相位编码量子密钥分发系统的电子学设计

杨 阳[1],王永纲[1],陈 巍[2],王 双[2],张丽君[1],黄大骏[1],章 涛[1],韩正甫[2]
(1.中国科学技术大学近代物理系,安徽合肥 230026;
2.中国科学技术大学中国科学院量子信息重点实验室,安徽合肥 230026)

摘 要: 相位编码是目前基于光纤传输的量子密钥分发(QKD)系统采用最多的方式,对控制电子学的设计提出了诸多挑战.本文在介绍相位编码 QKD 系统控制电子学整体设计基础上,重点分析相位编码 QKD 系统在同步机制、自动相位扫描补偿等方面的特殊要求和设计实现.本文设计的控制电子学和必要光学器件组成的 QKD 系统可以作为量子密钥分发网络中独立节点,已成功地运行于安徽省芜湖市电信商用通信光纤网络之上,实现了多个通信节点之间使用量子密码的加密通信.整个 QKD 系统在 20MHz 的光脉冲重复速率上实现了 BB84 相位编码协议,达到了在 20km 传输距离上 2.95%的量子比特误码率(QBER)以及 4.91kbps 的安全密钥生成率.

关键词: 量子密钥分发; 相位编码; 法拉第迈克尔逊干涉仪; 现场可编程门阵列
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2011) 11-2604-06

Design of Electronics for Phase Coding QKD System

YANG Yang[1], WANG Yong-gang[1], CHEN Wei[2], WANG Shuang[2], ZHANG Li-jun[1],
HUANG Da-jun[1], ZHANG Tao[1], HAN Zheng-fu[2]
(1. *Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui* 230026, *China*;
2. *Quantum Information Key Laboratory of Chinese Academy of Science, University of Science and Technology of China, Hefei, Anhui* 230026, *China*)

Abstract: Phase coding is frequently used in current quantum key distribution(QKD) systems. It has posed many technical challenges on the design of the control electronics. After the description to the overall design of our phase coding QKD system, the paper focuses on the special requirements and implementations on the synchronizing mechanism and automatic phase drift scanning and compensation. The electronics designed in this paper combining with the optical devices can be an independent node device of a QKD network. We have successfully used these node devices to build a practical encrypted communication system through the commercial communication optical fiber system of Wuhu Telecom in Anhui Province. Encrypted communication between multiple nodes by quantum cryptography is implemented in this system. The QKD system in the network actualizes BB84 phase coding protocol at 20MHz repetition rate of light pulses. It achieves quantum bit error rate(QBER) 2.95% and secure key generation rate 4.91kbps with a 20km transmission distance.

Key words: QKD; phase coding; Faraday-Michelson interferometer; FPGA

1 引言

现代信息加解密体制分为对称加密和非对称加密两类.目前应用最广泛的 RSA[1]公钥密码体制属于非对称加密方式,它的安全性是基于大合数素数分解的困难.随着高性能计算技术的发展,这种加密方式的安全性越来越低,例如 2009 年 12 月 12 日 RSA-768 就被成功分解.量子加密术则在为替代这种依赖硬件计算能力的加密术而兴起的研究中出现,这是一种基于“一次一密”的对称加密技术,它需要解决的问题是如何在通讯双方分发大量的密钥.QKD 是量子加密术中解决通讯双方共享密钥的一种方法,它是量子加密通信的核心技术.目前 QKD 使用的主要协议有 BB84、B92、差分相位编码协议等,本系统采用应用最广而且安全性得到严格证明的 BB84 协议[2],它描述了怎样在一个不安全的公共信道利用量子态传输在通信双方安全地分发密钥.BB84 协议提出利用单光子的量子状态来传输密钥,量子力学的基本原理[3]可以保证量子密钥传输的安全性.

