文章编号：0253-2239(2007)01-0021-5

湍流大气对量子密钥分布系统性能的影响

陈 彦 胡 渝

（电子科技大学 物理电子学院，成都 610054）

摘要： 自由空间量子密钥分布系统是全球性量子保密通信的关键组成部分之一。因此研究湍流大气信道对量子密钥分布系统性能的影响就非常重要。使用光束近场传播和统计分析的方法定量分析了湍流大气信道对基于 BB84 协议的自由空间量子密钥分布系统的误码率的影响。数值计算结果表明，大气衰减系数超过 −3 dB/km 时，大气衰减对量子密钥分布系统的误码率影响很大；在大气传输因子小于 0.5 的区域，系统误码率比无湍流影响时的系统误码率高出一个数量级。

关键词： 光通信；无线通信；误码率；光束近场传播；量子密钥分布

中图分类号：TN929.11；O431.2　　文献标识码：A

Effect of Turbulent Atmosphere on Quantum Key Distribution Systems

Chen Yan　Hu Yu

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

Abstract: Free-space quantum key distribution (QKD) system is one of the key parts of global quantum secure communications. So it is important to analyze the effect of turbulent atmosphere channel on quantum key distribution systems. The effect of turbulent atmosphere channel on quantum bit error rate (QBER) of a free-space QKD system based on BB84 protocol is described quantatively by near-field beam propagation theory and statistical method. The results indicate that, when the atmospheric attenuation coefficient is below −3 dB/km, it has a severe influence on the QBER of a free-space QKD system; and that in the area where atmospheric propagation factor coefficient is less than 0.5, QBER of system is ten times of that of the system operating without turbulence.

Key words: optical communication; wireless communication; bit error rate; near-field optical transmission; quantum key distribution

1 引　　言

1970 年 Wiesner 提出用共轭编码制造不可伪造的“电子钞票”，1984 年 Bennett 和 Brassard 提出了量子密码术方案 BB84[1]，而目前量子密钥分布(Quantum key distribution，QKD)的实验已经在光纤中和自由空间(即大气信道)中取得了巨大的成功。在不久的将来量子密码术将很快达到商用水平。前不久，中国科技大学的彭承志等[2]成功地在等效于星-地大气信道的近地面 13 km 大气信道中，进行了基于纠缠光子对的量子密钥分布实验。他们的工作在实验上证明了将量子通信应用于星-地通信链路，从而实现全球性量子保密通信的可行性。自由空间量子密钥分布系统是全球性量子保密通信的关键组成部分之一，但系统将不可避免地受到湍流大气的影响。因此为了进一步实现全球性的量子保密通信，研究湍流大气信道对量子密钥分布系统性能的影响就非常重要。本文将对湍流大气信道对基于 BB84 协议的自由空间量子密钥分布系统的误码率(QBER)的影响作出定量分析。

2 自由空间量子密钥分布系统工作模式

与大部分的自由空间光通信系统(即大气激光通信系统)不同，自由空间量子密钥分布系统工作于光学近场模式。这种工作模式下，收发天线的功率

作者简介：陈　彦(1978−)，男，四川成都人，博士研究生，主要从事无线光通信技术、量子密码术的研究。E-mail：blastchen@163.com

导师简介：胡　渝(1939−)，女，重庆人，教授，博士生导师，主要从事空间光通信技术和无线光通信技术方面的研究。E-mail：huyu3919@yahoo.com.cn

收稿日期：2006-03-30；收到修改稿日期：2006-05-22

耦合系数高；而普通的自由空间光通信系统通常工作于光学远场模式下，以便降低对光束跟瞄的要求。

激光传输的远场条件为[3]

$$|L| \gg \frac{k}{2}\max\{x^2+y^2\}, \tag{1}$$

式中 L 为传输距离，$k=2\pi/\lambda$ 为波数，λ 为波长，x、y 分别为接收平面上的点的位置坐标。对采用圆形接收天线（设天线半径为 d）的自由空间量子密钥分布系统，上式可写为菲涅耳数 N 的形式：

$$N=d^2/(\lambda L)\ll 1, \quad \text{远场} \tag{2}$$

$$N=d^2/(\lambda L)\gg 1, \quad \text{近场} \tag{3}$$

在光学远场模式下，由于衍射导致的光束扩展占主导地位，使得接收平面上的最小光斑尺寸远大于接收天线口径可达到的尺寸。这样只有一小部分光功率被接收端收到。对普通的自由空间光通信来说，接收机通常是处于发射光场中的一点，进行点探测。在近场模式下，接收平面上的最小光斑尺寸远小于接收天线口径可达到的尺寸，因而所有发射功率均被耦合到接收机当中，属于全光斑接收。由于量子密钥分布使用一个个光子来传输信息，因此其信号光功率极低，必然要求进行全光斑接收。

