

光纤信道应力作用对量子密钥分发误码率的影响

吴佳楠^{1,2}, 王世刚¹, 王新诚², 魏荣凯², 刘桂霞³

(1. 吉林大学 通信工程学院, 长春 130022; 2. 长春大学 计算机科学与技术学院, 长春 130022; 3. 吉林大学
计算机科学与技术学院, 长春 130012)

摘要: 基于 BB84 协议原理, 构建了应力环境下偏振编码的点对点实际量子密钥分发(QKD)系统。完成了商用光纤信道应力作用下的量子密钥分发实验, 对系统主要参数实时采集并进行数据分析。结果表明: 随着光纤信道上外界作用力的增加, QKD 系统诱骗态和信号态误码率均随之增大, 成码率降低; QKD 系统所能承受的拉力极值小于压力极值, 系统对于拉力变化更为敏感。本研究结果对指导密钥分发在军事和商用保密通信中的实际应用具有一定的参考价值。

关键词: 通信技术; 量子密钥分发; BB84 协议; 诱骗态; 信号态; 误码率

中图分类号: TN918 **文献标志码:** A **文章编号:** 1671-5497(2017)05-1612-05

DOI: 10.13229/j.cnki.jdxbgxb201705038

Influence of fiber channel stress on quantum key distribution bit error rate

WU Jia-nan^{1,2}, WANG Shi-gang¹, WANG Xin-cheng², WEI Rong-kai², LIU Gui-xia³

(1. College of Communication Engineering, Jilin University, Changchun 130022, China; 2. College of Computer Science and Technology, Changchun University, Changchun 130022, China; 3. College of Computer Science and Technology, Jilin University, Changchun 130012, China)

Abstract: An actual point to point Quantum Key Distribution (QKD) experimental system of polarization encoding was built based on BB84 protocol under stress testing conditions. QKD experiment under commercial fiber channel stress was carried out. The main parameters of the system were collected in real time for data analysis. The results show that, with the increase in the external forces on the fiber channel, both the decoy state error rate and the signal state error rate of the QKD system increase, but the bit generation rate decreases. The tensile limit value of the QKD system is less than the limit value of the pressure, the system is more sensitive to tension change. Results of this study may provide guidance for the application of key distribution in military and commercial secret communication.

Key words: communication technology; quantum key distribution; BB84 protocol; decoy state; signal state; bit error rate

收稿日期: 2016-07-24.

基金项目: 国家自然科学基金重点项目(61631009); 国家自然科学基金项目(61373051); 教育部春晖计划项目
(Z2015024); 吉林省科技发展项目(20150204006, 20160101259JC, 20170204023GX).

作者简介: 吴佳楠(1980-), 男, 讲师, 博士。研究方向: 计算智能和量子通信。E-mail:jiananwu@126.com

通信作者: 刘桂霞(1963-), 女, 教授, 博士生导师。研究方向: 计算智能和生物信息学。E-mail:liugx@jlu.edu.cn

0 引言

量子保密通信是一种基于物理学原理具有无条件安全特性^[1]的密码通信方法。量子密钥分发^[2](Quantum key distribution, QKD)利用海森堡不确定原理和量子不可克隆原理,窃听者即使截获了量子态,也无法精确地获得量子态的状态信息。目前,国内外专家学者逐渐从理论分析^[3-5]转向面向实际通信问题的研究^[6-12]。2009年至2010年,中国科学技术大学先后建立了3节点和5节点的QKD网络^[13,14];2016年,“墨子号”量子通讯卫星在酒泉发射成功,标志着量子保密通信技术已向实用化和商用化方向迈进。

量子保密通信的关键在于量子密钥的生成,因此,低误码率和稳定的QKD系统是量子保密通信应用的关键。在实际光纤量子通信中,由于单光子探测器的暗计数和光纤传输线路上环境振动、温度、应力等随机因素的影响,会导致接收端产生不同程度的误码,进而影响密钥的最终生成^[15]。本文结合BB84协议原理,构建了基于商用光纤的偏振编码点对点实际QKD系统及应力测试数据采集分析系统,研究并讨论了光纤信道在外界应力作用下对实际QKD系统中量子误码率的影响,研究结果对量子保密通信网络的实际敷设与运维具有重要的指导作用。

