第 56 卷 第 9 期 2007 年 9 月
1000-3290/2007/56(09)/5243-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.9,September,2007

偏振稳定控制下的量子密钥分发*

陈 杰 黎 遥 吴 光 曾和平†

(华东师范大学光谱学与波谱学教育部重点实验室,上海 200062)

(2006 年 11 月 20 日收到;2007 年 1 月 23 日收到修改稿)

由于长距离单模光纤传输中存在的双折射效应会引起偏振随机抖动,光纤中利用偏振编码进行量子密钥分发一直难以实现.利用光子计数分析光纤中的偏振变化情况,并通过反馈控制的方式补偿偏振变化,从而实现了基于 BB84 协议的偏振编码长时间稳定的量子密钥分发实验,传输距离为 100 km.

关键词:量子密钥分发,偏振反馈控制,单光子探测,偏振随机抖动

PACC:4250,4230,4281F

1. 引 言

自从 1984 年 Bennett 和 Brassard 提出第一个量子密钥分发协议[1]以来,量子保密通信获得了长足的发展.目前在光纤系统中的保密通信实验绝大多数都是采用相位编码的方案.这种方案需要进行精密的光程控制,由于长距离光纤中存在偏振色散和相位抖动,这种方案的实验难度较大.后来提出的“Plug&Play”的双向密钥分发系统[2]一定程度上解决了这个问题.中科院物理研究所[3]和华东师范大学[4]也相继完成了这种方案的改进实验.但是随着通信距离的增长,背向散射所引起的误码也将增加.并且双向通信的设计也为‘特洛伊木马’攻击提供了可能.文献[5]报道了 122 km 光纤中的单向量子密钥分发实验,误码率 8.9%,稳定时间 2 min.华南师范大学提出的差分相位编码方案[6],采用双 FM 干涉仪测量,一定程度提高了系统稳定性和安全性,误码率 3%,稳定时间大于 24 h.

与相位编码相比,偏振编码具有多项优点:编码与解码简单、不需要十分精确的控制、器件插损小、不需要进行主动调制[7—9].但是由于单模光纤无法保持绝对的圆对称性,任何微小的外力影响或温度变化都将引起光纤传输特性改变,引起偏振态的随机抖动,从而使稳定的量子密钥分发变得困难,限制了偏振编码方案在量子保密通信中的发展.

2. 偏振反馈控制

光纤中的偏振态(SOP)可以用邦加球进行描述,BB84 协议所使用的 4 个偏振态正好对应于邦加球赤道圆上的 4 个顶点(图 1),表示为 $H(0°)$,$V(90°)$,$R(135°)$,$Q(45°)$.偏振态的变化可以用邦加球上的点的轨迹表示.

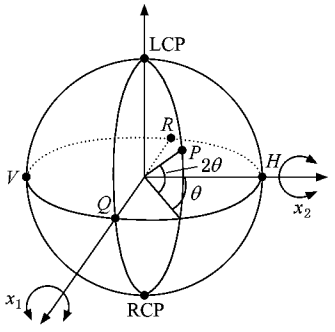

图 1 偏振态的邦加球表示

由于在传输过程中单模光纤所受应力不均,以及温度的变化都将影响光纤中的双折射,这种影响是随机的,从而引起偏振态的随机变化.比如初始偏振态为 Q 点的线偏振光,在经过长距离光纤传输后,可能成为偏振态为 P 点的椭圆偏振光.偏振控制的目的,就是使 P 点的偏振回到 Q 点,从而保证输出光的偏振态和初始偏振态相同.

* 国家自然科学基金(批准号:10374028)和教育部重点基金(批准号:104193)资助的课题.

† 通讯联系人.E-mail:hpzeng@phy.ecnu.edu.cn

实验中,我们使用光纤偏振控制器(型号为 GP-PolaRITE Ⅱ)对偏振进行调节.光纤偏振控制器的核心器件是两个轴向方向成 45°的压电陶瓷挤压器.压电陶瓷挤压光纤将在光纤中的产生双折射. 在邦加球上引起偏振态以赤道平面上的某个直径为主轴旋转.如图 2 所示,如果沿水平方向挤压光纤,那么偏振态绕 X_2 旋转,如果沿 45°的方向挤压光纤,那么偏振态绕 X_1 旋转.因此,对于邦加球上任何偏离初始偏振态的点,都可以通过绕 X_1,X_2 轴旋转一定角度使其回到初始偏振态[10—13].