图 1 所示为波长取 0.7 μm，菲涅耳数 N 分别取 5、10、15、20 时，系统的传输距离和接收天线孔径的关系。由图中曲线可知，要将自由空间量子密钥分布系统配置为近场工作模式是不难实现的。

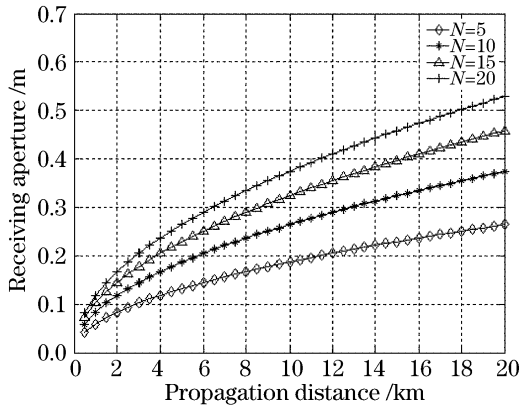

图 1 近场传输模式下自由空间量子密钥分布系统的传输距离和接收天线孔径的关系

Fig. 1 Rlationship between propagation distance field and receiving aperture of free-space quantum key distribution system working under near-field mode

另外，普通自由空间光通信系统与自由空间量子密钥分布系统不同的是，前者的信号光强度远远超过后者，因而前者的信噪比远远高于后者，导致前者的系统误码率（$<10^{-5}$）也远远小于后者的误码率（$10^{-2}\sim10^{-3}$）。

3 BB84 协议

BB84 协议使用理想单光子光源，但实际实验中只能以高度衰减的弱脉冲来代替。该协议规定，发送方 Alice 任意选择编码基⊗（±45°）和⊕（0°，90°）中的一个偏振角度，对发送光子进行偏振编码；接收方 Bob 也完全随机地从测量基⊗和⊕中选择一个偏振角度来测量由 Alice 发送的光子（编码规则如表 1 所示）。在一个量子比特（Qbit）时段内，当 Bob 的单光子探测器探测到光子后，记为“1”，否则记为“0”。

表 1 BB84 协议编码规则表

Table 1 Encoding regulation of BB84 protocol

Base \ Value	1	0
⊕	↑ (90°)	→ (0°)
⊗	↗ (+45°)	↘ (−45°)

只有当 Alice 和 Bob 选择同类偏振基时，Bob 才可能探测到光子；当 Alice 和 Bob 选择不同类型的偏振基时，Bob 以等概率记录“1”和“0”，即此时 Bob 既可能探测到光子，也可能探测不到光子，结果完全随机，不具备确定性。Alice 和 Bob 将此过程进行一段时间之后，将得到一定长度的二进制数据。这些最初的原始数据是未经筛选的二进制数串。此后，Alice 和 Bob 通过公共信道讨论偏振基的选择，对原始数据进行筛选。他们只保留那些偏振基选择一致的时候得到的数据，而丢弃所有偏振基选择不一致时的数据。再经过一系列的纠错和保密加强措施，Alice 和 Bob 就可以共享一个"一次一密"的密钥。整个过程用量子手段辅助，最终产生的是经典密钥。

4 湍流大气信道对自由空间量子密钥分布系统误码率影响的分析

4.1 理论分析

系统对密钥数据的筛选率 p(sift)和系统误码率 p(error)是衡量一个量子密钥分布系统性能的主要参量。对 BB84 量子密钥分布系统，Alice 和 Bob 选择一致的测量基进行编码和测量的过程，称为筛选事件(sift vent)；当 Alice 和 Bob 选择一致的测量基，而同时 Bob 得到错误输出的事件，称为错误事件(error event)。对使用任何协议的量子密钥分布系统，error 事件均包含于 sift 事件中，因此量子密钥分布系统误码率(QBER)均可表示为

$$\frac{N_{\text{error event}}}{N_{\text{sift event}}}=\frac{p(\text{error})}{p(\text{sift})}, \tag{4}$$

因此，只要分别找出湍流大气对 $p(\text{error})$ 和 $p(\text{sift})$ 的影响，即可找出其对系统误码率的影响。假设将大气湍流传输效应带来的影响记为湍流大气传输因子 γ（一个处于区间[0,1]的随机变量）。在湍流大气信道影响下，自由空间量子密钥分布系统的密钥筛选率和误码率可表示为以下条件概率的积分：

$$p(\text{sift}) = \int_0^1 p(\text{sift}|\gamma)p(\gamma)\mathrm{d}\gamma, \tag{5}$$

$$p(\text{error}) = \int_0^1 p(\text{error}|\gamma)p(\gamma)\mathrm{d}\gamma, \tag{6}$$

