文章编号:1001-9014(2016)02-0210-04 DOI:10.11972/j.issn.1001-9014.2016.02.016

量子密钥分发中偏振补偿算法

刘尉悦[1], 曹 蕾[1], 陈厦微[2], 张 亮[3], 李 杨[2], 曹 原[2],
任继刚[2], 蔡文奇[2], 廖胜凯[2], 彭承志[2]
(1. 宁波大学 信息科学与工程学院,浙江 宁波 315211;
2. 中国科学技术大学 合肥微尺度物质科学国家实验室,安徽 合肥 230026;
3. 中国科学院上海技术物理研究所, 上海 200083)

摘要:在以单模光纤作为量子信道,并采用光子偏振编码方式的量子密钥分发过程中,光纤的双折射效应会导致光子在光纤中传播时其偏振态发生随机变化,使安全密钥的最终成码率大幅度降低.利用两个四分之一波片和一个半波片的组合作为校正器,可以实现对任意偏振态的校正补偿.建立了一种以该类偏振校正器为执行机构的基于随机并行梯度下降控制算法的实时偏振补偿仿真控制模型,讨论了算法的随机扰动幅度、增益系数与收敛速度的关系,分析了算法对于偏振的校准能力.通过实验对算法的性能进行了验证.实验结果表明,经过一定次数的迭代后可将系统的偏振消光比校正到一个比较理想的状态.

关 键 词:量子信息;量子密钥分发;光纤偏振补偿;随机并行梯度下降控制算法
中图分类号:TN247 **文献标识码**: A

Polarization compensation algorithm for quantum key distribution

LIU Wei-Yue[1], CAO Lei[1], CHEN Xia-Wei[2], ZHANG Liang[3], LI Yang[2], CAO Yuan[2],
REN Ji-Gang[2], CAI Wen-Qi[2], LIAO Sheng-Kai[2], PENG Cheng-Zhi[2]
(1. College of Information and Engineering, Ningbo University, Ningbo 315211, China;
2. Hefei National Laboratory for Physical Science at Microscale,
University of Science and Technology of China, Hefei 230026, China;
3. Shanghai Institute of Technical Physics, Chinese Academy of Sciences, Shanghai 200083, China)

Abstract: In the process of the quantum key distribution based on the polarization coding of photons, the polarization state will be affected strongly and randomly by the birefringence effect of the single-mode fibers, which will lead to decrease the final secure key rate. Fortunately, this undesirable effect of single-mode fibers can be corrected by the combination of two quarter-wave plates and a half-wave plate. Utilizing the combination of three wave plates as the actuator, we build a simulation model of real-time polarization compensation based on stochastic parallel gradient descent algorithm. We study the relationship among the amplitude of the random disturbance, the gain factor and the convergent rate. Furthermore, we implement an experiment to demonstrate the algorithm we proposed. The results of the experiment show that the polarization extinction ratio of the simulation system can be corrected well after a certain number of iterations.

Key words: quantum information, quantum key distribution, fiber polarization compensation, stochastic parallel gradient descent control algorithm
PACS: 03.67.Ac

收稿日期:2015-06-12,**修回日期**:2015-12-02 **Received date**: 2015-06-12,**revised date**: 2015-12-02
基金项目:国家自然科学基金(11405172),安徽省自然科学基金(1408085QF114),宁波大学王宽诚幸福基金
Foundation items: Supported by National Natural Science Foundation of China (11405172), Natural Science Foundation of Anhui Province (1408085QF114), K. C. Wang Magna Fund in Ningbo University
作者简介(Biography):刘尉悦(1978-),男,江西萍乡人,副教授,博士,研究方向为量子通信与应用. E-mail:liuweiyue@nbu.edu.cn