3. 实验系统

具有偏振反馈控制功能的实验系统(图 2).

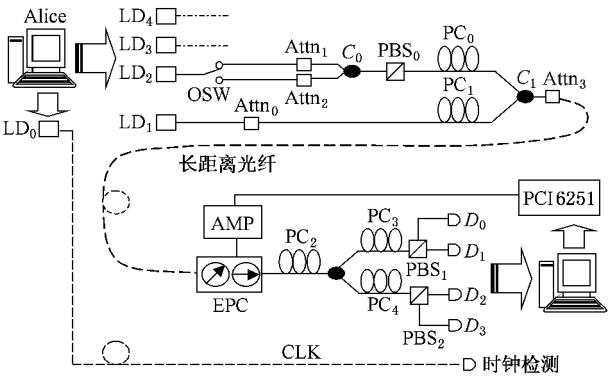

图 2 偏振控制下的量子密钥分发系统

我们仅取用垂直方向(V)和水平方向(H)演示偏振控制过程,LD_2 出射的光为 H 方向,通过光衰减器($Attn_0$ 和 $Attn_3$)后,光子能量衰减为每脉冲0.1个光子的水平,LD_1 出射的光为 V 方向,并通过光开关(OSW)连接到两个光衰减器,其中 $Attn_1$ 衰减量和 $Attn_0$ 一致,$Attn_2$ 的衰减量较小.$Attn_2$ 通道是专门为偏振反馈控制提供的,光脉冲通过后,每个脉冲为几个光子.多光子是为了增加 Bob 端的光子计数,从而减小由于误差造成的抖动对偏振分析的影响,提高反馈量的准确性.经过长距离光纤后,初始的线偏振光将变为随机的椭圆偏振光,Bob 端调节手动偏振控制器(PC_2,PC_3,PC_4)和偏振分束镜(PBS_1, PBS_2)将椭圆偏振光分为 4 个方向的分量,分别为 0°,90°,45°,135°方向,即对应邦加球上四个顶点. 每个分量的光强大小通过相应的单光子探测器(D_0,D_1,D_2,D_3)的计数表示.D_0,D_1,D_2,D_3 的计数构成两个斯托克斯参数 S_1 与 S_2,通常表示如下:

$$S_1 = \frac{I(H) - I(V)}{I(H) + I(V)} = \cos 2\varepsilon \cos 2\theta,$$

$$S_2 = \frac{I(Q) - I(R)}{I(Q) + I(R)} = \cos 2\varepsilon \sin 2\theta,$$

其中 $I(H)$,$I(V)$,$I(Q)$,$I(R)$分别表示四个偏振分量的光强,在这里即等效于四个单光子探测器的计数值.ε 和 θ 分别表示在邦加球的经线和纬线上转动的方位角.由公式可知,S_1 和 S_2 实际上分别表征了 H 和 V 方向、Q 和 R 方向偏振分量的对比度,如果初始偏振态为 H 方向,且在光纤中偏振变化量较小,那么经过 Bob 端的检偏以后,$I(H)$即为初始光强经过衰减后的值,而 $I(V)$是一个趋向 0 的微量,所以 S_1 是一个近似 1 但总小于 1 的数,$I(Q)$和 $I(R)$值相当,所以 S_2 是一个约等于 0 且在 0 值附近震荡的数.因此,如果我们定义两个阈值 T_1(略小于 1),T_2(略大于 0),并且在通信双方的控制程序中准备两套运行状态——“通讯”状态和“偏振控制”状态,则可以通过 S 与 T 的比较控制通信系统在两种运行状态之间切换.

