者简介**：陈 彦(1978—)，女，博士，讲师，主要从事无线光通信和量子密码术等方面的研究。

E-mail：blastchen@uestc.edu.cn

QKD 系统的漏洞。目前已有文献从信息论的角度分析了各种攻击(如选择性攻击、联合性攻击、路径攻击、克隆攻击等)对理想 QKD 系统、基于 WCP 光源的 QKD 系统和光纤 QKD 网络的安全性的影响[1~5]。事实上极简单的攻击对基于 WCP 光源的 QKD 系统的安全性就能构成严重威胁,如光子数分束(PNS)攻击。理论上诱骗态协议可以检测传输信道上是否有 PNS 攻击存在[6,7]。PNS 攻击会改变信号脉冲中的光子数,通过随机发送诱骗态信号并公开检测这些诱骗态可判断有无分光子窃听行为发生。在自由空间 QKD 系统(包括陆上无线链路和星地链路)中,信道传输损耗的变化具有随机性,因此即使在没有分光子窃听的情况下信号脉冲中的光子数也会发生变化,诱骗态协议的适用性大大降低。因此对基于 WCP 光源的自由空间 QKD 系统,如何保证系统在 PNS 攻击下的安全性成为量子密码术实用化面临的重要挑战之一。

量子密码术的最终目的是要实现全球化的量子保密通信网络。仅凭光纤和陆上自由空间 QKD 链路无法实现该目标。星地 QKD 链路可以弥补光纤和陆上自由空间 QKD 链路在传输距离上的不足,实现全球化的量子保密通信网络。本文以基于 WCP 光源和 BB84 协议的星地 QKD 系统为研究对象,提供一种在采用最佳窃听策略的 PNS 攻击下,保证密钥安全性的最大天顶角和发射平均光子数等关键系统参数的估算方法,还将对面临 PNS 攻击时,上述关键系统参数对星地 QKD 系统的密钥交换速率和传输容量的影响进行理论分析。

## 2 弱相干脉冲光源与光子数分束攻击

### 2.1 弱相干脉冲光源

对基于单光子源的偏振编码 QKD 系统,实际系统均采用 WCP 光源来代替理想单光子源。WCP 光源发出的脉冲包含的光子数 $n$ 服从泊松分布

$$p_{\text{Poisson}}(n)=\exp(-\mu)\frac{\mu^n}{n!}, \tag{1}$$

其中 $\mu$ 为每个脉冲所含的平均光子数。为减少多光子脉冲所占比例,一般 $\mu\ll 1$。这种光源的某些脉冲中会出现多于一个光子的情况。例如,对平均光子数为 $\mu=0.1$ 的 WCP 光源,它发出的所有脉冲当中,有 90%的脉冲是空脉冲,9.5%的脉冲含有一个光子,0.5%的脉冲为多光子脉冲(含有一个以上光子)。虽然多光子脉冲的比例很低,但这仍然给 Eve 留下了窃听的机会。

### 2.2 最佳窃听策略的光子数分束攻击

PNS 攻击通常在量子传输路径中插入分光装置以便截取信号脉冲中的部分光子,并经过测量获得关于密钥的信息。由于 WCP 光源发出的多光子脉冲,PNS 攻击可在不被发现的情况下访问光子并获得关于密钥的信息。同时单光子探测器无法分辨入射光子的数目,即无法分辨光子数态 $|m\rangle$ 和 $|n\rangle$ $(m\neq n, m>0, n>0)$,因此无法察觉窃听的存在。另外接收端的仪器设备以及量子传输信道均存在传输损耗,因此更加难以察觉 PNS 攻击的存在。

由于量子不可克隆定理的限制,Eve 无法窃听单光子。因此在 PNS 攻击中,Eve 的最佳窃听策略是:拦截所有单光子脉冲、窃听所有多光子脉冲,并使被窃听过的多光子脉冲中的所有剩余光子都成为密钥比特。因此 Eve 进行分光所获得的光子数越少,对最后能获得更多的密钥信息越有利。Eve 选择只分走多光子脉冲中的一个光子,将剩余 $n-1$ 个光子转发给 Bob。之后 Eve 将单光子态"真实的"保存下来,直到 Alice 和 Bob 在公开信道上讨论编码基时为止。通过对公开信道的窃听,Eve 获悉用于量子传输的偏振基,就可以获得所有由多光子脉冲产生的密钥的确定信息。

为实现上述攻击策略,PNS 攻击应具有以下能力和特性:

(1) Eve 可以对光子数进行量子无损测量(QND)因而可以在不扰动光子数态 $|n\rangle$ 的情况下区分单光子脉冲和多光子脉冲;