引言

量子保密通信是经典通信和量子力学相结合的产物,其无条件安全的特点使它成为一种全新的安全通信技术[1],而量子密钥分发作为其中最先获得应用的分支,近年来受到广泛关注[2]. 量子密钥分发广泛采用偏振编码方式,偏振编码的载体为光子的不同偏振态[3-4],偏振补偿可以使输出光的偏振态和初始偏振态保持一致,它的性能将影响量子密钥分发的成码率,是量子密钥分发中的一项关键环节[4-5]. 采用普通的单模光纤作为量子态传输的量子信道时,由于单模光纤的不完美,光纤在拉制过程中会产生双折射效应,从而使光子偏振态发生改变,引起误码. 同时,任何微小的温度变化或者外力的影响都会使光纤的传输特性发生改变,引起偏振态的随机抖动,这大大增加了偏振随机变化的不可预知性,使基于偏振编码的量子密钥分发变得困难. 因此,量子密钥分发过程中的偏振补偿是量子通信实用化道路上必须解决的难题[6-7]. 本文提出了一种基于随机并行梯度下降控制(SPGD)的偏振补偿算法,并仿真分析了算法的主要特性. 同时,搭建了实验平台,对该算法进行了实验验证. 该算法可直接应用于基于光子偏振编码的量子密钥分发中[8].

1　系统仿真模型的建立

1.1　系统结构

普通单模光纤对光子偏振态的影响可以近似地看成一个幺正变换. 而对于光子的偏振态,三个波片(通常采用两个四分之一波片和一个半波片的组合)能够实现任意的幺正变换[5],因此可以采用旋转的三个波片作为执行机构来实现光纤的偏振补偿[9].

实现偏振补偿的关键是计算出三个波片的角度值,由于量子通信过程中,光纤信道对光子偏振态的影响具有很强的随机性,所以准确无误地计算出波片的角度值是比较困难的,一个逐步逼近算法是必要的. SPGD 算法作为一种无模型的优化算法,特别适用于无法建立准确系统模型的复杂受控系统的控制过程[10],其原理主要发展于随机逼近理论.

基于 SPGD 算法的偏振补偿系统结构图如图 1 所示. 以两组偏振光的偏振消光比作为目标函数,利用 SPGD 算法对三个波片组成的执行机构进行直接控制,通过算法的迭代过程不断地调整三个波片的角度值,直到偏振消光比达到一个比较理想的状态.

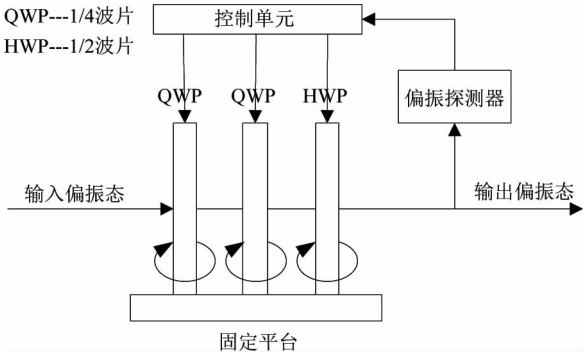

图 1　基于 SPGD 算法的偏振补偿系统结构图
Fig. 1　Schematic view of the polarization compensation system based on SPGD algorithm

1.2　仿真模型的建立

在性能指标分析模块中,偏振消光比是衡量偏振校正效果的一个通用标准. 量子密钥分发通常利用两组相互正交的偏振态,即水平偏振态 $|H>$,垂直偏振态 $|V>$ 以及 45^0 偏振态 $|D>$,135^o 偏振态 $|A>$ 进行编码,因此定义系统性能指标

$$C=\frac{1}{2}\cdot\left(\frac{DH}{DH+DV}+\frac{DD}{DD+DA}\right) \quad , \quad (1)$$

其中 DH、DV、DD、DA 分别表示测量反馈的 $|H>$、$|V>$、$|D>$、$|A>$ 四种偏振光的功率值.

