第 56 卷 第 7 期 2007 年 7 月
1000-3290/2007/56(07)/3695-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.7,July,2007

相位调制量子密钥分配系统中低频振动相移的实时跟踪补偿*

郭邦红[1)2)†] 路轶群[1)] 王发强[1)] 赵 峰[1)]
胡 敏[1)] 林一满[1)] 廖常俊[1)] 刘颂豪[1)]

1)(华南师范大学光子信息技术广东省高校重点实验室,广州 510006)
2)(广东茂名学院计算机与电子信息学院,茂名 525000)

(2006 年 10 月 1 日收到;2006 年 11 月 20 日收到修改稿)

环境变化引起的相位漂移是双 Mach-Zehnder 量子密钥分配系统中误码和不稳定性的主要来源.相位漂移由高频振动和低频振动两部分组成,大部分这类振动的影响采用隔振措施(如用泡沫、橡皮包垫隔音)可以消除,而周期为 3 ± 0.32 min 的低频振动依然存在.报道了对这种低频固有振动引起的相移进行实时跟踪和补偿的方法.实验表明,采用这种方法实验室内实现 75 km 量子密钥分配和量子保密通信,在 24 h 内能长期稳定运行,误码率低于 6%.

关键词:量子保密通信,量子密钥分配,低频振动,实时相位补偿
PACC:0365,4250

1. 引 言

由于信息安全的需要[1,2],量子密钥术正得到迅速发展[3—5],已经开始有部分产品投入市场[6].误码率是量子密钥分配(quantum key distribution,QKD)面临的一个重要问题.误码率的来源有两个:一个是窃听造成的,是量子通信系统发现窃听者的主要依据[7,8];另一个来源是系统的不稳定性,属于技术上的问题.只有 QKD 系统稳定,量子保密通信系统才能有效地发现窃听者和保持系统的成功运行.为解决系统的稳定性问题,已经提出了很多方案[9—12].由于随机双折射的影响,限制了偏振编码系统的传输距离.目前,传输距离最长的是相位调制编码系统.相位漂移是相位编码系统误码的主要来源.

目前有几种减少相位漂移的处理方法,1)采用法拉第镜补偿的即插即用干涉系统(往返光路传输,自动补偿),这种方式因为两次通过光路,易遭受木马攻击,而且码率很低.中国科技大学提出了改进的 Faraday-Michelson(FM)系统[10],完成了长距离的量子保密通信.2)严格的热和机械隔离,降低相位漂移速率[13,14].3)Marand 和 Townsend 等采用有源装置的强光衰减补偿方法[15].4)Brylevski 提出了对双 Mach-Zehnder(M-Z)干涉系统进行环境测试和相位跟踪的软件方案,但未见他们的 QKD 实验报道[16].

我们对双 M-Z 干涉仪的相位漂移特性进行分析研究,发现采取各种消除振动的措施之后,分钟量级的振动影响依然存在.本文报道以单光子探测光子统计计数表征的低频固有振动相位漂移进行实时跟踪和补偿的方法.实验室内实现 75 km 量子密钥分配和量子保密通信.在 24 h 内能长期稳定运行,误码率低于 6%.

2. 双 M-Z 型 QKD 系统相位漂移实验

2.1. 环境引起 M-Z 光纤干涉仪相位漂移的测试实验

Alice 端机和 Bob 端机用多孔泡沫塑料、海绵及弹簧进行高频振动隔离(主要消除了环境噪声通过空气对系统的影响).如图 1 为我们的 M-Z 光纤干涉实验系统,对环境等因素影响干涉仪的相位漂移进行实验测试,其中 LD 为激光器,C_1,C_2 为 50∶50 耦

* 国家重点基础研究发展计划(973)项目(批准号:G2001CB309302)和广州市科技攻关项目(1999-Z-035-01)资助的课题.
† 通信作者. E-mail:qkdslab@126.com

合器，D_1，D_2 为光电探测器．激光重复率为 1 MHz，脉冲宽度为 50 ps，两等臂光纤长度误差小于 0.5 cm．光电转换后用带宽为 100 MHz 的光电探测器探测，扫描时间全屏约 30 min，图 2 是示波器在 D_1 端的采样结果（取 5—25 min 时间段）．该系统基本隔离了空气传导的振动（噪声，汽车声、脚步声），实验发现周期性固有振动仍然存在，这种低频振动作用在光纤上产生附加光程 $\int \Delta n \mathrm{d}l = \Delta l$，引起周期性变化的相位漂移，周期为 3 ± 0.32 min．