1 理论与计算公式

1.1 BB84 协议原理

BB84协议是第一个量子密钥分配协议^[2]。协议包含4个偏振态和两组正交基。主要工作流程如下:发送方Alice制备并发送单光子序列,每个光子随机选取一种偏振态;接收方Bob随机选取+基和×基测量光子偏振态并记录光子位置信息;通过经典信道Bob将测量基发送给Alice,双方进行基矢比对,保留相同的测量基;最后,Alice和Bob将保留的光子偏振态信息转换成相应的密钥比特信息,经过纠错和私密放大得到最终的安全通信密钥。

1.2 计算公式

目前,量子密钥分发系统中并不存在完美的单光子源,因此通信双方实际使用的是衰减后的相干光,以及压缩光等亚泊松分布光源。假设光源相位完全随机, p_n 表示发送脉冲中出现n光子态的概率, μ 表示相干光的平均光子数,光源表达

式为:

$$\rho_A = \sum_{n=0}^{\infty} p_n | n \rangle \langle n | = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} | n \rangle \langle n | \quad (1)$$

采用强衰减方法得到的弱相干脉冲传输过程中易受环境影响,导致信号衰减。实验使用的1550 nm的商用单模光纤衰减系数 α 为0.20 dB/km, l 代表信道长度,信号脉冲在信道中的传输效率可表示为:

$$t_{AB} = 10^{-\alpha l / 10} \quad (2)$$

实际通讯过程中,探测器及其他光学设备中也包含一些固有损耗,以 t_{Bob} 表示探测器的探测效率, η_D 表示在光学设备固有损耗下的传输效率,则单光子在实际QKD系统中的总传输效率 η 可表示为:

$$\eta = t_{AB} t_{Bob} \eta_D \quad (3)$$

由式(3)可得, n 光子脉冲的总传输效率(假设多光子脉冲中的光子均为独立传输)为:

$$\eta_n = 1 - (1 - \eta)^n = 1 - (1 - t_{AB} t_{Bob} \eta_D)^n \quad (4)$$

Bob探测到Alice发出 n 个光子的脉冲概率可表示为:

$$Y_n = Y_0 + \eta_n - Y_0 \eta_n \approx Y_0 + \eta_n \quad (5)$$

光源的总计数率为:

$$Q_\mu = \sum_{n=0}^{\infty} Q_\mu = \sum_{n=0}^{\infty} p_n Y_n \quad (6)$$

结合式(4)(5)可得, n 光子态的量子比特错误率(Quantum bits error rate, QBER)为:

$$e_n = \frac{e_0 Y_0 + e_{det} \eta_n}{Y_n} \quad (7)$$

式中: e_{det} 为单光子错误到达探测器的概率;假设背景噪音完全随机进而引起的错误也完全随机,即 $e_0 = 1/2$ 。

由式(1)(5)(6)(7)可得系统总QBER:

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n p_n \quad (8)$$

式中: Q_μ 为探测效率; E_μ 为总误码率。

用 δ 表示原始密钥误码率, $H_2(\delta)$ 表示纠错泄露的信息量,则在理想单光子光源状态下QKD系统安全成码率可表示为:

$$R = 1 - H_2(\delta) - H_2(\delta_p) \quad (9)$$

但是,实际系统中会存在某些漏洞,GLLP公式给出了常用的弱相干光源BB84协议安全密钥率,可以写成如下的形式^[16]:

$$R \geq q \{-f(E_\mu)\} Q_\mu H_2(E_\mu) + Q_1 [1 - H_2(e_1)] \quad (10)$$

式中: q 为对基效率; $f(E_\mu)$ 为纠错效率。

本文采用的诱骗态方法中包含信号态、诱骗态、真空态 3 种不同平均光子数的脉冲。发射几率分别为 p_μ, p_v, p_0 , Y_k 表示 k 光子在接收端被探测到的几率, 则信号态和诱骗态误码率可分别表示为:

$$E_\mu = \frac{1}{Q_u} \left\{ e_0 p_{0,\mu} Y_0 + e_1 p_{1,\mu} Y_1 + \sum_{k=2}^{\infty} e_k p_{k,\mu} Y_k \right\}$$

$$E_v = \frac{1}{Q_\mu} \left\{ e_0 p_{0,v} Y_0 + e_1 p_{1,v} Y_1 + \sum_{k=2}^{\infty} e_k p_{k,v} Y_k \right\}$$

