第 56 卷 第 11 期 2007 年 11 月
1000-3290/2007/56(11)/6434-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.11,November,2007

运行双协议相位调制的量子密钥分发系统*

陈 霞 王发强† 路轶群 赵 峰 李明明 米景隆 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 12 月 25 日收到;2007 年 4 月 10 日收到修改稿)

基于差分编码方式提出一种改进方案.在 Alice 端用光纤马赫-曾德干涉仪产生双脉冲差分信号;在 Bob 端,用双法拉第反射式麦克尔逊干涉仪代替光纤马赫-曾德干涉仪,这种干涉仪能自动补偿环境引起的偏振抖动和光纤双折射引起的相位漂移,从而提高系统稳定性.双协议(即双脉冲差分协议联合 BB84 协议)的使用,增强了系统的安全性.该系统具有高效、安全、简洁、稳定等优点,在实验上实现了长期稳定的密钥分发和量子保密通信,误码率 $<5\%$,传输距离达 80 km.

关键词:量子保密通信,量子密钥分发,差分相位编码,双协议

PACC:4250,4230Q,4210J,0365

1. 引 言

量子密码学作为量子力学与密码学相结合的产物,不可克隆定理和海森伯不确定性原理保证了密码体系的安全性,量子力学的基本原理保证了窃听的可检测性,因此具有经典密码学无法比拟的优势,取得了飞速的发展[1—3].中国科技大学密钥分发实验最远已达 155 km,华东师大和物理所[4]已完成样机工作并提出了高效的量子密钥分发(QKD)方案[5—7].国外,美国的 MagiQ 和瑞士的 idQuantque 公司已推出产品[8],都采用‘即插即用’系统.但是,“即插即用”系统由于背向瑞利散射限制了密钥分发速率,往返式密钥传输方式也无法抵御木马攻击[9],密钥分配安全性从理论上就欠缺[10],因此寻找安全稳定的 QKD 方案成为关键.随即出现的集成化光学系统[11],强振动隔离加精确温度控制[12]和实时相位补偿[13]等方案,只是在一定程度上加强了系统的稳定性和安全性,并没有从根本上解决问题.Inoue 等提出了差分密钥传输方案(DPS-QKD)[14].此方案中,由于信号是连续光脉冲,时间差为 10 ns 量级,因此信号在光纤传输过程中,所经历的温度、压力等环境影响几乎相同,产生的偏振模式变换也几乎相同,从而不会影响出射端的干涉对比度.相对于其他密钥分发协议,此协议的安全性和稳定性都得到了极大地提高[15,16].

我们在 DPS-QKD 基础上,在 Alice 端,用光纤马赫-曾德(M-Z)干涉仪产生双脉冲差分信号,降低系统的复杂度;在 Bob 端,采用双法拉第旋转镜(FM)技术,完全补偿了 Bob 端的双折射现象和环境引起的偏振抖动,加强了系统的稳定性.我们拟定一种新的协议——双协议,即同时运行双脉冲二维调制差分协议(大部分时间运行)和 BB84 协议,来弥补双脉冲的差分信号对截获/重发攻击存在安全漏洞.在该协议中,我们采用分别评估不同测量基下误码率的安全性评估方法,进一步增强了系统的安全性.

2. 量子密钥分配方案

2.1. 系统原理图

实验方案如图 1 所示.一个单脉冲经 M-Z 干涉仪后,被分成两个脉冲,时间间隔为 Δt.这两个脉冲经过传输光纤 T 传送到 Bob 端.在 Bob 端,该双脉冲被分成 4 个脉冲.为在出射端满足相干条件,即在到达耦合器 C_4 时能使 4 个脉冲中存在发生相干作用的脉冲,要求

$$\frac{l_2 - l_1}{c} = \Delta t = \frac{2(l_4 - l_3)}{c}, \qquad (1)$$

* 国家自然科学基金(批准号:10404007)资助的课题.