由于光纤有良好的光学传输能力,所以很多 QKD 实验是以光纤为传输介质的.BB84 协议在光纤中可以采用偏振编码和相位编码,偏振编码受到光纤双折射现象影响很大[4],尽管 A.Muller 提出的“Plug&Play”[5]系统能够自动补偿双折射效应,但该方案难以避免特洛伊木马[6]攻击.1992 年,Bennett 在提出 B92 协议的同时提出了可以使用相位编码方式[7]实现 QKD 系统,他提出在通信两端(Alice 端和 Bob 端)各使用一个 Mach-Zehnder

收稿日期:2011-03-09;修回日期:2011-06-02

干涉仪,在两端分别经过干涉仪长臂和短臂的光脉冲会同时到达 Bob 端从而发生干涉,通过探测干涉结果可以实现 Alice 和 Bob 之间的密钥分发.中国科学院量子信息重点实验室莫小范等人设计的 Faraday-Michelson(F-M)单向 QKD 系统是在 Mach-Zehnder 干涉仪基础上添加了 Faraday 反射镜,它可抵御特洛伊木马攻击,并且由于干涉环采用了 Faraday 反射镜对光纤中的双折射进行了自补偿,系统有很高的光学稳定性.因此基于 F-M 干涉仪的 QKD 系统可以说是 BB84 协议实现的最佳方案之一.

无论是 QKD 系统的实验室研究阶段,还是目前已经开始出现商业化产品应用阶段,QKD 系统的实现以及性能的提高一直不断地对系统电子学的设计提出挑战.QKD 系统由光学系统和控制电子学系统两大部分组成,光学系统实现光信号的产甥、传输与干涉检出,除此之外的所有功能均由控制电子学实现,包括信号的调制、探测解调、系统定时同步,以及 BB84 协议所特有的对基、保密放大,和误码率估计、纠错等,还包括针对光纤量子传输通道特性所必须采取的相位自动扫描补偿、自动扫描跟踪来保持同步等功能的实现.在实验室试验阶段,多数电子学系统可以用商用电路板以及通用仪器拼接而成[8,9],仅满足物理实验要求即可.但目前 QKD 系统开始产品化的趋势,不仅要求电子学系统能够实现上述功能和最佳性能,还要求整个电子学系统结构独立和简洁,功能完善,能够成为量子通信网络中的一个独立节点,由多个这样的独立节点设备可以很方便地组网.

本文针对基于 F-M 干涉仪的光纤相位编码 QKD 系统,设计和实现了完整的 QKD 电子学系统.它包括硬件电路和软件系统两部分,其中硬件部分实现 QKD 通信系统中实时性要求较高的底层功能,而软件部分重点是实现 BB84 协议的高层部分.最终整个系统在 20km 传输距离上达到 4.91kbps 安全密钥生成率,超过了瑞士 IDQ 公司的实现 QKD 系统的产品 Clavis^2 在 25km 传输距离上 1kbps 的安全密钥生成率.若采用文献[10]中测量基重用的方法则可进一步提高密钥生成率.

2　QKD 系统基本原理

基于 Faraday-Michelson(F-M)干涉环的相位编码 QKD 系统的整体结构如图 1 所示,左侧是 Alice 发射端的组成,包括电子学系统和光路系统,右侧是 Bob 接收端的组成.Alice 和 Bob 之间有三个通道相连,它们分别是用于传输单光子量子状态的 20km 光纤通道,Alice 和 Bob 之间通信的同步光脉冲传输光纤通道(未来实际应用中可将同步光通道和单光子通道通过波分复用而使用一根光纤连接),和用于加密传输的经典信道(例如以太网络).在 Alice 和 Bob 端的干涉仪均为 F-M 干涉环,双方的电子学系统分别承担各自光路系统的底层控制和高层协议的执行.

Alice 端的电子学系统首先是产生脉冲信号驱动激光器产生激光,激光束经过 1:99 的分束器后,其中强光部分作为同步光经同步光传输光纤传送给 Bob 端,弱光部分进入干涉环被相位调制器(phase modulator, PM)调制,PM 的调相电压也由电子学系统产生.调相后的弱光再经过衰减器(attenuation, ATT)进一步衰减成为单光子束.在单光子束注入单光子光纤传输之前所经过的强度调制器(intensive modulator, IM),是用于增加诱骗态方式[11],通过控制 IM 的调强电压和偏置电压,可以实现诱骗态传输.

