第 56 卷 第 7 期 2007 年 7 月
1000-3290/2007/56(07)/3931-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.7,July,2007

自动补偿高效的差分相位编码 QKD 系统*

林一满[1)2)] 梁瑞生[1)†] 路轶群[1)] 路 洪[2)] 郭邦红[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)(佛山科学技术学院光电子与物理学系,佛山 528000)

(2006 年 9 月 18 日收到;2006 年 11 月 13 日收到修改稿)

提出一种自动补偿高效实用的改进型差分相位编码量子密钥分发方案.在 Alice 端采用偏振型强度调制器对连续激光进行调制,产生任意个相干脉冲进行差分相位调制编码;在 Bob 端采用双 FM 干涉仪代替传统的 M-Z 干涉仪,自动补偿了环境引起的偏振抖动,提高了系统的干涉稳定度.简化了系统的结构,提高了密钥生成效率,增强了系统的安全性.在实验上实现了稳定的 80 km 量子密钥分配,误码率 < 4%.

关键词:量子保密通信,量子密钥分发,差分相位编码,偏振型强度调制器

PACC:4250,4230Q,0365

1. 引 言

量子保密通信区别于经典保密通信的本质特征在于通信双方通过单个量子态传输构成的量子信息通道实现密钥分配;量子力学的量子态不可克隆原理和测不准原理从原理上保证了密码体系的绝对安全性.但实际上并不存在绝对安全的通信方式,如采用单光子量子保密通信,目前的光源采用激光衰减式光源,光子数分布服从泊松分布,原理上就不存在真正的单光子态,即使平均光子数为 0.1,双光子出现概率还有 3%—5%;另外还有环境,探测器等因素影响,安全性也有待研究.从总体来看,相比经典的保密通信方式,如混沌、对称和非对称密钥分配,量子保密通信的安全性能要优于其他方案的安全性能.继 1984 年 Bennett 等人提出第一个量子密钥分配(QKD)协议[1]之后,量子保密通信技术在理论和实验上都得到了蓬勃地发展[2,3].国际上已有两家公司(美国的 MagiQ 和瑞士的 idQuantque)推出产品,均采用'即插即用'系统,但由于背向瑞利散射,密钥分发速率低,同时双向传输无法抵御木马攻击.中国科学院物理所率先在国内实现单光子量子密钥分配[4].中国科技大学提出了双 FM 系统[5],取得了很大的进展.Inoue 等人提出了差分相位编码 QKD 方案[6,7],抗干扰能力强,单程传输免受木马攻击,并且提高了密钥生成效率.华东师范大学提出了高效的密钥分发方案[8—10],开拓了新思路.

我们在差分相位编码[7,11]的基础上,采用偏振型强度调制器产生任意个数的相干多脉冲,提高了成码效率,增加窃听分辨难度,增强了系统的安全性.另外在 Bob 端用双 FM 干涉仪代替其他干涉仪,可以全程自动补偿,提高了抗环境干扰能力.实验上实现了稳定的 80 km 密钥分配和图像传输.

2. 差分相位调制量子密钥分发系统

2.1. 偏振型强度调制器的研究

我们提出一种新的方法,采用偏振型强度调制器调制 CW 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°线起偏/检偏器和保偏光纤组成,如图 1 所示.

CW 连续光(1.55 μm)经 45°线起偏器起偏,经分束器 PBS_1 分成振幅相等且偏振方向互相垂直的两束线偏振光,经过相等光程光纤,在合束器 PBS_2 处合束,其电场可表示为

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

* 国家重点基础研究发展规划(973)项目(批准号:2007CB307001)资助的课题.

† 通讯联系人. E-mail:scnulrs@126.com

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

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.

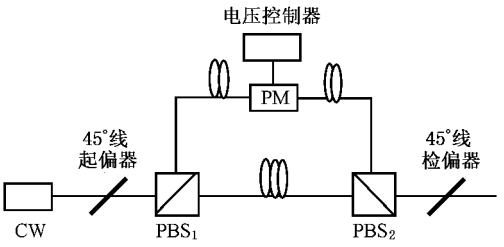

图 1 偏振型强度调制器结构示意图

调节相位调制器 PM 的输入电压，使其在 0—$2V_0$（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 上相应的输出光的偏振态可从 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 2 所示.

