第 57 卷 第 7 期 2008 年 7 月
1000-3290/2008/57(07)/4214-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.57, No.7, July, 2008

稳定的低噪声自由空间量子密钥分配实验研究*

王金东[1)†] 路 巍[2)] 赵 峰[1)] 刘小宝[1)] 郭邦红[1)] 张 静[1)] 黄宇娴[1)] 路轶群[1)] 刘颂豪[1)]

1)(华南师范大学信息光电子科技学院光子信息技术广东省高校重点实验室,广州 510631)

2)(中国科学院合肥智能机械研究所,合肥 230031)

(2007 年 11 月 12 日收到;2007 年 12 月 6 日收到修改稿)

基于量子密钥分配的基本原理,采用偏振短脉冲相干光源和双 FM 差分密钥分配的方案,进行了自由空间量子密钥分配的实验研究. 该方案具有噪声低,稳定性高,误码率低等优点,为空间量子保密通信提供了一个有意义的实施方案,具有一定的实用价值和学术意义.

关键词:量子保密通信,量子密钥,自由空间,差分相位编码

PACC:4250,0367,4230Q,0760

1. 引 言

量子保密通信的想法是 1983 年由 Stephen Wiesner 提出. 紧接着,量子保密通信第一个协议于 1984 年由 Bennett 和 Brassard 提出[1],其实验可行性验证由 Bennett 和他的合作者于 1989 年完成,实验结果在三年后发表[2]. 自此,量子保密通信在短短二十多年时间里得到了迅猛发展. 2000 年美国 Los Alamos 实验室在自由空间成功实现了传输距离为 1.6 km[3] 的 QKD 系统的运行,2002 年 Kurtsiefer 实现了自由空间 23.4 km 的量子通讯[4]. 2004 年,苗二龙等人完成了室内自由空间相位编码量子光通讯[5],同年,吴伟等人也实现了基于偏振编码的室内自由空间量子密钥分配[6]. 2006 年文献[7]在相距 144 km 的两海岛间实现了自由空间量子密钥分配,由于自由空间量子密钥传输对将来利用卫星进行量子密钥分配并进而建立全球量子保密通信网具有重大意义,所以,在自由空间进行量子密钥分配引起了人们的广泛关注和深入研究. 其关键难度主要来自大气、卫星的轨道运动跟踪以及太阳光背景干扰,影响了实用性和可靠性. 我们采用偏振短脉冲传输和窄门控技术抑制太阳光背景,减少噪声干扰,另外接收端 Bob 方采用双 FM 往返式干涉仪差分系统,自动补偿振动和偏振漂移的影响,提高了自由空间量子密钥分配的稳定性和实用性,有很好的实用价值.

2. 自由空间差分相位量子密钥分发系统实验研究

图 1 是自由空间差分相位量子密钥分发实验系统框图,图中 PBS_1 和 PBS_2 为偏振分束耦合器,PM_1 和 PM_2 为相位调制器,ATT 为光衰减器,量子信道为自由空间,CIR 为环行器,C 为耦合器,FM_1 和 FM_2 为法拉第反射镜,D_1 和 D_2 为单光子探测器. 连续激光经过偏振型强度调制器后产生确定偏振方向的短脉冲,此脉冲在衰减至准单光子源后进行差分相位编码,在接收端 Bob 方采用双 FM 往返式干涉仪差分系统,自动补偿振动和偏振漂移的影响.

2.1. 偏振型强度调制器[8]

我们采用偏振型强度调制器调制连续激光,产生相干多脉冲. 偏振型强度调制器由相位调制器(PM)、偏振分束/合束器(PBS_1/PBS_2)、电压控制器、45°和 135°线起偏/检偏器与保偏光纤组成,如图 2 所示.

波长为 1.55 μm 的连续激光经 45°线起偏器起偏,经分束器 PBS_1 后分成振幅相等且偏振方向互相垂直的两束线偏振光,之后经过相等光程光纤,在合束器 PBS_2 处合束,其电场可表示为

* 国家重点基础研究发展计划(973)项目(批准号:2001CB309302)和高等学校博士学科点专项科研基金(批准号:20050574001)资助的课题.

