**创新点说明：**

1. 光路部分。实际实验中，优良的光路系统应具备高的稳定性，同时还要便于调试。本文使用的Plug&Play量子密钥分发系统就满足上述的优点。在不需要修改光路的情况下，可以实现如BB84和B92等协议，并且根据需要，简单的修改光路，还可以实现量子密钥共享 (Quantum Secret Sharing, QSS) 等不同的实验目的。
2. MFC微软基础类库（英语：Microsoft Foundation Classes，简称MFC）界面控制部分。本文的工作是为了量子密钥分发系统的实用化而做的软件控制部分，目的是使操作尽可能的耗时短，易于操作，利用MFC编写图形界面可以很好的实现这一目的。我们利用MFC将整个实验的过程中需要操作到的参量集成到一个图形界面中，使得操作界面傻瓜化，同时又解决了搭建平台耗时的问题，通过自扫描加手动调制相结合的方式巧妙地优化了实验步骤。而MFC的可扩展性，也可以方便后来的研究，添加新的功能。

量子密钥分发系统中的软件控制部分研究

陈倚天,刘宏伟，屈文秀，窦天琦，王吉鹏，李月梅，马海强†

（北京邮电大学理学院, 北京 100876）

摘 要：本文的重点是在整个量子密钥分发的QKD层中的的软件部分进行设计研究。研究以实验操作为主，通过编写可操作的代码，为实验室搭建整个量子通讯过程的自动化操作平台。通过编写可视界面将过程封装起来，降低对使用者编程程度的要求。实验光路控制部分由三个不同部分组成，协同合作最后实现控制，扫描，判断于一身的相位自扫描工具。我们首先给出了纠正后的琼斯矩阵分析光路，然后详细的介绍了整个软件的设计流程。

关键词：量子通信；量子密钥分发；物理学；量子光学；光通信；激光

中图分类号：□□□; □□□ 文献标识码：A 文章编号：

**Research on software control in quantum key distribution system**

CHEN Yi-Tian,LIU Hong-Wei, QU Wen-Xiu, DOU Tian-Qi, WANG Ji-Peng, LI Yue-Mei, MA Hai-Qiang(corresponding author)

(Laboratory of Quantum information, *School of science*,

*Beijing University of Post and Telecommunication*, *Beijing,*100876, *China*)

**Abstract:** The key of this article is aimed to design the software part in whole QKD system. Our work is based on experimental, and our goal is to build the automatically QKD platform by writing operable code. The code packaging process as an operable interface. Reduce the requirement level of user. And optical control is separate into three part, and with corresponding work they accomplish, finally, the phase scanning tool is implemented to control, scan, and judge. We first show the analysis of optic and prove the stability, and then introduce the entire software design process.

**Key words:** Quantum communication**;** Quantum key distrubtion; physics; Quantum Optics; Optical Communication; Lasers

**OCIS Codes:** □□□□**;** □□□□**;** □□□□**;** □□□□

**0 引言**

量子通信是近二十年发展起来的新兴交叉学科。自BB84协议于1984年被提出以来[1]，量子通信已逐渐从理论阶段进入实验阶段。三十多年后的今天，量子通信商用化的脚步已越来越快。

在我国，量子通信研究受到了中国科技部、中国科学院以及国家自然科学基金委员会等部门的高度重视和大力支持。去年，中国科技部发布了“量子调控与量子信息”重点专项 2016 年度项目申报指南，其中量子通信被列为一个独立子项重点发展。 重点研究量子通信的载体和调控原理及方法等新原理和新技术。中国科技大学、中国科学院物理所、清华大学、半导体所、武汉物理和数学研究所、北京邮电大学等国内多所高校都在量子通信领域做了大量的工作，并且取得了一些重要的成果，在国际上享有重要的影响力。随着首颗量子卫星墨子号在酒泉成功发射，我国在量子通信的竞争中后来居上，跻身国际一流。量子京沪干线也即将建成并验收，京沪两地及沿线的金融，政务机构可以利用这条线路进行远程数据备灾和量子安全数据传输。