在算法模块中,性能指标 C 是三个波片角度向量 $\boldsymbol{P}$ 的函数,$C=C(\boldsymbol{P}_1,\boldsymbol{P}_2,\boldsymbol{P}_3)$. SPGD 算法采用

$$\boldsymbol{P}^{(k+1)}=\boldsymbol{P}^{(k)}+\gamma\Delta\boldsymbol{P}^{(k)}\Delta C^{(k)} \quad . \quad (2)$$

作为基本的迭代公式对波片角度向量进行更新. 其中 $\Delta\boldsymbol{P}^{(k)}=(\Delta\boldsymbol{P}_1,\Delta\boldsymbol{P}_2,\Delta\boldsymbol{P}_3)$ 表示第 k 次迭代时施加的扰动角度向量,各 $\Delta\boldsymbol{P}_i$ 相互独立且服从伯努利分布,即各分量幅值相同 $|\Delta\boldsymbol{P}_i|=\sigma$,取正负值的概率皆为 50%;$\Delta C^{(k)}$ 为性能指标 C 的变化量

$$\begin{aligned}&\Delta C^{(k)}=C_+^{(k)}-C_-^{(k)}\\&C_+^{(k)}=C[\boldsymbol{P}^{(k)}+\Delta\boldsymbol{P}^{(k)}]\\&C_-^{(k)}=C[\boldsymbol{P}^{(k)}-\Delta\boldsymbol{P}^{(k)}]\end{aligned} \quad . \quad (3)$$

γ 为增益系数,如使目标函数向着极大值方向优化则 γ 取正值,反之则取负值,在本系统中,偏振对比度要向着极大值的方向优化,故 γ 取正值.

1.3　仿真结果与分析

为了进一步分析算法的性能,根据仿真模型,分别编写了波片转动、功率测量以及 SPGD 算法控制的仿真程序,仿真程序之间的通信通过基于 TCP 的 socket 通信实现.

增益系数 γ 以及扰动幅度 σ 的值是影响算法收敛速度的关键参数,图 2 给出了固定增益系数 γ

=600,取不同扰动幅度时的性能指标变化曲线图. 由图2可以看出,扰动幅度从0.3增加到0.5时,算法的收敛速度有逐步加快的趋势;继续增加到0.6时,性能曲线随着迭代次数的增加出现了大幅度的抖动. 综合考虑算法的收敛速度和稳定性,取 σ 为0.5最优值. 图3给出了固定扰动幅度 $\sigma=0.5$,取不同的增益系数时的性能指标变化曲线图. 从图中可以看出,γ 从400增加到600时,算法的收敛速度逐步加快. 以性能指标达到0.998为标准,$\gamma=400$ 时,185次迭代后性能指标收敛到0.998;当 $\gamma=600$ 时,120次迭代后收敛到0.998;而当 $\gamma=700$ 时,虽然迭代过程较 $\gamma=600$ 时收敛速度加快,但是收敛过程中出现了很不稳定的抖动. 因此综合考虑算法的收敛速度和稳定性,γ 的最佳取值为600.

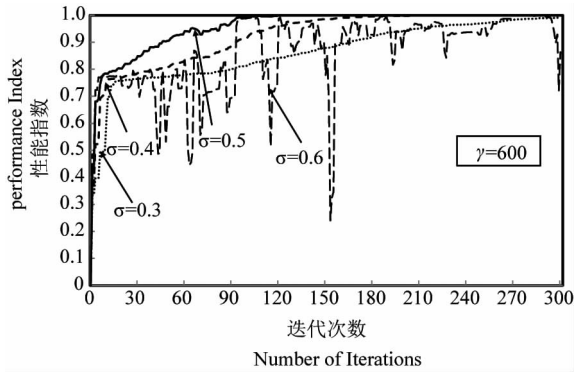

图2 不同扰动幅度时的性能指标变化曲线图
Fig. 2 Variation curve of the performance index with disturbance of different amplitudes

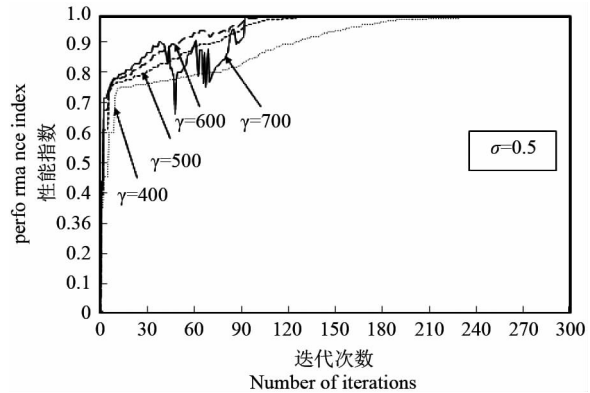

图3 不同的增益系数时的性能指标变化曲线图
Fig. 3 Variation curve of the performance index with different gain coefficients