其中，湍流大气传输因子定义为[4]

$$\gamma \equiv \int_0^1 \left(\frac{8\sqrt{N}}{\pi}\right)\exp\left[\frac{D(\rho)}{2}\right]\times (\arccos x - x\sqrt{1-x^2})\mathrm{J}_1(4x\sqrt{N})\mathrm{d}x, \tag{7}$$

$D(\rho) = 1.09K^2c_n^2L\rho^{5/3}$ 为球面波的结构函数，J_1 为一阶贝塞尔函数，N 为菲涅耳数。

考虑这样一个 BB84 量子密钥分布系统：光电探测器的暗电流计数为 n_D，背景噪声引起的光子计数为 n_B，总的噪声计数为 $n_\mathrm{N}=n_\mathrm{B}/2+n_\mathrm{D}$，Alice 发送的光子数为 n_s，由大气吸收、散射和湍流传输效应综合引起的湍流大气传输因子为 γ，光电探测器的量子效率为 η，光子态 $x,y\in\{\rightarrow,\uparrow;\nearrow,\searrow\}$。

则 Alice 发送 x 态，Bob 收到 y 态，可分为以下几种具体情况讨论：

1) Alice 发送 x 态，Bob 收到 y 态，且 $x=y$（隐含 x 与 y 属于同一个基 $\begin{pmatrix}x,y\in\otimes\\ x,y\in\oplus\end{pmatrix}$。

由表 2 可知，此时 Bob 探测到 y 态光子的概率为 $\frac{1}{2}\times1=\frac{1}{2}$。此时 Bob 的探测器可以同时对信号和噪声光子进行计数。

表 2　BB84 的数据筛选过程-1

Table 2　Data sift process of BB84 protocol

Base x for Alice	↑	→	↗	↘
Base for Bob	↑	→	↗	↘
Probability of Bob choosing the base	1/2	1/2	1/2	1/2
Probability of Bob receiving base y	1	1	1	1

2) Alice 发送 x 态，Bob 收到 y 态，且 $x\neq y$，x 与 y 属于同一个基 $\begin{pmatrix}x,y\in\otimes\\ x,y\in\oplus\end{pmatrix}$。

由表 3 可知，此时 Bob 探测到 y 态光子的概率为 $\frac{1}{2}\times0=0$。即，此时 Bob 的探测器只能探测到噪声，而没有任何信号输出。

表 3　BB84 的数据筛选过程-2

Table 3　Data sift process of BB84 protocol

Base x for Alice	↑	→	↗	↘
Base for Bob	→	↑	↘	↗
Probability of Bob choosing the base	1/2	1/2	1/2	1/2
Probability of Bob receiving base y	0	0	0	0

3) Alice 发送 x 态，Bob 收到 y 态，且 $x\neq y$，x 与 y 不属于同一个基 $\begin{pmatrix}x\in\otimes,y\in\oplus\\ x\in\oplus,y\in\otimes\end{pmatrix}$。

由表 4 可知，此时 Bob 探测到 y 态光子的概率为 $\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}$。此时 Bob 的探测器可以同时对信号和噪声光子进行计数。

表 4　BB84 的数据筛选过程-3

Table 4　Data sift process of BB84 protocol

Base x for Alice	↑	→	↑	→	↗	↘	↗	↘
Base for Bob	↘	↘	↗	↗	↑	↑	→	→
Probability of Bob choosing the base	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2
Probability of Bob receiving base y	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2

由以上三种情况可知，在湍流大气传输影响因子 γ 的作用下，Bob 探测到光子的平均值为

$$\langle N_y|x,\gamma\rangle=\begin{cases}\eta(n_s\gamma/2+n_N), & x=y\\ \eta n_N, & x\neq y,\text{且 } x,y\in\oplus,\text{或 } x,y\in\otimes\\ \eta(n_s\gamma/4+n_N), & x\neq y,\text{且 } x\in\oplus,y\in\otimes,\text{或 } x\in\otimes,y\in\oplus\end{cases}\tag{8}$$