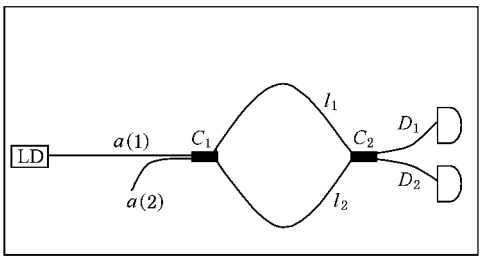

图 1 等臂光纤 M-Z 干涉仪，C_1，C_2 为 1∶1 耦合器

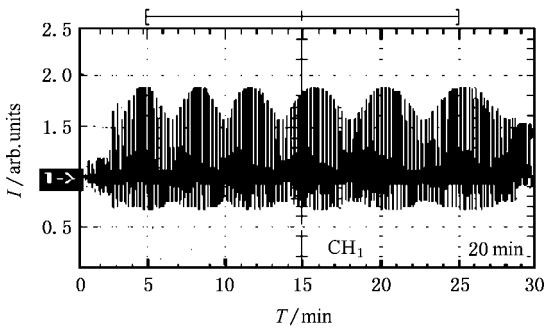

图 2 固有振动引起的相位漂移干涉图

周期性的变化可用傅里叶级数变换分解为多次小量谐波[17]叠加，表示为 $\Delta\phi_s \approx a\sin\omega t$，单位分钟时间内为 1.88 rad．

2.2. 双 M-Z 光纤干涉仪相位漂移

图 3 是双 M-Z 干涉相位漂移测量的示意图，其中 LD 为半导体激光器，C_1—C_4 为耦合器，PM_1，PM_2 为相位调制器，PC 为偏振控制器，optical fiber 为单模光纤盘传输光纤，det_1，det_2 为单光子探测器．实验中 PM_1，PM_2 均处于 0 相位（或固定值）不调相，单光子探测器门宽取为 2 ns，平均光子数 $\mu \approx 1$，脉冲重复率为 50 kHz，光电转换后用单光子探测器每 3 s 进行一次计数，计数时间为 30 min，然后经 RS232 通信串口进入计算机数据处理．干涉相对光强-时间曲线如图 8 中的‘○’曲线，从图中可以看到 PM_1，PM_2 不调相，计数仍出现周期性变化，变化周期与图 2 相同，这表明环境引起固有振动，产生了双 M-Z 干涉仪的相位漂移，单位时间分钟内为 1.84 rad（实验过程中温度稳定在 25℃）．

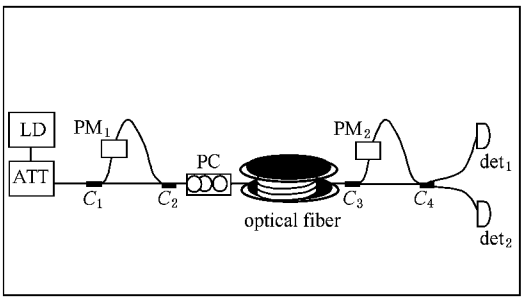

图 3 双 M-Z 光纤干涉仪相位漂移研究方案

3. 双 M-Z 型 QKD 系统相位漂移补偿方案和实验

3.1. 双 M-Z 干涉仪强度传输系数的分析

基于双 M-Z 干涉仪的 QKD 系统，是由 4 个 2×2 耦合器级联构成的不等臂干涉仪获得干涉进行量子密钥分配的．如图 3 所示，两个不等臂 M-Z 干涉仪的传输矩阵由下式给出：

$$\begin{aligned} M_{\mathrm{MZ}_1} &= M_{2\times2}(C_2)\,M_1\,M_{2\times2}(C_1), \\ M_{\mathrm{MZ}_2} &= M_{2\times2}(C_3)\,M_2\,M_{2\times2}(C_4), \\ M_{2\times2}(C_1) &= M_{2\times2}(C_2) \\ &= M_{2\times2}(C_3) = M_{2\times2}(C_4) \\ &= \begin{bmatrix} \sqrt{\varepsilon} & -i\sqrt{1-\phi} \\ -i\sqrt{1-\varepsilon} & \sqrt{\varepsilon} \end{bmatrix}, \end{aligned} \tag{1}$$

$$M_1 = \begin{bmatrix} \exp\left(\mathrm{i}\dfrac{L_1}{\lambda}\cdot 2\pi\right) A\exp(\mathrm{i}\phi_1) & 0 \\ 0 & \exp\left(\mathrm{i}\dfrac{L_2}{\lambda}\cdot 2\pi\right) \end{bmatrix}, \tag{2}$$

$$M_2 = \begin{bmatrix} \exp\left(\mathrm{i}\dfrac{L_3}{\lambda}\cdot 2\pi\right) A\exp(\mathrm{i}\phi_1) & 0 \\ 0 & \exp\left(\mathrm{i}\dfrac{L_4}{\lambda}\cdot 2\pi\right) \end{bmatrix}, \tag{3}$$

式中 $M_{2\times2}(C_1)$，$M_{2\times2}(C_2)$，$M_{2\times2}(C_3)$，$M_{2\times2}(C_4)$ 分别为耦合器的传输矩阵，M_{MZ_1}，M_{MZ_2} 为两个不等臂 M-Z 干涉仪的传输矩阵，M_1，M_2 为两对不等光纤臂

的传输矩阵，A 为调制器引起的衰减，ϕ_1，ϕ_2 为调制器引入的相移，ε 为光纤耦合器的分光比. L_1，L_2，L_3，L_4 为四个光纤臂的长度.