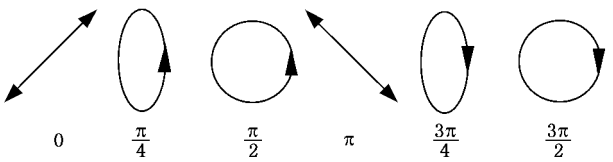

图 2 不同的 ϕ 对应输出不同的偏振态

我们只选取其中的两个状态：

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 45°线检偏器出来后，光强 $I = E_0^2$；

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 45°线检偏器出来后，光强 $I = 0$.

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 3 所示.

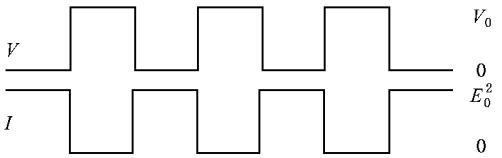

图 3 输入电压和输出光强的对应关系

由此可见，对应相位调制器随机输入 N 个电压脉冲，偏振型强度调制器可以随机输出 N 个相干光脉冲. 只要进行适当的振动隔离，就可以得到稳定的任意个数相干脉冲输出.

2.2. 量子密钥分配方案

我们的实验方案如图 4 所示. 图中 CW 为连续激光器，PM_1，PM_2 为相位调制器，PBS_1/PBS_2 为偏振分束/合束器，ATT 为衰减器，CIR 为环形器，C 为耦合器，FM_1，FM_2 是法拉第反射镜，D_1，D_2 为单光子探测器.

Alice 端用偏振型强度调制器对激光进行调制，随机产生 N 个在时间上均匀分布的相干光脉冲，脉冲时间间隔为 T，并被相位调制器 PM_2 随机调相（0，π）. Bob 端用双 FM 干涉仪代替传统的 M-Z 干涉仪，设置两臂臂差使其满足 $\frac{2(L_2 - L_1)n}{C} = T$. 相干光脉冲列被调相和衰减后经光纤传输进入 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 FM 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.

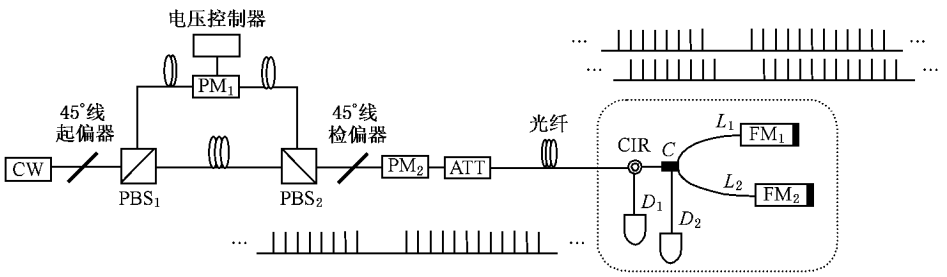

图 4 改进的差分相位编码 QKD 方案

密钥分配过程如下：1) Bob 记录下探测器响应的时刻和哪个探测器有响应. 2) Bob 通过经典信道告诉 Alice 在哪个时刻探测到光子. 3) Alice 根据它的调相情况和从 Bob 处得到的时间信息，就可以确切知道 Bob 在哪个探测器有计数. 4) 根据探测器 D_1 有计数记为“0”，D_2 有计数记为“1”的规则，Alice 和 Bob 之间就可以产生一组相同的密钥.

我们的方案中，相干脉冲的个数 N 可以随机选择，密钥生成效率为 $\eta = 1 - 1/N$. 可见，密钥生成效率和相干脉冲的个数成正比关系. 当 N 很大时，密钥生成效率接近于 1. 调整相干脉冲的个数，可以控制成码效率. 但 N 过大也有缺点，兼顾效率和可靠性，我们实验过程中，N 选择在 7—18 之间较佳. 本方案只需用一个偏振型强度调制器，就可以产生任意个相干脉冲，而无需扩展设备，简化了系统的结构，节约了成本，提高了系统的成码效率.