结合式(10)可以得到诱骗态方法安全码率的下限^[11]。

2 实验结果与分析

2.1 实验方案设计

基于 BB84 协议原理, 本文设计并搭建了 Alice 到 Bob 的点对点量子密钥分发及量子信道应力分析整合实验系统, 系统主要部件和结构如图 1 所示。QKD 系统工作频率为 40 MHz, 信号光脉宽为 200 ps。双方通过量子信道实现密钥分发, 通过经典信道实现基矢比对和数据传输。应力测试装置对量子信道实施外力作用, 应力分析系统采集信道应力变化相关数据和量子密钥分发相关数据信息。在整个应力分析实验中, 本文采用长度为 20 m、内径为 9 μm、外径为 125 μm、波长为 1550 nm 的商用单模光纤作为量子信道, 信道衰减为 0.2 dB。

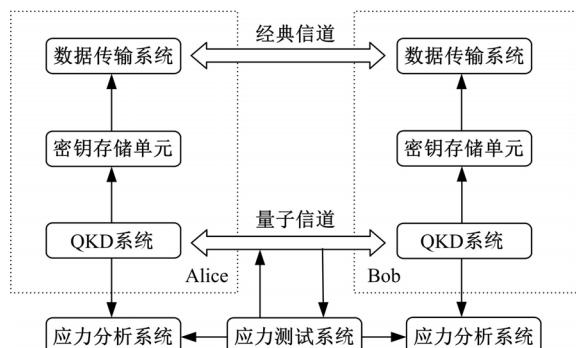


图 1 点对点量子保密通信应力分析系统

Fig. 1 Point to point quantum cryptography stress analysis system

2.2 结果与分析

(1) 压力作用下量子密钥分发误码率及成码率分析

量子信道对外力作用十分敏感, 为了保持系统稳定, 经多次验证, 本文将压力的位移速度设定

为 3.6 mm/s, 垂直下压光纤, 光纤受力长度为 30 cm。压力 F_{pre} 从 0 N 开始, 每次增加 30 N, 约 30 s 作用力稳定后, 采集数据。经计算后得到信号态误码率、诱骗态误码率以及成码率随压力的变化曲线, 如图 2、图 3 所示。从图 2 可以看出, 随着压力的增加, 无论是信号态错误率还是诱骗态错误率都随之增大。这与文献[15]通过 POVM 半正定算子测量方法仿真得出的理论结果相符。另外, 相同压力作用下, 诱骗态的错误率要明显高于信号态错误率。但是, 当压力增加到 300 N 时, 超出信道承载极限, 量子密钥分发系统会进行偏振反馈, 重新建立连接。