如图 3，激光器注入脉冲光，经耦合器 C_1 分成两束，通过 C_2 后(取上端口的输出)，再次被耦合器 C_3 分成四束到达耦合器 C_4，这四个脉冲的路径：脉冲 1 为 $C_1-L_1-C_2-C_3-L_3-C_4$，脉冲 2 为 $C_1-L_1-C_2-C_3-L_4-C_4$，脉冲 3 为 $C_1-L_2-C_2-C_3-L_3-C_4$，脉冲 4 为 $C_1-L_2-C_2-C_3-L_4-C_4$，其中 $L_1+L_2=L_3+L_4=L$，且 L_1+L_3 为短路径，L_2+L_4 为长路径，相差较大，脉冲 1 和脉冲 4 在耦合器 C_4 上先后错开，而脉冲 2 与脉冲 3 在耦合器 C_4 相遇发生干涉. 从激光器注入的光脉冲 $\begin{bmatrix} E \\ 0 \end{bmatrix}$，$E=\exp\left(-\frac{t^2}{T^2}\right)$，由此相干脉冲的输出电场为

$$\begin{bmatrix} E_1 \\ E_2 \end{bmatrix}=\begin{bmatrix} -\varepsilon\cdot(1-\varepsilon)\cdot E\cdot A\cdot\exp\left(\frac{\mathrm{i}2\pi L}{\lambda}\right)\cdot\exp(\mathrm{i}\phi_2)[1+\exp(\Delta\phi)] \\ -\mathrm{i}\cdot\sqrt{\varepsilon}\cdot\sqrt{1-\varepsilon}\cdot E\cdot A\cdot\exp\left(\frac{\mathrm{i}2\pi L}{\lambda}\right)\cdot\exp(\mathrm{i}\phi_2)[1-\varepsilon-\varepsilon\cdot\exp(\Delta\phi)] \end{bmatrix}, \tag{5}$$

式中 E_1，E_2 分别为 $\det_1$，$\det_2$ 的电场强度，则 $I_0=E^2$，$I_1=E_1^2=\alpha_1\cdot I_0$，$I_2=E_2^2=\alpha_2\cdot I_0$，那么，

$$\alpha_1=A_1(1+\cos\Delta\phi),$$

其中

$$A_1=2\cdot\varepsilon^2\cdot(1-\varepsilon^2)\cdot A^2. \tag{6}$$

$$\alpha_2=A_2+A'_2(1-\cos\Delta\phi), \tag{7}$$

其中 $A_2=(\varepsilon-\varepsilon^2)\cdot(1-4\varepsilon+4\varepsilon^2)\cdot A^2$，$A'_2=2\varepsilon^2\cdot(1-\varepsilon)^2\cdot A^2$.

实际应用的双 M-Z 干涉仪型 QKD 系统，$\Delta\phi=\Delta\phi_0+\Delta\phi_s$，其中 $\Delta\phi_s$ 为环境引起的相位漂移. 相位漂移由高频振动和低频振动两部分组成. 采用技术隔振措施消除高频部分，则 $\Delta\phi_s$ 为剩余低频部分，可分解为若干谐振波 $X(t)=A_V\sin(\omega t+\beta)$[17] 的叠加.

3.2. 补偿原理

3.2.1. 基于贝塞尔函数谐波分析的双 M-Z 干涉仪最佳工作点

输出的光强信号经光电检测、放大，由数据采集卡获取信号，计算机进行处理. 以 OUT_1 上端口为例，输出电压信号为

$$\begin{aligned} V&=KA_1[(1+\cos(\phi_0+\phi_s\sin\omega t)] \\ &=KA_1+KA_1[\cos\phi_0\cdot\cos(\phi_s\sin\omega t) \\ &\quad+\sin\phi_0\cdot\sin(\phi_s\sin\omega\tau)], \end{aligned} \tag{8}$$

式中 K 为正比于输入功率的常数，与光电转换效率、泊松比、波长等有关. ϕ_0 为干涉仪相位调制器引入的相位，ϕ_s 为环境引入的漂移. 根据贝塞尔函数定义，(8)式可展开为

$$\begin{aligned} V&=KA_1+KA_1\{\cos\phi_0[J_0(\phi_s) \\ &\quad-2J_2(\phi_s)\cos2\omega t \\ &\quad+2J_4(\phi)\cos4\omega t-\cdots)] \\ &\quad+\sin\phi_0[2J_1(\phi_s)\cos\omega t \\ &\quad-2J_3(\phi_s)\cos3\omega t \\ &\quad+2J_5(\phi)\cos5\omega t-\cdots)]\}, \end{aligned} \tag{9}$$

