文章编号:1001-5078(2019)02-0151-05　　·激光应用技术·

QKD 系统中基于 EA 电路的诱骗态实现

张博文[1],洪占勇[1],盛迎接[2],代云启[2]
(1. 合肥工业大学工业与装备技术研究院,安徽 合肥 230009;2. 科大国盾量子技术股份有限公司,安徽 合肥 230088)

摘　要:使用诱骗态量子秘钥方案可以解决因光子数分离攻击而导致的安全漏洞,保证了长距离量子通信的安全。本文介绍了量子通信的相关原理,通过对电吸收调制电路和激光器驱动电路的设计,精确控制产生了 1550 nm 波段的窄脉冲,经过内部调制成功制备诱骗态光脉冲,其强度约为信号态光脉冲的三分之一,因激光器的同一性而具有一致的光学特征从而避免了时频窃听,并具有强度可调的优点。

关键词:量子通信;诱骗态;驱动电路;电吸收调制;激光器
中图分类号:TN248.4　　**文献标识码:**A　　**DOI:**10.3969/j.issn.1001-5078.2019.02.004

Realization of decoy state based on EA circuit in QKD system

ZHANG Bo-wen[1], HONG Zhan-yong[1], SHENG Ying-jie[2], DAI Yun-qi[2]
(1. Institute of Industry & Equipment Technology, Hefei University of Technology, Hefei 230009, China;
2. QuantumCTek Co., Ltd., Hefei 230088, China)

Abstract: The security loopholes caused by the Photon-Number-Splitting Attack could be solved by using the decoy quantum key scheme, and the security of long-distance quantum communication could be guaranteed. The principle of quantum communication was introduced in this paper. The electro-absorption modulation circuit and the laser drive circuit were designed. The 1550 nm narrow pulse was precisely controlled and generated. After the internal modulation, the decoy light pulse was successfully prepared. Its intensity was about one-third of the signal state, and the uniform optical feature was owned by the same character of the laser so as to avoid time-frequency eavesdropping, and has the advantage of adjustable intensity.

Key words: quantum communication; decoy; drive circuit; electro-absorption modulation; laser

1　引　言

当今社会,随着科技的快速发展,人们关于隐私的安全性越来越重视,对于网络信息传输有了更高的要求。传统的信息加密方式主要依靠数学算法的复杂度,破解密码需要在有限时间内能够进行大量计算。但是现如今无法证明破解密码的运算量是现有技术或未来无法实现的,而且目前国内外超级计算机发展势头迅猛,经典信息加密技术的安全性受到严重威胁。

究此原因,发展潜力巨大的量子保密通信技术得到各国重视,利用量子态的特殊性质给通信双方提供安全的秘密通信,是结合量子物理学和密码学的新学科,其基础是量子力学不确定性原理和量子态不可克隆定理,但因为现有技术的限制,针对量子通信不同的攻击手段也层出不穷,如光子数分离攻击(Photon－Number－Splitting Attack, PNS)、侧信道攻击和木马攻击等,经过不懈努力,科研人员也研究出许多相对应的防范方法[1]。

作者简介:张博文(1994－),男,硕士研究生,主要研究方向为仪器及装备精度保障技术。E-mail:bowenjohn@163.com
收稿日期:2018-07-31

2 理论基础

2.1 量子通信

因“一次一密”的形式而具有理论上绝对安全性的量子秘钥分发(Quantum Key Distribution,QKD)系统受到学术界的广泛关注。由 Bennett 和 Brassard 于 1984 年首次提出的量子秘钥分发协议即 BB84 协议,基本原理如图 1 所示,这是一个采用 0°(H)、45°(P)、90°(V)和 135°(N)偏振态的四态协议,实现虽然简单但却具有无条件安全性,标志着量子密码时代的大门正式打开[2-5]。

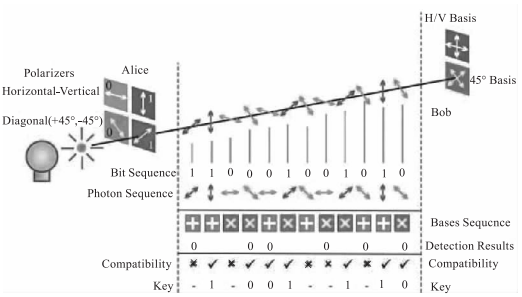


图 1 BB84 量子密钥分发协议原理图

Fig. 1 Diagram of BB84 quantum key distribution protocol

2.2 光子数分离攻击

假设窃听者 Eve 在不违背量子力学的前提下有无限资源可以利用,可将单光子从光脉冲中分离。Eve 首先测量发送端 Alice 的光脉冲,若为空脉冲则不作任何处理;若为单光子脉冲,则截取单光子;若为多光子脉冲,则分离出一个单光子保留,而将剩余的光脉冲通过无损信道传递给接收端 Bob。当基矢公开后,Eve 将会获得与 Alice 完全相同的量子秘钥。研究表明,PNS 攻击中的光子数仍然服从泊松分布,误码率不会浮动,所以通信双方无法发现窃听者的存在。