(2) Eve 有能力从多光子脉冲中仅分离出一个光子,将剩余 $n-1$ 个光子发送给 Bob;

(3) Eve 可用无损信道替代有损信道,使光子数态 $|n-1\rangle$ 直达 Bob;

(4) Eve 具备量子存储的能力,可将分光提取到的光子偏振态"真实地"保存。

对 PNS 攻击特性描述中的部分操作(如 QND、量子存储)在当前的技术水平下还无法完成,但一个实际 QKD 系统的无条件安全性必须在假设窃听者具备"无限的"窃听能力的情况下进行分析才是最严密的。因此暂不关注 Eve 如何具备上述能力。

使用最佳窃听策略进行 PNS 攻击时,Eve 只对光子数态为 $|n\rangle$ $(n\geqslant 2)$ 的信号脉冲进行窃听,并且总是转发光子态 $|n-1\rangle$ 给 Bob。因此不考虑传输损耗时,光子数态 $|n\rangle$ 到达 Bob 端的概率为

$$S(n)=\begin{cases}0, & n=0,1\\ p_{\text{Poisson}}(n+1)=\exp(-\mu)\dfrac{\mu^{n+1}}{(n+1)!}, & n\geqslant 2\end{cases} \tag{2}$$

当传输信道上存在采取最佳窃听策略的 PNS 攻击时，Bob 可探测到的光子均来源于多光子脉冲，其光子探测概率为

$$\begin{aligned}p_{\text{B}}&=\sum_{m=1}^{\infty}\sum_{n=1}^{m}\binom{m}{n}\eta_{\text{B}}^{n}(1-\eta_{\text{B}})^{m-n}\cdot S(n)=\\&\sum_{m-1}^{\infty}\exp(-\mu)\frac{\mu^{m+1}}{(m+1)!}[1-(1-\eta_{\text{B}})^{m}]=\\&1-\frac{\exp(-\mu\eta_{\text{B}})-\eta_{\text{B}}\exp(-\mu)}{1-\eta_{\text{B}}}=\\&p_{\text{B}}(\eta_{\text{B}},\mu),\end{aligned} \tag{3}$$

其中 $\eta_{\text{B}}=\eta_{\text{r}}\eta_{\text{D}}\eta_{\text{Q}}$ 为 Bob 端的光子接收效率。$\eta_{\text{r}}$ 是接收端的光学透过率。$\eta_{\text{D}}$ 为单光子探测器的量子效率。$\eta_{\text{Q}}$ 是由量子密钥分配协议决定的光子探测效率。

合法用户采用 BB84 协议进行量子密钥分发时，Eve 通过 PNS 攻击可获得的最大密钥比特数的均值应为多光子脉冲数的一半，即

$$\begin{aligned}N_{\text{E}}^{\max}&=\frac{N}{2}p_{\text{B}}(\eta_{\text{B}},\mu)=\\&\frac{N}{2}\left[1-\frac{\exp(-\mu\eta_{\text{B}})-\eta_{\text{B}}\exp(-\mu)}{1-\eta_{\text{B}}}\right],\end{aligned} \tag{4}$$

其中 $N$ 为 WCP 光源所发出的总脉冲数。

## 3　光子数分束攻击对星地量子密钥分配系统安全传输的影响

### 3.1　最大安全传输天顶角

信道中不存在窃听时，Bob 应收到的比特来源于所有的单光子脉冲和多光子脉冲，其数量为

$$\begin{aligned}N_{\text{B}}&=\frac{N}{2}\sum_{n-1}^{\infty}\exp(-\mu)\frac{\mu^{n}}{n!}\sum_{m-1}^{n}\binom{n}{m}\eta^{m}(1-\eta)^{n-m}=\\&\frac{N}{2}\sum_{n=1}^{\infty}\exp(-\mu)\frac{\mu^{n}}{n!}[1-(1-\eta_{\text{B}})^{n}]=\\&\frac{N}{2}[1-\exp(-\mu\eta)],\end{aligned} \tag{5}$$

其中 $\eta$ 为 QKD 系统光子传输效率。

当 Eve 使用最佳窃听策略时，QKD 系统安全传输条件为

$$N_{\text{B}}>N_{\text{E}}^{\max}, \tag{6}$$

即要求 Bob 应收到的比特数 $N_{\text{B}}$ 大于 Eve 通过窃听可以获得的最大比特数 $N_{\text{E}}^{\max}$。由(4)式～(6)式可得

$$\eta>\frac{1}{\mu}\ln\left[\frac{1-\eta_{\text{B}}}{\exp(-\mu\eta_{\text{B}})-\eta_{\text{B}}\exp(-\mu)}\right], \tag{7}$$