式中的直流项和基频分量(忽略高阶项)为

$$\begin{aligned} V&\propto KA_1+KA_1[\cos\phi_0(J_0(\phi_s)) \\ &\quad+\sin\phi_0(2J_1(\phi_s)\cos\omega t)]. \end{aligned} \tag{10}$$

当 ϕ_0 在 $\frac{\pi}{2}+k\pi$(k 为整数)附近时，(10)式中 $\cos\phi_0(J_0(\phi_s)$ 项可忽略，V 输出信号最大. 当 ϕ_0 在 $k\pi$ 附近时 $\sin\phi_0(2J_1(\phi_s)\cos\omega t)$ 项可忽略，$KA_1+KA_1[\cos\phi_0(J_0(\phi_s)]$ 趋近于 0，V 衰落严重.

因此，对基于双 M-Z 干涉仪的 QKD 系统，在密码分发之前(PM_1，PM_2 调相置零)，采用 PM_3(假定在如图 3 耦合器 C_3，C_4 的短臂引入)主动补偿 $\Delta\phi'=\left(\frac{\pi}{2}-\phi_0\right)$，使双 M-Z 干涉仪工作点保持在 $\Delta\phi_s=\frac{\pi}{2}+k\pi$ 可克服振动引起的漂移，V 输出信号最大，灵敏度高. 则(8)式中 ϕ_0 相当于由 $\phi_s\sin\omega t$ 引起的，此时补偿器 PM_3 相当于“外界环境”，单光子探测光子统计计数直接记录了相位漂移的光子干涉事件.

3.2.2. 以单光子探测光子统计计数表征的干涉相位漂移实时检测及补偿方案

基于上面的研究，实验中采用时间分通道，实时检测主动补偿(占 ms 量级)、量子密钥分配周期性交替进行，精密控制的 PM_2 代替了 PM_3.

以单光子探测光子统计计数表征的干涉信号曲线 $N(\varphi)$ 为

$$N(\varphi) = (N_{\max} - N_{\min})\sin^2\left[\frac{\varphi_2 - \varphi_1}{2}\right] + N_{\min}, \quad (11)$$

式中 $N_{\max}$ 为(0—2π)周期内的最大计数值,$N_{\min}$ 为最小计数值(实际上为暗计数).单光子计数器选择对称相位的 5 个采样点,记录光子事件,跟踪探测点 φ_1.

$$N(\varphi_0) = (N_{\max} - N_{\min}) \times \sin^2\left[\frac{(\varphi_0 - 0)}{2}\right] + N_{\min}, \quad (12)$$

$$N_{1+} = N\left(\varphi_0 + \frac{\pi}{2}\right) = (N_{\max 1} - N_{\min 1}) \times \sin^2\left[\frac{\left(\varphi_0 + \frac{\pi}{2}\right) - \varphi_1}{2}\right] + N_{\min 1}, \quad (\varphi_1 = \varphi_0 + \Delta\varphi'_{1+}), \quad (13)$$

$$N_{1-} = N\left(\varphi_0 - \frac{\pi}{2}\right) = (N_{\max 1} - N_{\min 1}) \times \sin^2\left[\frac{\left(\varphi_0 - \frac{\pi}{2}\right) - \varphi_1}{2}\right] + N_{\min 1}, \quad (\varphi_1 = \varphi_0 + \Delta\varphi'_{1-}), \quad (14)$$

$$N_{2+} = N\left(\varphi_0 + \frac{\pi}{2}\right) = (N_{\max 2} - N_{\min 2}) \times \sin^2\left[\frac{\left(\varphi_0 + \frac{\pi}{2}\right) - \varphi_1}{2}\right] + N_{\min 2}, \quad (\varphi_1 = \varphi_0 + \Delta\varphi'_{2+}), \quad (15)$$

$$N_{2-} = N\left(\varphi_0 - \frac{\pi}{2}\right) = (N_{\max 2} - N_{\min 2}) \times \sin^2\left[\frac{\left(\varphi_0 - \frac{\pi}{2}\right) - \varphi_1}{2}\right] + N_{\min 2}, \quad (\varphi_1 = \varphi_0 + \Delta\varphi'_{2-}), \quad (16)$$

可得

$$\Delta\varphi' = \frac{1}{2}\left(\frac{\Delta\varphi'_{1+} + \Delta\varphi_{1-}}{2} + \frac{\Delta\varphi'_{2+} + \Delta\varphi'_{2-}}{2}\right),$$

$$\Delta\varphi' = \frac{1}{4}\left[\arccos\left(2\frac{N_{\min 1} - N_{1+}}{N_{\max 1} - N_{\min 1}} + 1\right) - \arccos\left(2\frac{N_{\min 1} - N_{1-}}{N_{\max 1} - N_{\min 1}} + 1\right) + \arccos\left(2\frac{N_{\min 2} - N_{2-}}{N_{\max 2} - N_{\min 2}} + 1\right) - \arccos\left(2\frac{N_{\min 2} - N_{2+}}{N_{\max 2} - N_{\min 2}} + 1\right)\right]. \quad (17)$$

