第 54 卷 第 11 期 2005 年 11 月
1000-3290/2005/54(11)/5014-04

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.11,November,2005

基于双偏振分束器的量子密钥分发系统*

马海强[1)†] 李亚玲[1)2)] 赵 环[1)3)] 吴令安[1)]

[1)] (中国科学院物理研究所光物理开放实验室，北京 100080)

[2)] (北京交通大学，北京 100044)

[3)] (东南大学，南京 210096)

(2005 年 3 月 24 日收到；2005 年 4 月 27 日收到修改稿)

提出了利用两个偏振分束器的量子密钥分发系统，有效地解决了相位调制器的偏振依赖性问题. 以 1310nm 波长在通信距离为 25km 的光纤中实现了高密钥生成率，干涉对比度 99.4%. 有效密钥生成率大于 0.6kbit/s，误码率 0.5%.

关键词：量子密钥分发，偏振分束器，单光子干涉

PACC：0365，4230，4250

1. 引 言

量子信息科学是量子力学与信息科学相结合的产物，将对人类社会产生重大影响的新兴前沿科学. 量子密钥分发是量子信息科学中的重要分支，基于量子力学的基本原理——单量子态不可克隆原理与不确定性原理，也是当前量子信息中最接近实用的领域. 至 1991 年，三种协议方案：BB84 协议[1]、B92 协议[2]、相关粒子协议[3] 已基本形成. 1992 年，Bennett 等人基于 BB84 协议，以强烈衰减的激光脉冲做单光子源，信息加载在单光子的偏振上，第一次成功地在自由空间完成了演示性实验[4]，从而掀起了量子密钥分发实验研究的高潮[5—15]. 当前，实现光纤中量子密钥分发采用的是相位调制编码，实验方案主要有：1) 由 Bennett 提出的基于双不等臂马赫-曾德尔(Mach-Zehnder，M-Z)干涉仪的系统[2]，光子单向传输. 该方案有效地制止了木马攻击，在通信双方 Alice 和 Bob 各自的干涉仪内部光脉冲沿不同的路径传播，因此为了获得较好的实验结果，通信双方必须拥有完全对称的干涉仪，并且在工作过程中要保证各自的 M-Z 干涉仪的臂长不稳定性不超过十几纳米. 2) 由 Gisin 小组提出的基于法拉第旋转镜的时分复用干涉仪[16]，干涉光脉冲所经过的空间路径是完全相同的，因而保证了相当高的稳定性和偏振自动补偿性，但对于具有偏振相关损耗(polarization dependent losses，PDL)相位调制器，此系统将无法工作. 两种系统各有其缺点，均被不同的实验小组所采用. 目前，光纤中通信的最长距离是约 150km[17,18]，自由空间是 23km[19].

本文提出了基于双偏振分束器、自动偏振补偿的量子密钥分发系统，它可更广泛地应用于偏振相关、偏振无关、有偏振相关损耗、无偏振相关损耗相位调制器.

2. 双偏振分束器的量子密钥分发光路

实验原理如图 1 所示. Bob 先给 Alice 发送一个短激光脉冲，来初始化传输过程. 经环形器到达 X 形耦合器的光脉冲被分为两个路：一路 P_1，经 M-Z 干涉仪的短臂(图中上臂)，由偏振控制器 1、相位调制器 1、偏振控制器 2 组成，到达偏振分束/耦合器 1 的输入口 Port B_1，然后，径直地向 Alice 传播. 而另外一路 P_2，经 M-Z 干涉仪的长臂，由延时光纤圈和偏振控制器 3 组成，到达偏振分束/耦合器 1 的输入口 Port B2 后，也径直地向 Alice 传播. 长臂与短臂的差就使两路光相互之间有一定的时间延迟，实现了时间复用(time-multiplexing). 光脉冲 P_1，P_2 经干

* 国家重点基础研究发展规划(批准号：2001CB309301)和中国科学院创新基金(批准号：1731230300009)资助的课题.