2.3 诱骗态协议

诱骗态的概念最初为 Hwang 在 2003 年提出,经 Lo、王向斌等进一步发展日趋成熟。Alice 将诱骗态随机插入到光脉冲中,与信号态、真空态一起发送给 Bob,因为单光子经过检测后会发生塌缩,所以双方可以通过检测信道中脉冲的衰减或误码率的变化来判断有无 Eve。假如 Alice 向 Bob 发送多个不同强度的光脉冲,其中一个为信号态剩余的为诱骗态,因为 Eve 无法区分 n 光子是诱骗态还是信号态,其中 n 光子的计数率 Y_n 和误码率 e_n 仅依赖于光子数,所以 Eve 通过测量光子数是无法区分状态的,但若存在 PNS 攻击,Y_n 和 e_n 就会发生变化,从而被发现。诱骗态的本质可由下式表示:

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n$$

诱骗态的核心就是估计单光子计数率 Y_1 和误码率 e_1,Alice 向 Bob 发送一个信号态和 m 个诱骗态 $\mu,\nu_1,\cdots,\nu_m$,总的增益 Q 和误码率 E 为:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu}, E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu}$$

$$Q_{\nu_1} = \sum_{n=0}^{\infty} Y_n \frac{\nu_1^n}{n!} e^{-\nu_1}$$

$$E_{\nu_1} Q_{\nu_1} = \sum_{n=0}^{\infty} e_n Y_n \frac{\nu_1^n}{n!} e^{-\nu_1}$$

$$\cdots$$

$$Q_{\nu_m} = \sum_{n=0}^{\infty} Y_n \frac{\nu_m^n}{n!} e^{-\nu_m}$$

$$E_{\nu_m} Q_{\nu_m} = \sum_{n=0}^{\infty} e_n Y_n \frac{\nu_m^n}{n!} e^{-\nu_m}$$

在诱骗态无穷多的情况下,即 $m\to\infty$ 时,理论上来说 Y_n 和 e_n 的值是可以求出来的,代入如下 GLLP 公式可估算求出安全密钥率:

$$R \geqslant q\{-Q_\mu f(E_\mu) H(E_\mu) + P_1 Y_1[1 - H(e_1)]\}$$

其中,q 表示 BB84 协议对基率;μ 为弱相干脉冲平均光子数;Q_μ 和 E_μ 分别为 Alice 发送的光脉冲在 Bob 处引起探测器响应的总计数率和总误码率;$f(x)$ 表示纠错率,$H(x)$ 表示二进制香农熵[6-8]。

3 电吸收调制器与 EML

3.1 电吸收调制特器

电吸收调制器(Electro-absorption Modulator,EAM)基于半导体中的激子吸收效应,具有响应速度快,功耗低等优点。基本结构是一个 PIN 结,其中 N 区部分是交替生长的多层结构,类似于光学增反膜堆。I 区为多量子阱(Multiple Quantum Well,MQW)结构,主要表现为吸收边陡峭,热稳定性良好,且外加合适的反向电场时,激子吸收峰会明显的向长波方向移动,外电场取消后吸收光谱又能可逆还原。这种材料是通过设计多量子阱结构的阱和垒的组分和厚度以及周期数来实现的,其赖以实施的手段是补偿应变超晶格生长。压应变量子阱结构可以有效地提高Ⅲ-Ⅴ族半导体激光器的性能,如较低的阈值和较高的输出功率、高调制速率以及更好的温度稳定性等。但应变量子阱多层应变的积累厚