2.3. 系统稳定性分析

差分相位编码中，比特信息总是包含于两个相邻脉冲的相位差之间. 由于相邻脉冲在光纤传输过程中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纤传输中温度应力等因素变化的时间常数，相邻脉冲总是以相同的偏振态从光纤中出射，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干涉可见度不因环境影响而改变. 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，从而有效地降低误码率. 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，提高了干涉稳定性.

以下用矩阵光学的方法简单证明双 FM 干涉仪消除偏振衰落的原理. 双 FM 干涉仪原理图见图 4 虚框部分. 设从耦合器 C 入射光波电场矢量为 E_{in}，从干涉仪两臂出射电场矢量分别为

$$E_1 = J_{31} \cdot S_{-1} \cdot F_1 \cdot T \cdot S_{+1} \cdot F_1 \cdot J_{13} \cdot E_{\mathrm{in}} = \frac{1}{2}\alpha_{s1}^2 t_{s1}^2 t_J^2 t \begin{bmatrix} 0 & -j \\ -j & 0 \end{bmatrix} E_{\mathrm{in}} \exp(\mathrm{j}\phi_1), \quad (1)$$

$$E_2 = J_{41} \cdot S_{-2} \cdot F_2 \cdot T \cdot S_{+2} \cdot F_2 \cdot J_{14} \cdot E_{\mathrm{in}} = \frac{1}{2}\alpha_{s2}^2 t_{s2}^2 t_J^2 t \begin{bmatrix} 0 & -j \\ -j & 0 \end{bmatrix} E_{\mathrm{in}} \exp(\mathrm{j}\phi_2 + \mathrm{j}\pi), \quad (2)$$

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 L_1，L_2 长度都较短，并且长度差别不大，故 $\alpha_{s1} \approx \alpha_{s2}$，$t_{s1} \approx t_{s2}$. 比较(1)式和(2)式，可以得出，$E_1$ 和 E_2 是两个偏振方向始终相同的电场矢量，如果这两个信号发生干涉，不会产生偏振衰落. 其中，耦合比为 1∶1 的 2×2 耦合器的 Johes 矩阵为

$$J_{13} = J_{31} = J_{24} = J_{42} = \frac{\sqrt{2}}{2} t_J \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (3)$$

$$J_{14} = J_{41} = J_{23} = J_{32} = \frac{\sqrt{2}}{2} t_J \begin{bmatrix} j & 0 \\ 0 & j \end{bmatrix}, \quad (4)$$

法拉第镜的 Johes 矩阵为

$$T = t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \quad (5)$$

考虑光波分别在干涉仪两臂光纤 L_1，L_2 段传输的过程. 光纤段相位延迟和光强的衰减，可以用 F_i 来表示，即

$$F_i = t_{si} \mathrm{e}^{\mathrm{i}\varphi_{si}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = 1,2, \quad (6)$$

式中，t_{si} 为幅度传输系数. 低双折射光纤的效应可以看成一个椭圆延迟器，可以写成

$$S_{+,i} = \frac{\alpha_{si}}{d_{si}} \begin{bmatrix} a_{si} & -b_{si}^* \\ b_{si} & a_{si}^* \end{bmatrix}, \quad (7)$$

式中，$d_{si} = a_{si}a_{si}^* + b_{si}b_{si}^*$，$\alpha_{si}$ 为光纤段 L_i 的传输损耗，a_{si}，b_{si} 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，

$$S_{-,i} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} S_{+,i} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{\alpha_{si}}{d_{si}} \begin{bmatrix} a_{si} & -b_{si} \\ b_{si}^* & a_{si}^* \end{bmatrix}. \quad (8)$$

由此可见，差分相位编码的特性，偏振型强度调制器的使用和 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.