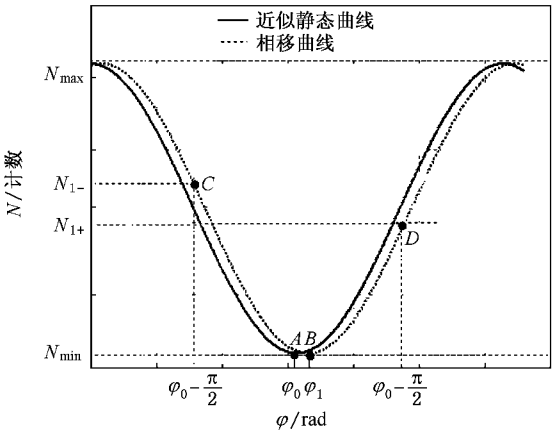

图 4 $\det_1$ 探测器端对称相移采样点计数

量子密钥分配通信之前,Alice 端的 PM_1 未调相,Bob 端的 PM_2 首先以一个较小步进数扫描整个相位范围(0—2π),$\det_1$ 和 $\det_2$ 探测器记录每一步扫描的光子数 N_i,Bob 记录与 PM_2 调制相位 φ_i 对应的 V_i 值,可获得 $N_{\max}$,$N_{\min}$ 光子计数对应的 $V'_{\max}$ 和 $V'_{\min}$,其中 $\varphi_0 = \frac{\varphi_{\det_1 \min} + \varphi_{\det_2 \min} + \pi}{2}$,第二步 PM_2 往返选择统计偏差率大的对称相移[18] $\varphi_0 + \frac{\pi}{2}$ 和 $\varphi_0 - \frac{\pi}{2}$ 采样点,单光子探测器 $\det_1$,$\det_2$ 进行光子统计,记录光子事件(如图 4 为 $\det_1$ 探测器采样点).

偏移量 $\Delta\varphi'$ 实时检测改善了精度,其对应的电压为 $\Delta V'$,为此我们获得工作点设定电压 $V_{\max} = V'_{\max} + \Delta V'$ 或 $V_{\min} = V'_{\min} + \Delta V'$,周期性测试实际工作点的 V_i,主动补偿 $\Delta V_i = V_{\max} - V_i$ 后,进行量子密钥分配.

3.3. 实验装置

图 5 是我们的实验装置框图.光源使用多通道皮秒二极管激光器(PDL808),脉冲宽度为 50 ps,经衰减后每脉冲平均光子数 $\mu \approx 0.2$.嵌入式模块 ARM_a 触发激光器的重复频率为 50 kHz. 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,Bob 端 ARM_b 主控 Bob 端单光子探测器(SPDM id200),并采用门控技术,其中 Track 模块进行干涉信号高速数据采集、相位调制电压输入,Comp 模块 D/A 输出反馈补偿电压,从而精密控制相位补偿调制器.