Bob 端电子学系统控制光学部分实现量子密钥的接收功能.首先是通过同步光探测器检出同步光传输光纤的光脉冲,产生 Bob 端的同步接收时钟信号.单光子信号通过单光子传输光纤到达 Bob 端后进入 F-M 干涉仪,干涉仪中 PM 对光子调节不同的相位后输出被两个单光子探测器(single photon detector, SPD)探测.Bob 端电子学要在同步时钟的控制下,产生调相电压,控制 SPD 的开门信号和接收 SPD 的信号输出.

相位编码和解码是通过对两端干涉仪调相器 PM 加上4种不同的相位电压(0、π/2、π、3π/2)实现的,本文

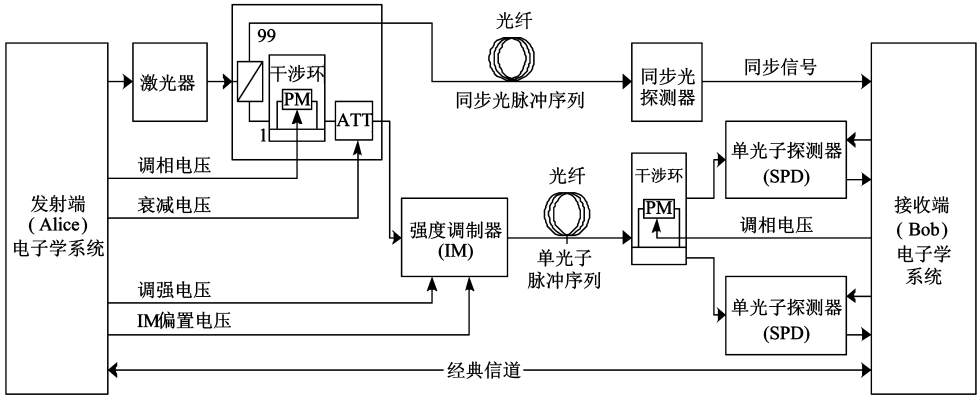

图1　相位编码QKD系统结构图

的 3.3 节将详细介绍如何确定这四个相位电压.这四个电压由各自的 2 比特随机数选择,其中 1 比特用来选择基(0、π)或者(π/2、3π/2),另 1 比特用来选择基内某一个相位,例如 0 选择 0 或 π/2 相位,1 选择 π 或 3π/2 相位.当 Alice 与 Bob 使用的基相同时,其中一个 SPD 会探测到单光子干涉而输出电脉冲,而当基不同时,则可能从任一个 SPD 输出.

Alice 和 Bob 各自随机地发送和接收单光子信号.一组密钥传输完成后,双方还要经过对基、纠错、保密放大等高层协议的处理过程,最后得到一组双方共享的密钥.这一过程是双方通过经典信道完成的,为此双方电子学都要具有较强的信号处理能力.

3 电子学系统设计

针对上述基于 F-M 干涉环的相位编码 QKD 的整体需要,以及面向实用化的设计要求,一个网络节点的整个电子学系统采用嵌入式系统架构设计(图 2),它包括一块嵌入式系统主板和一块 QKD 子板.两块电路板通过 100 针的插座相连.

嵌入式系统包括 MPC8260 CPU、存储 U-boot 启动代码的 EEPROM、存储 Linux 内核代码的 Flash、作为主内存的 SDRAM、作为主硬盘的 CF 卡、三个以太网口、RS232 串口、实时时钟等设备,这些设备组成了一个基本的计算机系统.主板上的三个以太网接口用于实现经典信道的通讯连接,RS232 串口用于连接外部计算机显示系统运行信息和检测 QKD 等运行状态.主板上运行 Linux-2.4.4 操作系统,利用 Linux 平台开发 QKD 系统的主控软件.

