基于法拉第-麦克尔逊干涉检测的低误码差分相位编码实验系统*

魏正军[1)] 万 伟[2)] 王金东[1)†] 廖常俊[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 510006)

2)(广东广播电视大学,广州 510091)

(2011 年 2 月 7 日收到;2011 年 4 月 9 日收到修改稿)

采用法拉第-麦克尔逊干涉仪检测的方法实现了基于强度调制的弱相干光脉冲的差分相位编码系统. 系统针对各个可能引起误码的关键环节提出并采用了相关物理方案来减小系统的误码,采用可以产生高精度任意频率的小数分频的锁相环时钟发生器为系统提供时钟信号,减小了由于通信双方时域不匹配而带来的误码;采用单光子计数水平下高精度实时测量行波相位调制器半波电压的新方法减小了由于不准确加载相位电压引起的误码;采用单光子计数水平下的法拉第-麦克尔逊干涉仪解决自动补偿单光子脉冲干涉的偏振匹配问题,提高了系统的干涉对比度,实验结果实现了 50 km 传输距离时误码率为 3.9% 的量子密钥分发.

关键词: 量子保密通信, 量子密钥分发, 差分相位编码, 法拉第-麦克尔逊干涉仪

PACS: 42.50.Ar,03.67.-a,42.79.Sz,95.75.Kk

1. 引 言

量子保密通信系统的安全性是基于物理学的基本原理,利用单量子作为密钥传输的载体,并和经典保密通信领域中唯一被证明是绝对安全的一次一密的密码体制相结合,为信息安全领域提供了一种可行的,理论上被证明绝对安全的通信机理. 量子力学的测不准原理和未知量子态不可克隆原理保证了单量子态用于密钥分配的理论安全性. 量子密码的最初思想是 1969 年 Wiesner 首先提出来的[1]. 1984 年, Bennett 和 Brassard 提出了量子密钥分配的概念[2],这个概念的提出标志着量子密码的真正开始. 自量子密钥分配的概念被提出以来,在近 30 年的时间里,该领域在理论和实验上都取得了显著的进展[3—7],成为量子光学领域最接近实际应用的方向之一,其广泛的应用前景也普遍受到了包括军事、商业、外交、金融等各领域的重视,目前已经进入应用研究阶段.

量子密钥分发系统常采用偏振编码或相位编码的方式,相比偏振编码而言, 光子信号在光纤中传输时其相位信息更易保持, 因此绝大多数现有的光纤量子密钥分发系统都采用相位编码方案[8]. 对于相位编码系统,由于差分相位编码系统具有较高的密钥生成效率、最大的高速潜力以及在安全性方面具有对光子数分裂攻击(PNS)的免疫力,因此受到了普遍的关注和研究[9—12]. 目前基于差分相位编码方案的量子密钥分发系统一般采用单比特 M-Z 延迟环的方法进行干涉检测,这种方法需要仔细地控制干涉叠加的相干单光子脉冲之间的偏振态以得到高的干涉对比度[12—14],而郭光灿小组将 F-M 干涉检测的方法应用于 BB84 相位编码系统取得了很好地效果,证明该结构可以在外界环境引起偏振特性随机变化时仍旧能够保持干涉输出的稳定性[15]. 除此之外,基于强度调制的弱相干光的差分相位编码系统中强度调制器的时钟周期和干涉检测环的匹配以及时间抖动都会在一定程度上影响系统的误码率[16].

* 广州市科技支撑计划(批准号:2008Z1-D501),广东省工业攻关项目(批准号:2007B010400009)和中国科学院量子信息技术重点实验室开放课题资助的课题.