由于量子通信的美好前景，同时近几年来相关技术上取得的飞速发展，使得除研究机构外，一些国内、国际著名的公司如美国的 IBM、Bell 实验室，英国的电话电报公司，日本的东芝公司、NEC、 NTT 等也在积极推动量子通信的商业化。这些公司的加入，也极大的推动了量子通信的发展。国际上许多大学与研究单位也相继成立了量子通信和量子密码技术产品商业化公司。如瑞士日内瓦大学 （ University of Geneva）成立的 id Quantique 公司[2]，中国科技大学潘建伟小组联合铜陵丰润集团和皖能集团合资成立的国盾量子公司。[3][4]

而最为重视量子信息科学领域的美国，在16年的七月连续发布了《推动量子信息科学：国家挑战与机遇》和《与基础科学、量子信息科学和计算交汇的量子传感器》两份报告，认真的讨论了量子信息技术的前景，机遇和挑战。指出了了量子信息前沿的方向，并详细的讨论了美国量子信息领域的相关进展和整个的科学布局。

如今，量子通信技术已经日趋成熟，一个新兴的通信产业正在孕育，兴起。

**1 量子密钥分发中软件控制部分的实验原理和实验方案**

本文重点的研究部分是量子通信系统的软件部分。

实用化量子信息通讯平台的软件设计部分一共由四个层面组成，分别是QKD层，量子密钥库层，编码层和传输层。这四个层面中QKD层是最底层的部分，是整个系统的基础，也是最为关键的部分。本文的工作也是基于QKD层。

QKD层是利用量子通信协议为基础，通过量子信道和经典的信道相结合的方式来协同获得最终的量子密钥。我们使用BB84作为实现的协议进行密钥的通信。在Alice端利用MFC进行界面的操作，并利用FPGA进行相位调制器（PM）的控制，Bob端利用Labview控制单光子探测器协助完成实现相位的自扫描过程。

本文一共分为三大部分。我们首先利用琼斯矩阵分析光路，并给出光路稳定性的证明。第二部分介绍软件部分的组成和实际软件的设计思路，最后的部分展示了实验流程并给出了分析和展望。

**1.1 实验光路部分**

量子密钥分发可以利用纠缠光、连续光以及单光子在光纤或自由空间中实现。在光纤传输中，由于相位具有很好地稳定性而被广泛使用。相位编码QKD系统普遍使用双不等臂马赫-曾德尔干涉仪，而为了使干涉仪有较好的干涉效果，常常需要借助补偿系统，而这种补偿系统价格高昂且使用复杂[5]。穆勒等人提出的plug&play QKD模型，借助法拉第镜的自补偿性质，使得光在传输过程中色散，偏振等变化自动得到补偿，进而提高了QKD系统的稳定性，降低了系统复杂性和成本。

我们提出了一种更加稳定的plug&play QKD系统，如图1所示，光脉冲由激光二极管(LD)发出，经过环形器(Cir)到达一个50/50分光镜后被分成了上下两路相同的光脉冲。上臂首先经过偏振分束器(PBS)，脉冲中的水平偏振部分可以通过，从公共口port1离开Bob端。到达Alice端后经过法拉第镜的反射伴随着光偏振方向旋转了90°，再次回到Bob端。值得注意的是，相位调制器是线性调制光相位，所以偏振光旋转90°后再次通过相位调制器可以巧妙将全部偏振方向的光调制相位。同时由于偏振的旋转，光会反射到下臂中经过下路的相位调制器和法拉第镜。再次旋转后到透射经过下臂PBS。同时下臂光会经过相同的反射过程，于是两路光总共经过的路径相同，最后到达耦合器C，并发生干涉。根据在两端调制的不同相位差在两个探测器中显示出结果。

