单光子相位编码量子密钥分发系统中的偏振控制

刘令令 景明勇 于 波 胡建勇 肖连团 贾锁堂

山西大学激光光谱研究所量子光学与光量子器件国家重点实验室, 山西 太原 030006

摘要 在量子密钥分发系统中,由于长距离光纤信道传输引入的偏振漂移将导致密钥分发效率下降。给出了一种基于遗传算法结合数控偏振控制器实现在单光子量级下对单光子偏振的优化控制与长时间锁定的方法。在25 km单模光纤传输每脉冲平均光子数小于0.1的单光子相位编码量子密钥分发系统中,将信号光偏振优化到最佳值,并实现了系统长期稳定运行,密钥分发成码率高于1.5 kbps。

关键词 量子光学; 量子保密通信; 偏振控制; 遗传算法; 单光子

中图分类号 O436 **文献标识码** A

doi: 10.3788/LOP52.072701

Polarization Control in Single Photons Phase Coding Quantum Key Distribution System

Liu Lingling Jing Mingyong Yu Bo Hu Jianyong Xiao Liantuan Jia Suotang

State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Laser Spectroscopy, Shanxi University, Taiyuan, Shanxi 030006, *China*

Abstract In fiber-based quantum key distribution systems, the photons polarization fluctuation can lead to a decrease of the key generation rate. A method for polarization controlling, based on the genetic algorithm and the numerical control polarization controller is introduced. It is shown that the system could be quickly optimized and the polarization of signal beam has been locked in long term at the single-photons level. In our phase-modulated quantum key distribution system, the average photon number is less than 0.1 photon per pulse. After transmitted through 25 km single mode optical fiber, the polarization state of signal beam is realized to optimum value and keep the stable transmission for a long time, and the final key rate is up to 1.5 kpbs.

Key words quantum optics; quantum key distribution; polarization control; genetic algorithm; single photons

OCIS codes 270.5565; 060.1660; 060.2400; 060.4510; 060.5565

1 引 言

近年来,量子密钥分发(QKD)成为国内外研究的热点[1],基于经典密码学与量子力学相结合,其无条件安全性由量子力学的基本原理保证,而无关窃听者的计算能力。起初的基于BB84及B92协议的QKD系统都是通过偏振编码[2]实现的,与单光子偏振特性相比,单光子相位受光纤双折射影响较小,而且相位调制边带干涉更易于进行多路复用传输,因此基于相位编码[3]的密钥分发方式得到人们的重视与应用。然而由于光纤自身缺陷、光纤受到的随机外力以及光纤周围温度变化等因素会引起光纤局部折射率发生变化,引发双折射效应,单光子在长距离单模光纤传输过程中会引起光偏振态的随机变化[4,5],影响系统的稳定性及密钥分发的成码率。因此,在光纤传输中单光子偏振态的准确、快速的调节及锁定研究受到了人们的高度重视[6-8]。

控制偏振漂移通常采用的方法是双向往返光路偏振自补偿法[9],在光路中加入法拉第镜,利用与输入光偏振态正交的反射光抵消光纤中的偏振漂移。这种方法操作简单、成本低,但严重限制了传输距离及效

收稿日期: 2015-01-23; **收到修改稿日期**: 2015-03-01; **网络出版日期**: 2015-05-13

基金项目: 国家973计划(2012CB921603)、国家863计划(2011AA010801)、国家自然科学基金(11374196,11174187,10934004,11204166)、教育部创新团队发展计划(IRT13076)、高等学校博士学科点专项科研基金(20121401120016)

作者简介: 刘令令(1991—),女,硕士研究生,主要从事量子密钥分发方面的研究。E-mail: liulinglingsxdx@163.com

导师简介: 肖连团(1966—),男,教授,博士生导师,主要从事量子光学与激光光谱方面的研究。

E-mail: xlt@sxu.edu.cn(通信联系人)

率。2007年Chen等[10]提出中断式偏振补偿法，当发现码率降低时中断通信补偿调整偏振，然后继续进行密钥传输。这种方法解决了传输距离受限的问题，但其中断时间对通信系统正常工作造成严重干扰。2008年Xavier等[11]提出利用波分复用技术同时传输信号光和参考光，利用参考光对偏振进行实时控制，但是由波长不同引起的偏振漂移的差异限制了调制系统的精确性。