† 通讯联系人. E-mail:jindongwqkd@126.com

本文在基于强度调制弱相干光的差分相位编码系统中首次引入了法拉第-麦克尔逊(F-M)干涉检测的方法进行量子密钥信息的检测,可以自动补偿偏振态的变化. 实验中我们还进一步针对可能引入误码的各个环节提出了相应的技术方案,引入了一系列相关技术来减小系统误码. 这些方案包括利用小数分频的锁相环时钟产生技术实现了低抖动的强度调制器的任意时钟发生器,利用该时钟发生器可达到 0.02 ps 的时间分辨率,可以很好地解决强度调制的时钟周期和干涉检测环延迟时间的匹配问题;采用单光子计数水平下高精度实时测量行波相位调制器半波电压的新方法减小了系统由于相位信息加载不准确带来的系统误码;采用单光子计数水平下高效的主动相位补偿的方法使得系统可以长期高效稳定工作;采用在同一条光纤中同时传输同步时钟降低了实际应用中用户应用环境的需求,实验结果实现了 50 km 传输距离时误码率为 3.9% 的量子密钥分发.

2. 基于 F-M 干涉检测的弱相干光差分相位编码系统

图 1 是采用 F-M 干涉检测的弱相干光差分相位编码量子密钥分发系统的示意图. 系统采用嵌入式计算机控制系统,系统通过自制的 D/A 转换电路控制 1550 nm 连续激光器的输出功率,强度调制器(IM)由系统时钟触发,利用自制的窄脉冲发生器调制生成脉冲宽度为 5 ns 的矩形激光脉冲,在系统时钟的触发下,自制随机码发生器控制相位调制器的驱动电路使相位调制器(PM)随机加载 0 或 π 的相位信息. 然后通过衰减器进行强衰减至安全传输的最佳每脉冲平均光子数 0.2[17] 后通过传输光纤发送给 Bob. Alice 端通过系统时钟控制一个 1310 nm 的时钟激光器(clock)产生窄激光脉冲,和量子信号通过高隔离度波分复用器(WDM)后进入传输信道,传送给 Bob. Bob 首先利用高隔离度解波分复用器将时钟信号光和量子信号光分离,时钟信号光通过一个带时钟恢复功能的光电探测器后转变为 TTL 的时钟信号,Bob 端的控制系统由该时钟信号进行控制. 量子信号光经过一个偏振无关的环形器之后进入 F-M 干涉仪对 Alice 调制的相位信息进行检测,干涉输出经过两个单光子探测器 APD1 和 APD2 进行光子计数后输出. 和其他差分相位编码系统文献不同的是,系统采用了 F-M 干涉检测的方法,可以自动补偿单光子脉冲干涉时的偏振态使得光学系统可以达到较高的干涉对比度.

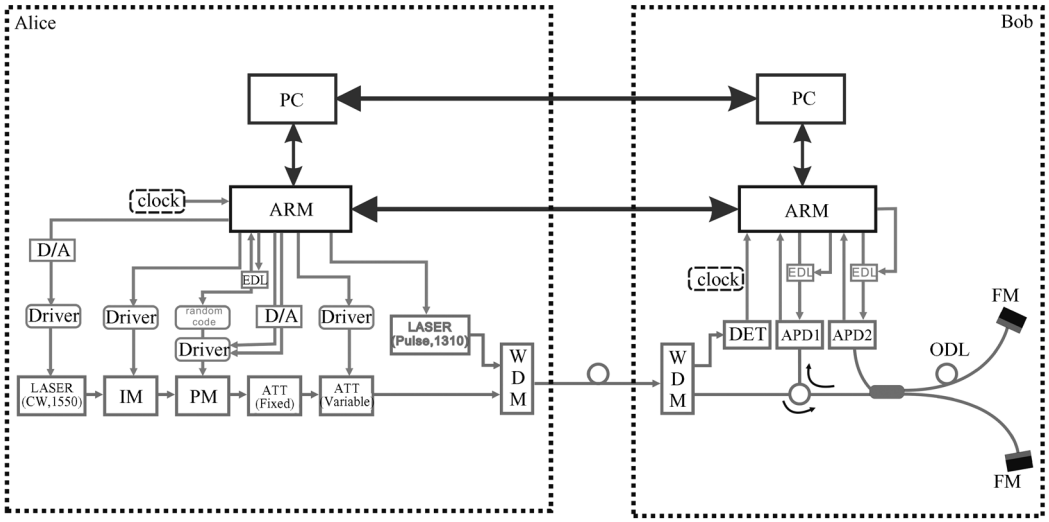

图 1 基于 F-M 干涉检测的弱相干光差分相位编码量子密钥分发系统示意图(图中,IM 为强度调制器,PM 为相位调制器,ATT 为光衰减器,WDM 为波分复用器,DET 为光电探测器,APD 为基于雪崩光电二极管的单光子探测器,EDL 为电延迟线,ODL 为光延迟线,FM 为法拉第反射旋转镜)

