第 55 卷 第 9 期 2006 年 9 月
1000-3290/2006/55(09)/4642-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.55,No.9,September,2006

高稳定的差分相位编码量子密钥分发系统

李明明 王发强† 路轶群 赵 峰 陈 霞 梁瑞生 刘颂豪

(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)

(2006 年 1 月 9 日收到;2006 年 3 月 1 日收到修改稿)

在差分法基础上提出了一种改进的差分相位编码量子密钥分发(QKD)方案. Alice 采用脉冲激光光源,通过两个串联光纤延迟环产生四个均匀的相干脉冲,并对脉冲进行差分调制,补偿了传输过程中环境对偏振的扰动. Bob 采用双 FM 干涉仪,在窄脉冲门控模式下进行单光子探测. 单程传输避免了木马攻击,增强了方案的安全性. 实验结果表明,系统可以长期稳定运转(大于 24h),误码率为 3%. 改进的系统具有高效、稳定、低成本的优点,实施方便,有很好的实用价值.

关键词:量子保密通信,量子密钥分发,差分相位编码

PACC:4250,4230Q,4210J,0365

1. 引 言

量子密码术是量子物理和密码学相结合的产物,它是在异地授权双方间无条件安全分发密钥的唯一方法. 自 1984 年 Bennett 和 Brassard 提出量子密钥分发(QKD)协议[1] 以来,量子密码术得到了广泛深入的研究并一步步向实用化迈进. 美国的 MagiQ 公司和瑞士的 idQuantque 公司已经开始有部分产品进入市场[2],2005 年基于量子加密技术的网络安全芯片已经面世[3]. 可以说 QKD 已经成为量子信息最成熟的研究领域.

在国内,量子保密通信也有很大进展,中国科学院物理研究所[4] 和华东师范大学相继完成了远距离的'即插即用'系统,后者同时提出了高效的密钥分配方案[5—7] 并实现了稳定的长距离 QKD 系统[8];中国科技大学提出了 Faraday-Michelson 系统[9],完成了长距离的量子保密通信. 2002 年,Inoue 等人提出了差分相位编码的 QKD 方案[10],适合实现于光纤线路,继承了相位编码方案编码的速度快、抗干扰能力强、单程传输不受木马攻击、极限传输距离远的优点,对码生成效率有很大的提高. 我们提出了一种改进的差分相位编码 QKD 系统,比以往的差分相位编码 QKD 系统[5,6,10,11] 更加稳定.

2. 差分相位编码方案

差分相位编码 QKD 系统因其高效的优势备受瞩目,提出了各种基于差分相位编码的实验方案[5,6,11]. 为了实现更稳定、安全的差分相位编码 QKD 系统,我们提出了一种改进的差分相位编码 QKD 实验方案,见图 1. 图中 LD 是脉冲激光器,PM 为相位调制器,G 为门控装置,C_1-C_5 为耦合器,FM_1,FM_2 是法拉第镜,D_1,D_2 为单光子探测器.

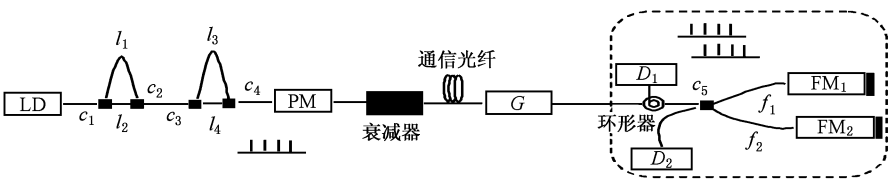

图 1 改进的差分相位编码 QKD 方案

† 通信作者. E-mail:fqwang98@sina.com

激光脉冲光源 LD 发出的脉冲光入射两个光纤环,在光纤环中经不同的路径(l_2,l_4),(l_1,l_4),(l_2,l_3),(l_1,l_3)到达耦合器 C_4 处时,成为相干的多脉冲.设计两个光纤环的臂长满足

$$l_3 - l_4 = 2(l_1 - l_2), \tag{1}$$

就可以得到分布均匀的四个相干脉冲,如图中所示.这样就实现了相干脉冲光源.

多脉冲幅度相等时才能有较好干涉对比度和稳定的系统性能.我们提出的改进方案,由于两个光纤环的臂长差不同,实现了脉冲在时域、空域上的无重叠地均匀分布,入射到相位调制器 PM 中的脉冲是等幅度的,在双 FM 干涉仪上保证了良好的干涉对比度.该方案并不需要以增加相位调制器和占用系统资源为代价,具有很好的实用前景.