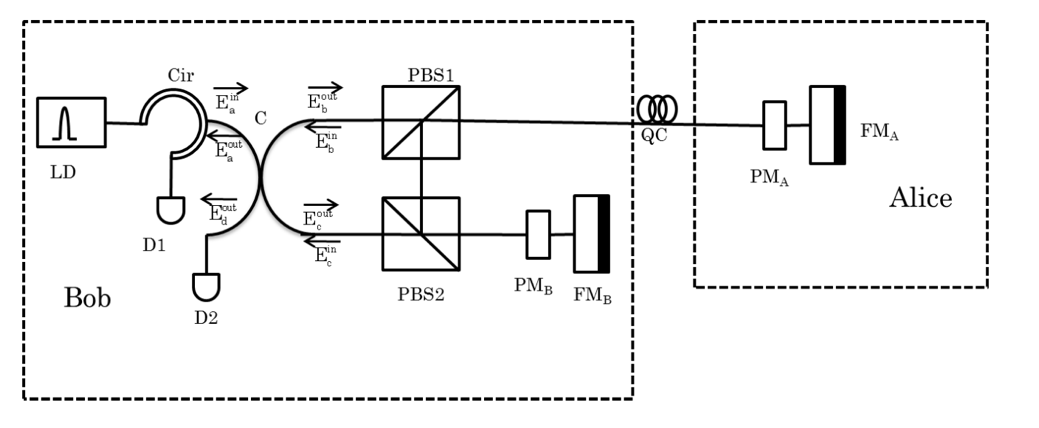


Fig.1Plug&Play干涉装置图。LD：激光二极管；Cir：环行器；C：50/50耦合器；PBS1，PBS2：偏振光束分离器；FMA,FMB法拉第镜；PMA,PMB：相位调制器；D1，D2：单光子探测器：QC：量子信道

下面我们给出光路的稳定性分析。

法拉第旋转镜是光路最核心的器件，它使得光脉冲在每个环的每条臂上来回走了两次。并且保证了两臂光传播了相同的距离。法拉第旋转镜的琼斯矩阵为



我们令光路中任意无损的光学元件的琼斯矩阵为M。当光信号在法拉第旋转镜反射前经过，琼斯矩阵为，而反射后的琼斯矩阵为。由于法拉第镜自身的性质，两个琼斯矩阵会有一些区别。所以在入射无损光学元件经法拉第镜反射再经过法拉第镜的整个过程中，我们用琼斯矩阵表示为



其中是无损光学元件引入的相位信息。我们从上式可以看出，法拉第旋转镜将输入光的偏振方向旋转了90°，相位也同时发生了变化，但无损光学元件的偏振效应被巧妙的抵消掉了。我们令这个光学元件两个轴向的损耗分别是和，则上式可以写为



同样我们看到对于偏振相关的损耗也可以进行补偿。

利用上述证明的法拉第旋转镜对于偏振自动补偿的特点，我们可以大大简化光路的分析。如图一所示，上臂干涉光先经过上臂被反射经过下臂后到达耦合器C整个过程的琼斯矩阵为



= 

同样我们给出下臂光经过整个路程的琼斯矩阵



= 

其中，和分别是相位调制器加载在上臂光和下臂光的相位，是光纤信道光程的等效相位。而则是上臂和下臂光程的等效相位，为干涉系统的光学损耗。于是我们可以用表达式表达出输入矩阵与输出矩阵脉冲关系表达式