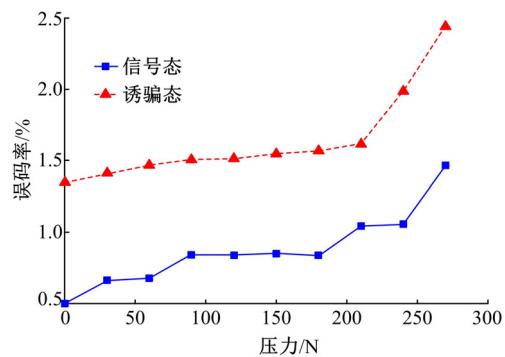


图 2 压力作用下误码率曲线

Fig. 2 Bit error rate curve under pressure

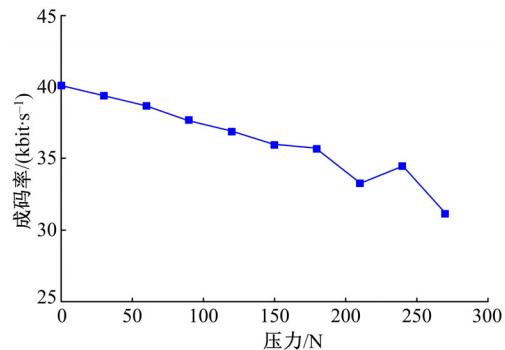


图 3 压力作用下成码率曲线

Fig. 3 Bit generation rate curve under pressure

图 3 中数据点纵坐标为系统 30 s 内成码率均值。可以看出, 随着压力的增大, 系统成码率呈下降趋势。值得注意的是, 当压力小于 180 N 时下降趋势比较稳定, 而当压力大于 210 N 时震荡较为明显, 此阶段诱骗态错误率上升趋势极为明显, 迅速逼近误码率极限。可见, 量子信道在小于 210 N 压力作用下, 量子密钥分发过程是相对稳定的。

(2) 拉力作用下量子密钥分发误码率及成码率分析

将拉力的位移速度设定为2.5 mm/s,沿光纤轴向进行拉伸实验。拉力 F_{ten} 从0 N开始,每次增加10 N,系统稳定后采集数据。信号态误码率、诱骗态误码率以及成码率随拉力的变化曲线如图4、图5所示。从图4可以看出,随着拉力的增加,信号态错误率和诱骗态错误率都相应增大,总体呈现震荡上升趋势。相同拉力作用下,信号态错误率低于诱骗态的错误率。值的注意的是,当拉力大于70 N时,错误率急速上升后又转而下降,呈现不稳定状态,超过90 N时量子密钥分配发生错误。另外,随着拉力的增加,系统成码率呈震荡下降趋势,如图5所示。相对于压力作用,拉力对误码率和成码率的影响更为明显。

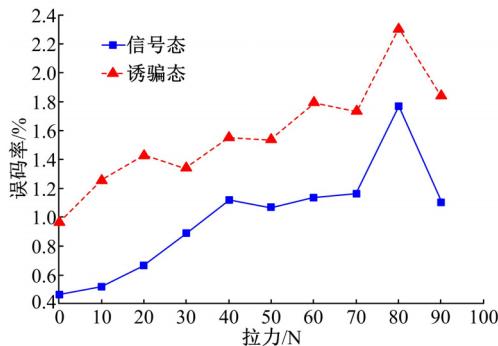


图4 拉力作用下误码率曲线

Fig. 4 Bit error rate curve under tension

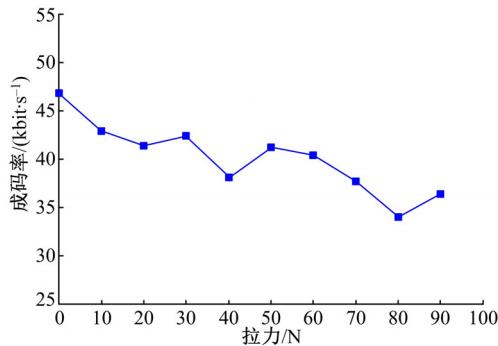


图5 压力作用下成码率曲线

Fig. 5 Bit generation rate curve under tension

另外,本文采集了拉力变化下光纤量子信道的衰减数据,与相同作用力下的信号态误码率、诱骗态误码率进行对比,如表1所示。可以看出,随着衰减的增加,误码率也相应增大。当衰减大于4.85 dB后,QKD系统无法正常生成密钥。

综合以上分析可以推断,应力导致光纤信道衰减发生变化,进而使QKD系统误码率增加,最终影响密钥的生成。

表1 衰减与误码率的关系

Table 1 Relationship of attenuation and bit error rate

	拉力/N								
	10	20	30	40	50	60	70	80	90
信道衰减/dB	0.22	0.33	0.57	0.82	1.69	2.17	3.71	4.25	4.85
信号态误码率/%	0.52	0.66	0.88	1.12	1.06	1.13	1.16	1.77	1.10
诱骗态误码率/%	1.25	1.42	1.34	1.55	1.53	1.79	1.73	2.30	1.84