2.1. 密钥分配方案

通常,差分相位调制 QKD 方案[4—7,11]中,Bob 端允许脉冲串全部通过.脉冲的透明传输使协议效率得到了最大限度的提高,但脉冲个数和干涉模式的确定性也给窃听者的窃听带来了方便,给系统安全性带来了隐患.为了搭建既高效又安全的差分相位调制 QKD 系统,我们在 Bob 端采用了窄门控技术,采用多模式的脉冲传输来提高系统的安全性.图 2 是门控方案图,其中 m 为方案(1)被选中的比例,$0 < m \leqslant 1$,方案(2)—(4)被选中的比例为$(1-m)/3$.

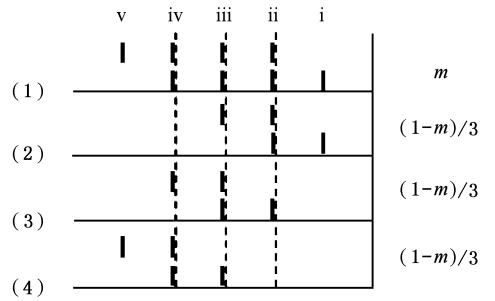

图 2　Bob 端的门控方案

Bob 端采用如图 2 所示的四种方案选择性地开启门控装置.方案(1)中,允许四个脉冲全部通过,方案(2)—(4)选择性地允许相邻脉冲通过.Bob 端随机采用以上四种方案,抗窃听能力得到了提高,增强了系统的安全性.

与基本协议不同的是,Alice 和 Bob 间事先有一个绝对安全的密码本,规定了 Bob 端如何选择开启门的方案.Bob 端选用方案(1)时,将告知 Alice 探测器探测到光子的时刻;在选用方案(2)—(4)时,Bob 只要告知 Alice 是否探测到光子的时刻,Alice 结合规定的方案次序和 Bob 的探测结果,就知道是哪个探测器响应,Alice 和 Bob 双方就获得一致的密码本序列.

传统的四脉冲差分相位调制 QKD 系统的协议效率为 3/4[7].改进方案采用了门控技术.因为方案(2)—(4)只分别在 ii,iii,iv 时刻才能干涉,这样协议的效率不可避免的要降低.基于门控技术的改进差分相位编码 QKD 系统的协议效率可用下式计算:

$$\eta_G = \frac{1}{4} + \frac{m}{2}, \tag{2}$$

可见协议效率 η_G 与 m 成线性关系,只要调整 m 的大小就可以控制协议效率.

2.2. 稳定性分析

差分相位编码 QKD 方案是用相邻脉冲的相位差来携带信息.脉冲在光纤传输过程中经历相同的相位、偏振变化,因此光纤中的起伏对相邻脉冲的相位差和相对偏振影响很小,这样就保证了差分相位编码 QKD 系统的干涉稳定性[10].这种相邻脉冲之间的互补偿只能对于时间为几十纳秒的快过程有效,并不能补偿环境因素引起的长周期性变化.但由于这个周期较之脉冲宽度很长,对系统的稳定性危害较小.

相位编码 QKD 实验方案一般使用 MZ 干涉仪,因此保证稳定的干涉对比度对于降低系统误码率至关重要.然而光纤中存在随机双折射,并且环境对 MZ 干涉仪的干扰是随机的,尤其是温度的变化、振动会引起显著的相位起伏[12].这些都对采用 MZ 干涉仪的系统的稳定性十分不利.以往的差分相位编码 QKD 方案[5—7,10,11]都采用了 MZ 干涉仪,也同样需要解决接收端干涉稳定性的问题.为了改善系统的稳定性,有的方案采用基于平面波导技术的光集成 MZ 干涉仪.我们的改进方案采用双 FM 干涉仪(见图 1 虚框内部分),代替了传统的 MZ 干涉仪,可以提高干涉稳定度.

脉冲由相位调制器 PM 进行‘0’或‘π’相位的调相后,经耦合器 C_5 耦合进两段光纤线路中,经过法拉第镜反射到 C_5 处干涉.只要保证连接法拉第镜的两段光纤长度满足

$$f_2 - f_1 = l_1 - l_2, \tag{3}$$

就可以实现图 1 所示的干涉.根据探测器 D_1 和 D_2

的计数结果,按照差分相位编码协议[10]得到密码本序列.

下面以探测器 D_1 的探测结果为例,分析双 FM 干涉仪对稳定性的影响.