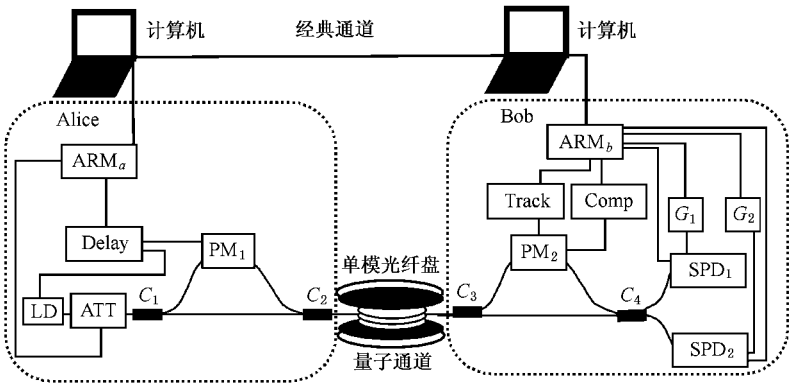

图 5　实时检测相位跟踪补偿实验装置功能框图

单光子计数器光子统计计数实时监测，跟踪采集的数据先存入 2×32 Mb 的 FIFO(fist in fist out)缓存，PC 机后台高速处理. 将实时检测的电压 $V_i=\varphi'\frac{V}{\pi}$(与实时相位相对应，其中 PM_2 的半波电压 V 为 ±5 V)与设定工作电压值比较 $V'_i=V_{\max}-V_i$，输出反馈电压，加载 Bob 端 PM_2 电压，获得补偿. 量子密钥分配由两个 ARM 嵌入式计算机模块完成，采用 BB84 协议. 两个 ARM 嵌入计算机，由短于 5 m 导线连接同步，传输距离为 75 km 单模光纤盘提供. 量子密钥分配前自动实时跟踪补偿，通信时计算机向 ARM 发指令，ARM_a 启动激光器，随机调相 PM_1，ARM_b 控制相位调制器 PM_2，光子计数器的门控，以及单光子探测光子统计计数实时采集，经双方 ARM 进行密码比对、筛选分配，提取密钥，并经 RS232 串口进入计算机，应用于文档、图像等文件的加密解密，通过局域网完成量子保密通信. 环境引起的低频振动相位变化周期在数 min 量级(3—10 min)，一次密钥分配时间为数 s 量级，而相位实时检测、跟踪补偿时间为 ms 量级，占用时间通道小，因此利用计算机可以顺利完成相位检测、自动跟踪补偿、密钥分配. 每 3 s 进行一次跟踪补偿，可以长期稳定运转. 表 1、表 2 是实验室内实现 75 km 长期稳定量子保密通信所获得的 16 进制密钥.

3.4. 补偿精度及实时性分析

经典的双 M-Z 型 QKD 系统的相位漂移为 0.60 rad/min[15]，我们实验室构建的双 M-Z 量子密钥分配方案，实验测得漂移 R_{drift} 速率最快为 2.85 rad/min. 实验中扫描周期 $T=3$ s. 下面对补偿精度及跟踪实时性分析.

对(11)式在 $\frac{\pi}{2}$ 处求导，得 $\frac{\Delta N}{\Delta\varphi}=\frac{N_{\max}-N_{\min}}{2}$，由于光子数 N 符合泊松分布，近似为高斯分布 $\Delta N=k\sigma=\sqrt{\frac{N_{\max}-N_{\min}}{2}}$，可得瞬时探测最大光子数

$$N_{\text{total}}=2\frac{k^2}{\Delta\varphi^2}. \tag{18}$$

对于一个误码率较低为 1% 的系统，其对应的相位不匹配量为 $\Delta\varphi=0.17$ rad(等价于相位漂移[19])，根据(18)式，k 为标准偏差数取 2，则 $N_{\text{total}}=2\frac{k^2}{\Delta\varphi^2}=262$ 计数量，而 APD 型(SPDM id200)探测器在量子比特误码率(QBER)极限值 11% 时，最低探测速率不低于 5000 counts/s，则计数时间约为 50 ms. 50 ms 计数时间内(ARM_b 高速数据采集和控制的后台处理几乎同时进行)以最快漂移速度发生的相位漂移为 $\varphi_{\text{drift}_{\max}}=50\times\frac{1}{6000}\text{min}\times2.85\text{ rad/min}=0.0024\text{ rad}$.

定义补偿实时效率为有效相位补偿量和实际相位漂移量的比值

$$\eta=\frac{\Delta\varphi}{\Delta\varphi+\varphi_{\text{drift}}}=\frac{0.17}{0.17+0.0024}\%=98.6\%.$$

定义补偿精度为补偿相位漂移量与工作点相位的比值

$$C=\frac{\Delta\varphi}{\phi_0}=\frac{R_{\text{drift}}\cdot(T-t_1-t_2)}{\pi/2},$$

式中 T 为探测周期，t_1 为计数器计数时间，t_2 为软件数据处理和控制时间，t_1，t_2 为 ms 量级，可忽略，

取 $T = 3$ s，最大的 $R_{\text{drift}} = 2.85$ rad/min，则 $C = \frac{3\text{s} \times 2.85\ \text{rad}/60\ \text{s}}{\pi/2\ \text{rad}} = 0.091$ 为最粗糙的精度. 若取经典的双 M-Z 量子密钥分配系统[15] $R_{\text{drift}} = 0.60$ rad/min，则可达到 $C = 0.019$ 的精度.

4. 实验结果与讨论

4.1. 相位漂移实时跟踪实验结果

图 6 是 2π 周期内 18 步长静态扫描的结果，可快速确定极值点. 图 7 是双 M-Z 干涉仪 QKD 系统 ϕ_s 工作点单光子干涉实时监测.

