光纤信道压力作用下量子密钥分发误码率建模与仿真*

裴昌幸，韩宝彬，赵楠，刘丹，阎毅

（西安电子科技大学 综合业务网与关键技术国家重点实验室，西安 710071）

摘　要：采用半正定算子测量建立了光纤信道压力作用下的误码率分析模型. 以熊猫型保偏光纤为例，用所建模型进行了数值分析. 结果表明：相同作用角下，接收端误码随外界压力的增加呈上升趋势；相同压力下，除 0 和 $\pi/2$ 外，接收端误码随着作用角度的增加而增加. 在归一化力参量小于 0.4 或作用角小于 $\pi/12$ 时，误码率小于 5%.

关键词：光纤信道；误码率；半正定算子测量；量子密钥分发

中图分类号：TN913.3　　**文献标识码**：A　　**文章编号**：1004-4213(2009)02-422-3

0 引言

自 1984 年量子密钥分发协议提出和 1992 年量子密钥分发演示实验成功后[1-2]，由于其具有无条件安全的优点[3]，国内外都在积极地开展理论和实验研究[4-5]. 瑞士于 1996 年在日内瓦湖底铺设的 23 km民用光通信线缆中进行商用密钥传输试验；2004 年 6 月 3 日，美国国防高级研究计划局资助开发的第一个量子密码通信网络在马萨诸塞州剑桥城正式投入运行. 自 1995 年我国进行第一个 BB84 实验后，量子密钥研究取得了飞速进展. 2000 年在单模光纤中完成了 1.1 km 的量子密码演示性实验；2007 年初，中科大郭光灿教授利用民用光纤网络在北京建立了国内第一个四节点的量子密钥分发网络[6].

误码率偏高是制约量子密钥分发进一步发展的障碍. 目前，量子密钥分发误码率约在 3.4～6%，而国内外研究的热点多集中于单光子脉冲技术[7]、单光子探测技术以及提高实际光纤量子密钥分发系统的安全性等方面[8-12]. 目前密钥分发多采用光纤信道，而光纤信道和外界环境的交互作用会隐含测量量子态，导致在接收端产生大量误码.

本文采用半正定算子测量方法（Positive Operator-Valued Measure，POVM）建立了光纤在压力作用下的误码率分析模型，并以 BB84 为例，用典型的熊猫保偏光纤（Panda）进行数值分析. 结果表明外界压力和作用方向都会在接收端引起误码.

*国家自然科学基金（60572147）、国家重点实验室专项资金（ISN02080002）和陕西省科技攻关计划（2006K04-G33）资助

Tel：029-88204486　　Email：chxpei@xidian.edu.cn

收稿日期：2007-11-07

1 POVM 测量误判概率模型

1.1 BB84 和 POVM 测量

如图 1，BB84 协议主要由两个步骤组成：首先 Alice 随机选择单光子的四种不同极化方式向 Bob 发送单光子序列，接收端的 Bob 随机地选择两组不同的测量基（×、+）对单光子进行接收. 然后 Bob 将他随机选择的测量基通过公共信道告诉 Alice. Alice 将 Bob 的测量基序列与自己所发出的光子序列进行比较，确定 Bob 在哪些位上用的是正确的测量基，然后通过公共信道将该信息告诉 Bob. 这样 Alice 和 Bob 同时保留了那些 Bob 使用正确测量基的位，作为他们下一步协商的原始密钥. 经证明，这种密钥分发方式是无条件安全的.

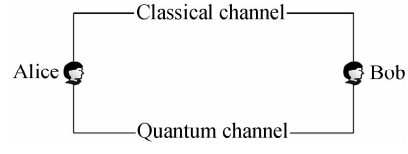

图 1　BB84 模型

Fig. 1　BB84 model

在采用 POVM 测量时，“+”基由两个测量算子 $M_0=|0\rangle\langle 0|$ 和 $M_1=|1\rangle\langle 1|$ 定义，假设被测状态 $|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$，则测得为 0 的概率

$$p(0)=\langle\Psi|M_0^H M_0|\Psi\rangle=|\alpha|^2 \tag{1}$$

“×”基由测量算子 $M_+=|+\rangle\langle +|$ 和 $M_-=|-\rangle\langle -|$ 定义，其中

$$|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2},\ |-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}.$$