最近人们提出利用与信号光偏振态正交的参考光作为反馈，通过优化算法调节偏振控制器来达到偏振补偿目的。这种方法既没有传输距离的限制，又降低了光强损耗。常用的优化算法有梯度算法[12]、模拟退火算法[13]和遗传算法[14]等。其中遗传算法能够有效地进行概率意义的全局搜索，寻优过程有较大的灵活性，可以避免陷入局部最优值，能够保证算法的长期有效性。然而已有的优化算法控制偏振都是在连续强光上进行的。基于单光子相位编码量子密钥分发系统的特点，本文提出利用遗传算法结合数控偏振控制器的方法实现了在单光子量级下对任意偏振态的输入光进行实时精确控制，使输出光的偏振态锁定在编码所需的最优值。

2 实验装置

基于单光子相位编码量子密钥分发系统实现偏振控制的实验装置如图1所示(FOI：光纤隔离器，FOA：光纤衰减器，AM：强度调制器，PM：相位调制器，PC：偏振控制器，PBS：偏振分束器，OF：光学滤波器，SPD：单光子探测器，MCU：单片机)。激光器发出的波长为1550 nm的连续光经过隔离器和衰减器后，由强度调制器(AM)斩成单光子量级的脉冲光，经过相位调制器(PM_1)调制后携带Alice端编码的相位信息进入25 km光纤。传输到Bob端后首先经过偏振控制器，随后被一偏振分束器分成偏振方向相互垂直的两路脉冲光(I_x、I_y)。其中一路作为信号光(I_y)，由相位调制器(PM_2)调制后完成密钥分发，另一路作为参考光(I_x)提供偏振控制所需的反馈信号。要获得最佳的偏振态，需要在Bob端调节偏振控制器使得用于编码的信号光最强，相应地与其偏振方向垂直的参考光功率最小，通过减小由偏振漂移引起的光子数损耗，稳定用于编码的单光子光强。

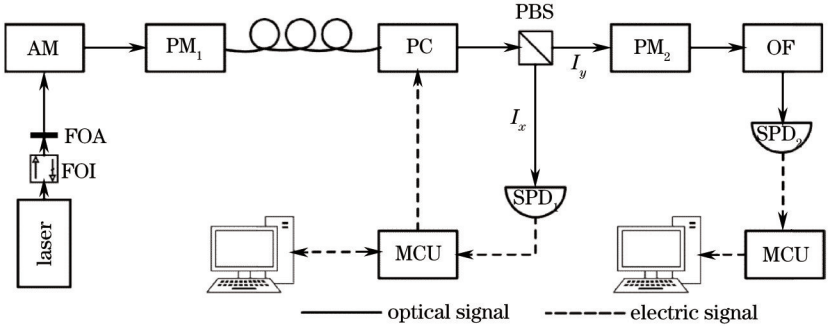

图1 单光子相位编码量子密钥分发系统中偏振控制的实验装置图

Fig.1 Schematic diagram of polarization control in phase-encoding quantum key distribution system

采用General Photonics公司生产的PCD-M02偏振控制模块，此模块与一全光纤动态偏振控制器结合，输入端由4路0~5 V模拟电压信号或12 BitTTL数字信号控制，输出4通道0~140 V直流信号作为偏振控制器的调制电压，分别控制其内部的4个光纤挤压装置，这4个光纤挤压装置相继有45°偏差用来调节光的偏振态。此数控偏振控制器能够由单片机输出的数字信号控制，实时调整任意输入偏振态，不需要复位操作。其偏振调节速度可达15 kHz，确保偏振控制器可以快速的控制偏振态，及时补偿外部应力、温度等造成的影响。

在参考端单片机(MCU)使用外部中断同步采集单光子探测器(SPD_1)计数，通过与上位机通信，将计数变化传递给计算机，这时计算机调用Matlab程序执行遗传算法，分别计算出偏振控制器4个通道的延迟量及控制电压值，再通过单片机，将这4路电压反馈回偏振控制器进而实现对光脉冲偏振态的调节。如此循环多次，最终使参考端消光，以达到信号光功率稳定在最强的目的。

