光纤量子密钥分发系统中的偏振无关相位调制

李瑞雪 马海强 韦克金 朱 武 刘宏伟

北京邮电大学理学院信息光子学与光通信国家重点实验室, 北京, 100876

摘要 提出并实验验证了一种简单稳健的实现偏振无关相位调制的方法。基于偏振相关的相位调制器,借助法拉第旋转镜,根据光在反射前和反射后的偏振状态的变化,实现了光的偏振无关的调制,实验的中心波长为1550 nm,可见度达到96.96%,且可长时间保持稳定。将其应用于“即插即用”的量子密钥分配方案中有效地保证了传输的稳定性和实用性。

关键词 量子光学; 量子密钥分配; 即插即用; 偏振无关; 相位调制

中图分类号 O436.1 **文献标识码** A

doi: 10.3788/LOP53.040601

Polarization-Insensitive Phase Modulation in Fiber Quantum Key Distribution System

Li Ruixue Ma Haiqiang Wei Kejin Zhu Wu Liu Hongwei

Key Laboratory of Information Photonics and Optical Communications, School of Science and State, Beijing University of Posts and Telecommunications, Beijing 100876, *China*

Abstract It introduces a simple and robust polarization-insensitive phase modulation method that is suitable for a plug and play quantum key distribution system, with a Faraday mirror and polarization sensitive phase modulator. The pulse is modulated twice acorrding to its polarization before and after it is reflected by a Faraday mirror. Preliminary experiments at 1550 nm wavelength demonstrate an interference visibility as high as 96%, regardless of the polarization of the signal.

Key words quantum optics; quantum key distribution; plug and play; polarization-insensitive; phase modulation

OCIS codes 270.5565; 270.5568; 060.2330; 260.5430

1 引 言

在量子信息技术众多的领域中,量子密钥分发(QKD)是被公认为最接近实际应用的领域,通信双方Alice和Bob共享一组绝对安全的密钥[1]。1984年,Bennett等[2]提出第一个量子密钥分配BB84协议。此后从基础理论到实验验证再到可行性探索都取得了重要的发展[3-6]。QKD以量子力学和信息论为基础,具有无条件安全性的特点。但基于当前技术并不能真正俘获单光子,只能以衰减弱激光脉冲模拟单光子源,学者们研究利用“强光”,即连续变量量子态为信号载波的量子密钥分发方案,并且在传输距离的问题上取得了突破进展[7-8]。当前,根据量子信道的不同,可以分为自由空间[9-10]和光纤[11]两类,光纤量子密钥分发系统受到更多科研小组的关注;根据量子态载体的不同,可分为相位和偏振态编码两类。在自由空间量子信道中多采用偏振编码,例如通过卫星有望实现全球化的量子通信[12],在光纤量子信道中多采用稳健性更强的相位编码的方式[13]。

相位编码方式的量子密钥分发实验系统一般基于不等臂的马赫-曾德尔干涉仪。但是,为了实现稳定的

收稿日期: 2015-08-17; **收到修改稿日期**: 2015-10-19; **网络出版日期**: 2016-03-17

基金项目: 国家自然科学基金(61178010)、信息光子学与光通信国家重点实验室项目基金(201318)、中央高校基本科研业务费专项资金(bupt2014TS01)

作者简介: 李瑞雪(1991—),女,硕士研究生,主要从事量子密钥分发方面的研究。E-mail: lruixue@126.com

导师简介: 马海强(1975—),男,副教授,博士生导师,主要从事量子密钥分发方面的研究。

E-mail: hqma@bupt.edu.cn(通信联系人)

密钥传输,马赫-曾德尔干涉仪需要额外的偏振补偿装置。这极大地增加了实验系统的复杂性。Muller等[14]提出了一种结构简单“即插即用”的QKD实验方案。在无需额外补偿装置的情况下,光纤对光脉冲的传输产生的影响得到了自动补偿。尽管即插即用装置结构简单,但是仍有一个技术上的难题需要解决。由于偏振相关的相位调制器调制电压低,速率高[15],所以经典的“即插即用”QKD系统一般采用偏振有关的相位调制器。为了保证实现准确的相位调制需要偏振无关的相位调制系统[16]。Sagnac环即是基于偏振无关的相位调制的一种尝试。但在Sagnac环的光纤中需要另外的偏振控制器来维持此偏振态。