整个实验流程如下:当通信双方准备完毕后,将各自的运行状态设定到“通讯”状态,由 Bob 通过局域网向 Alice 发出通信请求,Alice 收到请求后开始准备随机码并通过数据采集卡给 LD 提供驱动信号,并将光开关(OSW)跳转到 $Attn_1$ 位置,Bob 端只采集 D_0,D_1 的数据,并保存为一个比特序列.当 N(N 通过程序设定)组数据采集完成后,转入“偏振控制”状态,Bob 向 Alice 发出“偏振检测”请求,Alice 接到请求后,固定的触发 LD_2(即由 0 和 1 组成的随机信号改为全 1 信号),因此信号光的初始偏振态为确定的 H 方向,同时光开关跳转到 $Attn_2$ 通道.Bob 端将 D_0,D_2,D_2,D_3 四个探测器的计数送入计算机,通过程序计算斯托克斯参量,并与设定阈值进行比较,如果 $S_1 > T_1$,$|S_2| < T_2$,那么说明偏振态依然较好地保持在 H 方向,则 Bob 再次向 Alice 发出状态转换请求,程序转为“通讯”状态,量子密钥分发继续进行 如果 $S_1 < T_1$ 或者 $|S_2| > T_2$ 那么 Bob 通过偏振偏移量(即 S 和 T 的差量)的大小提供两个反馈信号,由数据采集卡输出两个模拟电压信号,经过电压放大以后,分别控制偏振控制器的两个压电陶瓷挤压光纤,实现偏振方向绕 X_1、X_2 旋转,同时程序对偏振变化情况进行实时监测,当 $S_1 > T_1$,$|S_2| < T_2$ 时,说明偏振方向已经调整到允许范围

内，则 Bob 向 Alice 发出状态转换请求，停止偏振控制，继续进行通讯.

这种控制方式是一种自适应的逻辑反馈控制，因为反馈信号的滞后性，偏振调节行为和检测到调节结果之间有一定的时差，无法实现快速响应下的即时控制，所以每一次反馈量的给出都应该首先预测其控制结果，如果上一次控制所引起的偏振变化方向与希望的变化方向一致，则保持此电压的方向，并根据偏振偏移量的大小适当减小反馈量，否则改变电压方向并适当增加反馈量. 最终使偏振方向趋于初始偏振态，实现对偏振的调节.

需要指出的是，偏振控制器存在一个极限控制电压，反馈电压的大小应该严格控制在偏振控制器允许的电压范围之内，但是我们所采用的这种自动搜索的反馈控制方式，有时将导致反馈电压超出极限值，控制无法继续进行，这时就需要对电压值进行复位. 实际上，每一个偏振控制器都有一个周期电压 $V\pi$，只要在当前电压值的基础上加减 $V\pi$，就可以使反馈控制不改变调节效果，在邦加球上即相当于偏振点围绕主轴旋转了 2π 的角度，又回到原来的偏振态. 利用这个原理，我们在程序中也实现了电压保护，在反馈电压接近极限值时，引入 $V\pi$ 的改变量，从而使整个控制系统能够无中断地进行.

另外，阈值 T 的设定应该根据当时的环境变化情况和传输距离决定，T 值越接近理论极限值（$T_1=1, T_2=0$），偏振控制的结果越理想，但同时也会增加反馈控制的难度，特别是当环境不稳定或者传输距离增加时，$S_1 > T_1$，与 $|S_2| < T_2$ 的情况很不容易实现，这无疑将延长偏振控制的时间，相应的通讯时间被缩短，导致密钥分发的效率降低. 同理，N 值也应根据偏振漂移的快慢设定，当传输距离短时，偏振能在无控制的情况下稳定较长时间，则 N 的取值应该增大，否则应减小.

4. 偏振控制系统外围电路

电路框图（图 3）主要分为 LD 驱动、时钟同步、反馈控制三部分. Alice 方面，计算机程序随机触发数据采集卡上的 4 个 I/O 口，将该口电平拉高，然后通过电平转换将 TTL 信号转为 ECL 信号，驱动电路板提供一个方波信号，当某一 I/O 口电平置高时，通过“与”门电路和方波信号做与运算即可得到同频率的驱动信号. 另外将一路 I/O 口持续拉高，通过“与”门后驱动 LD，用作通信系统的时钟信号. 驱动板还具有延时调节和功率调节的功能.