† 通讯联系人. E-mail:jindongwqkd@126.com

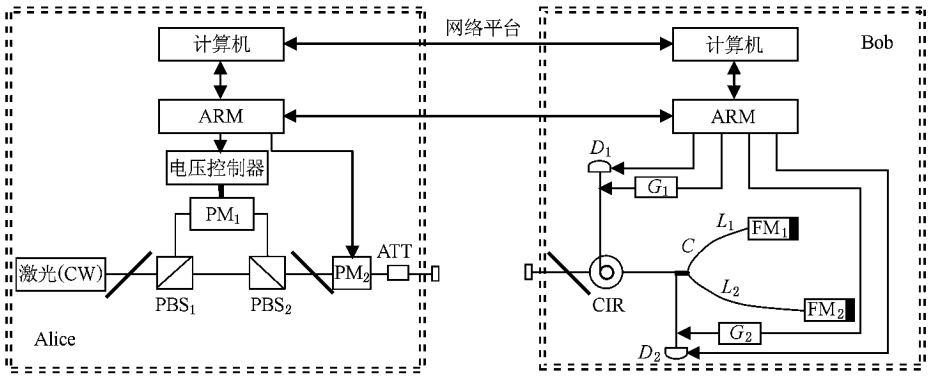

图 1　自由空间差分密钥分发的实验方案框图

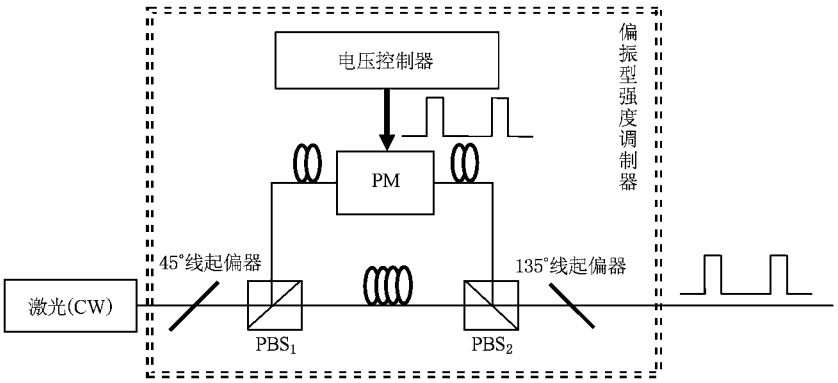

图 2　偏振型强度调制器示意图

$E_x = E_{x_0} e^{i(\omega t - kz + \phi_{x_0})}$，$E_y = E_{y_0} e^{i(\omega t - kz + \phi_{y_0})}$.

用矩阵形式表示为 $E = \frac{\sqrt{2}}{2} E_0 \begin{pmatrix} 1 \\ e^{i\phi} \end{pmatrix}$，其中，$E_0^2 = E_x^2 + E_y^2$，$\phi = \phi_{y_0} - \phi_{x_0}$，因两束光经历相同光程的光纤，$\phi$ 实际为相位调制器 PM 的调相值. 调节相位调制器 PM 的输入电压，使其在 0—2 V_0（V_0 为相位调制器的半波电压）连续变化时，相位调制器 PM 产生 0—2π 的相位变化，则在偏振合束器 PBS_2 上相应输出光的偏振态将在 45°线偏振—左旋椭圆偏振—左旋圆偏振—135°线偏振—右旋椭圆偏振—右旋圆偏振的范围内连续变化，如图 3 所示.

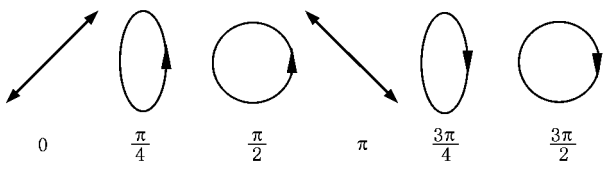

图 3　不同的 ϕ 对应输出不同的偏振态

我们只选取其中两个状态：

1）若相位调制器的输入电压 $V = 0$ 时，对应 $\phi = 0$，出射光为 45°线偏振光，经过 135°线检偏器出来后，光强 $I = 0$.