† E-mail:fqwang98@sina.com

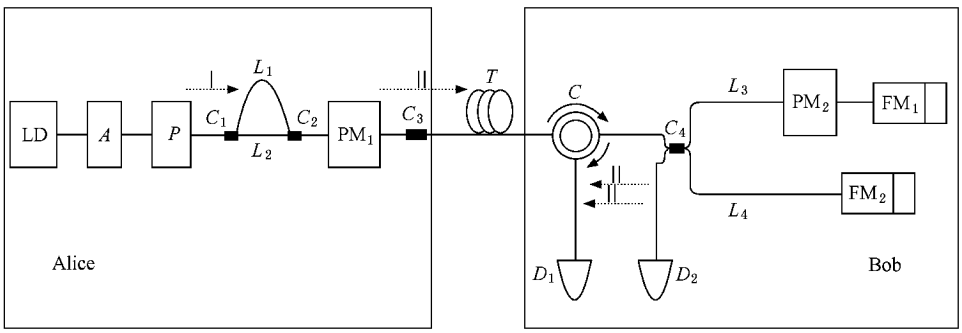

图 1　系统原理图(LD 为半导体激光脉冲光源；A 为衰减器；P 为偏振控制器；C_n ($n=1,2,3,4$)为 2×2 耦合器；PM_n ($n=1,2,3$)为相位调制器；T 为保偏光纤；C 为环形器；L_n ($n=1,2,3,4$)为光纤；FM_n ($n=1,2$)为法拉第镜；D_n ($n=1,2$)为单光子探测器)

其中 l_n 为光纤 L_n 的长度.

以上为实验的总体方案,光脉冲的具体传输路径以及如何发生相干作用,将在 2.4 节稳定性分析中进一步阐明.

2.2. 密钥分发协议

以下将阐述为何和如何在我们的系统中运用双协议.

2.2.1. 使用双协议的原因

这里的双协议是指双脉冲的差分协议和 BB84 协议.

传统意义上的差分相位调制系统具有高效、安全、稳定的特点.但是双脉冲的差分系统在安全性上有所欠缺.

说明如下:观察图 1 我们发现,对于 Alice 发出的光脉冲,进入 Bob 后,在出射端,于三个时刻被探测器响应,概率比为 1∶2∶1.我们假设 Eve 采用一种最简单的截获/重发窃听策略[14]进行攻击,发现系统存在安全性隐患.如图 2 所示,Eve 截获 Alice 端的信号,并重发出攻击信号,为一个光子被安置在两个连续的光脉冲之中.对于这样的信号,会在 3 个不同的时间间隔响应.在中间时刻的响应是依据两个脉冲之间的相位差,响应还可能随机的发生在第 1 和第 3 个时间间隔.显而易见,探测器响应在这三个时刻的概率比为 1∶2∶1.注意到:这个概率值与无 Eve 窃听时 Bob 探测器的响应概率相同.所以可以说,在这种攻击方式下,窃听很难被发现,从而双脉冲的安全性存在缺陷[17].

虽然如此,相对于由干涉仪产生多脉冲的差分系统,双脉冲的差分系统存在显著的优点:1)结构简单,2)不存在多脉冲系统中,非线性的环境振动的影响,3)不存在多脉冲差分系统为产生等时间间隔脉冲而对干涉仪臂长的苛刻要求.基于此,双脉冲系统具有很好的应用前景.同时,对于其他的常用攻击,双脉冲的差分系统安全性是有保障的[18].

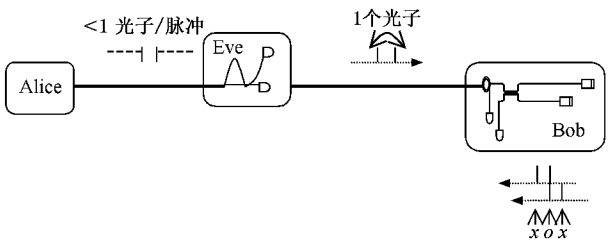

图 2　在 DPS-QKD 系统中截获-重发攻击下的探测器的响应状态

为了能应用双脉冲差分系统的优点,同时克服它的安全性漏洞,我们提出运行双协议.仅调制 PM_1 时,运行差分协议;同时调制 PM_1,PM_2 时,运行 BB84 协议.