QKD 子板包括一片 EP2C20F484 FPGA、DDR 存储器芯片、USB 接口、以太网接口,以及光学器件的控制电路、信号发送或接收电路,例如 DAC 电路、放大电路、延迟器电路,以及 SPD 信号接收电路等.子板的 FPGA 和 MPC8260 的 Local Bus 相连,实现子母板之间的通信.

3.1 传输光学控制电路

Alice 和 Bob 端母板结构完全一致,它们是完全相同的系统主板,而子板根据其完成的光学控制任务有所差异,为了工程化的简单和方便,两者的子板也使用同一种板但它们分别配置为发射端和接收端.

Alice 作为发射端首先要提供一路驱动激光器的信号,它由子板通过 FPGA 直接产生 20MHz 的脉冲信号来实现.由于调相器需要加上精确快速可调的电压对每个光脉冲调制不同相位,子板上提供一路 10bit 的 DAC2900(ADI 公司).DAC 输出的信号经过 THS3001 放大器放大产生 + 3V 到 - 3V 范围的电压加到调相器.Alice 子板上还设计有 10bit 的 THS5651A DAC 和 THS3001 放大器产生 + 4V 到 - 4V 范围的电压,用于调节光衰减器将激光衰减成单光子状态.为了实现诱骗态传输,Alice 光学控制电路中还设计了一路 10bit 的 DAC(DAC2900)和 THS3001 放大器产生精确快速可调电压控制 IM 来调节光脉冲强度.

接收方 Bob 端除了接受同步光脉冲,产生系统同步时钟以外,Bob 子板的主要功能是量子态探测和接收.和 Alice 端的调相控制电压的产生方式相同,子板上设计一路 DAC(DAC2900)和 THS3001 放大器用于产生接收方的调相电压.由于单光子探测器的开门信号要和干涉光到达时刻保持一定的相位关系,我们设计使用一片数控延迟芯片(DS1023)用于将由 FPGA 产生的开门信号进行延迟调节,以使它和干涉光的到达时刻一致.延迟芯片的调节步长是 0.5ns.同样的设计需要,另一片相同的延迟芯片用于调节驱动 PM 的 DAC 信号,使得调相信号与量子信道保持同步.