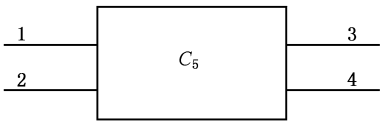

图 3 耦合器端口示意图

图 3 中 1,2 端口为耦合器 C_5 输入端,3,4 端口为输出端.依据耦合波理论[13],耦合器的分散矩阵为

$$J = \begin{bmatrix} \alpha_J & \mathrm{j}\beta_J \\ \mathrm{j}\beta_J & \alpha_J \end{bmatrix}, \tag{4}$$

式中,α_J,β_J 为耦合器的耦合系数,当耦合比为 1∶1 时,$\alpha_J = \beta_J = \sqrt{2}/2$.假设耦合器是偏振无关的,考虑传输损耗,可以得到

$$J_{13} = J_{31} = J_{24} = J_{42} = t_J \begin{bmatrix} \alpha_J & 0 \\ 0 & \alpha_J \end{bmatrix}, \tag{5}$$

$$J_{14} = J_{41} = J_{23} = J_{32} = t_J \begin{bmatrix} \mathrm{j}\beta_J & 0 \\ 0 & \mathrm{j}\beta_J \end{bmatrix}, \tag{6}$$

t_J 为损耗的幅度传输系数.J_{mn}($m,n = 1$—4)表示耦合器从 m 端输入到 n 端输出的 Jones 矩阵.法拉第镜的 Jones 矩阵为

$$F = t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \tag{7}$$

t 为考虑到传输和反射损耗的幅度系数.

考虑光波分别在光纤 f_1,f_2 段传输的过程.低双折射光纤的效应可以看成一个椭圆延迟器,可以写成[13]

$$T_{R,1} = C_1 \begin{bmatrix} a_s & -b_s^* \\ b_s & a_s^* \end{bmatrix}, \tag{8}$$

$$T_{R,2} = C_2 \begin{bmatrix} a_s & -b_s^* \\ b_s & a_s^* \end{bmatrix}, \tag{9}$$

式中 $C_1 = \alpha_{s,1}/d_s$,$C_2 = \alpha_{s,2}/d_s$,$d_s = a_s a_s^* + b_s b_s^*$,$\alpha_{s,1}$,$\alpha_{s,2}$分别为干涉结构中光纤段 f_1,f_2 的传输损耗,a_s,b_s 与光纤的双折射特性有关.当光波由 FM 反射后传输时,双折射效应等效为一个反向的椭圆延迟器,如下:

$$T_{L,i} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} T_{R,i} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = C_i \begin{bmatrix} a_s & -b_s \\ b_s^* & a_s^* \end{bmatrix}, i = 1,2. \tag{10}$$

因此,设入射光波电场矢量为 E_{in},耦合到输出端 3,4 的两路光波经由 FM 反射在光纤段 f_1,f_2 中往返,而后在耦合器 C_5 处的电场矢量分别为

$$E_1 = J_{31} g T_{L,1} g F g T_{R,1} g J_{13} g E_{\mathrm{in}} = t_J^2 t C_1^2 d_s \alpha_J^2 \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} E_{\mathrm{in}} \exp(\mathrm{j}\phi_1), \tag{11}$$

$$E_2 = J_{41} g T_{L,2} g F g T_{R,2} g J_{14} g E_{\mathrm{in}} = t_J^2 t C_2^2 d_s \beta_J^2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} E_{\mathrm{in}} \exp(\mathrm{j}\phi_2) = t_J^2 t C_2^2 d_s \beta_J^2 \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} E_{\mathrm{in}} \exp(\mathrm{j}\pi + \mathrm{j}\phi_2) = \frac{C_2^2}{C_1^2} g E_1 \exp(\mathrm{j}\pi + \mathrm{j}\phi_2), \tag{12}$$

式中 ϕ_1,ϕ_2 分别为光波经上、下支路经历的相位延迟.由于臂 f_1,f_2 长度都比较短,故 $\alpha_{s,1} \approx \alpha_{s,2}$,则 $C_1 \approx C_2$.则(12)式可以重写为

$$E_2 = \frac{C_2^2}{C_1^2} g E_1 \exp(\mathrm{j}\pi + \mathrm{j}\phi_2) \approx E_1 \exp(\mathrm{j}\pi + \mathrm{j}\phi_2). \tag{13}$$

比较(11),(13)式可见,经 f_1 和 f_2 反射至端口 1 的两光波的电场矢量的偏振方向始终相同.如果两信号干涉,不会产生偏振衰落的情形.法拉第镜主动补偿了光纤双折射效应以及偏振相关损耗,因此无需 MZ 系统中的偏振控制技术就可以消除偏振衰落.双 FM 干涉仪偏振稳定度和相位稳定度两方面性能都得到了改善,提高了系统的稳定性,同时继承了差分相位编码的优点,可以单向传输,避免了木马攻击.