密钥信息加载的方法按照弱相干光差分相位编码系统的协议进行,Alice 端通过自己的相位调制器随机加载 0 或 π 的相位信息,单光子脉冲在 Bob 端经过 F-M 干涉仪后分为两路,最后在 F-M 干涉仪的分束耦合器处进行干涉叠加,这两路单光子概率幅脉冲延迟时间为相邻两个光脉冲之间的时间间隔,干涉叠加的相位差取决于 Alice 端在相邻两个光脉冲上加载的相位差信息,如果 Alice 端在相邻

两个光脉冲之间的相位差为 0,则从 Bob 端的探测器 APD1 计数输出,如果相位差为 π,则从 Bob 端的探测器 APD2 输出. 由于平均每脉冲光子数被衰减为 0.2,所以系统在每个脉冲时刻探测到光子的时间不确定性保证了系统的安全性. 已有文献证明,基于强度调制的弱相干光差分相位编码系统可以较好地抵御分光子数攻击[18].

在利用 F-M 干涉仪补偿偏振衰落和光纤双折射效应的分析方面,针对本系统,我们假设 Alice 端强度调制光脉冲之间的时间间隔远小于偏振态发生变化和光纤双折射的相位变化的速度,因此,按照法拉第反射旋转镜共轭效应的结论,对于入射 F-M 干涉仪之前的两个相干单光子脉冲的偏振态完全相同,入射 F-M 干涉仪后,由于其共轭效应,可以保证干涉时两个单光子脉冲的偏振态完全相同,并可以自动补偿光纤双折射带来的相位漂移.

除此之外,差分相位编码系统需要强度调制器具有高精度的时钟调频功能以配合 Bob 端的干涉环长短两臂的光程差,相位调制器准确加载相位电压以及系统同步时钟的传输都需要进行仔细的技术处理,因此系统还针对以上物理问题提出了相应的物理原理对这些细节进行处理来进一步提高系统的量子密钥分发性能.

2.1. 任意频率精密时钟发生技术

在双 M-Z 干涉仪系统中,通信双方的两个 M-Z 干涉仪长短两臂的光程差必须要求完全相等,而在基于强度调制的弱相干光差分相位编码系统中,Alice 端调制的前后两个单光子脉冲要通过 Bob 端的 F-M 单比特延迟环进行干涉,所以要求 Alice 端必须有时钟周期可以任意调制的功能以配合 Bob 端的单比特延迟环,而该时钟的频率调制精度直接影响了系统的干涉对比度,进而影响了系统总的误码率.

如果时钟周期和 Bob 端的长短两臂光程差所对应的时间参数之间的差值为 Δt,光脉冲宽度为 t,那么干涉叠加时,相邻两个光脉冲之间无法在时域上完全叠加从而造成额外的系统误码. 这部分误码和相关时间参数之间的关系推导如下. 我们假设单光子脉冲无法在时域上完全重叠进行干涉,那么完全重叠的部分为 $t - \Delta t$, 而无法在时域上重叠的部分为 $2\Delta t$,假设总是可以通过调节相位加载电压使得重叠部分发生理想的干涉,那么不重叠部分的误码为 50%,因此,由于不完全干涉叠加带来的误码为

$$\mathrm{QBER}_{\mathrm{t}} = \frac{50\% \times 2\Delta t}{t + \Delta t}.$$

如果系统采用光脉冲的脉宽为 5 ns,那么由于通信双方时域上不完全匹配带来的误码率和时间误差 Δt 之间的关系即为上式关系,可描绘成如图 2 所示的关系曲线.