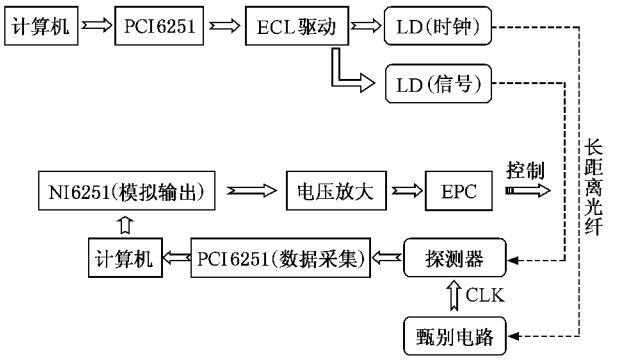

图 3　密钥分发系统外部电路框图

Bob 方面，首先利用甄别电路提取时钟信号，并分为四路分别提供给四个单光子探测器. 探测信号通过数据采集卡送入计算机，经过程序的分析运算后再通过数据采集卡提供模拟电压信号，由于 PCI6251 的电压输出范围较小（－10 V—＋10 V），而偏振控制器所需的驱动电压在 0—150 V 范围内，所以通过一个电压放大电路，并且加入一个 80 V 的偏置电压，使得偏振控制器工作在 80 V 左右的安全范围内.

5. 实验结果

我们选择通信距离为 50 km，75 km，100 km 进行了偏振稳定控制下的量子密钥分发实验，其中 50 km 实验中参数选择为 $T_1=0.96$，$T_2=0.05$，稳定通讯时间达到 10 h，平均误码率（QBER）为 3.1%；75 km 和 100 km 实验中参数选择分别为 $T_1=0.95$，$T_2=0.08$，系统稳定通讯时间分别为 10 h 和 7 h，平均误码率分别为 4.8%和 6.6%.（图 4，表 1）.

表 1　实验参数和结果

	S_1	S_2	QBER	T/min	Key Rate
50 km	0.96(±0.01)	0.02(±0.06)	3.1(±1.0)	352	110
75 km	0.95(±0.01)	0.023(±0.07)	4.9(±1.4)	342	44
100 km	0.94(±0.01)	−0.027(±0.07)	6.6(±2.0)	189	16

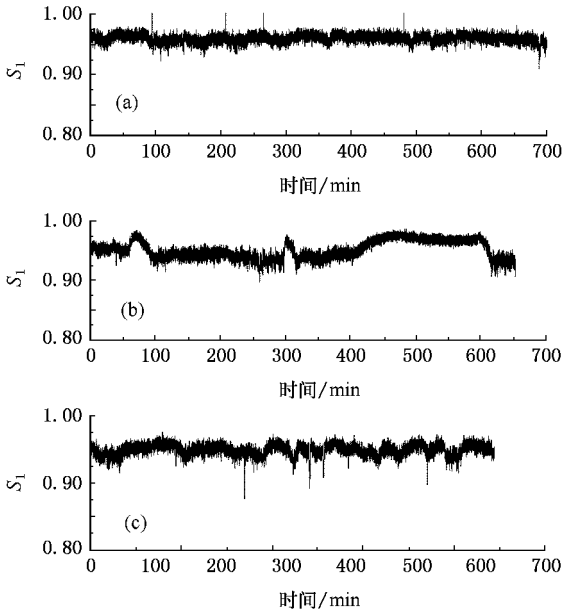

图 4 偏振控制下 S_1 随时间变化情况,(a),(b),(c)分别表示通信距离为 50 km,75 km,100 km

6. 讨论和结论

整个实验过程通过计算机程序控制,我们选择在 LABview 7.1 平台上完成了包括局域网(TCP/IP 协议)建立,数据储存分析、反馈判断等多项工作,这是因为 LABview 在计算机接口和可视化方面的具有操作简单、调试方便的优势.但是由于 LABview 运行速度稍慢,将会增加运行周期,影响通信效率.目前我们在进行改进的实验,通过偏振控制器分析得到的电压直接接入单片机,通过单片机完成判断和提供反馈电压,这将大大提高通信速度.