以上的两组仿真结果为了便于分析找出最佳参数,皆是在同样的光纤初始状态下得到的. 图4给出了固定增益系数 $\gamma=600$ 和扰动幅度 $\sigma=0.5$ 时,通过每次复位波片转动及功率测量的仿真程序使每次模拟的光纤的初始状态不同,随机运行40次程序,即对40种不同的偏振畸变进行校正,验证算法对不同偏振畸变的校正能力. 由图4可以看出,根据不同的初始状态,40条曲线表征的偏振补偿性能指标收敛的速度以及抖动大小虽各不相同,但经过一定的校正次数后,最终系统的偏振补偿性能指标全部可以收敛到1,这充分证明了系统对于不同偏振畸变的补偿能力.

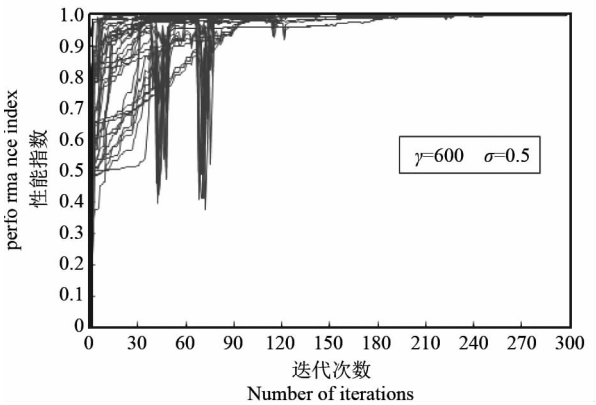

图4 固定增益和扰动幅度时对不同畸变的校正能力
Fig. 4 Correction ability of different distortions with fixed gain coefficient and disturbance

2 实验验证

为了检测实际应用中算法的性能,利用现有的实验设备搭建了如图5所示的实验平台. 以1 550 nm半导体激光器作为光源,通过偏振控制器控制光源发出任意偏振态的光线,光出射后再经过一段单模光纤后利用光纤准直器输出到自由空间信道. 光纤在自由空间信道中通过三波片组成的偏振校正器,其中每个波片都安装在电控旋转台上,可以通过电机控制旋转. 经过三波片后的光经过BB84协议中的偏振态分析模块后被四个探测器探测. 四个探测器分别测量|H>、|V>、|D>、|A>四种光分量的功率值,并将结果反馈给PC端进行SPGD算法的分析处理. PC端根据算法的处理结果控制三个波片的旋转,一直到系统的偏振消光比达到一个理想的状态.

当光源发出H光时,测量值DH/DV对应为H偏振光的消光比;当光源发出D光时,测量值DD/DA对应D光的消光比;而平均消光比为两种偏振光消光比的平均值. 旋转三波片的角度为零值,单模光纤和三波片组成了系统无偏振调制时的初态,初

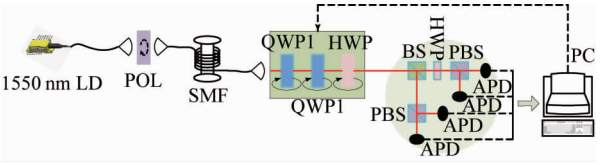

图 5　算法性能测试实验平台示意图
Fig. 5　Experiment platform of testing the algorithm's performance

始时 H 偏振光和 D 偏振光的消光比分别为 0.49 和 4.68,按照并行梯度下降算法逐次更新三波片角度值和系统的偏振消光比,在经过 60 多次的算法迭代后使得两者逐渐趋于最佳极值. 图 6 为实验过程中,H 偏振光的消光比、D 偏振光的消光比和平均消光比随着迭代次数的增加的变化情况,可以看出算法处于一种寻找最佳极值的过程中,并且最终的消光比均优于 500∶1,该结果已完全满足量子密钥分发的需求,充分说明了该算法在实际应用过程中的有效性.