2.4. 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[6,12,13]. 从量子机制上讲，当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.

差分编码的比特信息是由相邻脉冲的相位差携带的，所以 Eve 只能以 50% 的概率获得信息. 为了不被发现，Eve 如果拦截测量到比特信息，她就要再伪

造一个光子发送给 Bob. 一个伪造的光子在三个相邻的时隙以 1∶2∶1 的比例使 Bob 端的探测器有响应. 在所有不同的时隙,Bob 的探测器有响应的总比例是所有可能情况的总和,即为 1∶3∶4∶4…4∶3∶1. 而在没有拦截/再发送窃听的情况下,探测器响应的总比例为 1∶2∶2∶2…2∶2∶1. 这样,Bob 通过监测探测器响应的比例就可以发现 Eve 的窃听.

在 Alice 和 Bob 共享密钥之前,他们抽取出一小部分密码通过公共信道进行比对,探测误码,以检查是否存在窃听. 因为对密钥生成没有贡献的脉冲,其误码不能被探测到,所以由窃听引起的误码能够被探测到的概率和密钥生成效率是相等的. 因此,在差分编码方案中,Bob 探测到窃听者存在的概率比 BB84 方案大. BB84 方案的密钥生成效率仅有 1/4,只有 1/4 的误码能被检测到. 而差分编码的密钥生成效率为 $1-1/N$,相应地,探测到误码的概率也为 $1-1/N$. 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于 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 窃听判断的难度,提高了系统的安全性.

3. 量子密钥分配实验与结果

量子密钥分发系统实验框图如图 5 所示.

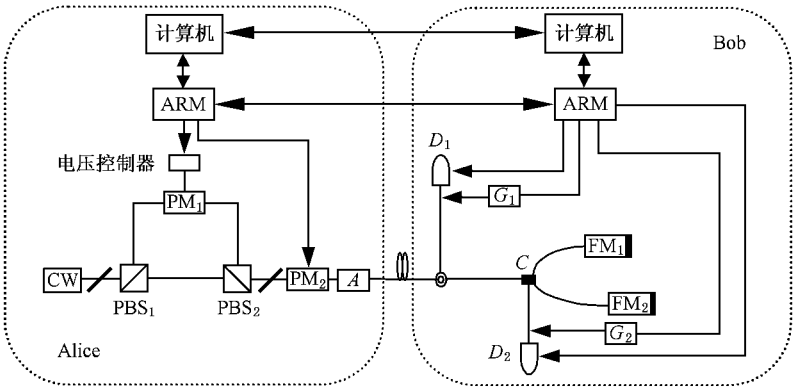

图 5 量子密钥分发系统实验框图

量子密钥分配由两个嵌入式 ARM 模块完成. 系统采用差分相位编码,同步由 5 m 短导线连接的两个 ARM 模块实现. Alice 端计算机启动 ARM,控制 PM_1 产生光脉冲序列,同时指令 PM_2 对脉冲序列进行随机相位调制(0,π). Bob 端 ARM 产生门控信号(脉宽 2 ns)触发光子探测器,并采集两个光子探测器的计数值. Alice 和 Bob 的两个 ARM 通过密钥分配软件处理,形成各自的 16 进制密钥,然后经 RS232 通信串口进入各自的计算机. Alice 用量子密钥本对图 6(a)所示的图像加密,通过局域网传送加密的图像,Bob 收到如图 6(b)所示的加密图像,然后,Bob 用量子密钥本对接收到的密文进行解密,得到如图 6(c)所示的解密后的图像,实现了 80 km 的量子密钥分配和图像传送. 我们从几次密钥分发实