2.2.2. 密钥分发协议

1. 密钥传输过程中

(A) Alice 随机选择 $0,\pi/2,\pi,3\pi/2$ 四种相位中的一种对双脉冲的相位进行调制,Alice 记录:调制时间、使用的是 $\{0,\pi\}$ 还是 $\{\pi/2,3\pi/2\}$ 基和具体调制相位.

(B) Bob 随机地独立选择时段调制 PM_2. Bob 端记录:调制 PM_2 的时段.说明:为充分利用差分系统的优势,在随机时段选取方式上满足大多时间不调制 PM_2.

(C) 在 PM_2 调制时段,Bob 随机独立选择 $\{0,\pi\}$ 或 $\{\pi/2,3\pi/2\}$ 基中的相位来调制 PM_2. Bob 记录:调制 PM_2 的时间,调制时选取的基和具体调制相位.

(D) 在 PM_2 未调制时段,Bob 记录:探测器 D_1,

D_2 的响应时间.

2. 密钥传输结束后

(E) Bob 通过公开信道告知 Alice:Bob 端调制 PM_2 的时段.

(F) 在 PM_2 调制时段,系统采用 BB84 编码方式.Bob 通过公开信道通知 Alice,自己选用的是何种基来进行调制,但不会公布具体使用的是哪个相位;Alice 根据自己对双脉冲中后一个脉冲的调相记录(此时要求 Alice 对双脉冲中前一个脉冲的调制为 0),告诉 Bob 哪些测量基是正确的并保留下来,其余的丢弃.之后,Bob 根据 Alice 通知的正确测量基所对应的时刻探测器的响应情况建立密钥:探测器 D_1 响应 D_2 不响应时,为"0";探测器 D_1 不响应 D_2 响应时,为"1"(根据探测器响应的编码方式的补充说明见 2.4 稳定性分析).

(G) 在 PM_2 未调制时段,系统采用差分编码方式.Bob 通知 Alice 单光子探测器响应的时间. Alice 根据此时间和自己调制相位的记录,建立密钥:即在这个时间下,对应双脉冲调制信号相位差为 0 时,为"0";对应双脉冲调制信号相位差为 π 时,为"1";对应双脉冲调制信号相位差为 $\pi/2$,$3\pi/2$ 时,舍弃.Bob 建立密钥:探测器 D_1 响应 D_2 不响应时,为"0";探测器 D_1 不响应 D_2 响应时,为"1";探测器 D_1,D_2 同时响应时,舍弃.成码率为 50%.

(H) 安全性评估.在差分编码方式和 BB84 编码方式下,对密钥进行分段,分别抽取部分 $\{0,\pi\}$ 基和 $\{\pi/2,3\pi/2\}$ 基下产生的密钥段进行分析,分别记误码率为 e_1,e_2,并根据实际测量和计算结果设定安全上限 $e_{\max}$.e_1 和 e_2 是彼此独立的,若都小于 $e_{\max}$,则保留;若 e_1 和 e_2 中有大于 $e_{\max}$,则舍弃密钥,进行重发[11].这种安全性评估方法较现在二维基下用 $\bar{e}=\frac{e_1+e_2}{2}$,使 $\bar{e}\leqslant e_{\max}$ 的方法,提高了安全性(定量分析见 2.3 安全性分析).

(I) 保密放大[19].

2.2.3. 密钥分发协议的扩展方向

在我们的系统中,除了可以应用以上我们谈到的编码方式外,还可以用其他的编码方式.如联合使用 B92 和 BB84 的编码方式进行编码.可以看出,此套系统具有很强的灵活性.

2.3. 安全性分析

系统安全性的增强体现在三个方面:第一,双协议的运行,对于 Eve 判断系统何时采用何种协议进而采用相应的攻击增加了难度;第二,我们系统中的密钥产生于二维基的空间调制,空间维度的增加会增大误码率[17],从而易于发现 Eve;第三,也是最重要的一点,我们采用的分别计算每种测量基下误码率的安全性评估方法,增加了系统的信息传输率,以下我们将用碰撞概率分析方法对这一点进行量化分析.

碰撞概率分析方法是量化分析系统安全性方面的一种流行且经过证明的方法[20],它将量子密钥分发系统抽象化为探针系统进行表述,这种分析方法是基于实际系统采用的单光子源是由符合泊松分布的激光衰减而成的.