相应地，该输出端的光强为



所以当为零时我们可以得到最大输出强度为



当为时可以得到最小输出



将得到的结果带入干涉对比度公式中，可以得到干涉条纹的可见度为



以上，我们证明了光路的干涉稳定性。

**1.2 实验实现流程**

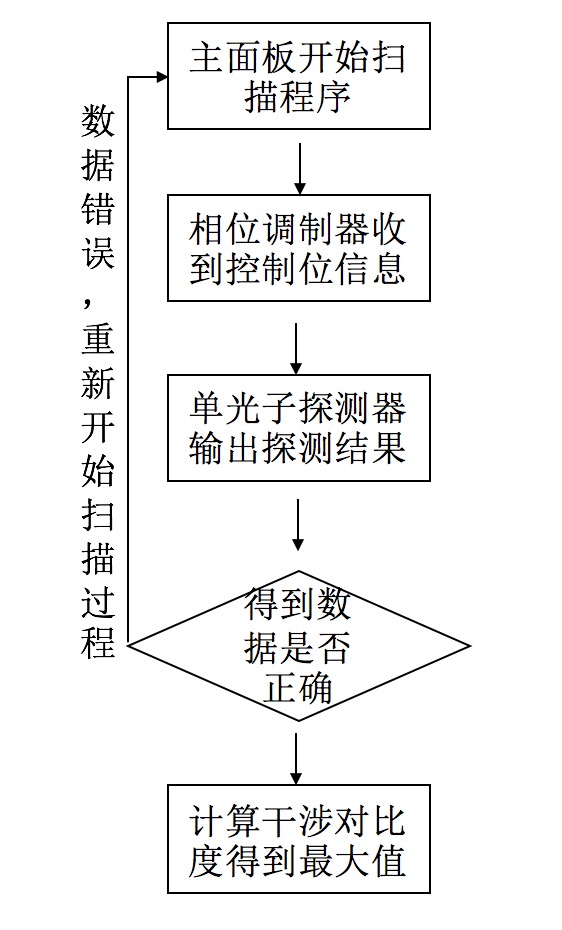


Fig.2 实现自扫描过程流程图

图二所示为相位自扫描过程的流程图。主控制面板首先触发自扫描功能，通过FPGA不断向相位调制器发送控制位信息，调制相位调制器两端的电压和时间延时。与此同时，单光子探测器通过Labview不断的输出探测信息。当单光子探测器的门宽PMW小于20ns时，由于门宽过小，探测器无法抓到相应，输出结果为0。利用上述特性，我们会在扫描即将开始和已经结束时置门宽为10ns。在读取程序中，当出现大于10个0点我们认为扫描开始，而在此出现大量0点时我们视为扫描完成。在扫描完成后，我们首先判断认定扫描数据量大于参考值(40000)时认为得到了正确扫描数据。最后我们将两个探测器得到的数据值利用干涉对比度公式进行计算，得到干涉对比度最大值的点以及对应这个点的三个变量值。至此，完成了整个的自扫描过程。

**1.3 实验软件设计**

1.3.1 MFC部分



Fig.3 用MFC编写的操作面板，其中DA1为相位调制器电压，PWM为加载脉宽，Delay1为相位调制器延时，Delay2为单光子探测器总延时。参数调制栏下面为得到的结果栏。

MFC是微软公司提供的一个类库。它将c语言程序封装起来，当我们点击按钮会触发相应的程序。实验中我们在MFC主面板中集成了控制位扫描，文件读取，数据处理功能。集成后的程序在完全满足实验要求的情况下，易于操作，即使没有编程基础也可以完成实验。

如图三所示，MFC作为整个扫描平台的中枢，它首先负责通过FPGA向相位调制器发送控制位信息，进行参数变量的循环遍历过程。我们一共有四个参数：DA1为相位调制器电压，PWM为加载脉宽，Delay1为相位调制器延时，Delay2为单光子探测器总延时。在实际的操作过程中，为了降低计算的复杂度，我们使用剪枝法，即把一定不会出现的参数变量进行人为的剔除。从而，我们选定DA1的控制范围为3.74v~5.86v；Delay1的控制范围为40ns~80ns；Delay2的控制范围为5ns~45ns。另外，我们可以进一步将PMW固定在86ms。这样可以更为精确且节约时间的进行扫描。

在扫描控制位的同时，单光子探测器利用Labview的端口读写模块将探测到的结果响应，并输出到指定文件中。最后我们读取得到的结果进行干涉对比度的计算，得到最大干涉对比度点，并将得到干涉对比度最大点时的电压，延时以及扫描总位数输出到控制面板中。

1.3.2 LabView部分

利用Labview进行数据采集有多种方式。最为简便的方式便是利用NI公司生产的数据采集板卡和Labview中的数据采集VI实现。但这种方式价格成本高，并不适合一般的科研机构。实验中，我们选用直接端口读写的(I/O)方式进行并口驱动设计。