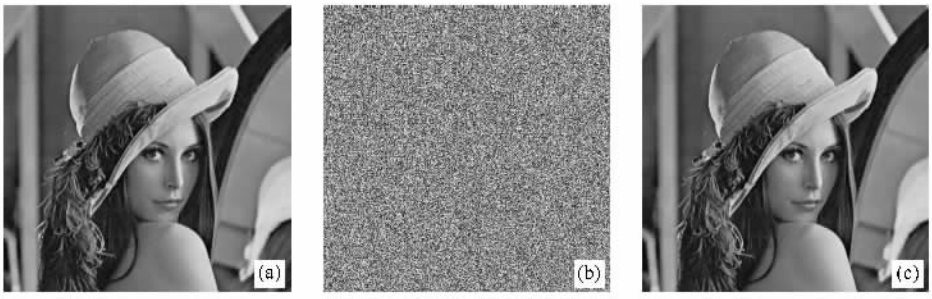

图 6 使用量子保密通信系统传送的图像 (a)发送方的原始图像;(b)接收到的加密图像;(c)接收方解密后的图像

验的原始密钥中取出 1024 位进行分析，其误码率均 $<4\%$，在安全的范围内，通过误码协调和保密增强后可以供“一次一密”方式加密与解密使用. 由于我们的实验采用的是电同步方式，随着传输距离的增加，同步信号出现时间抖动，在我们目前的实验条件下无法进行准确的调整，这使得我们无法完成 100 km 以上的量子密钥分发. 若使用光信号进行同步，在进一步提高密钥分发速率和降低误码率后，可望实现更长距离的量子密钥分发.

4. 结　论

本文提出一种改进的差分相位编码 QKD 方案，利用偏振型强度调制器，产生任意个相干脉冲，进行差分相位编码量子密钥分配，在实验上实现了稳定的 80 km 量子保密通信. 由于采用了偏振型强度调制器，差分相位编码以及双 FM 干涉仪技术，系统稳定可靠，能长期运转，向实用化又迈进了一步.

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

[2] Liu J F, Tang Z L, Liang R S, Li L Y, Wei Z J, Chen Z X, Liao C J, Liu S H 2005 *Acta Phys. Sin.* **54** 0517 (in Chinese) [刘景锋、唐志列、梁瑞生、李凌燕、魏正军、陈志新、廖常俊、刘颂豪 2005 物理学报 **54** 0517]

[3] He G Q, Zeng G H 2005 *Chin. Phys.* **14** 0541

[4] 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]

[5] Mo X F, Zhu B, Han Z F, Gui Y Z, Guo G C 2005 *Opt. Lett.* **30** 2632

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

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

[8] Zhou C Y, Wu G, Chen X L, Zeng H P 2003 *Appl. Phys. Lett.* **83** 1692

[9] Chen X L, Zhou C Y, Wu G, Zeng H P 2004 *Appl. Phys. Lett.* **85** 1648

[10] Wu G, Zhou C Y, Chen X L, Han X H, Zeng H P 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese) [吴　光、周春源、陈修亮、韩晓红、曾和平 2005 物理学报 **54** 3622]

[11] 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]

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

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

An auto-compensating and efficient differential phase shift quantum key distribution system *

Lin Yi-Man[1)2)] Liang Rui-Sheng[1)†] Lu Yi-Qun[1)]
Lu Hong[2)] Guo Bang-Hong[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)(*Department of Photoelectronics and Physics, Foshan University, Foshan* 528000, *China*)

(Received 18 September 2006; revised manuscript received 13 November 2006)

Abstract

We present an improved differential phase shift quantum key distribution scheme which features auto-compensation, high efficiency, and excellent practicality. Alice modulates continuous laser using an intensity modulator based on polarization to generate coherent pulse train. Bob employs a Fraday-Michelson interferometer instead of a traditional M-Z interferometer, which automatically compensates for the polarization mode dispersion caused by the changes of environment and improves the stability of the interference visibility. The present scheme not only has a simpler configuration, but also offers a higher key creation efficiency than traditional schemes. Furthermore, it enhances the security of the system. With the proposed experimental setup, a stable quantum key distribution was performed over 80 km fiber with a quantum bit-error rate of less than 4%.

Keywords: quantum cryptography, quantum key distribution, differential phase shift, intensity modulator based on polarization
PACC: 4250, 4230Q, 0365

* Project supported by the National 973 Project of China (Grant No. 2007CB307001).

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