假设探针系统(a photon-probe system)的初始态为

$$|\Psi\rangle=\frac{1}{\sqrt{N}}\sum_n e^{i\phi_n}|n\rangle|E_i\rangle, \tag{2}$$

这里 $|n\rangle$ 被定义为 $\hat{a}_n^+|0\rangle$,表示在时间间隙 n 处的一个光子.窃听者 Eve 往往使用探针进行测量,Eve 最常用的攻击可以被描述为 $|n\rangle|E_i\rangle\rightarrow\sum_m|m\rangle|E_{n,m}\rangle$,式中 $|E_{n,m}\rangle$ 是 Eve 在 Hilbert 空间中的态并且没有被假设为归一化和对角化.把该式带入(2)式得

$$\begin{aligned}|\Psi\rangle&=\frac{1}{\sqrt{N}}\sum_m|m\rangle\sum_n^{i\phi_n}|E_{n,m}\rangle\\&=\frac{1}{\sqrt{N}}\sum_m|m\rangle|J_m\rangle.\end{aligned} \tag{3}$$

经过 Bob 端的干涉仪,这个状态被转换为

$$\begin{aligned}|\Psi\rangle=\frac{1}{4\sqrt{N}}\sum_m&[(|J_m\rangle+|J_{m+1}\rangle)|0_m\rangle\\&+(|J_m\rangle-|J_{m+1}\rangle)|1_m\rangle\\&+i(|J_m\rangle+|J_{m+1}\rangle)|+_m\rangle\\&+i(|J_m\rangle-|J_{m+1}\rangle)|\times_m\rangle],\end{aligned} \tag{4}$$

式中,我们将 $|0_m\rangle$ 和 $|+_m\rangle$ 统一编码为 0,$|1_m\rangle$ 和 $|\times_m\rangle$ 统一编码为 1,这样编码是基于前面我们拟定的双协议.

分析系统的安全性,常使用信道信息传输率参数来进行说明.在给定传输距离条件下,信息传输率越高则说明系统安全性越高.对于探针系统模型中的信息传输率 R 可表示为

$$R=P_{\text{click}}[-(1-2\bar{n})\log_2 P_{C0}(e)-f(e)h(e)], \tag{5}$$

式中,P_{click} 表示 Bob 探测到光子的概率,e 表示误码率,$f(e)$ 为纠错效率,$h(e)$ 为相容熵,在不同的系统条件下,$f(e)$ 和 $h(e)$ 有不同的表述.在我们系统

中，$f(e)=1$，$h(e)=-e\log_2 e-(1-e)\log_2(1-e)$.

系统的碰撞概率通常表示为

$$P_{C0}\leqslant 1-\frac{1}{4}[4e^2+2(1-6e)^2]. \tag{6}$$

由(6)式可以看出 P_{C0}为小于 1 的数.

对于二维调制系统，常用的误码率分析方法为 $\bar{e}=\frac{e_1+e_2}{2}$，则其碰撞概率 P_{C0B}为

$$\begin{aligned}P_{C0B}&\leqslant 1-\frac{1}{4}[4\bar{e}^2+2(1-6\bar{e})^2]\\&=\frac{1}{2}-\frac{1}{4}(19e_1^2+19e_2^2+38e_1e_2\\&\quad-12e_1-12e_2)=B,\end{aligned} \tag{7}$$

式中，B 为碰撞概率 P_{C0B}的上限.对于我们的安全性分析方法，即将每种调制基下产生的误码率 e_1，e_2 分别分析，则其碰撞概率 P_{C0D}为

$$\begin{aligned}P_{C0D}&\leqslant 1-\frac{1}{4}[4e_1^2+2(1-6e_1^2)]\\&\quad-\frac{1}{4}[4e_2^2+2(1-6e_2)^2]\\&=-19e_1^2-19e_2^2+6e_1+6e_2=D,\end{aligned} \tag{8}$$

式中，D 为碰撞概率 P_{C0D}的上限.(7)式减(8)式得

$$\begin{aligned}B-D&=\frac{57}{4}\left(e_1-\frac{e_2}{3}\right)^2+\frac{114}{9}e_2^2\\&\quad+3e_1+3e_2+\frac{1}{2}>0.\end{aligned} \tag{9}$$

由(9)式可知 相对于常用的求误码率均值的安全性评估方法，我们采用的分别评估不同测量基下的误码率的安全性评估方法所得到的碰撞概率小.由于 P_{C0}为小于 1 的数，由(5)式可以看出，随着 P_{C0} 的减小，整个系统的信息传输率会增加.又在给定传输距离条件下，信息传输率越高则说明系统安全性越高，所以我们可以得到如下结论 我们采用的将每种调制基下产生的误码率 e_1，e_2 分别分析的安全性评估方法增强了系统的安全性.