由(5)式、(6)式可得,对于 BB84 协议,筛选事件数和错误事件数分别为

$$N_{\text{sift event}}=\eta(\gamma n_s/2+2n_N),\tag{9}$$

$$N_{\text{error event}}=\eta n_N,\tag{10}$$

Bob 端的光电探测器的光子计数在统计上服从泊松分布。因而在湍流大气传输因子 γ 的作用下,BB84 自由空间量子密钥分布系统的密钥筛选率和错误事件率为

$$p(\text{sift}|\gamma)=\eta(\gamma n_s/2+2n_N)\exp[-\eta(\gamma n_s+4n_N)],\tag{11}$$

$$p(\text{error}|\gamma)=\eta n_N\exp[-\eta(\gamma n_s+4n_N)],\tag{12}$$

由(5)式~(7)式、(11)式、(12)式可得,BB84 协议自由空间量子密钥分布系统的密钥筛选率和错误事件率为

$$p(\text{sift})=2\eta n_N\exp(-4\eta n_N)(1-\gamma)+\frac{1}{2}\gamma\eta[n_s\exp(-\alpha L)+4n_N]\exp\{-\eta[n_s\exp(-\alpha L)+4n_N]\},\tag{13}$$

$$p(\text{error})=\eta n_N\exp(-4\eta n_N)(1-\gamma)+\gamma\eta n_N\exp\{-\eta[n_s(\exp(-\alpha L)+4n_N]\},\tag{14}$$

其中 α 为大气衰减系数,是大气散射和大气吸收的总和。对水平传输的自由空间量子密钥分布系统将 α 考虑为依赖能见度的常量。将式(13)式、(14)式代入(4)式就可计算出湍流大气信道影响下的自由空间量子密钥分布系统误码率。

4.2 数值分析和讨论

本节将根据(4)式和(13)式、(14)式的表达式来计算湍流信道对自由空间量子密钥分布系统误码率的影响。所有计算的基本条件为,传输波长 $\lambda=0.7\ \mu$m,传输距离 $L=2$ km,$n_s=1$,探测器量子效率 $\eta=0.85$(普通 Si-APD 在 0.7 μm 波段的量子效率),探测器暗计数 $n_D=10^{-6}$(Si-APD 在 1 ns 时间间隔内的常规水平),背景噪声 $n_B=10^{-3}$。

1) 大气衰减对系统误码率的影响。

图 2 为大气衰减系数 α 分别取 −2 dB/km、−3 dB/km、−6 dB/km 和 −9 dB/km,对应能见度 $V=7.8$ km、5.15 km、2.61 km、1.74 km,自由空间量子密钥分布系统误码率的变化曲线。

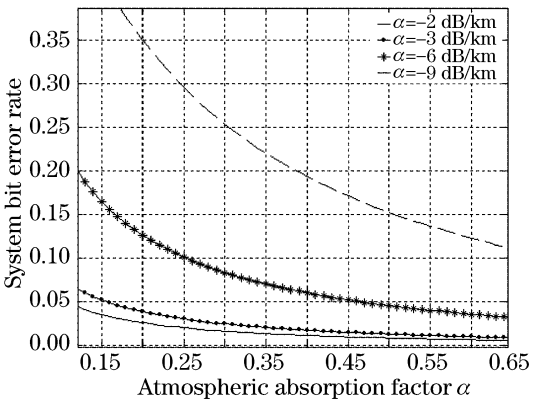

图 2 大气衰减对系统误码率的影响

Fig. 2 Effect of atmospheric absorption on system bit error rate

图 2 说明,大气衰减系数 α 越大(能见度越低)时,自由空间量子密钥分布误码率越大。当湍流大气传输因子 γ 超过 0.3 的情况下(这也是符合大多数实际条件的情况),大气衰减系数 $\alpha=-6$ dB/km(对应能见度低于 2.6 km)时的系统误码率就比 $\alpha=-3$ dB/km(对应能见度低于 5.15 km)时的系统误码率高一个数量级。因此大气衰减系数对自由空间量子密钥分布误码率的影响较大。

2) 湍流大气对系统误码率的影响。

图 3 所示为大气衰减系数 α 取 −2 dB/km 时,大气湍流对自由空间量子密钥分布系统误码率的变化曲线。图 3 中曲线显示,在湍流传输因子小 γ 于 0.5 的区域内,湍流对量子密钥分布系统误码率的影响十分显著;而在湍流传输因子 γ 超过 0.5 的区域内,湍流对量子密钥分布系统误码率造成的影响急剧减小,并趋于平缓。通过进一步计算,分别得出