(7)式说明，对一个实际 QKD 系统，在给定的系统参数下(如平均光子数、接收端光学效率等)，系统光子传输效率有一个安全下限，太小的光子传输效率使得系统不再安全。QKD 系统光子传输效率 $\eta$ 取决于量子传输信道、系统所采用光电子仪器和 QKD 协议：

$$\eta=\langle T_{\text{atm}}\rangle\eta_{\text{G}}\eta_{\text{B}}, \tag{8}$$

其中 $T_{\text{atm}}$ 描述了量子传输信道的光学透过率，它往往是一随机变化量。$\eta_{\text{G}}$ 是与接收光学天线的功率耦合系数，对实际 QKD 系统，$\eta_{\text{G}}$ 为一小于 1 的定值。

对星地 QKD 系统，$T_{\text{atm}}$ 是大气衰减系数 $\alpha$ 和天顶角 $\varphi$ 的函数：

$$T_{\text{atm}}=\exp\left[-\sec\varphi\int_{H_{\text{T}}}^{H_{\text{S}}}\alpha(l)\,\text{d}l\right], \tag{9}$$

由(7)式～(9)式可得，要保证星地 QKD 系统在 PNS 攻击下的绝对安全性，必须满足以下关系：

$$\varphi<\varphi_{\max}^{\text{secure}}=\text{arc sec}\left\{-\frac{\ln\{1/(\mu\eta_{\text{B}}\eta_{\text{G}})\cdot\ln(1-\eta_{\text{B}})/[\exp(-\mu\eta_{\text{B}})-\eta_{\text{B}}\exp(-\mu)]\}}{\int_{H_{\text{T}}}^{H_{\text{A}}}\alpha(l)\,\text{d}l}\right\}, \tag{10}$$

(10)式说明，为保证系统在 PNS 攻击下的安全性，星地 QKD 系统天顶角的取值存在一上限，即 $\varphi_{\max}^{\text{secure}}$。

### 3.2　光子数分束攻击对星地量子密钥分配系统容量的影响

天顶角是指星-地 QKD 发射端的天线指向偏离天顶方向的角度，如图 1 所示。实际的星地链路传输过程中，天顶角随卫星(地球同步轨道卫星除外)的运动而变化，当卫星经过地面站的天顶位置时，天顶角为零。最大传输天顶角不仅决定了星地系统的最大传输距离，还决定了地面站与卫星可进行链接的总时间，进而影响星地链路的最大容量。天顶角是实际系统设计和操作中的一个重要参数。

一个星-地 QKD 系统的传输容量为

$$C_{\text{QC}}=t\,R_{\text{K}}=\frac{2L\sin\varphi}{\nu_{\text{S}}}\cdot R_{\text{K}}, \tag{11}$$

其中 $R_{\text{K}}$ 为量子密钥交换速率，它与 WCP 光源的平均光子数 $\mu$ 有关。$\nu_{\text{S}}$ 为卫星在轨飞行速度。系统传输距离为 $L=\Delta H/\cos\varphi$，$\Delta H=H_{\text{S}}-H_{\text{T}}$ 为卫星与地

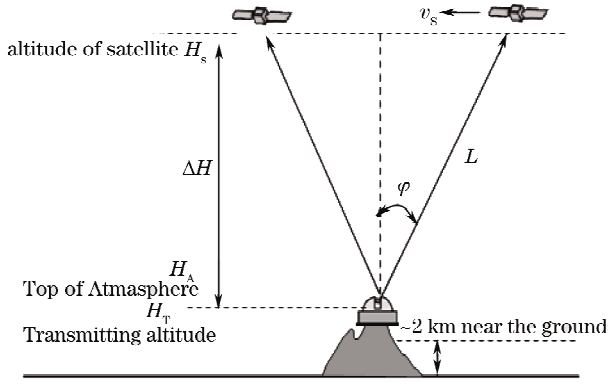


图 1 星地量子密钥分配链路示意图

Fig. 1 Sketch of satellite-to-ground QKD links

面发射平台的海拔之差。

星-地 QKD 系统的传输容量为

$$C_{QC} = 2\tan\varphi\Delta H R_K/\nu_S \approx 2\tan\varphi H_S R_K/\nu_S, \quad (12)$$

由(10)式和(12)式可知，最大安全传输天顶角 $\varphi_{max}^{secure}$ 不仅决定了星地 QKD 系统在 PNS 攻击下的最大传输距离，还决定了一个地面站与一个 LEO 卫星进行安全量子密钥传输的总时间 $t$，进而影响星地量子密钥交换的最大容量。