此时，测得 0 的概率

$$p(0)=\langle\Psi|M_+^H M_+|\Psi\rangle=\frac{|\alpha+\beta|^2}{2} \tag{2}$$

1.2 光纤横向压力作用下 BB84 误码分析

设保偏光纤半径为 r，单位长度内受力为 f(N/

mm)，通过保偏光纤快慢轴建立(x，y)坐标系，x 轴为慢轴，y 轴为快轴，作用力和快轴夹角为 α. 横向压力的作用长度为 l，光线垂直于(x，y)平面沿 z 方向传播，压力引起的极化角改变量 θ，有

$$\tan 2\theta = F\sin 2\alpha/(1+F\cos 2\alpha) \tag{3}$$

式中，F 为归一化力参量

$$F=\frac{5.4614L_{b0}}{r\lambda}f \tag{4}$$

假设 Alice 发送量子态 $|\varphi\rangle$，其向量形式为 $\begin{pmatrix}|\cos(\alpha)\rangle\\|\sin(\alpha)\rangle\end{pmatrix}$，有

$$|\varphi\rangle\rightarrow\begin{pmatrix}|\cos(\alpha)\rangle\\|\sin(\alpha)\rangle\end{pmatrix}=R_z(\alpha)\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix} \tag{5}$$

式中 $R_z(\alpha)=\begin{pmatrix}\cos\alpha & \sin\alpha\\-\sin\alpha & \cos\alpha\end{pmatrix}$，$\alpha$ 为光子偏振方向.

由于外界压力和光纤的相互作用，导致光纤传输的量子态被隐含地测量，从而引起相位振动. 从前面分析可知，相位振动角即为 θ，设传输后量子态为 $|\varphi'\rangle$，则该振动过程的向量表示为

$$|\varphi'\rangle=R_z(\theta)|\varphi\rangle=R_z(\alpha+\theta)\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix} \tag{6}$$

式中，$R_z(\theta)=\begin{pmatrix}\cos\theta & \sin\theta\\-\sin\theta & \cos\theta\end{pmatrix}$，$R_z(\alpha+\theta)=\begin{pmatrix}\cos(\alpha+\theta) & \sin(\alpha+\theta)\\-\sin(\alpha+\theta) & \cos(\alpha+\theta)\end{pmatrix}$.

利用式(1)，可以得出量子态 $|\varphi\rangle$ 经光纤传输后用“+”基测量为 0 的概率和归一化力参量间的关系式为

$$p(0)=\cos^2(\alpha+\theta) \tag{7}$$

式中，$\theta=\frac{1}{2}\tan^{-1}[F\sin 2\alpha/(1+F\cos 2\alpha)]$.

2　实际光纤模型误码率仿真

为了能更好地反映密钥分发的实际情况，假设传输光纤为 PM1310G-125 型熊猫光纤，其工作波长为 1 310 nm，拍长为 2.6 mm，光纤外径为 125 μm，发送量子态为 $|0\rangle$. 由于在外径、拍长和波长确定的情况下，归一化力参量和力的大小成正比. 为了分析方便，仿真参量使用归一化力参量 F，力的作用角分别取 0、15°、30°和 45°；同时考虑到 Alice 和 Bob 仅保留测量基一致的量子比特，故采用式(7)得出图 2 曲线.

从图 2 可以看出，随着作用力的增大，误判的可能性也越来越大. 另外，误判概率受作用角的影响也非常明显，图 2 中显示随着作用角的增大，相同的作用力对判决的误码影响越来越大. 但在大于 pi/4 后，小作用力情况下，作用角对量子比特影响不大.

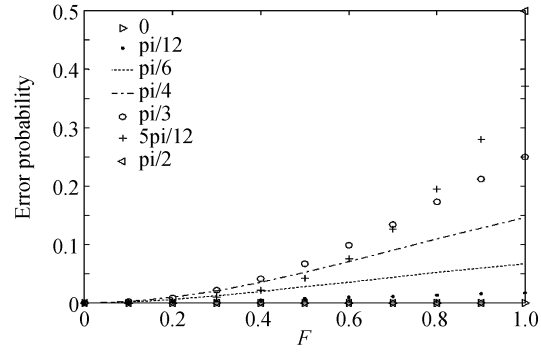

图 2　误判概率

Fig. 2　Error probability

3　结论

本文以 BB84 为例对压力环境中量子密钥分发系统的误码率进行了分析. 首先建立了压力作用下 POVM 测量的误码率模型，并用熊猫型保偏光纤为例进行数值分析，结果表明外界压力的方向和大小变化都会引起接收端的误码率的改变. 研究结果对指导密钥分发在军事和商用保密通信中的应用具有重要的意义.