2）若相位调制器的输入电压为 $V = V_0$ 时，对应 $\phi = \pi$，出射光为 135°线偏振光，经过 135°线检偏器出来后，光强 $I = E_0^2$. 相位调制器输入电压和偏振型强度调制器输出光强的对应关系如图 4 所示.

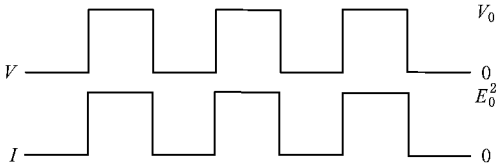

图 4　输入电压和输出光强的对应关系

可见，连续激光经过偏振型强度调制器后变成相干的偏振脉冲串，已实现频率为 1 MHz、脉宽数纳秒到 1 μs 的脉冲串，可作为差分密钥分配的相干脉冲光源.

2.2. 自由空间差分相位量子密钥分发系统

我们采用的自由空间差分相位量子密钥分发实验方案如图 1 所示. 连续激光经过偏振型强度调制器后输出 135°线偏振相干激光脉冲序列,相邻脉冲的间隔时间为 T. 相干脉冲经过光衰减器衰减至每脉冲光子数为 0.1,衰减后的准单光子源经过 PM_2 进行(0,π)随机调相后进入自由空间传输. 在 Bob 端,采用 135°的线检偏器进行背景光的空间滤波后,被光分束耦合器 C 等概率地分为两路,分别经过两个法拉第反射镜反射后在耦合器 C 处进行干涉. 要求双 FM 干涉仪的两臂光程差 $\frac{2(L_2-L_1)n}{c}=T$,这样在耦合器 C 处,Alice 发出的经过调相的相干脉冲序列就会和延迟时间 T 后的脉冲序列进行干涉,干涉结果取决于相位调制器 PM 在相干脉冲序列相邻两个脉冲上的相位差. 两个 ARM 用小于 5 m 的双绞线同步,公用通道由网络平台连接两台计算机完成. 通信时 Alice 通过网络平台和 Bob 握手,然后指令 ARM 启动密钥分配.

量子密钥分配过程为:1) Alice 通过网络平台和 Bob 握手,并指令 ARM 启动 QKD 程序;2) Bob 端的探测器从第二个脉冲时刻处开始有响应,这样,Bob 记录下每个脉冲时刻哪个探测器(D_1 或 D_2)发生响应;3) Bob 告诉 Alice 探测器有效响应(只有一个探测器有响应称为有效响应,其他情况,如两个探测器都有响应或都没有响应则做丢弃处理)的时刻;4) 从以上信息以及 PM_2 的调制数据,Alice 就可以知道每个脉冲时刻 Bob 端究竟是哪个探测器发生响应;5) 假设探测器 D_1 发生响应代表‘0’,而探测器 D_2 发生响应代表‘1’,这样,Alice 和 Bob 就拥有了一组可以作为密钥的字符串. 显然,整个量子密钥分配过程中,Alice 和 Bob 只是向外公布了一系列时刻数据,最后生成的字符串信息并没有泄露给外界. 因在实验室做空间通信,公用信道仍采用网络平台,ARM 采用小于 5 m 的双绞线进行同步. 发射端用光纤准直镜(M)送发,BOB 接收端用 Φ100,焦距 200(F) 的透镜聚焦在光纤准直镜 N 上进入双 FM 干涉仪.

Alice 端用偏振型强度调制器对连续激光进行调制,产生 N 个在时间上均匀分布的相干偏振光脉冲,脉冲时间间隔为 T,之后被相位调制器 PM_2 随机调相(0,π). Bob 端采用双 FM 干涉仪代替传统的 M-Z干涉仪,相干光脉冲序列被调相和衰减后经自由空间传输进入 Bob 端,经过耦合器 C 后,以相同的概率分成两路,然后经两臂末端的法拉第反射镜反射至 C 处发生干涉. 干涉结果取决于从 Alice 出射的相邻两个脉冲之间的相对相位. 当相对相位为 0 时,探测器 D_1 探测到光子,当相对相位为 $\pm\pi$ 时,探测器 D_2 探测到光子. Alice 和 Bob 靠嵌入式计算机 ARM 和公用信道完成密钥分配,双方 ARM 获得各自密钥通过 RS232 端口分别送入计算机. Alice 和 Bob 采用此密钥对明文进行加密解密通信. 在实验室暗室条件下误码率小于 6%,所生成的密钥如表 1 所示.