3.2 QKD 运行参数自动扫描

由于 QKD 系统目前阶段有同步光纤和传输单光子

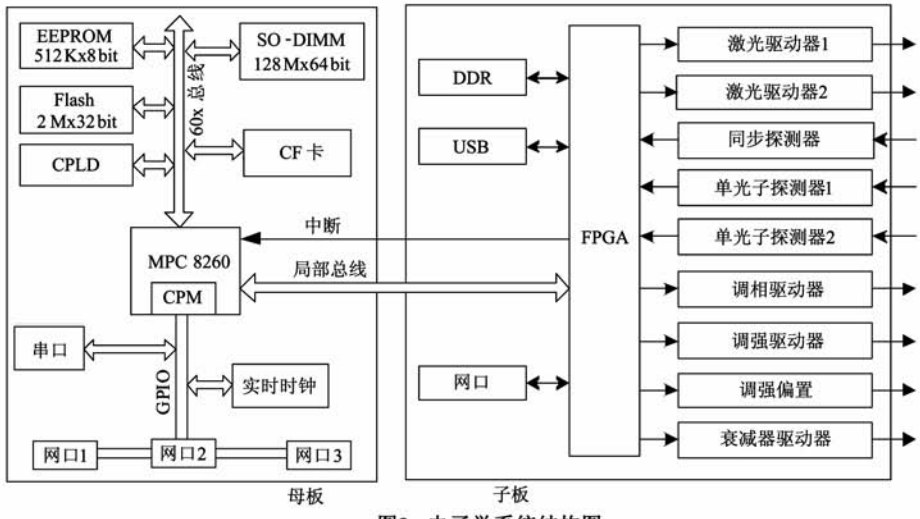

图2 电子学系统结构图

光纤两个独立信道,这两个信道所在的环境温度等的不同会造成信号同步的不稳定,甚至不能同步.尽管将来实用化中将通过波分复用方式将它们合并到一条光纤上,但因群速度不同这两路信号依然会出现同步不稳定的情况[13].在 Bob 端的信号接收过程中,SPD 门控信号、DAC 输出的调相电压信号都必须和同步时钟保持固定的相位关系,这些相位关系随时间和环境温度的变化会发生变化,这就要求系统要经常地通过某种机制来保证发送方和接收方的同步,要能自动地探测和确定系统运行的相关参数.同步机制和系统运行参数自动确定是目前 QKD 系统都要妥善处理和解决的问题,在文献[12,13]中对这一问题都进行了讨论.文献[12,13]介绍的同步方法比较复杂,需要专门为此再添加一个信道[12]或者增加器件[13].本文提出另一种解决方案,通过电子学灵活的设计,通过自动扫描和比较在不同延时相位下,系统探测到的光产额或者 QBER 变化趋势来自动追踪系统同步和信号探测所需要的工作参数.

下面以 SPD 门控信号和光量子之间延时为例说明扫描过程.InGaAs 探测器内部雪崩光电二极管(APD)需要一个门控信号来触发和粹灭雪崩过程,将此门宽内到达的单光子引起的雪崩信号放大产生输出信号送到后级电路.量子信道中单光子脉冲经过 Bob 端干涉环之后输出表现为时间上先后排列的三个波包,波包时间间隔由长短臂的光程差决定.我们要探测的是第二个波包,即干涉峰,所以要调节 SPD 门控信号恰好仅出现在干涉发生的时刻.

实际调试中寻找此延时值的过程如下:Bob 端 QKD 子板将同步时钟信号经过一片延时芯片出来之后作为 SPD 的门控信号,通过对延时芯片调节不同延时值探测此时的光产额,得到一个光产额随门控信号延迟的变化曲线.如图 3 所示.图中清楚看到每个周期(50ns)先后排列的三个波包,波包间隔 15ns 正是长短臂的光程差对应的时间,标注为①③位置的横坐标是在两端光

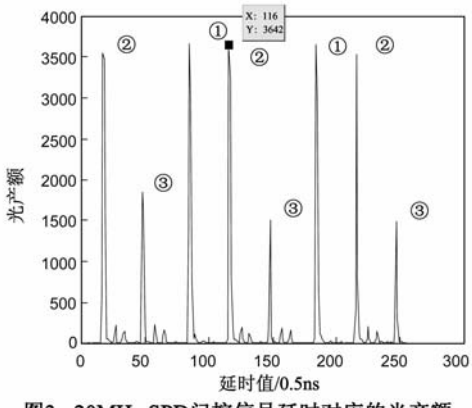

图3　20MHz SPD门控信号延时对应的光产额

脉冲均经过短臂或者长臂的波包对应的延时值,标注为②位置的横坐标就是要找的干涉峰对应的延时值.有多个②位置是因为扫描区间跨过了多个时钟周期.

3.3　相位漂移补偿

采用相位编码 QKD 系统主要困难是存在相位漂移[14,15],产生漂移的根本原因是光学系统光程发生变化,干涉环长短臂变化却不相同,导致两个相干光脉冲相位差发生变化.针对这个问题一般有两种方法:一是被动的保持恒温,避震;二是主动实时地获取并更新系统的相位参数.前者在实际系统中实现起来困难,本文采用后者.

主动实时相位补偿是指在每次 QKD 之前做相位扫描,确定实时的 4 个相位电压值.Alice 端相位电压是事先确定的,方法是固定 Bob 端调相电压,渐变 Alice 端调相电压,使得光产额最小和最大的两个调相电压的差值就是半波电压 V_{π}.若规定 Alice 端 0 电压是 0 相位,则 π/2、π、3π/2 相位分别对应 $V_{\pi}/2$、V_{π}、$3V_{\pi}/2$.以往确定 Bob 端相位电压所采用的单相位扫描方法是仅扫描一次 Bob 端调相电压得到产出最少的位置,将其对应 DAC 电压作为 π 相位,再结合半波电压值(π 相位和 0 相位电压差值多次平均得到)线性计算出 0、π/2、3π/2 三个相位电压.这样做的弊病主要是人为规定四个相位电压差值都是线性的以及假设半波电压是恒定的.但实际上由于受到 PM 的线性范围等因素影响这四个相位电压值并不是线性的,所以本文使用了一种称为四相位扫描的算法来实时确定四个相位电压值.它是分别在 Alice 端调到 0、π/2、π、3π/2 四个相位时对 Bob 端调相电压扫描,将四次扫描得到产出最少的值作为 Bob 端 π、3π/2、0、π/2 电压.相位补偿扫描在 FPGA 内的实现如图 4 所示.典型的相位补偿扫描结果如图 5 所示.