2.3. 安全性分析

高度安全的 QKD 系统需要理想的单光子源,但实现理想的单光子源目前技术上还有困难.单光子源的 QKD 系统通常采用强衰减的弱激光脉冲来实现.经过衰减的弱脉冲仍然含有一定数目的多光子.因此,Eve 可以实施所谓的光子数分裂(PNS)攻击[14].PNS 攻击对于广泛采用的 BB84 方案十分有效,它严重限制 QKD 系统的通信距离[14].基于差分相位编码的 QKD 系统不但比传统 BB84 方案的码生成效率高,而且已经证明了使用相干脉冲串的差分

相位编码 QKD 系统能够很好地抵御 PNS 攻击,大大提高安全通信距离[14].

对于用相干弱脉冲实现的差分相位编码 QKD 系统,信息包含于两个相邻的脉冲中,若有 Eve 在进行 PNS 攻击时,需要获得相邻脉冲叠加得到光子.对于含光子数多于两个的相邻脉冲,Eve 就从中取出一个光子并存储起来,让这两个脉冲通过无损信道传向 Bob.而对于其他脉冲,Eve 就全部过滤掉,因此这部分脉冲就不能形成密码比特.这种 PNS 攻击方案会引入 1/4 的误码率.本文提出的差分相位编码 QKD 方案采用了门控技术.在采用方案(2)—(4)时,Bob 端仅通知 Alice 是否测量到光子,则 Eve 只能从 ii,iii,iv 时刻的测量结果中选择一个作为量子比特,这样必然会使得 Eve 获得的信息量减少.当 Bob 端仅使用方案(1)时,设 Eve 实施 PNS 攻击获得的信息量为 I.当 Bob 采用图 3 的门控方案时,Eve 获得的信息量可由下式计算:

$$I' = mgI + \frac{1-m}{3} \times 3 \times \left(\frac{1}{3} \times I + \frac{2}{3} \times \frac{I}{2} \right)$$

$$= \frac{2+m}{3} gI, 0 < m \leqslant 1, \qquad (14)$$

上式可见 $I' \leqslant I$,采用门控方案后,Eve 获得的信息量减小了.当然,减小 m 以阻止 Eve 获得更小的信息量是以降低系统的码生成效率为代价的.我们在通信中要从实际的需求出发,兼顾码生成效率和安全性.

3. 实验和结果

图 4 是我们的实验装置框图.光源使用多通道飞秒二极管激光器(PDL808),脉冲宽度为 50ps,经衰减后每脉冲平均光子数 $N \approx 0.2$.嵌入式模块 ARM_a 触发激光器的重复频率为 75kHz. Alice 端 ARM_a 触发计算机控制相位调制器对脉冲进行随机调相,并经 154ns 延迟后门控 Bob 端单光子探测器(id200).本实验只是对实验方案原理性的证明,故两端机采用了电同步.

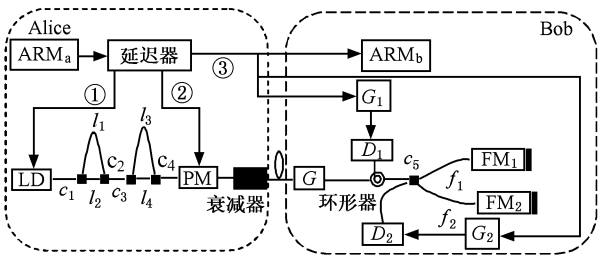

图 4　实验装置框图

表 1 是 Alice 获得的密钥,表 2 是 Bob 端获得的密钥,用十六进制表示.密钥序列为 1028 bit,误码率为 3%.双方利用所得的密钥可以进行量子保密通信.经多次实验,误码率都稳定在 ≤4%.从实验结果分析,该系统性能长期稳定.