本文提出了一种结构简单的稳健的实现偏振无关的相位调制方法。能够在不需要借助其他控制系统的情况下实现,并且将这种方法应用于“即插即用”的QKD,实验结果显示可见度可达96.96%,系统的可见度可保持并且优于96%,有效地保证了量子密钥分发系统的稳定性和实用性。

2 实验原理和实验方案

2.1 实验装置图

实现偏振无关相位调制的实验方案如图1所示[14]。Bob从激光器(LD)发射一个中心波长为1550 nm的单光子脉冲,经过环形器(cir)后,被一个2×2的光纤耦合器(C)分成两束相同的脉冲光。其中一束(F光)从下支路经相位调制器(PM_B)传输到偏振分束器(PBS),而另一束(S光)从上支路通过一段12 m延时60 ns的单模光纤(DL)后传输到PBS。两束脉冲经量子通道(QC)传输到Alice,通过相位调制器(PM_A)被法拉第镜(FM)反射回来,同时偏振态旋转90°。PBS的工作原理是透射平行偏振态光,反射垂直偏振态光,因此,返回时两束脉冲光的路径反转,也就是F光会反射到上支路,而S光透射通过下支路,最终两束光同时回到光纤耦合器,产生干涉。干涉结果使用两台单光子探测器D1,D2进行探测。干涉只与PM_A和PM_B调制后的相位有关。

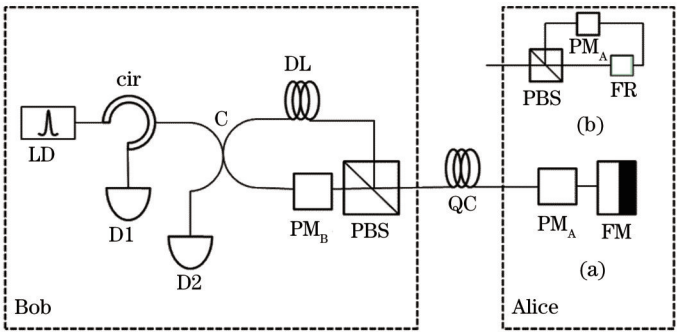

图1 实现偏振无关相位调制的实验方案。(a) 实验方案; (b) Sagnac环

Fig.1 Scheme of polarization-insensitive phase modulation in quantum key distribution system. (a) Experimental scheme; (b) Sagnac loop

2.2 理论分析

提出一种偏振无关的相位调制方法,利用偏振有关的装置但需要经过两次相位调制。第一次相位调制是Bob向Alice发射脉冲光时在PM_A进行调制,第二次是脉冲光从法拉第镜反射回来时在PM_A进行调制。这种方法不需要任何附加的硬件设备或者复杂的控制系统。

理论上的解释如下:

在PM_A进行第一次相位调制前,由于光纤双折射特性的影响,偏振态为任意偏振态。因此可以表示为

$$\left|\psi\right\rangle_{F} = \alpha\left|V\right\rangle + \beta\left|H\right\rangle, \tag{1}$$

式中α和β是概率振幅并满足$|\alpha|^2 + |\beta|^2 = 1$。$\left|V\right\rangle$和$\left|H\right\rangle$表示垂直(V)和水平(H)偏振态。$PM_A$首先对先到达的脉冲光($F_l$)进行相位调制,调制后先到达的脉冲光的偏振态表示为

$$\left|\psi\right\rangle_{F_l} = \exp(\mathrm{i}\phi_{AV})\alpha\left|V\right\rangle + \exp(\mathrm{i}\phi_{AH})\beta\left|H\right\rangle, \tag{2}$$

式中ϕ_{AV}和ϕ_{AH}垂直方向V和水平方向H的相位偏移,脉冲光经法拉第镜反射后(F_b)偏振方向旋转90°,偏振态表示为

$$\left|\psi\right\rangle_{F_b} = \exp(\mathrm{i}\phi_{AV})\alpha\left|H\right\rangle + \exp(\mathrm{i}\phi_{AH})\beta\left|V\right\rangle. \tag{3}$$

当反射后的脉冲光经过PM_A时，偏振态表示为

$$|\psi\rangle_{F_b}=\exp(i\phi_{AV})\exp(i\phi_{AH})\alpha|H\rangle+\exp(i\phi_{AH})\exp(i\phi_{AV})\beta|V\rangle=\exp[i(\phi_{AV}+\phi_{AH})](\alpha|H\rangle+\beta|V\rangle). \tag{4}$$