3 结束语

结合BB84协议原理,设计并构建了基于商用光纤的点对点QKD实验系统及量子信道应力作用数据分析系统,完成了压力及拉力作用下的QKD实验。实验结果表明:在基于商用光纤的实际量子密钥分配过程中,随着光纤量子信道上外界作用力的增加,QKD系统的误码率随之增大。另外,QKD系统所能承受的拉力极值要远小于压力极值,系统对于拉力变化更为敏感,而信道衰减是影响成码率的关键因素。本研究结果对指导密钥分发在军事和商用保密通信中的实际应用具有一定的参考价值。

参考文献:

- [1] Mayers D. Unconditional security in quantum cryptography[J]. Journal of the ACM , 2001, 48(3): 351-406.
- [2] Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[C]// Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984: 175-179.
- [3] Bouwmeester D, Pan J W, Mattle K, et al. Experimental quantum teleportation [J]. Nature, 1997, 390: 575-579.
- [4] Hwang W Y. Quantum key distribution with high loss: toward global secure communication[J]. Phys Rev Lett, 2003, 91(5): 057901.
- [5] Duan L M, Lukin M D, Cirac J I, et al. Long-distance quantum communication with atomic ensembles and linear optics[J]. Nature, 2001, 414: 413-418.
- [6] 周小清,邬云文,赵晗.量子隐形传态网络的互联与路由策略[J].物理学报,2011, 60(4): 35-40.
Zhou Xiao-qing, Wu Yun-wen, Zhao Han. Quantum teleportation internetworking and routing strategy[J]. Acta Physica Sinica, 2011 , 60 (4) :35-40.
- [7] 秦晓娟,王金东,魏正军,等.长程光纤传输的时间

- 抖动对相位编码量子密钥分发系统的影响[J]. 物理学报, 2010, 59 (8): 5514-5522.
 Qin Xiao-juan, Wang Jin-dong, Wei Zheng-jun, et al. The influence of the time delay through long trunk fiber on the phase-coding quantum key distribution system[J]. Acta Physica Sinica, 2010, 59 (8): 5514-5522.
- [8] 周南润, 曾宾阳, 王立军, 等. 基于纠缠的选择自动重传量子同步通信协议[J]. 物理学报, 2010, 59 (4): 2193-2199.
 Zhou Nan-run, Zeng Bin-yang, Wang Li-jun, et al. Selective automatic repeat quantum synchronous communication protocol based on quantum entanglement[J]. Acta Physica Sinica, 2010, 59(4):2193-2199.
- [9] Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding[J]. Phys Rev Lett, 2007, 98: 010505.
- [10] 岳孝林, 王金东, 魏正军, 等. 一种新的单光源多波长双向量子密钥分发系统[J]. 物理学报, 2012, 61 (18): 234-240.
 Yue Xiao-lin, Wang Jin-dong, Wei Zheng-jun, et al. A new multi-wavelength two-way quantum key distribution system with a single optical source[J]. Acta Physica Sinica, 2012, 61(18): 234-240.
- [11] 焦荣珍, 唐少杰, 张弨. 诱惑态量子密钥分配系统中统计涨落的研究[J]. 物理学报, 2012, 61 (5): 050302.
 Jiao Rong-zhen, Tang Shao-jie, Zhang Chao. Analysis of statistical fluctuation in decoy state quantum key distribution system[J]. Acta Physica Sinica, 2012,61(5):050302.
- [12] Sasaki M, Fujiwara M, Ishizuka H, et al. Field test of quantum key distribution in the Tokyo QKD network[J]. Opt Express, 2011, 19:10387-10409.
- [13] Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography [J]. Opt Express, 2009, 17: 6540-6549.
- [14] Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network[J]. Opt Express, 2010, 18: 27217-27225.
- [15] 裴昌幸, 韩宝彬, 赵楠, 等. 光纤信道压力作用下量子密钥分发误码率建模与仿真[J]. 光子学报, 2009,38(2):422-424.
 Pei Chang-xing, Han Bao-bin, Zhao Nan, et al. QBER modeling and simulation of QKD in optical fiber with force[J]. Acta Physica Sinica, 2009, 38 (2):422-424.
- [16] Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices[J]. International Symposium on Information Theory,2003,4(5):136.