3.4　QKD 系统软件

我们编写了 QKD 过程控制软件 qkeg,这是运行于

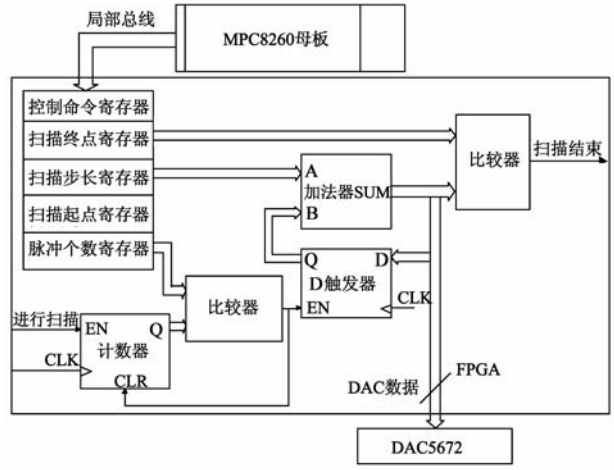

图4　相位补偿在FPGA内实现

母板 Linux 系统上的一个应用软件,用户通过 qkeg 控制整个 QKD 过程运行.它功能有:控制 QKD 过程自动运行,提供 Alice 和 Bob 经典通讯信道,接收 QKD 子板传递的中断以及探测结果信息,自适应的计算相关工作参数,密钥后处理等 BB84 的上层协议.软件执行流程如图 6 所示.