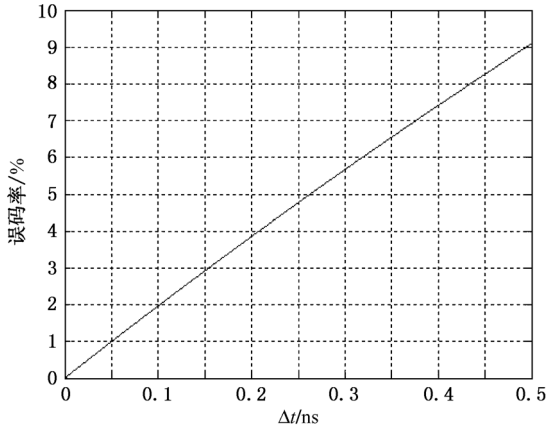

图 2 系统误码率与时域误差 Δt 之间的关系曲线

我们采用小数分频的锁相环时钟发生器方案,自制了任意频率时钟发生器,可以通过嵌入式控制系统进行设置后输出和 Bob 端干涉仪长短两臂光程差相匹配的时钟周期. 采用一级我们所研制的控制电路时,周期变化的最大步进值可以达到 150 ps,此时根据上述关系曲线,对应的误码率为 2.91%,两级串联后可以达到 0.02 ps 的步进值,其对应的误码率为 0.00039%,因此,该分辨率已经可以在系统采用 5 ns 单光子脉冲宽度的条件下足够匹配 Bob 端的单比特延迟环,产生的误码可以忽略.

2.2. 系统相位调制器半波电压的实时测量与相位电压的精确加载技术

在相位编码系统中,还有一个误码率的重要来源就是由于不准确加载相位电压引起的误码. 例如在差分相位编码系统中,按照协议要求,需要随机加载 0 或 V_π 的调相电压,但是如果系统所采用的行波相位调制器的半波电压测量不准确的话,那么最后的干涉输出将不能得到好的干涉对比度.

我们在系统中采用了单光子计数的方法实时获取相位调制器的半波电压,其数值和强光条件下测量获得的半波电压有一定的区别. 该方法还有一个重要的优势,就是在我们将测量程序固化到实际

应用系统的开机设置程序中后,当系统工作条件发生变化时,尽管行波相位调制器的半波电压会在一定程度上进行变化,但是系统的运行不会受到影响.

其物理原理是:系统开始运行时,Alice 端的相位调制器不加载任何相位,此时 Bob 端得到的单光子干涉曲线将会随着外界环境引起的相位变化而不断变化,我们首先采用被动补偿技术将外界环境引起的相位变化速度控制在可以接受的范围内. 被动补偿技术采用了九层高分子隔温隔震涂料,将 F-M 干涉仪封装在一个尺寸为 15 cm × 15 cm × 5 cm 的盒子内,实现了低至 0.0007rad/(s·m) 的相位漂移速度. 控制系统利用计算机程序实时判断 4×10^3 个单光子干涉脉冲中的单光子探测器的计数输出,当系统判断单光子探测器的输出刚好为一个计数最大和一个计数最小时,此时我们认为自然漂移的相位差为 π 的整数倍,控制系统马上通知 Alice 进行全 1 的相位调制以进行确定性量子密钥分发[19—21],全 1 的相位调制指的是在 Alice 端对相邻的两个单光子脉冲交替进行 0 和 π 的相位调制. 我们首先根据强光条件下测量的半波电压加载 π 的相位,然后根据 Bob 端输出的干涉对比度进行判断. 理论上,如果所加载的相位电压为 V_π 时,在 Bob 端将得到和判断条件完全相反的计数输出,即计数最大的单光子探测器变为计数最小,计数最小的单光子探测器变为计数最大,并且按照协议规则,在加载全 1 的相位后,Bob 端接收到的密钥信息应该全为“1”. Bob 端在一定的相位电压下得到“1”和“0”的比例,如果出现“1”的概率最大时,那么此时加载的电压即为半波电压的最优值. 我们通过实验在变化精度为 2 mV 情况下,测量了系统所采用的半波电压的数值为 3.360 V,系统未做长程传输时对应的系统误码在 0.9% 到 2% 之间变化,我们取多次平均后获得最低误码率的数据为 1.2%.