† E-mail：hqma@aphy.iphy.ac.cn

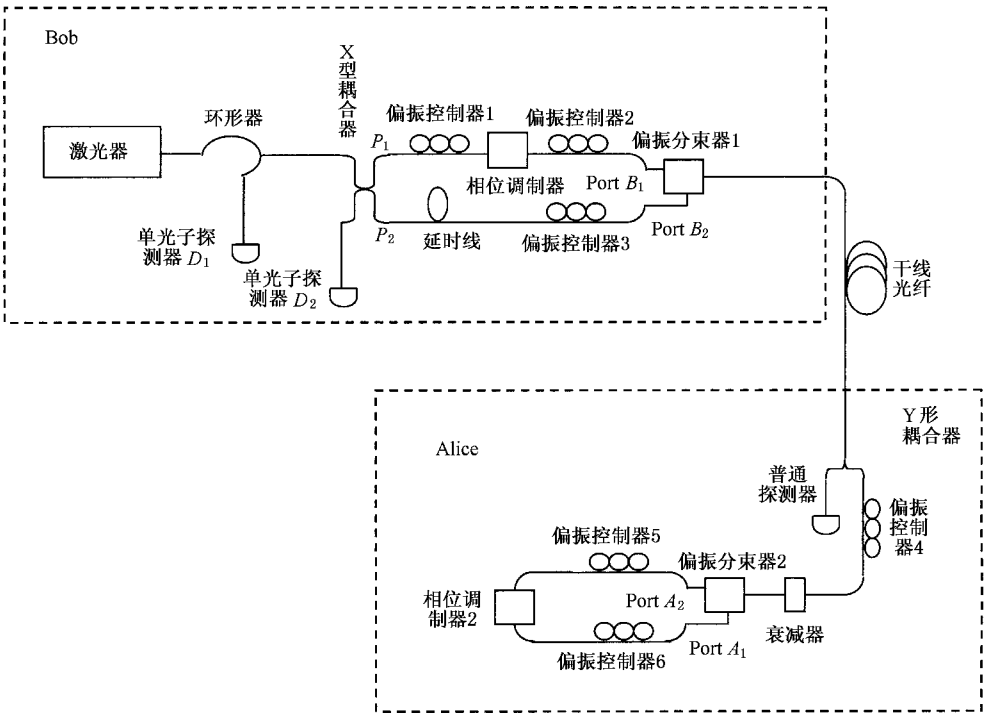

图 1　实验光路原理图

线、Y形耦合器、偏振控制器 4 和衰减器到偏振分束/耦合器 2，分别从偏振分束/耦合器 2 的输出口 Port A_1，Port A_2 输出并且分别沿着顺时针方向与逆时针方向在 Sagnac 环中传播. Sagnac 环由偏振分束/耦合器 2、偏振控制器 5、相位调制器 2、偏振控制器 6 组成. 这样设计 Sagnac 环的原因是由于相位调制器 2 单偏振工作状态和具有偏振相关损耗，该环的工作原理是从 Port A_1 输出的光经偏振控制器 6 调整其偏振状态与相位调制器 2 单偏振工作状态一样，同样从 Port A_2 输出的光经偏振控制器 5 调整也将其偏振状态与相位调制器 2 单偏振工作状态一样，这样顺时针、逆时针方向的光均可以通过相位调制器 2，由偏振控制器工作的可逆性可知顺时针、逆时针方向的光脉冲从该环中绕一圈后就互换了偏振状态，再经过偏振分束/耦合器 2 返回时就实现了偏振自动补偿. 根据普通探测器示数，调整衰减器，使返回时光脉冲近似成为单光子源. 利用普通探测器监视到来的光脉冲的另一个优点是：如果窃听者 Eve 向系统发送强度大得多的光脉冲并试图测量返回来的光脉冲的相位，Alice 就能够检测到 Eve 妄想获得相位的企图. Alice 为了给她的比特编码，使用相位调制器 2 只调制光脉冲 P_1 的相位. Bob 使用另一个相位调制器 1 只对 P_2 进行调制，然后观察 P_1 与 P_2 的干涉结果，并通过单光子探测器 D_1，D_2 进行探测. 如果 Alice 和 Bob 各自的相位调制器都没打开，那么干涉结果为相长干涉（两个脉冲经过了完全相同的路径）即 $\phi_A - \phi_B = 0$，其中 ϕ_A 和 ϕ_B 分别为 Alice 和 Bob 引入的总的相移，此时单光子探测器 D_1 有计数. 如果 Alice 和 Bob 改变了干涉脉冲之间的相位，即 $\phi_A - \phi_B = \pi$，则干涉结果将变为相消干涉，单光子探测器 D_2 有计数. 这就是说，相关的相位调制了 D_1，D_2 处的光强，可以用来从 Alice 向 Bob 传送信息. 这套装置的第一特性是干涉仪自动调整的，因为两个干涉光脉冲都是通过同一条路经传播的；第二个特性是利用 Lefever 光纤偏振控制器的可逆性工作特点，解决了铌酸锂波导式相位调制器的偏振相关性以及偏振相关损耗的问题.