实验所使用的探测器是我们自行开发制造的单光子探测器,APD 工作温度为 180 K,探测效率 20%,暗计数分别为 4×10^{-7}/pulse(D_0),8×10^{-7}/pulse(D_1).所使用的光脉冲频率为 1 MHz,增加脉冲频率对于提高通信效率作用最为明显,但是受探测端的后脉冲的影响,频率的提高将带来更多的误码,特别是在通信距离远的情况下,由于本身的成码较少,误码率的提高尤其突出.这个问题可以通过增加探测器的死时间来改善,即在 APD 探测到雪崩信号后将探测门关断一断时间,可以减少后脉冲产生的概率.另外,提高脉冲频率还需要增加驱动电路的响应速度.

本文提出了将偏振控制的思想运用于量子密钥分发系统中,通过对偏振偏移量的实时监测提供反馈电压,控制压电陶瓷挤压光纤,补偿了由于偏振随机抖动引起的偏振漂移,从而实现了基于偏振编码的长距离高稳定性的量子密钥分发实验.相信这将有利于偏振编码方案在量子保密通信中的应用和发展,发挥其器件差损小,编解码结构简单的优势.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Computer Systems & Signal Processing* (New York: IEEE) pp175—179

[2] Bethune D S, Risk W P 2002 *New J. Phys.* **4** 42

[3] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C, Lü S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁 创、符东浩、梁 冰、廖 静、吴令安、姚德成、吕述望 2001 物理学报 **50** 1429]

[4] Wu G, Zhou C Y, Chen X L, Han X H, Zeng H P 2005 *Acta Phys. Sin.* **54** 3626 (in Chinese) [吴 光、周春源、陈修亮、韩晓红、曾和平 2005 物理学报 **54** 3626]

[5] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[6] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S, Liu S H 2006 *Acta. Phys. Sin.* **55** 4642 (in Chinese) [李明明、王发强、路轶群、赵 峰、陈 霞、梁瑞生、刘颂豪 2006 物理学报 **55** 4642]

[7] Bienfang J, Gross A, Mink A, Hershman B, Nakassis A, Tang X, Lu R, Su D, Clark C, Williams C, Hagley E, Wen J 2004 *Opt. Express* **12** 2011

[8] Gordon K, Fernandez V, Townsend P, Buller G 2004 *Quant Electron* **40** 900

[9] Gordon K, Fernandez V, Buller G, Rech I, Cova S, Townsend P 2005 *Opt. Express* **13** 3015

[10] Ulrich R 1979 *Appl. Phys. Lett.* **35** 840

[11] Noe R 1986 *Electron. Lett.* **22** 772

[12] Walker N, Walker G 1987 *Electron. Lett.* **23** 290

[13] Noe R, Heidrich H, Hoffmann D 1988 *J. Lightwave Technol.* **6** 1199

Stable quantum key distribution with polarization control *

Chen Jie　Li Yao　Wu Guang　Zeng He-Ping†

(*Key Laboratory of Optical and Magnetic Resonance Spectroscopy of Ministry of Education*, *Department of Physics*, *East China Normal University*, *Shanghai* 200062, *China*)

(Received 20 November 2006; revised manuscript received 23 January 2007)

Abstract

In this paper, we promote a principle of polarization feedback which keeps polarization states stable in long-distance fiber. It is quite difficult to realize long-term stable quantum key distribution (QKD) with polarization encoding due to the effect of irregular polarization fluctuation in single mode fiber. We have designed a polarization feedback control system to compensate for the birefringence. And a polarization encoded QKD experiment has been realized in 100 km fiber.

Keywords: quantum key distribution, polarization control, single photon detection, polarization fluctuation

PACC: 4250, 4230, 4281F

* Project supported by the National Natural Science Foundation of China (Grant No. 10374028), and the Key Project Sponsored by National Education Ministry of China (Grant No. 104193).

† Corresponding author. E-mail: hpzeng@phy.ecnu.edu.cn