3 遗传算法

遗传算法是人工智能领域中的一种启发式寻优算法，它借鉴生物进化论中的遗传现象，把问题求解演化成生物种群中染色体逐代更新的过程，基于自然选择、适者生存的原则，逐渐得到最适应环境的个体，达到寻求全局最优解的目的[15]。遗传算法中有三个基本操作：选择、交叉、突变，分别与生物遗传中繁殖、杂交、

变异相对应[16]。在实际偏振控制过程中,遗传算法的程序由Matlab语言编写,具体过程如图2所示。

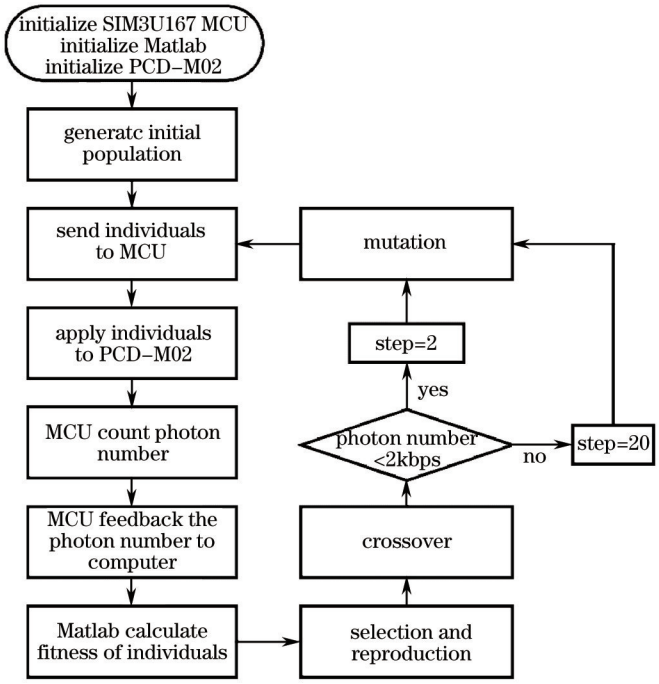

图2 遗传算法偏振控制流程图

Fig.2 Flowchart of genetic algorithm for polarization controlling

1) 由遗传算法产生第一代均匀分布的10个个体,每个个体由4个0~4095的整数组成,分别对应偏振控制器的4路调节电压。将这10个个体通过串口发送给单片机,根据对应电压值控制偏振控制器PCD-M02,依次对光束偏振态进行调制;

2) 单片机采集10次偏振调制后SPD_1的单光子计数,并将此计数反馈给计算机遗传算法;

3) 遗传算法根据单光子计数对这10个个体进行评分(评分规则:10次偏振调制之后,根据单光子计数从小到大将这10个个体排序,序号为r(1~10),每个个体的评分为$1/\sqrt{r}$,即光子数越小评分越高。此规则的优点是经过排序处理可以防止随着代数的增加分数分布的扩散);

4) 评分最高的4个个体遗传到下一代直接组成下一代中的4个个体,即选择遗传,也叫精英遗传;

5) 根据交叉概率(0.5)计算出剩余6个个体中进行交叉遗传的个体数(3),根据评分选择进行交叉遗传的3个个体(选择规则:在选择时绘制一条线段,每一个母方个体所占长度与其评分成正比,遗传算法在这条线上等步长移动,每一步遗传算法都会选择与它所在位置对应的母方个体用于交叉遗传,即评分越高,被选择的概率越大),交叉产生子个体(选用散点式交叉),即交叉遗传;

6) 随着时间的推移,个体间差异越来越小,逐步向最优个体靠拢,会导致在之后的演化过程中调制电压恒定不变,无法达到偏振锁定的效果,所以要对剩余的3个个体保持突变遗传。突变大小=步长×方向,方向由计算机随机产生,步长由每个个体调制偏振后单光子探测器计数而定,计数小步长小、计数大步长大。在实验中,当计数小于2 kbps时,步长为2,计数大于2 kbps时,步长为20。剩余3个个体根据各自步长产生突变个体遗传到下一代,完成突变遗传;