表 1 实验生成的密码表

Alice
B0 B0 B0 B0 B1 B2 B3 B4 55 AA D2 5E 3A EE 1E 3A 52 DE 1E E6 AA 12 12 7E 2E A6 7A 4E 12 9E 8A B6 16 6E F6 F2 AA DE 96 56 CE 0A F2 42 96 DA 96 76 5E D2 FA 9A 12 16 9E 32 CA 7E D6 92 9A EE AA 9A AA 9E 7A 4E 22 6E E6 EA DA CA 92 AA 5A BE 6E E6 2E 52 22 B2 BE 4A 32 1E 16 5A CE B2 AE 26 C6 2A 1E 5E BE 16 16 16 6E 16 D2 E6 86 0A 3A BA 4A 32 EA 1E F6 76 7E 82 C6 7E DA 62 36 3E FE 02 9E 32 FE 46 9A EE DE 3E 1E C2 2A 1A 55 AA
Bob
B0 B0 B0 B0 B1 B2 B3 B4 55 AA D2 5E 3B AE 1E 3A 82 DE 1E E6 AA 02 12 7A 21 A6 7A 4E 12 9E 8A B6 16 6E F6 F2 AA DE 96 56 CE 0A F2 42 96 DA 96 76 5E D2 FA 9E 12 76 9E 32 CF 7E D6 72 9A 1E AA 9A AA 9E 7A 4E F2 6E E6 EA DE CA 9F AA 5A BE 6E E6 FE 52 22 BD BE 4F 32 FE 16 5A CE B2 FE 26 C6 7A FE 5E BE 16 E6 16 6E 16 D2 E6 86 1A 3A BA 4A 72 EA 1E F6 76 7A 8F C6 1E DA 62 36 3E FA 12 9E 32 FE 46 9F EE DE 3E 1E C2 2A 1A 55 AA

3. 讨 论

3.1. 稳定性讨论

差分相位编码中,比特信息总是存在于两个相邻脉冲之间的相位差. 影响激光脉冲相位和偏振的大气变化一般是慢过程起主要作用,因此间隔很短的相邻脉冲在大气中传输的过程可以认为经历了相同的相位变化和偏振变化. 只要脉冲的时间间隔远小于光传输中温度压力等因素变化的时间常数,相邻脉冲总是以相同的偏振态到达,而这一条件在实际的系统中是可以得到满足的. 因此,差分相位编码的特性保证了较好的干涉可见度,激光脉宽选得适当可以使得干涉可见度不因大气环境影响而发生

较大的变化. 另外，我们的方案中，Alice 端节省了干涉仪，改用偏振型强度调制器对激光进行调制，对光的偏振态和相位进行精确补偿，从而有效降低误码率. 而 Bob 端采用双 FM 干涉仪代替传统的 M-Z 干涉仪，自动补偿了该端的偏振抖动，提高了干涉稳定度. 文献[9]已在理论和实验上证明了这一点.

由此可见，差分相位编码的特性，偏振型相位调制器的使用和 Bob 端的来回往返机理相结合，自动补偿了环境变化带来的偏振抖动和相位漂移，提高了系统的稳定性，实现了高稳定的密钥分配.

3.2. 系统安全性分析

差分相位编码 QKD 系统的安全性已经得到部分的证明[10—12]. 从量子机理上讲，当平均光子数小于 1 的相干脉冲之间携带的相位信息相反时，它们是相互非正交的. 而非正交态不能通过单次测量得到区分这一事实保证了差分相位编码 QKD 系统的安全性. 在 Alice 和 Bob 共享密钥之前，他们抽取出其中一小部分密码通过公共信道进行比对，探测误码，以检测是否存在窃听. BB84 方案的密钥生成效率仅有 1/4，也就是说，在 BB84 协议中，只有 1/4 的码能被检测到，而差分编码的密钥生成效率为 $1-1/N$，相应地，探测到码的概率也为 $1-1/N$. N 越大，成码率越高. 在实验中 N 可随机选取，N 越大，系统抗窃听的能力就越强. 我们在方案中采用的方式是 Alice 随机发送任意个弱相干光的脉冲串，可以选择相干脉冲的个数 N，当 N 很大时，Bob 探测到窃听存在的概率接近 1. 另外，发送脉冲串的时间间隔也是随机的，这样就增加了 Eve 窃听的难度，大大提高了系统的安全性.