## 4 讨 论

考虑一个采用 BB84 协议的星地 QKD 系统(取 $\eta_R = \eta_D = \eta_G = 1$，$\eta_Q = 0.5$，$H_S = 300$ km)。由(10)式可得 PNS 攻击下的最大安全传输天顶角与平均光子数以及信道上的大气衰减的关系，如图 2，表 1 所示。

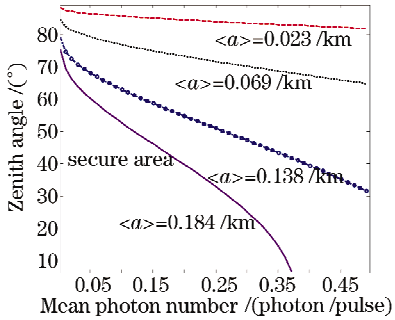


图 2 不同大气衰减时最大安全传输天顶角与平均光子数的关系

Fig. 2 Relation between the maximal zenith angles and mean photon numbers for secure transmissions under different atmospheric attenuations

由图 2 可见，为保证星地 QKD 系统在 PNS 攻击下的安全性，最大安全传输天顶角随平均光子数的增加呈减小趋势。这意味着取更大传输天顶角的星地 QKD 系统必须使用更低的发射平均光子数。随着发射的平均光子数减小，WCP 光源发出的多光子脉冲(即 Eve 可窃听的脉冲)所占的比例也减小，系统受到 PNS 攻击的可能性越小，但同时 QKD 系统的密钥交换速率也大大降低，最终将导致系统传输容量减小。另外，较小的发射平均光子数可允许较大的传输天顶角，导致系统密钥交换时间的增加，将使系统传输容量有所增加。考虑两种极端情况：1)$\varphi_{max}^{secure}\to 0$ 时，平均光子数 $\mu$ 达到上限，密钥交换速率 $R_K$ 达到上限，但系统可进行密钥交换的时间仅为卫星处于地面站天顶位置的一瞬间，系统容量 $C_{QC}\to 0$，没有实际意义；2)$\mu\to 0$ 时，天顶角 $\varphi$ 可取最大值 $\varphi_{max}^{secure}$，密钥交换时间达到上限，但过低的密钥交换速率 $R_K$ 导数，系统容量 $C_{QC}\to 0$，也没有实际意义。因此平均光子数 $\mu$ 和天顶角 $\varphi$ 的取值对 QKD 系统容量的影响是矛盾的。实际应用中需要综合考虑两方面影响，适当选取 $\mu$ 和 $\varphi$ 的值。

表 1 不同大气衰减时平均光子数与最大天顶角的关系

Table 1 Relation between the maximal zenith angles and mean photon numbers for secure transmissions under different atmospheric attenuations

| $\mu$/( photon /pulse) | $\langle\alpha\rangle=$ 0.023 km$^{-1}$ | $\langle\alpha\rangle=$ 0.069 km$^{-1}$ | $\langle\alpha\rangle=$ 0.138 km$^{-1}$ | $\langle\alpha\rangle=$ 0.184 km$^{-1}$ |
|---|---|---|---|---|
| 0.05 | 86 | 79 | 68 | 60 |
| 0.1 | 85 | 77 | 63 | 52 |
| 0.2 | 84 | 73 | 55 | 40 |
| 0.3 | 83 | 70 | 48 | 25 |
| 0.5 | 82 | 65 | 30 | — |
| $\Delta\varphi_{max}^{secure}$(°) | 4 | 14 | 38 | ~70 |

由图表还可看出，大气衰减越大，最大安全传输天顶角减小得越迅速。当大气衰减很小时，随着平均光子数的增加安全传输天顶角呈缓慢减小趋势。如 $\langle\alpha\rangle=0.023$ km$^{-1}$ 时，星地 QKD 系统的最大安全传输天顶角仅仅从 86°($\mu$=0.05 photon /pulse)减小到 82°($\mu$=0.5 photon /pulse)，$\Delta\varphi_{max}^{secure}=4°$。此时，PNS 攻击对最大安全传输天顶角的影响不明显。而当大气衰减较大时，如 $\langle\alpha\rangle=0.138$ km$^{-1}$ 时，$\Delta\varphi_{max}^{secure}=38°$；$\langle\alpha\rangle=0.184$ km$^{-1}$ 时，$\Delta\varphi_{max}^{secure}$ 超过了 70°。此时，随着大气衰减的增加，PNS 攻击愈发明显地显现出对系统可使用的天顶角的限制。因此选择在大气衰减较小的地点建立星地 QKD 链路，可使系统受 PNS 攻击的影响更小。