7) 通过精英遗传、交叉遗传和突变遗传产生的新一代10个个体返回步骤2)。

重复此过程,即可使参考光I_x保持在最小值,达到偏振控制的目的。

4 实验结果与讨论

图3为没有进行偏振控制时信号光和参考光强度随时间的变化曲线。当调节偏振控制器使参考光光强达到最小后开始计时,观测由于环境变化对25 km光纤中光束偏振态的影响,由图3发现两束光光强随着时间变化非常严重,信号光的不稳定度几乎达到100%,在单光子密钥分发系统中这种剧烈起伏的光强无法用于生成密钥。

图4为经过偏振控制后信号光和参考光随时间的变化情况。经过基于遗传算法的偏振实时控制后,在30 s内将参考光调节到最小值,而信号光被锁定在最大20 kbps的光子计数,抖动不超过5%,消光比保持在30 dB以上,达到了偏振实时控制的目的。

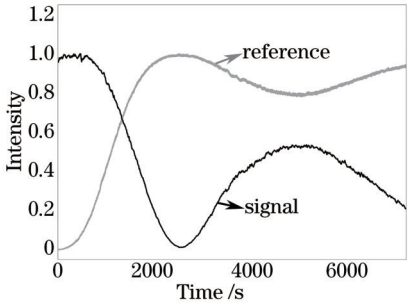

图3 没有进行偏振控制时信号光和参考光强度随时间的变化情况

Fig.3 Time-varying light intensity of reference and signal beam without polarization-controlled

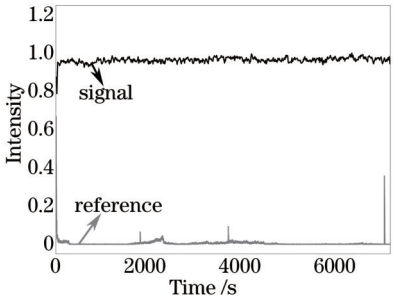

图4 经过偏振控制后时信号光和参考光强度随时间的变化情况

Fig.4 Time-varying light intensity of reference and signal beam with polarization-controlled

图5(a)~(d)分别为偏振控制过程中偏振控制器的4路调制电压的变化。从图中可以看出在将光束调制到最佳偏振态后,4路电压保持相对稳定,对偏振态进行微调优化,证实了偏振实时控制的有效性。

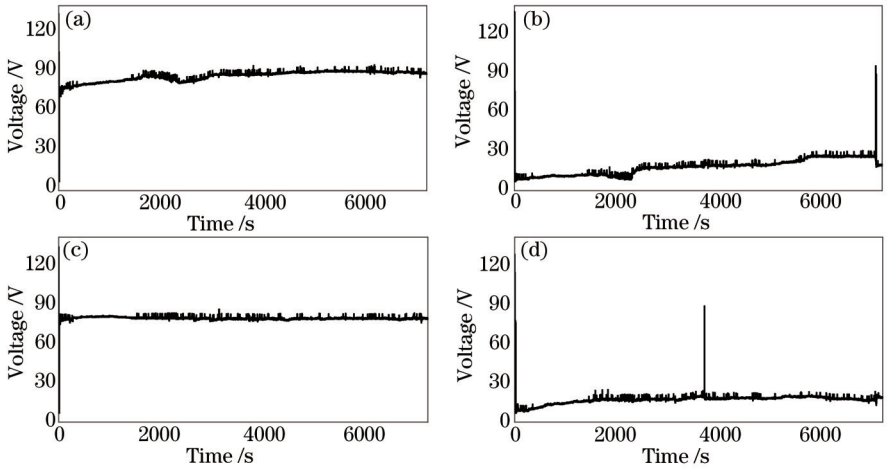

图5 偏振控制器的四路调制电压

Fig.5 Four parts modulation voltages applied on polarization controller

将此偏振控制方法用于基于B92协议的相位编码量子密钥分发系统中,在250 kbps的重复频率下,将信号光主峰锁定在20 kbps的计数,抖动控制在5%以内,相位调制深度为0.1,单边带光强为0.06光子每脉冲。最终成码率稳定在1.5 kbps,误码率低于4%。

5 结 论

给出了基于遗传算法进行偏振调制电压最优值选取的方法,用于在单光子相位编码量子通信系统中对偏振漂移进行实时控制,信号光光子计数漂移小于5%,成码率稳定在1.5 kbps,误码率低于4%。这种方法有效提高了单光子密钥分发系统的工作性能,同时可以有效应用于需要控制单光子偏振的其他领域。

参 考 文 献

1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing[C]. Processing of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, 1984: 175-179.