该实验数据表明,采用了单光子计数的方法实时判断相位调制器的半波电压可以较好的控制系统的误码率,并且由于在系统改变运行条件时可以不受影响,因此在实际应用中有一定的实用价值.

2.3. 基于光波分复用(WDM)技术的同步时钟传输技术

由于量子密钥分发系统采用了基于雪崩光电二极管的红外单光子探测器,所以在 Bob 端对单光子干涉结果进行检测时需要进行同步探测,因此,时钟传输技术也是系统中非常重要的部分.

由于采用电缆传输不适合进行长程传输,而采用两条光纤传输同步时钟和量子信号时,如果两条光纤的外界环境差异较大,同步性能也会缓慢恶化,图 3(a)是我们的实验系统户外测试的同步实验结果[22],实验数据表明从同步精度上讲,利用同一条光纤传输时钟信号和量子信号是最理想的选择. 我们的差分相位编码系统采用了波分复用技术,将 Alice 端的时钟信号转换为 1310 nm 的激光脉冲,通过高隔离度波分复用器和量子信号耦合到同一条光纤中进行传输. 在这种情况下,两种光信号的相互作用和器件的隔离不完善性就会在一定程度上引入系统误码. 我们和珠海光库公司合作研发了高达 80 dB 的高隔离度波分复用器以及通过窄带干涉滤光片进一步减小较强的时钟信号光到量子信道的耦合,在 75 km 同步时钟传输实验中,可以通过这些器件的处理将时钟信号光带来的误码降低到暗计数的水平,图 3(b)是通过控制注入波分复用器的时间参数得到的误码率曲线[22].

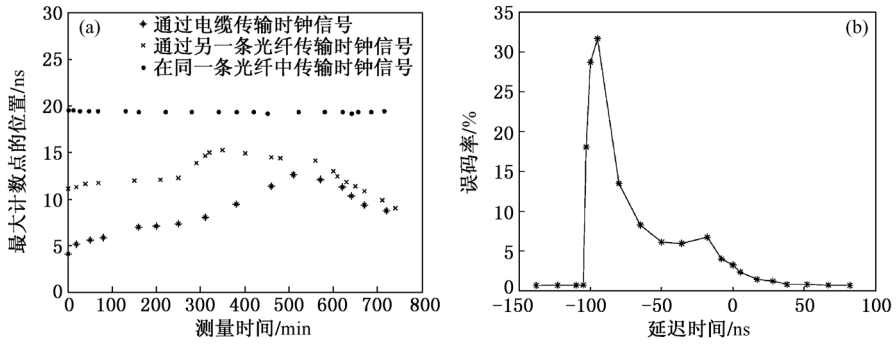

图 3 光波分复用同步传输技术户外光纤测试数据 (a)三种同步传输方式的对比数据;(b)注入光波分复用器件的时间参数和系统误码之间的关系

3. 实验结果分析

系统采用 2 MHz 的光脉冲频率,光脉冲宽度为 5 ns,上升下降时间 100 ps,传输距离为 50 km,相位调制器所加载的 0 和 V_π 的电压经过系统开机自检时进行单光子计数水平的精确测量,扫描电压的步进为 2 mV,测得 V_π 在系统工作频率下为 3.360 V,利用该半波电压的数值进行相位信息加载,同步时钟通过光波分复用技术进行传输,通过解复用利用自制电路恢复成标准的 TTL 时钟以触发单光子探测器进行光子计数. 系统进行随机相位调制编码后生成了量子密钥,密码表如表 1 所示.