参考文献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, 1984: 175-179.

[2] BENNETT C H. Quantum cryptography: uncertainty in the service of privacy[J]. *Science*, 1992, **257**(7): 752-753.

[3] MAYERS D. Unconditional security in quantum cryptography [J]. *Journal of the ACM*, 2001, **48**(3): 351-406.

[4] CHENG Zhi-xin, TANG Zhi-lie, WEI Zheng-jun, *et al*. On the Breidbart eavesdropping information problem of BB84 QKD protocol[J]. *Acta Photonica Sinica*, 2004, **33**(12): 1469-1472.
陈志新，唐志列，魏正军，等. QKD 系统在 Breidbart 基窃听下 BB84 协议的信息量研究[J]. 光子学报，2004，**33**(12)：1469-1472.

[5] SU Xiao-qin, GUO Guang-can. Two typical quantum communication technology[J]. *Journal of Guangxi University (Natural Science Edition)*, 2005, **30**(1): 30-39.
苏晓琴，郭光灿. 两种典型的量子通信技术[J]. 广西大学学报(自然科学版)，2005，**30**(1)：30-39.

[6] 方芳. 我国量子密码通信网测试成功可检测窃听行为[EB/OL]. (2007-04-03)[2007-06-27]. http://tech.sina.com.cn/t/2007-04-03/08381445628.shtml.

[7] LIU Jing-feng, LIANG Rui-sheng, LIU Song-hao, *et al*. Precise controlled optical attenuator for quantum security communication[J]. *Acta Photonica Sinica*, 2004, **33**(7): 867-870.
刘景锋，梁瑞生，刘颂豪，等. 量子保密通信用的光精密控制强衰减技术[J]. 光子学报，2004，**33**(7)：867-870.

[8] LO H K, CHAU H F, ARDEHALI M. Efficient quantum key distribution scheme and a proof of its unconditional security [J]. *Journal of Cryptology*, 2005, **18**(2): 133-165.

[9] WEI Zheng-jun, LIAO Chang-jun, WANG Jin-dong, *et al*. Randomicity of physical random number generator [J]. *Acta Photonica Sinica*, 2006, **35**(7): 1086-1089.
魏正军, 廖常俊, 王金东, 等. 物理真随机码发生器随机性分析 [J]. 光子学报, 2006, **35**(7): 1086-1089.

[10] WANG Xiang-bin. Beating the PNS attack in practical quantum cryptography [J]. *Phy Rev Lett*, 2005, **94**(23): 503-506.

[11] GOTTESMAN D, PRESKILL J. Secure quantum key distribution using squeezed states [J]. *Phys Rev A*, 2001, **63**(2): 022309.

[12] OU Z Y. Multi-photon interference and temporal distinguishability of photons [DB/OL]. (2007-08-24) [2007-09-01]. http://arxiv.org/abs/0708.0077v1.

QBER Modeling and Simulation of QKD in Optical Fiber with Force

PEI Chang-xing, HAN Bao-bin, ZHAO Nan, LIU Dan, YAN Yi

(*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*)

Received date: 2007-11-12

Abstract: The theoretical model of QBER (Quantum Bit Error Rate) was established with POVM (Positive Operator Valued Measurement). PANDA fiber as an example was simulated based on the model. The research results show that under the same angle, bit error rate (BER) increases with increase of force amplitude; and BER increases with increase of angle, under the same force without the consideration of 0 and $\pi/2$. For normalized force less than 0.4 or the angle less than $\pi/12$, the BER could be lower than 5%.

Key words: Optical fiber channel; BER; POVM; QKD

PEI Chang-xing is a professor at Xidian University. His research interests focus on quantum communication, network measurement and anti-jamming communication.