图 2 中曲线为实际星地 QKD 系统的平均光子数 $\mu$ 和天顶角 $\varphi$ 的取值提供了一个安全上限。即处于图 2 中曲线下方区域内的 $\mu$ 和 $\varphi$ 的取值可保证

QKD 系统面临 PNS 攻击时得到的密钥仍然安全；任何超过(10)式限制的 $\mu$ 和 $\varphi$ 的取值(即图 2 中的曲线上方区域)都使系统面临 PNS 攻击时，所得量子密钥不再安全。在实际应用中，人们可对大气衰减进行实地测量，再根据(10)式对 $\mu$ 和 $\varphi$ 取值进行估算(计算中取实测所得最大衰减值)，使这两个系统参数值选取在安全区域内，保证密钥在 PNS 攻击下的安全性。

## 5 结　　论

实用化的 QKD 系统面临的重要挑战之一是保证密钥在各种窃听方式下的绝对安全性。光子数分束(PNS)攻击可以拦截单光脉冲并窃听多光子脉冲，是一种极具威胁的攻击方式。由于 WCP 光源发出的多光子脉冲、信道传输损耗和探测器性能缺陷的存在，窃听者 Eve 通过 PNS 攻击可以窃听所有形成量子密钥的光脉冲而不被察觉，从而对实际 QKD 系统的安全性构成极大威胁。本文给出了基于 WCP 光源的星地 QKD 系统在 PNS 攻击下的最大安全传输天顶角 $\varphi_{\max}^{\text{secure}}$ 的表达式，并分析了 $\varphi_{\max}^{\text{secure}}$ 与系统可用平均光字数和传输信道上的大气衰减的关系。通过分析证明，PNS 攻击限制了星地 QKD 系统的最大安全传输天顶角和可使用的平均光子数，最终限制了系统的安全密钥交换速率和传输容量。在实际应用中，可对针对不同的大气衰减情况，根据(10)式来估算基于 WCP 光源的星地 QKD 系统在 PNS 攻击下的安全传输天顶角和系统可采用的平均光子数的上限。

## 参　考　文　献


1 Nikolopoulos G. M, Alber G. Security bound of two-basis quantum-key-distribution protocols using qudits[J]. *Phys. Rev. A*, 2005, **72**(3): 032320-1

2 Grassard G, Lutkenhaus N, Mor T *et al*.. Limitations on practical quantum cryptography[J]. *Phys. Rev. Lett.*, 2000, **85**(6): 1330～1333

3 Niederberger A, Scarani V, Gisin N. Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum ryptography[J]. *Phys. Rev. A*, 2005, **71**(4): 042316-1

4 Fu Mingxing. Influence of path-attack on security of quantum key distribution networks[J]. *Chinese J. Quant. Electron.*, 2008, **25**(5): 572～576
傅明星. 路径攻击对量子密钥分发网络安全性的影响[J]. 量子电子学报, 2008, **25**(5): 572～576

5 Zhao Shengmei, Li Fei, Zheng Baoyu. The security of quantum key distribution under probabilistic clone/resend attack[J]. *Journal of Electronics&Information Technology*, 2005, **27**(10): 1639～1642
赵生妹，李　飞，郑宝玉. 量子密钥分配协议在概率克隆/重发攻击下的安全性[J]. 电子与信息学报, 2005, **27**(10): 1639～1642

6 Lo H. K, Ma X. F, Chen K. Decoy state quantum key distribution [J]. *Phys. Rev. Lett.*, 2005, **94**(23): 230504

7 Xiangbin Wang. Beating the photon-number-splitting attack in practical quantum cryptography[J]. *Phys. Rev. Lett.*, 2005, **94**(23): 230503-1

8 Jiao Rongzhen, Feng Chenxu, Tang Shaojie. Communication rate and error rate in the quantum-key-distribution system [J]. *Acta Optica Sinica*, 2008, **28**(s2): 167～169
焦荣珍，冯晨旭，唐少杰. 量子密钥分配系统中的通信速率和误码率[J]. 光学学报, 2008, **28**(s2): 167～169

9 Jian Peng, Yifei Fu, Xudong Shang. Quick single-photon detector with many avalanche photo diodes working on the time division [J]. *Chin. Opt. Lett.*, 2008, **6**(5): 320～322

10 He Guangqiang, Zeng Guihua, Zhu Jun. An integrable optic-fiber coherent state quantum identification system [J]. *Chinese J. Lasers*, 2007, **34**(7): 924～929
何广强，曾贵华，朱　俊. 可光纤集成的相干态量子身份认证系统[J]. 中国激光, 2007, **34**(7): 924～929