由(3)和(4)式可以看出，最先到达的脉冲经过两次调制后有$\phi_{AV}+\phi_{AH}$的相位偏移，相位调制的结果取决于$\phi_{AV}+\phi_{AH}$相位偏移而不是最初的偏振态，或者说如果只经过一次相位调制，则偏振态会影响到相位调制结果。比如实验采用垂直偏振态有关的相位调制器，进入的光脉冲为垂直偏振态则会得到比较理想的干涉结果，若进入的光脉冲为水平偏振态，则会产生较大的损耗而使干涉结果不理想。

这种方法的另一个优点是，由于调制了两次，所以相位调制时的半波电压相对小一些。调制结果相位偏移了$\phi_{AV}+\phi_{AH}$而不是ϕ_{AV}或者ϕ_{AH}，得到了比单次调制的方法相对大一些的相位调制结果。

3 实验结果和讨论

实验中采用的激光器是瑞士IDQ-id300短脉冲激光器，中心波长为1550 nm，光脉冲宽度为2 ns，峰值功率为1 mW。光纤耦合器是50/50的光分束器。采用的是IDQuantique的id200单光子探测器，暗计数5×10^{-5} ns^{-1}。

首先测试偏振有关相位控制系统的偏振特性，即当未经过延时的脉冲光F到达PM_A时，对PM_A加偏置电压，PM_B的偏置电压为0，进行相位调制，只调制一次。示意如图2(a)所示。DL为12 m延时60 ns。

D1和D2探测结果如图3(a)所示，由于进入的光脉冲偏振态不确定，因而垂直和水平偏振态经过调制的量也不相同，因而造成干涉结果不理想。在偏振相关的相位控制下，由于偏振态的改变相位也随之发生了改变。因此为了得到高可见度的干涉结果还需要其他辅助系统。

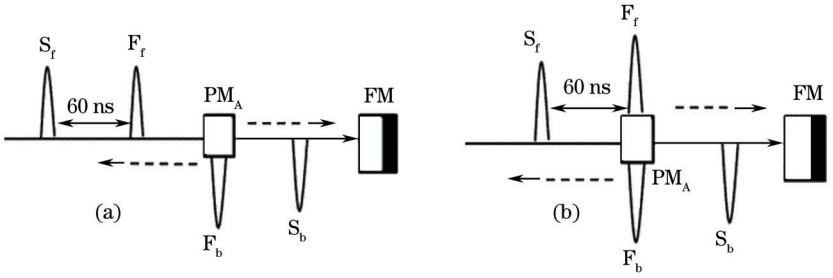

图2 (a) 单次调制方案示意图; (b) 两次调制方案示意图

Fig.2 (a) Scheme of single phase modulation; (b) scheme of double phase modulation

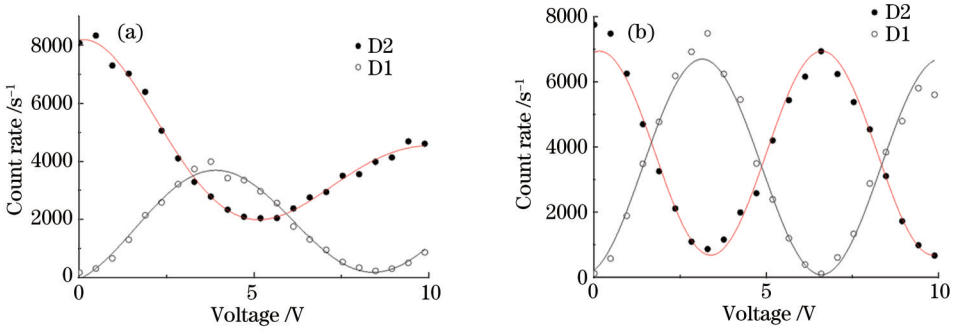

图3 (a) 单次调制后D1、D2的探测结果; (b) 两次调制后D1、D2的探测结果

Fig.3 (a) Results of D1、D2 after single phase modulation; (b) results of D1、D2 after double phase modulation