2.4. 稳定性分析

我们采用矩阵光学的方法对此套系统的稳定性进行分析.

2.4.1. 系统部分光器件及光纤传输的矩阵表示方法

1)2×2 波导耦合器

2×2 波导耦合器的 Johes 矩阵为

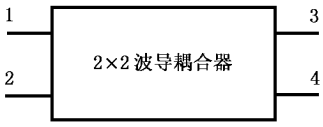

图 3　2×2 波导耦合器端口示意图(其中 1,2,3,4 表示端口号)

$$\begin{aligned}J_{13}&=J_{31}=J_{24}=J_{42}\\&=t_J\begin{bmatrix}\sqrt{1-k}&0\\0&\sqrt{1-k}\end{bmatrix},\end{aligned} \tag{10}$$

$$\begin{aligned}J_{14}&=J_{41}=J_{23}=J_{32}\\&=t_J\begin{bmatrix}\mathrm{j}\sqrt{k}&0\\0&\mathrm{j}\sqrt{k}\end{bmatrix},\end{aligned} \tag{11}$$

(10)式，(11)式中，k 是一个介于 0—1 之间的实数，表示(1—k)倍的从 1 端输入的功率出现在输出端 3，而 k 倍的该功率出现在输出端 4.(2)式，(3)式中：t_J 为幅度传输系数；J_{mn}(m，n=1—4)表示 2×2 光纤耦合器的 Johes 矩阵.

2)光纤

传输光纤对于系统的影响主要为相位的延迟，光强的衰减和双折射效应.

对于其中的相位延迟和光强的衰减，用 F_i 来表示：

$$F_i=t_{si}\mathrm{e}^{\mathrm{j}\varphi_{si}}\begin{bmatrix}1&0\\0&1\end{bmatrix}, \tag{12}$$

式中 t_{si}为幅度传输系数，表示经过此段后光强衰减为原来的 t_{si} 倍，易理解 t_{si}为 0—1 之间的小数，i 的取值为 1—4 和 T，以下同.

而其中光纤的双折射效应可看成是一个椭圆延迟器，其可表示为[21]

$$S_{i+}=\frac{\alpha_{si}}{d_{si}}\begin{bmatrix}a_{si}&-b_{si}^*\\b_{si}&a_{si}^*\end{bmatrix}, \tag{13}$$

式中，α_{si}表示第 i 段光纤的光纤衰减系数；* 表示复共轭；a_{si}，b_{si}与光纤的双折射特性有关.其中，$d_{si}^2=a_{si}a_{si}^*+b_{si}b_{si}^*$.

光脉冲经过反射镜后，由镜面反射回来，反相的椭圆延迟器可以写成

$$S_{i-}=\frac{\alpha_{si}}{d_{si}}\begin{bmatrix}a_{si}&-b_{si}\\b_{si}^*&a_{si}^*\end{bmatrix}. \tag{14}$$

3)相位调制器

对于相位调制器，可以用 Φ_i 表示相位调制器的传输矩阵

$$\Phi_i = t_{\varphi i} e^{i\varphi_i} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (15)$$

式中，i 取 1，2.

4）法拉第旋转镜

法拉第旋转镜是安置在平面反射镜前面，它的旋转角度 $\theta = 45°$，则它的 Johes 矩阵可表示为

$$T = t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \quad (16)$$

2.4.2. 系统光路说明及传输矩阵表示

以下公式的计算中将运用(10)式到(16)式. 对于发生相干作用的脉冲，我们用 P_2，P_3 来表示.