表 1 系统生成的量子密钥对比表

Alice	1	1	0	1	1	0	1	1	1	0	1	1	0	0	0	1	0	1
Bob	1	1	0	1	1	0	1	1	1	0	1	1	0	0	0	1	0	1
Alice	1	1	0	**1**	1	0	0	0	0	1	0	0	0	0	0	1	1	1
Bob	1	1	0	**0**	1	0	0	0	0	1	0	0	0	0	0	1	1	1
Alice	1	1	0	1	0	0	0	0	0	1	0	0	0	**1**	1	0	1	0
Bob	1	1	0	1	0	0	0	0	0	1	0	0	0	**0**	1	0	1	0

表中错误的比特用黑体表示,经过程序对所生成密钥的统计,系统总的筛选码误码率为 3.9%. 系统最终达到的速率仍旧为 MHz 的水平,这是由于系统采用了基于雪崩光电二极管的红外单光子探测器,系统实验得到的误码率,也主要由于所采用的单光子探测器的暗计数所造成. 理想的单光子源和单光子探测器仍旧是量子密钥分发领域最关键的瓶颈技术. 如果这两种关键技术能够在实际应用中获得突破,那么本实验所采用的差分相位编码系统将可以达到很高的性能.

本实验方案中,由于采用了 F-M 干涉检测的光学结构以及一系列相关技术,达到了更低的误码率,文献[23]采用 M-Z 检测的方法,其误码率在 25 km 传输距离时为 3.2%,而我们的系统在 25 km 传输距离时误码率为 2.2%. 在所采用的精密时钟发生技术、单光子水平下精确测定半波电压的技术以及用同一条光纤传输时钟光信号的复用技术中,我们均根据误码率最低的标准进行了参数优化. 其中精密时钟发生技术在较高的工作频率下可以达到更低的抖动,系统的相位稳定性也会加强,在下一步的工作中,我们准备进一步提高系统频率,改善整体系统的性能. 而本文中采用的时钟复用技术的优点是可以高精度补偿时间漂移带来的系统性能的恶化,但其缺点是采用这种方案有一定的速率限制,在传输 100 km 时,采用目前的时钟波长,其速率限制理论计算为 3 MHz,当速率提高时,需要根据两种光相互作用的特征优化波长选择参数和光强参数来提高系统的性能,这也是我们接下来的一个研究工作.

4. 结 论

采用了 F-M 干涉检测的方法实现了基于强度调制的低误码弱相干光差分相位编码系统. 在本文提出的实验系统中,针对影响系统性能的各个环节提出了利用小数分频加锁相环技术的高精度任意时钟发生技术;在单光子计数水平下实时测定最优相位加载电压的技术以减小由于不准确加载相位电压带来的误码;利用光波分复用技术实现了在同一条光纤中传输同步时钟和量子信号光的模型,并通过相关技术处理将时钟信号光带来的附加误码降低到暗计数的水平. 采用这些技术,实现了系统 50km 传输距离时误码率为 3.9% 的差分相位编码量子密钥分发,为差分相位编码量子密钥分发系统提供了一种高效的实现方案,而各个环节的技术方案也对量子密钥分发系统的实际应用有一定的实用价值.

[1] Wiesner S 1983 *SIGACT News* **15** 78

[2] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, New York: IEEE 1984 p175

[3] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[4] Tobias S M, Henning W, Martin F, Rupert U, Felix T, Thomas S, Josep P, Zoran S, Christian K, John G R, Anton Z, Harald W 2007 *Phys. Rev. Lett.* **98** 010504

[5] Hiskett P A, Rosenberg D, Peterson C G, Hughes R J, Nam S W, Lita A E, Miller A J, Nordholt J E 2006 *New J. Phys.* **8** 193

[6] Wang J D, Lu W, Zhao F, Liu X B, Guo B H, Zhang J, Huang Y X, Lu Y Q, Liu S H 2008 *Acta Phys. Sin.* **57** 4214 (in Chinese) [王金东、路 巍、赵 峰、刘小宝、郭邦红、张 静、黄宇娴、路轶群、刘颂豪 2008 物理学报 **57** 4214]