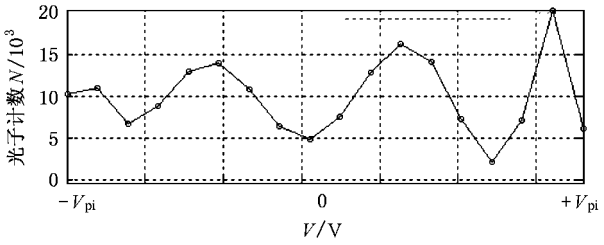

图 6 2 pi 周期内 18 步长静态扫描

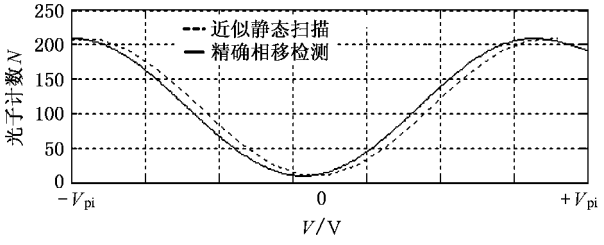

图 7 M-Z 工作点单光子干涉实时检测

4.2. 相位补偿结果及量子密钥分配

图 8 是双 M-Z 干涉仪型 QKD 系统工作点 ϕ_s 单光子干涉光强-时间曲线对照，稳定工作点相位补偿偏差约为 $1.06/16.6 = 6.39\%$. 图 9 是以 18 步长静态扫描补偿电压、理论补偿电压和经过偏置测量的补偿电压控制稳定工作点过程的对照，图中约 0.5 min 处抖动为系统启动时间. 表 1、表 2 是 75 km 量子通道上的密钥分配，密钥序列为 1024 bits，误码率 $< 6\%$.

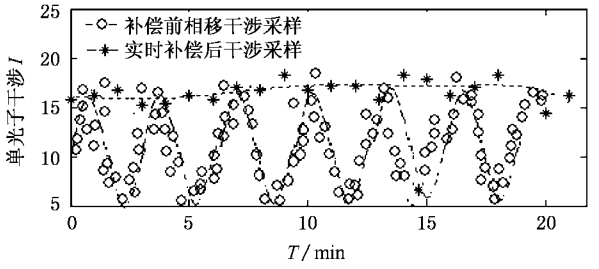

图 8 QKD 系统工作点单光子干涉相对光强-时间曲线对照

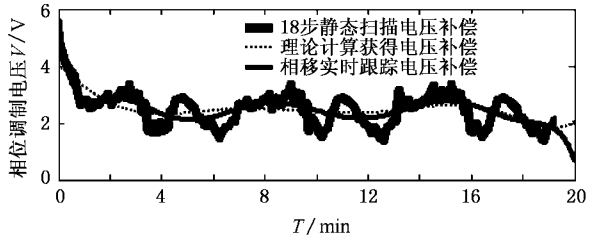

图 9 相位补偿电压控制工作点过程电压-时间曲线

表 1 Alice 端密码本

B0 B0 B1 B2 B3 B4 55 AA 15 F9 79 B5 28 95 ED 56 E2 E9 ED 65 5D 8D 2D 09 29 B4 D1 A5 79 3D B5 F5 55 D5 2D E8 75 3D DD 42 99 89 51 DD FD 79 71 5D F2 F3 11 4D CD F9 45 55 6D E9 ED B9 25 29 A5 69 6D 5E FD E2 D9 C9 D4 F9 69 4D A9 39 65 7D D9 C9 E8 31 31 2D 2D F9 35 61 39 62 05 F4 89 D9 A5 DD D7 61 71 E5 65 A1 25 B5 B1 35 A9 89 E8 0D 15 3D 99 B9 B1 39 D8 A5 35 ED 85 E9 42 A9 79 B5 F5 CD E8 FD 55 AD 15 F5 11 05 AA 55

表 2 Bob 端密码本

B0 B0 B1 B2 B3 B4 AA55 25 F9 79 B5 29 95 ED 55 E1 E9 ED 65 5D 8D 1D 09 29 B5 D1 A5 79 2D B5 F5 65 D5 2D E9 75 3D DD 41 99 89 51 D D FD 89 71 5D F1 F1 11 4D CD F9 45 65 7D E9 ED B9 15 29 A5 69 7D E9 FD E1 D9 C9 D5 F8 69 4D A9 49 65 7D D9 C9 E9 41 31 2D 2D F9 35 61 39 61 05 F5 89 D9 A5 DD D9 71 71 E5 65 A1 25 B5 B1 35 A9 89 E9 0D 25 3D 99 B9 B1 39 D9 A5 35 ED 85 E9 41 A9 79 B5 F5 CD E9 FD 55 AD 15 F5 11 05 AA 55

4.3. 讨　论

FM 方案[10]、严格的热和机械隔离方案[13,14]侧重于结构化方式，改变原有方案、增加器件，表 3 是三种主动补偿方案的比较，本文的方案不引入器件，补偿量是其他方案的几倍，稳定实现量子通信.

在本文的方案中，令当前补偿周期 T 秒内相位漂移量 $\Delta\varphi = T \cdot R_i$，$t_1$，$t_2$ 时间（ms 量级）内实时发生的漂移量 $\Delta\varphi = (t_1 + t_2) \cdot R_{i+1}$，则 $R_{\max} = R_{i+1} \leq \frac{T}{t_1 + t_2} R_i$（其中 R_i，R_{i+1} 为即时漂移速率）为补偿对相位漂移速率的限制，通常的基于双 M-Z 干涉仪量子密钥分配系统都能满足.根据(6)，(7)式耦合器分光比可选（通常取 $\varepsilon = \frac{1}{2}$），适用范围宽.