3.3. 低噪声

在自由空间量子密钥分配实验中，太阳背景干扰是一个极为严重的问题. 虽然可以使用窄带干涉滤光片来减小背景干扰. 即便在一般实验室环境中阳光背景仍然是个重要问题. 本实验考虑到用偏振短脉冲传送，借助门控技术，减少阳光背景噪声. 实验证明偏振传送/偏振光接收方式可以使得背景噪声减小到 1/4—1/5，采用纳秒量级脉冲和门控技术的单光子探测器，背景噪声可以减小一个量级. 但由于大气抖动影响光程漂移，若脉冲宽度取得更小(如皮秒脉冲)，双 FM 干涉仪相干条纹稳定度和能见度明显变坏，大气抖动不能忽略.

4. 结　论

实验采用偏振短脉冲差分方案在 1.55 μm 波段上完成了自由空间量子密钥分配. 用双 FM 反射镜干涉仪作差分接收可以补偿振动引起的偏振漂移. 偏振传送/偏振接收的方式可以有效降低阳光背景噪声. 实验表明该系统稳定性好，采用纳秒级脉冲和单光子探测器门控技术可减少背景噪声，有很好的应用前景.

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, New York: IEEE 175

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

[3] Buttler W T 2000 *Phys. Rev. Lett.* **84** 5652

[4] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P R, Rarity J G 2002 *Nature* **419** 450

[5] Miao E L, Mo X F, Gui Y Z 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙、莫小范、桂有珍 2004 物理学报 **53** 2123]

[6] Wu W, Liu W T, Feng S H, Ou B Q, Liang L M, Li C Z 2004 *Acta Sinica Quantum Optica* **10** 135 (in Chinese) [吴　伟、刘伟涛、冯少晖、欧保全、梁林梅、李承祖 2004 量子光学学报 **10** 135]

[7] http://arxiv.org/abs/quant-ph/0607182

[8] Lin Y M, Liang R S, Lu Y Q, Lu H, Guo B H, Liu S H 2007 *Acta Phys. Sin.* **56** 3931 (in Chinese) [林一满、梁瑞生、路轶群、路　洪、郭邦红、刘颂豪 2007 物理学报 **56** 3931]

[9] 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]

[10] Inoue K, Waks E, Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[11] Acin A, Gisin N, Searani V 2004 *Phys. Rev.* A **69** 012309

[12] Inoue K, Honjo T 2005 *Phys. Rev.* A **71** 042305

The experimental research on a stable free-space quantum key distribution system with low noise *

Wang Jin-Dong[1)†] Lu Wei[2)] Zhao Feng[1)] Liu Xiao-Bao[1)] Guo Bang-Hong[1)] Zhang Jing[1)]
Huang Yu-Xian[1)] Lu Yi-Qun[1)] Liu Song-Hao[1)]

1)(*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510631, *China*)

2)(*Institute of Intelligent Machines, Chinese Academy of Sciences, Hefei* 230031, *China*)

(Received 12 November 2007; revised manuscript received 6 December 2007)

Abstract

A free-space quantum key distribution system is demonstrated experimentally which makes use of polarized coherent short laser pulses and the differential phase shift scheme with a Faraday-Michelson interferometer. The system features low noise, high stability and low bit-error rate. In the proposed experimental scheme, polarizated short laser pulse of several nanoseconds duration is made to transmit through the free space to decrease noise and a low bit-error rate less than 6% is achieved.

Keywords: quantum cryptography, quantum key distribution, free space, differential phase shift
PACC: 4250, 0367, 4230Q, 0760

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2001CB309302) and by the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20050574001).

† Corresponding author. E-mail: jindongwqkd@126.com