2 Bennett C H, Bessette F, Brassard G, *et al*.. Experimental quantum cryptography[J]. Journal of Cryptology, 1992, 5(1): 3-28.

3 Merolla J M, Mazurenko Y, Godegebuer J P, *et al*.. Quantum cryptographic device using single- photon phase modulation[J]. Phys Rev A, 1999, 60(3): 1899-1905.

4 Pu C A, Lin L Y, Goldstain E L, *et al*.. Micromachined integrated optical polarization-state rotator[J]. IEEE Photonics Technology Letters, 2000, 12(10): 1358-1360.

5 Kersey A D, Marrone M J, Dandridge A. Analysis of input-polarization-induced phase noise in interferometric fiber-optic sensors and its reduction using polarization scrambling[J]. Journal of Lightwave Technology, 1990, 8(6): 838-845.

6 Qin Zengguang, Zhu Tao, Chen Liang, *et al*.. High sensitivity distributed vibration sensor based on polarization-maintaining configurations of phase-OTDR[J]. IEEE Photonics Technology Letters, 2011, 23(15): 1091-1093.

7 Kim H J, Han Y G. Polarization-dependent in-line Mach-Zehnder interferometer for discrimination of temperature and ambient index sensitivities[J]. Journal of Lightwave Technology, 2012, 30(8): 1037-1041.

8 Wang Jian, Zhu Yong, Zhou Hua, *et al*.. Several kinds of polarization compensation techniques of optical fiber quantum key distribution system[J]. Laser & Optoelectronics Progress, 2014, 51(9): 090603.
王 剑, 朱 勇, 周 华, 等. 光纤量子密钥分发系统的几种偏振补偿技术[J]. 激光与光电子学进展, 2014, 51(9): 090603.

9 Martinelli M. A universal compensator for polarization changes induced by birefringence on a retracing beam[J]. Optics Communications, 1989, 72(6): 341-344.

10 Chen J, Wu G, Li Y, *et al*.. Active polarization stabilization in optical fibers suitable for quantum key distribution[J]. Optics Express, 2007, 15(26): 17928-17936.

11 Xavier G B, Faria G V, Temporao G P, *et al*.. Full polarization control for fiber optical quantum communication systems using polarization encoding[J]. Optics Express, 2008, 16(3): 1867-1873.

12 F Heismann, M S Whalen. Fast automatic polarization control system[J]. IEEE Photonics Technology Letters, 1992, 4 (5): 503-505.

13 Li Weiwen, Zhang Xianmin, Chen Kangsheng, *et al*.. A study for phase-shift characteristics of polarization controller based on simulated annealing algorithm[J]. Acta Optica Sinica, 2005, 25(4): 449-453.
李伟文, 章献民, 陈抗生, 等. 基于模拟退火算法的偏振控制器波片相移特性研究[J]. 光学学报, 2005, 25(4): 449-453.

14 Li Weiwen, Jin Xiaofeng, Zhang Xianmin, *et al*.. Application of genetic algorithms in polarization control[J]. Journal of Zhejiang University (Engineering Science), 2006, 40(3): 443-447.
李伟文, 金晓峰, 章献民, 等. 遗传算法在偏振态控制中的应用[J]. 浙江大学学报(工学版), 2006, 40(3): 443-447.

15 John E Galletly. An overview of genetic algorithms[J]. Kybernetes, 1992, 21(6): 26-30.

16 Ge Jike, Qiu Yuhui, Wu Chunming, *et al*.. Summary of genetic algorithms research[J]. Application Research of Computers, 2008, 25(10): 2911-2916.
葛继科, 邱玉辉, 吴春明, 等. 遗传算法研究综述[J]. 计算机应用研究, 2008, 25(10): 2911-2916.

栏目编辑: 刘丰瑞