表 3　主动补偿方案比较

补偿方案	系统漂移速率 /(rad/min)	检测周期/s	补偿相移量 (ms 量级时间内)/rad	附加有源器件	量子比特误码率
Marand 等[15]	0.60	5	0.05	PZT	4%
Brylevski[16]	2.00	3	0.10	–	未进行量子保密通信
本文的跟踪补偿	2.85	3	0.15	–	<6%

5. 结　论

双 M-Z 量子密钥分配系统是最早实现量子密钥分配的实验系统，有较好的安全性，但对环境影响敏感.我们对相位漂移进行了测量和分析，发现双 M-Z 量子密钥分配系统的相位漂移由高频快变化和低谱慢变化组成，研究表明，配合其他隔振措施长达分钟量级的周期性固有振动依然存在，而且对量子密钥分发系统有重要影响.采用单光子计数表征的干涉相位实时跟踪补偿是一种有效的方法，既继承较好的安全性，又实现了较高的稳定性 能实现双 M-Z 型量子密钥分配系统长距离稳定运行，为实用提供了可能.

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

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

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

[4] Tang Z L, Li M, Wei Z J, Lu F, Liao C J, Liu S H 2005 *Acta Phys. Sin.* **54** 2534 (in Chinese) [唐志列、李　铭、魏正军、卢　非、廖常俊、刘颂豪 2005 物理学报 **54** 2534]

[5] 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]

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

[7] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 0961 (in Chinese) [杨　理、吴令安、刘颂豪 2002 物理学报 **51** 0961]

[8] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨　理、吴令安、刘颂豪 2002 物理学报 **51** 2446]

[9] Liu J M, Li J, Guo G C 2002 *Chin. Phys.* **11** 339

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

[11] Inoue K, Waks, Yamamoto Y 2002 *Phys. Rev. Lett.* **890** 37902

[12] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **52** 2123 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **52** 2123]

[13] Hugo Zbinden, Rue de l 'E' cole-de-Me' decine 20, CH-1211 Geneva 4, Switzerland (personal communication 2001)

[14] Pellegrini S, "EQUIS project," http://www.phy.hw.ac.uk/resrev/EQUIS/; see p. WP4, "Integrated Mach-Zehnder/Michelson interferometer."

[15] Marand C, Townsend P D 1995 *Opt. Lett.* **20** 1695

[16] Brylevski A (M.S. thesis) [written at the Department of Physical Electronics, Norwegian University of Science and Technology and defended at the Department of Radiophysics, St. Petersburg State Technical University, St. Petersburg, Russia, 2002]

[17] Wu X M 2001 *Ph. D. Dissertation* (Nanjing University of Science and Technology) p17—26

[18] Hui M, Wand D S, Deng M N, Li Q X, Xu Y X 2003 *Acta Phot. Sin.* **32** 477 [惠　梅、王东生、邓茂年、李庆祥、徐毓娴 2003 光子学报 **32** 477]

[19] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Quantum Cryptography Reviews of Modern Physics*. **74** 166

Real-time low-frequency vibration phase drift tracking and auto-compensation in phase-coded quantum key distribution system*

Guo Bang-Hong[1)2)†] Lu Yi-Qun[1)] Wang Fa-Qiang[1)] Zhao Feng[1)] Hu Ming[1)]
Lin Yi-Man[1)] Liao Chang-Jun[1)] Liu Song-Hao[1)]

1)(*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2)(*School for Computer and Electronic Information Maoming College, Maoming* 525000, *China*)

(Received 1 October 2006; revised manuscript received 20 November 2006)

Abstract

Phase drift caused by environment is the main source of quantum bit error rate and instability in the double M-Z interferometer quantum key distribution (QKD) system. The phase drift consists of both high-frequency and low-frequency vibrations, the former, which is due to environment noise, is usually conducted via the atmosphere and can be isolated by technological measures (e.g. using foamed-plastics wrapping or rubber pillow), the latter comes from building-vibration, which vibrates slowly with a serious impact on M-Z interferometer, with a period of 3 ± 0.32 min (min level). A novel real-time tracking and compensation method for phase drift caused by low-frequency vibration is proposed. With the improved scheme, the QKD system based on double M-Z interferometers can operate stably for 24 hours, and key exchange with an error below 6% over 75 kilometers has been achieved in the lab.

Keywords: quantum cryptography, quantum key distribution, low-frequency concuss, real-time phase compensation
PACC: 0365, 4250

* Project supported by the State Key Development Program for Basic Research of China (Grant No. G2001CB309302), also by the Gangzhou Committee of Science and Technology of Guangdong Province of China (Grant No. 1999-Z-035-01).

† E-mail: qkdslab@126.com