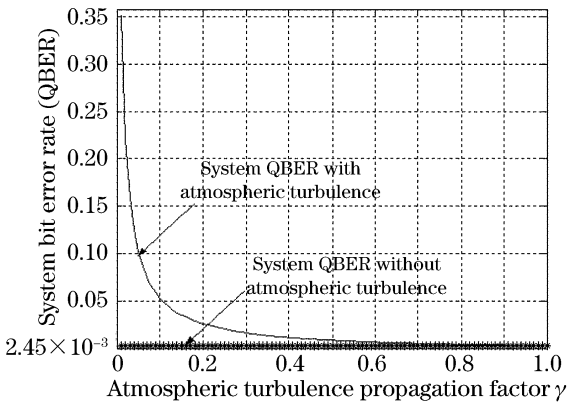

图 3 大气湍流对量子密钥分布系统误码率的影响

Fig. 3 Effect of atmospheric turbulence on system bit error rate

湍流传输因子 γ 大于和小于 0.5 的情况下，系统误码率受到的影响，如图 4(a)、图 4(b)所示。

由图 4(b)中曲线可知，在大气湍流较强时，自由空间量子密钥分布系统的误码率大大增加，比无湍流情况下的系统误码率增加了一个数量级；而图 4(a)说明，在大气湍流较弱时，自由空间量子密钥分布系统的误码率也比无湍流情况下的系统误码率有所增加，但上升幅度不如强湍流情况下明显，基本处于同一数量级。

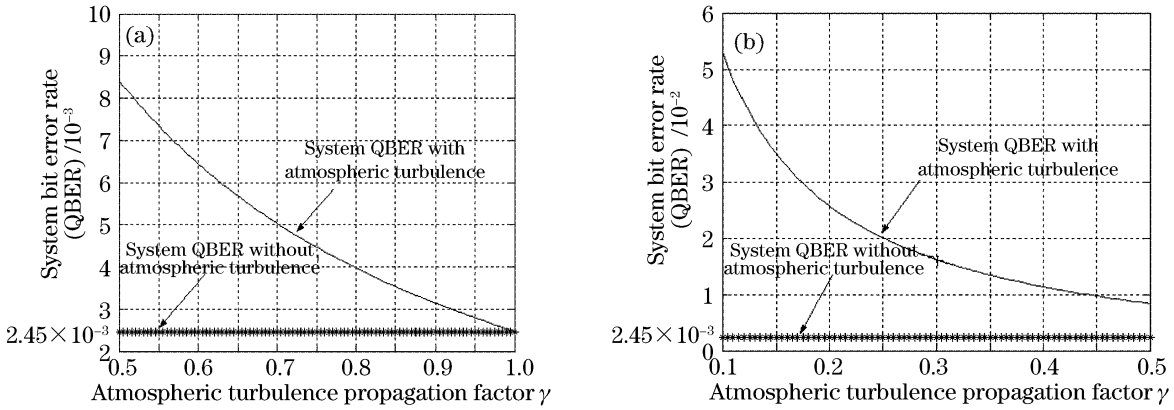

图 4　大气湍流对自由空间量子密钥分布系统误码率系统误码率的影响。(a) 湍流传输因子较大时，(b) 湍流传输因子较小时

Fig. 4　Effect of atmospheric turbulence on free-space quantum key distribution system bit error rate. (a) With relatively big turbulence propagation factor, (b) with relatively small turbulence propagation factor

5　结　　论

从第一个量子密码术方案 BB84 的提出，到现在人们已经从实验上证实了全球性量子保密通信的可行性，量子通信和量子密码术已经取得了巨大的进展。本文依据光束近场传输理论，分别针对大气衰减和湍流两个因素，定量分析了它们对基于 BB84 协议的自由空间量子密钥分布系统误码率的影响。计算结果表明，大气衰减系数超过 −3 dB/km时，大气衰减对量子密钥分布系统的误码率影响很大；在大气传输因子小于 0.5 的区域(湍流较强的区域)，系统误码率比无湍流影响时的系统误码率高出一个数量级。本文的分析为全球性的量子保密通信的进一步工程化实现提供了理论基础。

参　考　文　献

1 C. H. Bennett , G. Brassard. Quantum cryptography: public key distribution and coin tossing[C]. *Proc. IEEE Internet Conf. on Computer, Systems and Signal Processing*, 1984, Bangalore, New York: 175

2 Chengzhi 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

3 Wang Shifan, Zhu Ziqiang. *Principles of Modern Optics* [M]. Chengdu: Publishing House of University of Electronic Science and Technology of China, 1998. 1～392 (in Chinese)
王仕蕃，朱自强. 现代光学原理[M]. 成都：电子科技大学出版社，1998. 1～392

4 M. Gabay, S. Arnon. The effect of turbulence on a quantum-key distribution scheme based on transformation from the polarization to the time domain: laboratory experiment[C]. *Proc. SPIE*, 2004, **5551**: 197～205