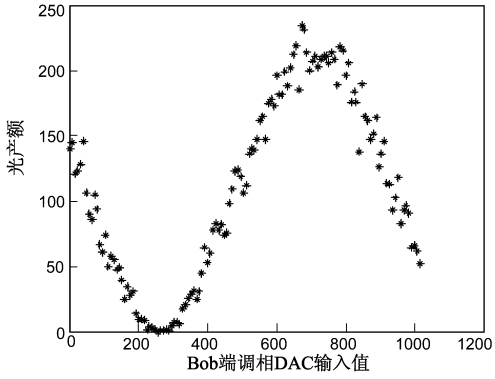

图5 相位补偿时调相电压与对应的光产额

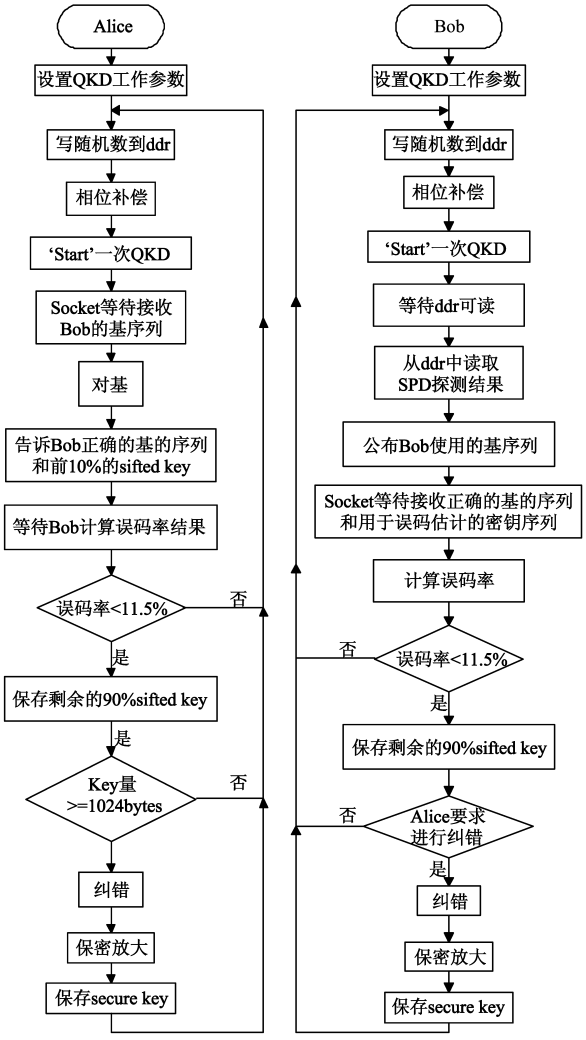

图6 qkeg软件工作流程图

4 实验测试

整个 QKD 系统以及其中电子学系统部分实物如图 7 所示.

测试平台是 Princeton Lightwave 研制的 PGA-604 InGaAs 单光子探测器结合我们研制的 QKD 电子学控制系统,此探测器最大工作频率 20MHz.整个系统在 20MHz 工作频率下运行了 2 万次 QKD,每次 QKD 发送 2×10^7 个光量子,接收端 SPD 平均探测计数是 1.975×10^4.实验结果如图 8 所示.可看出 QBER 集中在 4%以下.

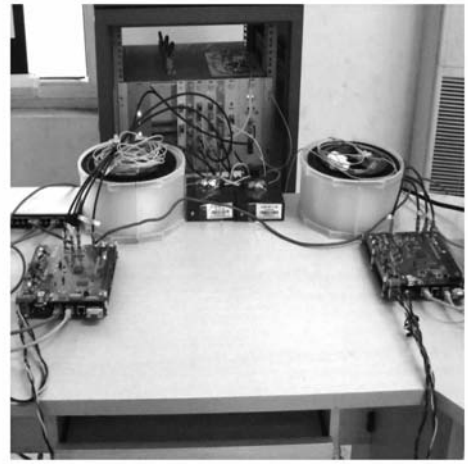

图7 完整QKD系统

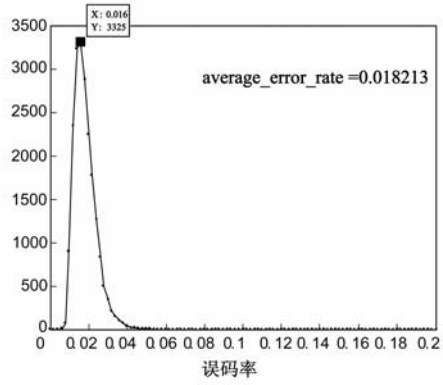

图8 InGaAs SPD 误码率分布曲线

我们还在不同传输光纤长度下测试了整套系统实际运行 QKD,结果如表 1 所示.

表 1 QKD 系统在不同传输距离和波长下运行情况

波长 (nm)	1530	1550	1550	1530
信道损耗 (dB)	7.24	8.78	10.79	14.77
死时间 (μs)	5	10	25	50
筛选密钥率 (Kbps)	31	17.64	8.16	3.83
量子比特误码率(%)	2.92	2.84	2.78	3.76
安全密钥率 (Kbps)	4.91	2.02	1.82	0.41

5 结论

针对量子密钥分发系统对控制电子学系统的特殊

要求,本文设计和实现了基于 BB84 相位编码协议的 QKD 电子学控制系统,并与光学系统有机结合,成功地通过现有的商用光纤网络联网,进行了量子密钥的分发和量子加密信息的传输实验,整个 QKD 系统在 20MHz 的光脉冲重复速率上实现了 BB84 相位编码协议,在 20km 传输距离上,量子比特误码率(QBER)为 2.95%,安全密钥生成率为 4.91kbps,密钥生成率能满足实时语音传输的加密需要.