当脉冲光被调制两次，向法拉第镜传输以及被法拉第镜反射后，如图2(b)所示，D1和D2的探测结果如图3(b)所示，可见度达到96.96%，可见度定义为

$$V=\frac{I_{max}-I_{min}}{I_{max}+I_{min}}, \tag{5}$$

式中I_{max}和I_{min}分别表示最高和最低光子计数率。而单光子探测器的相干条纹的可见度与量子误比特率(QBER)是有很大联系的[17]。由BB84协议得QBER定义为

$$Q=\frac{1-V}{2}. \tag{6}$$

误比特率为1.5%,半波电压为3.3 V。

通过实验可以证明,偏振有关的相位控制系统经过两次调制的方法能够实现偏振无关的相位控制。

4 结 论

提出并实验验证了一种应用于“即插即用”量子密钥分配的方案的偏振无关相位控制器的实现方法。根据单光子探测器的探测结果,可见度达到96.96%,证明了该方案的稳定性和可行性。应用于“即插即用”的QKD系统中,误比特率为1.5%。两次调制的方案不需要额外的硬件设备和控制系统。该方案不仅在量子密钥分配中得到广泛应用,未来也可应用于需要相位调制的其他领域。

参 考 文 献

1 Gisin N, Ribordy G, Tittel W, *et al*.. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

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, 1984: 175-179.

3 Wei Kejin, Ma Haiqiang, Wang Long. A quantum secret sharing scheme based on two polarization beam splitters[J]. Acta Physica Sinica, 2013, 62(10): 104205.
韦克金, 马海强, 汪 龙. 一种基于双偏振分束器的量子密码共享方案[J]. 物理学报, 2013, 62(10): 104205.

4 Wei Kejin, Ma Haiqiang, Yang Jianhui. Experimental circular quantum secret sharing over telecom fiber network[J]. Opt Express, 2013, 21(14): 16663-16669.

5 Zhao Yi, Qi Bing, Ma Xiongfeng, *et al*.. Experimental quantum key distribution with decoy states[J]. Phys Rev Lett, 2006, 96(7): 070502.

6 Peng Chengzhi, Zhang Jun, Yang Dong, *et al*.. Experimental long-distance decoy-state quantum key distribution based on polarization encoding[J]. Phys Rev Lett, 2007, 98(1): 010505.

7 Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*.. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

8 Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimazation for the reconciliation of Gaussian quantum key distribution[J]. Acta Optica Sinica, 2014, 34(1): 0127001.
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.

9 Jacobs B C, Franson J D. Quantum cryptography in free space[J]. Opt Lett, 1996, 21(22): 1854-1856.

10 Wang Yan, Li Hongzuo, Zhang Meng, *et al*.. Research of pulse position modulation modulation characteristics of fiber laser in space optical communications[J]. Chinese J Lasers, 2015, 42(8): 0805001.
王 岩, 李洪祚, 张 猛, 等. 空间光通信光纤激光器脉冲位置调制特性研究[J]. 中国激光, 2015, 42(8): 0805001.

11 Townsend P D, Rarity J G, Tapster P R. Single photon interference in 10 km long optical fibre interferometer[J]. Electron Letters, 1993, 29(7): 634-635.

12 Wu Hua, Wang Xiangbin, Pan Jianwei. Quantum communication: status and prospects[J]. Science China, 2014, 44(3): 296-311.
吴 华, 王向斌, 潘建伟. 量子通信现状与展望[J]. 中国科学, 2014, 44(3): 296-311.

13 Townsend P D, Marand C. Quantum key distribution over distances as long as 30 km[J]. Opt Lett, 1995, 20(16): 1695-1697.

14 Muller A, Herzog T, Huttner B, *et al*.. "Plug and Play" systems for quantum cryptography[J]. Appl Phys Lett, 1996, 70(7): 793-795.

15 Bethune D S, Navarro M, Risk W P. Enhanced autocompensating quantum cryptography system[J]. Appl Phys Lett, 2002, 41(9): 1640-1648.

16 Peng Xiao, Jiang Hao, Guo Hong. Multi-wavelength QKD for reducing Rayleigh backscattering and increasing the key rate [J]. Journal of Physics B-Atomic Molecular and Optical Physics, 2008, 41(8): 085509.

17 Jeong Y C, Kim Y S, Kim Y H. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols [J]. Laser Physics, 2011, 21(8): 1438-1442.

栏目编辑: 刘丰瑞