在 Alice 端，设产生的单光子的光强为 E_0，初相位为 φ_0，P_2，P_3 脉冲从 Alice 端的输出场强分别为 E_{A2}，E_{A3}.

$$E_{A2} = J_{13} F_1 S_{1+} J_{13} \Phi_1 E_{in} = \frac{t_J^2 \alpha_{s1} t_{s1} t_{\varphi 1} a_{s1} (1-k)}{d_{s1}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} E_0 e^{i(\varphi_0 + \varphi_{i1} + \varphi_1)}, \quad (17)$$

$$E_{A3} = J_{23} F_2 S_{2+} J_{23} \Phi_2 E_{in} = \frac{t_J^2 \alpha_{s2} t_{s2} t_{\varphi 2} a_{s2} (1-k)}{d_{s2}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} E_0 e^{i(\varphi_0 + \varphi_{i2} + \varphi_2)}. \quad (18)$$

之后，P_2，P_3 将进入传输光纤 T. 由于在光纤传输过程中，P_2，P_3 时间差十分微小，此时的实验环境又相同，所以可以近似的认为光纤 T 对它们的传输矩阵相同. 之后，P_2，P_3 将进入 Bob 端. 在这里，环形器对系统的影响十分微弱，只是起到控制光路的作用，因此我们可以将其影响忽略. 用 E_{B2}，E_{B3} 分别表示 P_2，P_3 脉冲通过 Bob 端后由耦合器 C_3 的 1 端口出射的场强.

$$E_{B2} = J_{41} F_4 S_{4-} T S_{4+} F_4 J_{14} F_T S_{T+} E_{A2} = -\frac{t_J^4 \alpha_{s1} \alpha_{sT} \alpha_{s4}^2 t t_{s1} t_{\varphi 1} t_{sT} a_{s1} a_{sT} (1-k) k}{d_{s1} \alpha_{sT}} \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} E_0 e^{i(\varphi_0 + \varphi_{s1} + \varphi_{sT} + \varphi_1)}, \quad (19)$$

$$E_{B3} = J_{31} F_3 S_{3-} T S_{3+} F_3 J_{13} F_T S_{T+} E_{A3} = -\frac{t_J^4 \alpha_{s2} \alpha_{sT} \alpha_{s3}^2 t t_{s2} t_{\varphi 2} t_{sT} a_{s2} a_{sT} k (1-k)}{d_{s2} \alpha_{sT}} \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} E_0 e^{i(\varphi_0 + \varphi_{s2} + \varphi_{sT} + \varphi_2)}. \quad (20)$$

由于脉冲在系统传输过程中，所用的光纤都是统一型号的高质量的保偏光纤，并且相位调制器的型号也相同，且在 M-Z 干涉仪中的两臂和法拉第旋转镜所用的两根光纤都较短，并且长度差别不大，又在实验环境下，这些光纤和器件所处的环境条件基本一致，所以

$$\alpha_{s1} \alpha_{s4}^2 = \alpha_{s2} \alpha_{s3}^2, t_{s1} \approx t_{s2},$$
$$t_{\varphi 1} \approx t_{\varphi 2}, a_{s1} \approx a_{s2},$$
$$d_{s1} \approx d_{s2}, \varphi_{s1} \approx \varphi_{s2}.$$

基于此，我们做如下近似，令

$$\varphi_0 + \varphi_{s1} + \varphi_{sT} = \varphi,$$
$$-\frac{t_J^4 \alpha_{s1} \alpha_{sT} \alpha_{s4}^2 t t_{s1} t_{\varphi 1} t_{sT} a_{s1} a_{sT}}{d_{s1} d_{sT}}$$
$$= -\frac{t_J^4 \alpha_{s2} \alpha_{sT} \alpha_{s3}^2 t t_{s2} t_{\varphi 2} t_{sT} a_{s2} a_{sT}}{d_{s2} d_{sT}} = C,$$

代入(19)式和(20)式，得

$$E_{B2} = C(1-k) k E_0 e^{i(\varphi + \varphi_1)}, \quad (21)$$

$$E_{B3} = C(1-k) k E_0 e^{i(\varphi + \varphi_2)}. \quad (22)$$

那么从耦合器 C_3 的 3 端口输出的电场强度表达形式为

$$E_{out} = E_{B2} + E_{B3} = \frac{C' e^{i\varphi}}{4} (e^{i\varphi_1} + e^{i\varphi_2}). \quad (23)$$