此外,本文设计和实现的电子学系统在保证高性能的同时,还兼顾实用化的要求.测试结果和实际使用情况表明整个系统性能稳定,调试方便,自动程度高,系统上电后可自动启动 QKD 过程,不断产生和更新密钥;整个节点电子学系统结构简洁,其子母板结构各自分工明确,QKD 子板完成量子态制备和传输,母板控制整个系统和数据处理;电子学系统是一个完全独立的节点系统,通讯中的一方就是一个这样的节点,多个这样的节点可以方便地组成一个量子密码通讯网络.本文的研究工作虽然是针对基于 Faraday-Michelson 干涉仪的相位编码 QKD 系统而进行的,但其基本思路和设计实现技术对其它种类的 QKD 系统电子学的设计也有借鉴作用.

参考文献

[1] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[2] Charles H Bennett, Gilles Brassard. Quantum cryptography: public key distribution and coin tossing[A]. Proceedings of International Conference on Computers, Systems and Signal Processing[C]. Bangalore, India, 1984. 175 – 179.

[3] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, et al. The security of practical quantum key distribution[J]. Reviews of Modern Physics, 2009, 81(3): 1301 – 1351.

[4] A Muller, H Zbinden, N Gisin. Underwater quantum coding [J]. Nature, 1995, 378: 449.

[5] A Muller, T Herzog, B Huttner, et al. "Plug and play" systems for quantum cryptography[J]. Appl Phys Lett, 1997, 70: 793 – 795.

[6] J C Boileau, D Gottesman, R Laflamme, et al. Robust polarization-based quantum key distribution over a collective-noise channel[J]. Phys Rev Lett, 2004, 92(1): 179011 – 179014.

[7] Charles H Bennett, Francois Bessette, Gilles Brassard, et al. Experimental quantum cryptography [J]. Jounal of Cryptology, 1992, 5(1): 3 – 28.

[8] Honjo, Toshimori. Gigahertz clocked quantum key distribution system using FPGA[A]. 35th European Conference on Optical Communication[C]. Vienna, Austria, 2009. 1 – 2.

[9] Alan Mink, Xiao Tang, LiJun Ma, et al. High speed quantum key distribution system supports one-time pad encryption of real-time video[A]. Proceedings of SPIE-v6244 Quantum Information and Computation IV [C]. Orlando, USA, 2006. 62440M.

[10] 孙莹,温巧燕,朱甫臣.基于可重用基序列的量子安全通信方案[J].电子学报,2010,38(1):111 – 116.
Sun Ying, Wen Qiao-yan, Zhu Fu-chen. Quantum secure communication based on the reusable bases sequences[J]. Acta Electronica Sinica, 2010, 38(1): 111 – 116. (in Chinese)

[11] Won-Young Hwang. Quantum key distribution with high loss: toward global secure communication[J]. Phys Rev Lett, 2003, 91(5): 579011 – 579014.

[12] 刘玉,叶俊,王长强.自由空间量子密钥分发中的信号同步解决方案[J].光电工程,2006,33(4):68 – 71.
LIU Yu, YE Jun, WANG Chang-qiang. Solution for synchronization of signal in free-space quantum key distribution[J]. Opto-Electronic Engineering, 2006, 33(4): 68 – 71. (in Chinese)

[13] W Maeda, et al. High-speed QKD system synchronized by automatic phase-alignment mechanism[A]. OFC/NFOEC 2005 Optical Fiber Communication Conference, Technical Digest [C]. California, USA, 2005. 205 – 207.

[14] Christophe Marand, Paul D Townsend. Quantum key distribution over distances as long as 30km[J]. Optic Letters, 1995, 20 (16): 1695 – 1697.

[15] Paul D Townsend. Quantum cryptography in optical fiber networks[J]. Optical Fiber Technology, 1998, 4(4): 345 – 370.

作者简介

杨　阳　男,1985 年 1 月出生于安徽省安庆市,现为中国科技大学物理电子学专业博士研究生.主要从事高速电路设计以及嵌入式系统设计.

E-mail: yyanghh@mail.ustc.edu.cn

王永纲　男,1965 年 10 月出生于安徽省淮北市,现为中国科技大学物理电子学专业教授,博士生导师.主要从事高速信号处理.