表 1　Alice 端密钥本

Alice 端密钥本
BD E5 DD 61 7D E9 45 89 FD 99 01 BD 8D B9 5D 59 35 95 75 B5 E5 D9 85 F9 E1 C9 5D 15 D1 61 E5 55 BD 39 FD 11 7D 19 7D E9 75 A5 25 81 2D 3D 31 2D D9 85 3D 75 C5 F5 DD A5 35 21 A1 01 C1 39 0D 8D 75 A5 9D 11 19 5D 79 61 8D 1D E9 41 31 F9 E1 51 AD 69 49 21 91 0D E1 1D C5 5D 05 F1 ED 11 19 E5 D9 C9 B1 C1 39 21 A1 DD 2D 81 C9 E9 51 DD 2D 41 DD 95 45 75 F9 9D ED 11 D1 51 99 CD 2D 3D 21 6D

表 2　Bob 端密钥本

Bob 端密钥本
BD E5 DD 41 7D C9 45 A9 FD 99 01 BD 8D B9 5D 59 35 95 75 B5 E5 F9 85 D9 E1 C9 5F 15 D1 61 E5 75 BD 3B FD 31 7D 19 7D E9 75 A5 25 81 2F 3D 31 2D D9 85 3D 75 C5 F5 DD A5 35 21 A1 21 C1 39 0D 8D 75 A7 BD 11 39 5D 79 61 8D 1D EB 61 31 FB E1 51 8D 69 4B 21 91 0D E1 1D C5 5F 05 F3 ED 11 39 C5 DB C9 B1 C1 39 21 A1 DD 0D 81 CB E9 51 DD 2D 41 DD 95 65 75 F9 9F EF 13 F1 51 99 CD 2D 3D 21 4D

4. 结　论

差分相位编码 QKD 系统适合在光纤中实现,比传统的方案更高效,能实现更长距离的通信.差分相位编码 QKD 方案的信息是靠相邻脉冲的相位共同决定的,这样就降低了窃听者的成功概率和窃取信息量,增强了 QKD 系统的安全性.本文提出了一种改进的差分相位编码量子密钥分发 QKD 方案,不但具有上述的优势,而且以双 FM 干涉仪代替 MZ 干涉

仪,并证明它可以主动补偿光纤传输中的随机双折射效应和极化相关损耗,消除偏振衰落现象,系统的稳定性得到了提高.窄脉冲门控技术的采用使得脉冲数目和干涉模式实现了多样化,一定程度上改善了系统的安全性,可能是一种实用的长距离量子光通信系统.

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

[2] Opics.org-News. Quantum crypto hits the markets. http://optics.org/articles/news/9/11/10/1

[3] http://www.eetchina.com/ART-8800371086-480801-9d3dbfca-no.HTM

[4] Liang C, Fu D H, Liang B *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁 创、符东浩、梁 冰等 2001 物理学报 **50** 1429]

[5] Zhou C Y, Wu G, Chen X L et al 2003 *Appl. Phys. Lett.* **83** 1692

[6] Chen X L, Zhou C Y, Wu G *et al* 2004 *Appl. Phys. Lett.* **85** 1648

[7] Chen X L, Zhou C Y, Wu G *et al* 2004 *Appl. Phys. Lett.* **84** 2691

[8] Wu G, Zhou C Y, Chen X L *et al* 2005 *Acta Phys. Sin.* **54** 3626 (in Chinese) [吴 光、周春源、陈修亮等 2005 物理学报 **54** 3626]

[9] Mo X F, Zhu B, Han Z F *et al* 2005 *Opt. Lett.* **30** 2632

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

[11] Inoue K, Waks E, Yamamoto Y 2003 *Phys. Rev.* A **68** 022317

[12] Zheng L M, Wang F Q, Liu W P 2005 *Acta Photonica Sincia* **34** 797 (in Chinese) [郑力明、王发强、刘伟平 2005 光子学报 **34** 797]

[13] Liu D M, Xiang Q, Huang D X 1995 *Fibre optics* (Bejing: National Defense Industry Press)

[14] Acin A, Gisin N, Searani V 2004 *Phys. Rev.* A **69** 01230

A highly stable differential phase shift key distribution QKD system

Li Ming-Ming Wang Fa-Qiang† Lu Yi-Qun Zhao Feng Chen Xia
Liang Rui-Sheng Liu Song-Hao

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

(Received 9 January 2006; revised manuscript received 1 March 2006)

Abstract

We propose and demonstrate an improved differential phase shift key distribution scheme. Alice uses a pulsed laser source and two cascaded fiber loops to get coherent pulses, then modulates them randomly under differential phase shift scheme, which compensates for the random polarization mode dispersion and phase shift. An interferometer made up of two Faraday mirrors is employed to detect single photon under gate mode. In one-way transmission, QKD is free from Trojan attack. Our experiment at setup can work stably for a long time (at least 24h) with an error ratio of 3%. The stable scheme is efficient, economical and favorable for practical application.

Keywords: quantum cryptography, quantum key distribution, differential phase shift
PACC: 4250, 4230Q, 4210J, 0365

† E-mail: fqwang98@sina.com