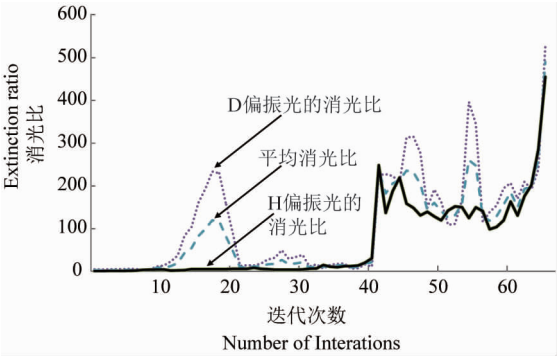

图 6　实验结果分析图
Fig. 6　Analysis diagram of the experiment results

3　结论

介绍了一种将随机并行梯度下降算法应用于量子密钥分发中的偏振补偿的方案. 以两个四分之一波片和一个半波片的组合为校正器,建立了采用 SPGD 算法的偏振补偿系统的仿真模型,通过仿真分析了找出系统的最优参数,并验证了系统对不同光纤初始状态皆具有很好的校正能力. 为了进一步说明此种偏振补偿方案在实际量子密钥分发中的有效性,搭建了专门的实验系统对该算法进行验证,实验结果表明基于 SPGD 算法的偏振补偿方案能够调整系统的偏振消光比达到一个比较理想的状态,在实际的应用中是有效可行的.

在本方案中,算法的收敛速度和波片的转动速度是影响偏振补偿速度的关键因素. 采用 SPGD 算法可以有效地减少算法收敛所需要的迭代次数,而波片转动旋转机构的速度决定了每次迭代所需的时间,在实际系统设计时应加以考虑.

References

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, New York, 1984, 175 - 179.

[2] WU Hua, WANG Xiang-Bin, PAN Jian-Wei. Quantum communication: status and prospects [J]. *Scientia Sinica Informationis* (吴华,王向斌,潘建伟. 量子通信现状与展望. **中国科学:信息科学**),2014,**44**(3):296 - 311.

[3] Lo H K, Curty M, Tamaki K. Secure quantum key distribution [J]. *Nature Photonics*,2014,**8**(8):595 - 604.

[4] Stucki D, Gisin N, Guinnard O, *et al*. Quantum key distribution over 67 km with a plug & play system [J]. *New J. Phys.*, 2002,**4**(41):1 - 8.

[5] Wang S K, Ren J G, Peng C Z, *et al*. Realization of Arbitrary Inverse Unitary Transformation of Single Mode Fibre by Using Three Wave Plates [J]. *Chinese Physics Letters*, 2007,**24**(9):2471.

[6] WANG Jian, ZHU Yong, ZHOU Hua, *et al*. Several kinds of polarization compensation techniques of optical fiber quantum key distribution systems[J]. *Laser & Optoelectronics Progress* (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. **激光与光电子进展**),2014,**51**:090603.

[7] CHEN Jie, LI Yao, WU Guang, *et al*. Stable quantum key distribution with polarization control[J]. *Acta Physica Sinica* (陈杰,黎遥,吴光,等. 偏振稳定控制下的量子密钥分发分发. **物理学报**),2007,**56**(09):5243 - 5245.

[8] 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.

[9] Wang C Z, Guo H, Ren J G, *et al*. Experimental validation of dynamic polarization compensation in ground-satellite quantum key distribution [J]. *Science China Physics, Mechanics & Astronomy*, 2014,**57**(7):1233 - 1237.

[10] ZHOU Pu, WANG Xiao-Lin, MA Yan-Xing, *et al*. Analysis on residual error for adaptive optical system based on stochastic parallel gradient descent control algorithm [J]. *Acta Optica Sinica* (周朴,王小林,马阎星,等. 基于随机并行梯度下降算法自适应光学系统的校正残差分析. **光学学报**),2010,**30**(3):613 - 617.