对应的输出光强表达式为

$$p_{out} = E_{out} E_{out}^* = \frac{C'}{2} [1 + \cos(\varphi_2 - \varphi_1)]. \quad (24)$$

同理可得，在端口 4，输出光强的表达式为

$$p_{out} = \frac{C'}{2} [1 - \cos(\varphi_2 - \varphi_1)]. \quad (25)$$

由(19)式，(20)式可以看出：P_2，P_3 两光波的电场矢量的偏振方向始终相同，即法拉弟镜的法拉第共扼效应使得出射光的偏振态总是垂直于入射光的偏振态，不论光沿光纤传输过程中偏振态的演化方式如何，都能够自动抵消包括干涉环内以及传输干线中任何偏振旋转，因而不会发生消偏振现象；由(21)式，(22)式可以看出，通过此系统，P_2，P_3 两光波的振幅强度几乎完全相同，保证了输出光的高相干性. 由(24)式，(25)式，我们可以看出：此套系统，出射端条纹的干涉对比度只决定于相位调制器调制信号. 根据以上分析证明，我们得出结论：该系统可以抵抗外界的影响，稳定性高.

3. 实 验

实验装置如图 4 所示. Alice 端，激光的中心波长是 1551 nm，脉冲的宽度是 5 ps，重复率是 50 kHz. 之后，光脉冲能量就衰减到每个脉冲 0.2 个光子，并且注入到 80 km 的光纤中. Bob 端，用法拉第反射式迈克尔逊干涉仪，补偿了环境影响下的相位差. 单光子探测器的型号为 Id200，它的门宽是 5 ns，门脉冲

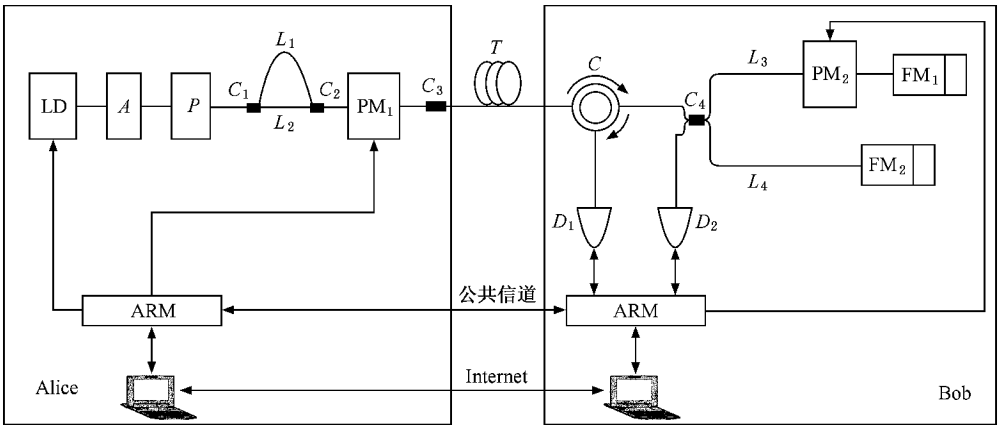

图 4　系统实验框图

是与光脉冲同步的，量子效率是 8%，暗计数为 2.21×10^{-5}．在探测光子的时候，Bob 记录了光子到达时刻和哪个探测器在响应，根据我们定义的密钥分发协议，在 Alice 和 Bob 双方建立密钥．

在实验系统中，CPU 选用基于 ARM7 的 SOC 芯片 EP7312，以此做为我们的控制系统核心．实验产生的密钥通过 RS232 口被送到各自端的计算机，以显示给用户．从产生的密钥中检测出的误码率小于 5%．我们用此密钥对图像进行加解密，效果良好．该系统实现了在 80 km 的光纤实验条件下，以低于 5% 的误码率，超出 12 h 的稳定运行．