Labview中的Advanced模块中带有两个可以直接访问物理接口设备的节点，即In Port.vi和Out Port.vi。它们可以把一个带符号的整数写入到指定的内存地址中去或读取内存地址转化为一个带符号的整数。我们通过得到PC端并口数据，状态以及控制位在寄存器中的地址，便能够实现对于探测到信号的读取与写入。当我们不断通过读取In Port.vi模块输出得到探测器端的探测数据后，再交由Labview信号输出模块处理，将输出的信号存入指定位置。实现将扫描结果输出的目的。

1.3.2 FPGA部分

实验中，我们选用的USB主机芯片EZ-Host具有功耗低，扩展性高，易于编程等特点。其

拥有两种工作模式:stand-alone, co-processor。在co-processor模式下，我们需要从三种（HPI，HSS，SPI）物理接口以及众多的外部处理器(比如：FPGA,DSP,ARM)中进行选择。

在深入研究了Cypress公司的CY7C67300 USB主机的工作原理，固件程序设计方法以及嵌入式系统相关技术后，我们选择了HPI与外部处理器FPGA相结合的方式，最终实现了FPGA和USB主机通信的嵌入式系统。

因为HPI其16根数据线具有传输速率高（16M/s），支持断点处理，控制位发送等特点，所以选择HPI实现大量数据传输自然而然。HPI的接口原理图如图四所示。

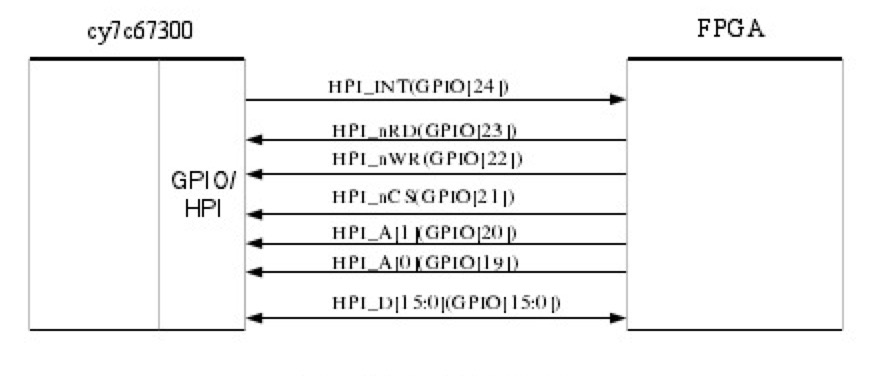


Fig.3 HPI接口原理图

我们选择co-processor模式，在此模式下FPGA将控制位描述成一套传输描述列表Todo\_list，然后再将列表发送到USB主机的BIOS，然后FPGA会根据检查到的反馈信息，以及Todo\_list信息判断进一步应该进行的操作，从而达到FPGA和USB主机通信系统的设计需求：通过FPGA控制USB主机，使得PC端控制位与USB主机进行通信。