3. 实验装置

实验所用激光器为 Advanced Laser Diode Systems PIL131DFB-SM，工作的中心波长是 1310nm，线宽为 0.1nm，光脉冲宽度约为 10ps，重复频率 500kHz，平均功率约为 500nW. Bob 侧的单向损耗约为 7dB，标准的通信光纤在 1310nm 通信窗口的损耗约为 0.37 dB/km，25km 的通信光纤的单向损耗约为 9.27dB，Y

形耦合器采用的是 50/50% 的光分路器，Alice 侧的环形损耗约为 15 dB. 光脉冲在返回时的平均光功率约为 $500\times10^{-3.5}$ nW，实验时所用的平均每脉冲光子数$\langle n\rangle=0.1$，衰减器的衰减量为 24.5 dB. 造成误码的一个原因就是每个连接处的回波损耗，这些回波损耗最终会到达单光子探测器 D_1，D_2，虽然都是在不同的时刻，通过控制探测器的开门时间可以有效地分辨开，但很难彻底消除掉，只能尽量降低回波损耗. 实验系统在 Bob 侧大部分采用 FC/APC 连接器(APC 类型连接器采用斜 8°的端面，反射光根据非涅尔公式理论上可以降到 118 dB，实验中通常是 68dB).

实验所用偏振控制器为光纤线圈式结构(天津大学精密仪器系生产)，由三个可旋转的波片组成，一个 $\lambda/2$ 波片处于两个 $\lambda/4$ 波片中间，通过调整波片的相对角度就能获得任何希望得到的输出偏振态. 相位调制器为重庆中国电子科技集团公司第四十四研究所生产，工作于单线偏振状态，器件的输入、输出口均用保偏光纤. 自制相位驱动电路，半波电压约为 4V，计算机控制模拟开关，选择 0，2.2，4.2，6.4V 分别实现 0，π/2，π，3π/2 的相位.

单光子探测器管芯是 JDS Uniphase EPM 239BA 的 InGaAs 雪崩二极管，自制外围电路，工作于门控有源抑制的盖革模式下，工作温度 −62.5℃，采用双门符合计数，门控脉宽 95ns，计数门宽 30ns，暗计数为 6×10^{-7} ns^{-1}，输出为 TTL 电平.

主控方 Bob 与从控方 Alice 由两台计算机来完成，分别控制相位调制器 1，2，主控方同时还要完成数据的采集任务. 单光子探测器 1，2 的门控信号，相位调制器 1，2，两台计算机工作在与激光器光脉冲同步的电脉冲时钟下. 在实验室内，计算机间的握手线、同步时钟由同轴电缆线和延迟芯片来传递.

4. 实验结果

在干涉实验测试中，不给相位调制器 1 加驱动电压，给相位调制器 2 加幅度可调的方波 0 —5.8 V 驱动电压，从干涉输出口单光子探测器 D_1，D_2 的计数情况如图 2 所示.

从图 2 可以看出，本实验所用 1310nm 波段铌酸锂相位调制器的半波工作电压约是 4.2V.

在系统的稳定性测试过程中，给相位调制器 1 和 2 均加半波电压，近三个小时的测试过程中，该系统的干涉对比度始终保持在 99.4% 以上. 测试曲线如图 3 所示.