[7] Hu H P, Zhang J, Wang J D, Huang Y X, Lu Y Q, Liu S H, Lu W 2008 *Acta Phys. Sin.* **57** 5605 (in Chinese) [胡华鹏、张 静、王金东、黄宇娴、路轶群、刘颂豪、路 巍 2008 物理学报 **57** 5605]

[8] Wang J D, Qin X J, Zhang H N, Wei Z J, Liao C J, Liu S H 2009 *Optics Communications* **282** 3379

[9] Wang J D, Wei Z J, Zhang H, Xiao J Q, Liu X B, Zhang Z M, Liao C J, Liu S H 2010 *J. Phys.* B: *At. Mol. Opt. Phys.* **43** 095504

[10] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

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

[12] Honjo T, Inoue K, Takahashi H 2004 *Optics Lett.* **29** 2797

[13] Eleni D, Hiroki T, Carsten L, Fejer M M, Yamamoto Y 2006 *Optics Experss* **14** 13073

[14] Zhang Q, Takesue H, Honjo T, Wen K, Hirohata T, Suyama M, Takiguchi Y, Kamada H, Tokura Y, Tadanaga O, Nishida Y, Asobe M, Yamamoto Y 2009 *New Journal of Physics* **11** 045010

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

[16] Wang J D, Qin x J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东、秦晓娟、刘小宝、廖常俊、刘颂豪 2010 物理学报 **59** 281]

[17] Takesue H, Sae W N, Qiang Z, Robert H, Toshimori H, Kiyoshi T, Yamamoto Y 2007 *Nat. Photonics* **1** 343

[18] Zhao Y B, Fung F C, Han Z F, Guo G C 2008 *Phys. Rev.* A **78** 042330

[19] A Eusebi, S Mancini 2009 *Quant Inf & Comp* **9** 950

[20] Zhou N R, Wang L J, Ding J, Gong L H 2010 *Physica Scripta* **81** 045009

[21] Zhou N R, Wang L J, Ding J, Gong L H 2010 *International Journal of Theoretical Physics* **49** 2035

[22] Zhong P P, Zhang H N, Wang J D, Qin X J, Wei Z J, Chen S, Liu S H 2011 *Chin. Phys.* B **20** 050307

[23] Toshimori Honjo, Atsushi Uchida, Kazuya Amano, Kunihito Hirano, Hiroyuki Someya, Haruka Okumura, Kazuyuki Yoshimura, Peter Davis and Yasuhiro Tokura 2009 *Optics Express* **17** 9053

A new differential phase shift quantum key distribution system with Faraday-Michelson interferometer*

Wei Zheng-Jun[1)] Wan Wei[2)] Wang Jin-Dong[1)†] Liao Chang-Jun[1)] Liu Song-Hao[1)]

1) (*Laboratory of Photonic Information Technology SIPSE & LQIT, South China Normal University, Guangzhou* 510006, *China*)

2) (*Guangdong Radio&TV University, Guangzhou* 510091, *China*)

(Received 7 February 2011; revised manuscript received 9 April 2011)

Abstract

A new differential phase shift quantum key distribution system based on the intensity modulator with Faraday-Michelson interferometer is demonstrated experimentally. Some technologies are employed to improve the performance of the quantum key distribution system. These technologies include the clock generation technology of arbitrary frequency by a small scale frequency-split and phase locked loop scheme, the new method to acquire the half-wave voltage of the phase modulator with a high accuracy in the condition of the single photon count, and the auto-compensated polarization technology by the Faraday-Michelson interferometer. Finally, the quantum key distribution is achieved with a quantum bit error rate of 3.9% when the transmission distance reaches 50 km.

Keywords: quantum cryptography, quantum key distribution, differential phase shift, Faraday-Michelson interferometer

PACS: 42.50.Ar, 03.67-A, 42.79.Sz, 95.75.Kk

* Project supported by the Key Projects in the Guangzhou Science & Technology Pillar Program (Grant No. 2008Z1-D501) and the Guangdong Key Technologies R&D Program (Grant No. 2007B010400009).

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