**2 实验结果和讨论**

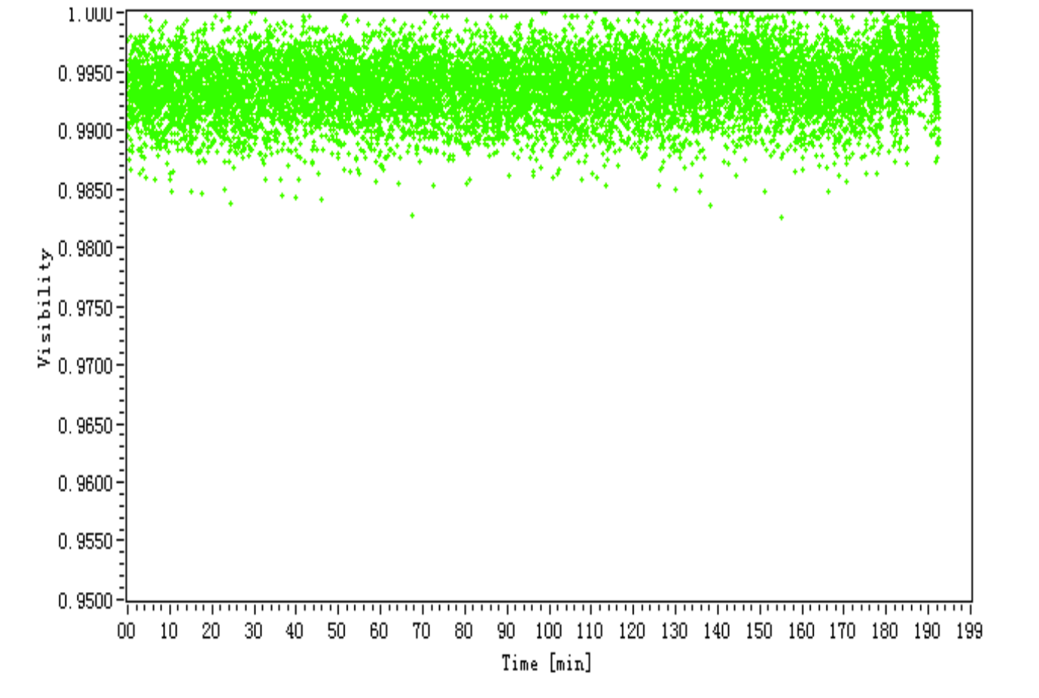


Fig.5 对于得到的干涉对比度结果进行稳定性测试

在扫描过程完成后点击GET RESULT按钮，触发程序从指定位置读取文件进行数据合理性判断，判断正确后会根据干涉对比度公式得到最终的结果。如图五所示，我们将扫描得到的最大干涉对比度结果对应值在此以手动方式输入到面板中，对得到的点进行干涉对比度的验证。我们可以看到，干涉对比度的稳定性十分稳定。这不仅证明了扫描点的正确性，也同样证明了我们实验装置的稳定性。

3 结论

量子通信的进步一定是伴随着整体实验技术的进步。而实验技术的进步就是为了使得实验过程更加的简明化，可操作性更好，耗时更短。我们所做的软件控制部分自扫描就是为了实现更快更易上手的需求。通过完成自扫描我们加快了整个平台的的搭建速度，封装了整个的扫描流程，方便了其他对于软件不太熟悉的实验操作人员。通过我们的优化已经实现了基本功能，可以实现自扫描相位，大大的节约了每次实验之前都要人为扫描的长时间操作。并且，对于实验光路图在不需要修改光路的情况下，我们还可以完成如B92等相似的协议。并且根据之后所需要完成的目标不同，简单的修改光路，还可以实现QSS等不同的实验目的。而MFC的可扩展性，也可以方便后来的研究，添加新的功能。为以后QKD进一步系统化奠定了强有力的基础。

参考文献

1. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution  and coin tossing. International
2. beam. Optics Com Conference on Computers, Systems & Signal  Processing, Bangalore, India, Dec 9-12, 1984, 1984 175-179.  .
3. idQuantique www.idquantique.com/.
4. 国盾量子 http://www.quantum-info.com/.
5. 安徽问天量子科技股份有限公司 http://www.qasky.com/.
6. Marand C., Townsend P. D. Quantum key distribution over distances as long as 30 km. Optics Letters, 20(16) 1995 1695-1697.
7. ？Muller A., Herzog T., Huttner B., et al., “Plug and play” systems for  quantum cryptography. Applied Physics Letters, 70(7) 1997 793-795.
8. ？Martinelli M. A universal compensator for polarization changes induced by birefringence on a retracing munications, 72(6) 1989 341-344.
9. Bogdanski J., Rafiei N., Bourennane M. Experimental quantum secret sharing using telecommunication fiber. Physical Review A, 78(6) 2008.
10. Pistoni N. C. Simplified approach to the Jones calculus in retracing optical circuits. Applied Optics, 34(34) 1995 7870-7876.
11. Analysis of Faraday Mirror in Auto-Compensating Quantum Key Distribution.CHIN.PHIC.LETT Vol.32,No.8(2015)080303