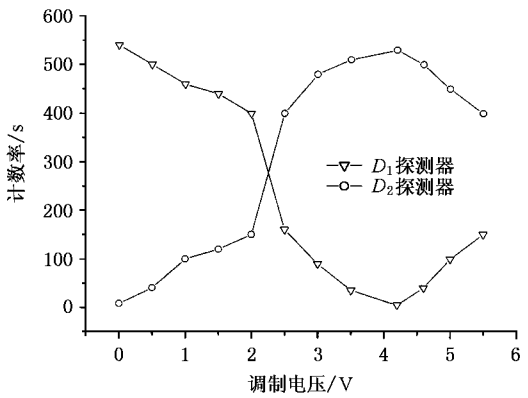

图 2 相位调制器工作图

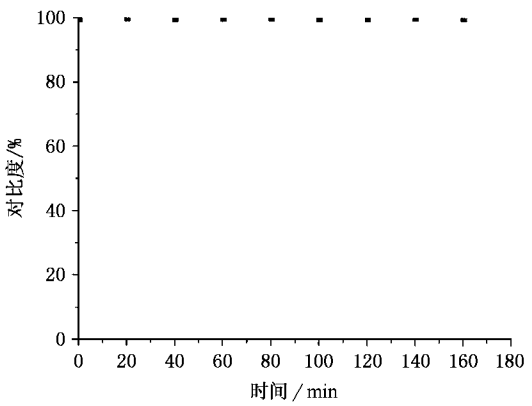

图 3 系统干涉稳定图

在密钥的生成过程中，采用 B92 协议的相位编码方案，Alice 利用计算机产生的二进制伪随机数驱动相位调制器 2 对光脉冲 P_1 进行 0，π/2 相位调制，Bob 则利用另一个相位调制器 1 对光脉冲 P_2 进行 0，π/2 相位调制. 总相位差为零时，即 Alice，Bob 利用(0，0)或(π/2，π/2)调制，干涉为相长干涉，只有单光子探测器 1 有计数. 当 Alice，Bob 利用(0，π/2)或(π/2，0)调制时，单光子探测器 D_1，D_2 以相同概率(50%)探测到光子. 模拟通信双方 Alice，Bob 通过该量子信道得到了密钥生成率 0.6kbit/s，误码率 0.5%.

5. 结 论

本文利用了偏振分束器的分束和耦合特性以及光纤圈式偏振控制器的可逆工作特性，构建了一套

1310nm 波长全光纤的量子密钥分发实验系统，有效地解决了相位调制器的偏振依赖性问题. 经过 25km 的通信距离之后该系统的干涉对比度仍很高，在三小时内保持在 99.4% 以上，有效密钥生成率大于 0.6kbit/s，误码率 0.5%，已达到国际水平. 下一步的任务是进一步优化实验装置，提高系统的抗干扰能力，使量子密钥分发技术早日成为实用化的信息加密设备.

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Internat. Conf. Computers, Systems and Signal Processing* (Bangalore, New York, IEEE)

[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[3] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H *et al* 1992 *J. Cryptol.* **5** 3

[5] Ekert A K, Rarity J G, Tapster P R and Palma G M 1992 *Phys. Rev. Lett.* **69** 1293

[6] Townsend P D, Rarity J G and Tapster P R 1993 *Electronics Lett.* **29** 634

[7] Shao J and Wu L A 1995 *Quantum Optics* **1** 41 (in Chinese) [邵进、吴令安、量子光学 1995 **1** 41]

[8] Muller A, Zbinden H and Gisin N 1996 *Europhys. Lett.* **33** 335

[9] Hughes R J, Morgan G L and Peterson C G 2000 *J. Mod. Opt.* **47** 533

[10] Liang C *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁创 等 2001 物理学报 **50** 1429]

[11] Hiskett P A *et al* 2001 *J. Mod Optics* **50** 1957

[12] Hughes R J *et al* 2002 *New J. Phys.* **4** 43

[13] Kosaka H *et al* 2003 *Electron. Lett.* **39** 1199

[14] Zhou C, Wu G and Zeng H 2003 *Appl. Phys. Lett.* **83** 1692

[15] Wu W *et al* 2004 *Quantum Optics* **10** 135 (in Chinese) [吴　伟 等 2004 量子光学 **10** 135]

[16] Muller A *et al* 1997 *Appl. Phys. Lett.* **70** 793
Zbinden H *et al* 1997 *Electron. Lett.* **33** 586

[17] Kimura T *et al* Los Alamos eprint quant-ph/0403104

[18] Mo X F *et al* Los Alamos eprint quant-ph/0412023

[19] Kurtsiefer C *et al* 2002 *Nature* **419** 450

A quantum key distribution system based on two polarization beam splitters*

Ma Hai-Qiang[1)†]　Li Ya-Ling[1)2)]　Zhao Huan[1)3)]　Wu Ling-An[1)]

[1)] (*Laboratory of Optical Physics, Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*)

[2)] (*Beijing Jiaotong University, Beijing* 100044, *China*)

[3)] (*South East University, Nanjing* 210096, *China*)

(Received 24 March 2005; revised manuscript received 27 April 2005)

Abstract

We present a quantum key distribution system based on two polarization beam splitters, by means of which the phase modulator's polarization dependence is cancelled out. A high key generation rate has been obtained for the first time at 1310nm transmitted over a 25 km long fiber, with a fringe visibility of 99.4%. A sifted key rate of about 0.6 kbits/s and quantum bit error rate of about 0.5% are obtained.

Keywords: quantum key distribution, polarization beam splitter, single photon interference

PACC: 0365, 4230, 4250

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2001CB309301) and by the Chinese Academy of Sciences (Grant No. 1731230300009).

† E-mail: hqma@aphy.iphy.ac.cn