4. 结　论

此实验方案特点如下：

1. 安全性高．双协议的运行，对于 Eve 判断系统何时采用何种协议进而采用相应的攻击增加了难度；二维基调制增加了系统的空间维度，易于发现 Eve 采用分别计算每种测量基下误码率的安全性评估方法，增加了系统的信息传输率．

2. 稳定性好．在 Alice 端，双脉冲的系统具有不存在多脉冲系统中，非线性的环境振动的影响和不存在多脉冲差分系统为产生等时间间隔脉冲而对干涉仪臂长的苛刻要求的优点；在 Bob 端，利用双 FM 反射式干涉仪代替光纤 M-Z 干涉仪，自动补偿了环境引起的偏振抖动和光纤双折射引起的相位漂移．

3. 虽然我们定义的这种双协议，使得系统的成码率降低（低于 1/2），但是采用高的脉冲重复率（本系统中为 50 kHz），同样可拥有高密钥生成率．

4. 结构简单，成本低，有很好的应用前景．

[1] You J，Li J H，Xie X 2005 *Chin. Phys.* **14** 1329

[2] He G Q，Zeng G Hua 2006 *Chin. Phys.* **15** 371

[3] Ma H Q，Li Y L，Zhao H，Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese) [马海强、李亚玲、赵　环、吴令安 2005 物理学报 **54** 5014]

[4] Liang C，Fu H D，Liang B，Liao J，Wu L，Yao D C，Lv 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] Gao T，Yan F L，Wang Z X 2005 *Chin. Phys.* **14** 893

[6] Zhou C，Zeng H P 2003 *Appl. Phys. Lett.* **82** 832

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

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

[9] Boileau J C，Gottesman D，Laflamme R，Poulin D，Spekkens R W 2004 *Phys. Rev. Lett.* **92** 017901

[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] Honjo T，Inoue K 2004 *NTT Tech. Rev.* **2**(12) 26

[12] Tittel W，Brendel J，Zbinden H，Gisin N 2000 *Phys. Rev. Lett.* **84** 4737

[13] Makarov V，Brylevski A，Hjelme D R 2004 *Appl. Opt.* **43** 4393

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

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

[16] 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]

[17] Honjo T, Inoue K 2006 *Opt. Lett.* **31** 522

[18] Ardehali M, Chau F, Hoi-Kwong L 1999 arXiv: quant-ph/9803007 v4 29

[19] Zhao F, Lu Y Q, Wang F Q, Chen X, Li M M, Guo B H, Liao C J, Liu S H have been accepted by *Acta Phys. Sin.* 200061122 (in Chinese) [赵 峰、路轶群、陈 霞、郭邦红、李明明、廖常俊、刘颂豪、王发强 物理学报已录用 200061122]

[20] Waks E, Takesue H, Yoshihisa Y 2006 *Phys. Rev.* A **73** 012344

[21] Liu D M, Xiang Q, Huang D X *Fibre optics* (Bejing: National Defense Industry Press) p23

A phase modulated QKD system with two quantum cryptography protocols*

Chen Xia Wang Fa-Qiang† Lu Yi-Qun Zhao Feng
Li Ming-Ming Mi Jing-Long Liang Rui-Sheng Liu Song-Hao
(*Laboratory of Photonic Information Technology, South China Normal University, Guangzhou* 510631, *China*)

(Received 25 December 2006; revised manuscript received 10 April 2007)

Abstract

An improved DPS-QKD scheme is proposed and demonstrated in this paper. At Alice's site, we use a M-Z interferometer to produce two coherent pulses. At Bob's site, a Faraday-mirrors-based Michelson interferometer is used instead of a M-Z interferometer to auto-compensate for the phase drifts and polarization mode dispersions in the fiber. It enhances the security of the whole system to use the two quantum cryptography protocols (namely the two pulse DPS-QKD scheme associated with the BB84 scheme). It is shown in our experiment that such a system features perfect stability with a quantum bit error rate less than 5% and high key generation rate. This scheme has been implemented successfully during the 80 km fiber transmission.

Keywords: quantum secure communication, quantum key distribution, differential-phase-shift phase modulation, two quantum cryptography protocols

PACC: 4250, 4230Q, 4210J, 0365

* Project supported by the National Natural Science Foundation of China (Grant No. 10404007).

† E-mail: fqwang98@sina.com