度存在一个临界限度,后又发展了应变补偿技术,来降低净应变,增加 MQW 的总厚度和提高结构的稳定性[9]。

3.2　EML 激光器

电吸收调制器与 DFB 激光器结合可制备电吸收调制激光器(Electro-absorption Modulated Distributed Feedback Laser,EML)。EAM 施加适当的反向直流偏置和射频脉冲驱动电压,激光器的输出经 EAM 受到外加脉冲信号调制,因其非线性吸收特性,即随反向偏压的增大,EAM 对光强的吸收呈指数增长,经适当调节便可以产生诱骗态短脉冲,重复频率等同于脉冲调制速率,脉宽由 EAM 吸收特性和外加 DC、RF 的幅度确定。具有输出脉冲啁啾小,非线性吸收能力强,脉宽可调等特点。通过使用行波电容、减小结电容和寄生电容的方法可提高其频率响应。

如图 2 所示为 EML 激光器的内部封装结构,当按需设置的偏置电流通过 LD 时,其发出的光一部分会进入到背光检测 PD(光电二极管)转换成电流,用作 APC(自动光功率控制)的反馈量;另一部分进入电吸收调制器 EA,一部分会被 EA 吸收转换成电流,其他的则通过光隔离器后形成输出光。在正常工作模式下,LD 光电二极管需正向偏置,而 PD 和 EA 处于反向偏置状态。内部的热敏电阻用于探测激光器的温度,作为 ATC(自动温度控制)的反馈量,通过控制制冷器 TEC 两端的电压差来维持激光器内部温度稳定到预设温度(控制精度目前达到 ± 0.02 ℃)。

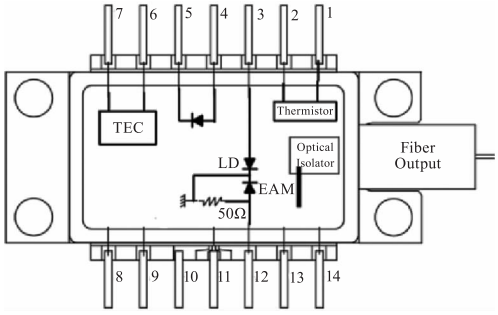


图 2　EML 的内部封装结构

Fig. 2 Internal packaging structure of EML

4　诱骗态制备方案

4.1　总体设计

本方案采用的是一款蝶形 EML 激光器,在 1550 nm 波段具有 10 Gb/s 的比特传输速率。设计了基于 FPGA 的激光器驱动信号用于驱动 LD 输出窄脉冲,EA 驱动信号用于实现诱骗态光脉冲的制备,其中,驱动信号的来源分为两种,一种是通过外部信号源产生驱动信号,另一种是通过单板上锁相环电路产生驱动信号。

目前在 QKD 系统中采用的单光子源通常是基于弱相干光源的强衰减制备而成的伪单光子源,并不是理论上的"单光子源"[10],本方案的 EML 激光器内部集成了 TEC 温控单元、EAM 电吸收调制单元、光隔离器单元以及 PD 背光检测单元,具有集成度高、速率快、传输距离远、隔离度高等优点。目前商用的 EML 驱动采用集成芯片为 LD 提供恒定偏置电流使其输出连续光,同时集成芯片输出调制驱动信号到 EML 内部的 EA 上,从而调制连续光经过 EA 后输出为调制的脉冲光。由于本方案中需要 LD 做窄脉冲随机信号驱动,则商用 EML 驱动芯片无法适用于本方案,所以本方案采用两路自行设计的驱动电路分别对 EA 和 LD 进行驱动,具体的原理如图 3 所示。

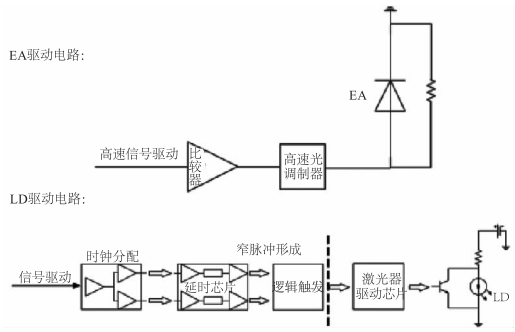


图 3　驱动电路原理图

Fig. 3 Diagram of drive circuit

4.2　EA 驱动电路设计

使用内部集成了电吸收调制单元 EA 的激光器来调制信号的状态,避免了因额外加入电吸收调制器而产生的误差。如图 4 所示的 EA 驱动电路原理图,采用的超快速电压比较器,信号传播性能好,最小脉宽为 100 ps,等效输入上升时间带宽为 8 GHz,输入信号范围宽,而且典型输出上升/下降时间只有 37 ps。因差分输入较小,通常需要在超快速电压比较器中添加迟滞,用适当大小的下拉电阻将 14 引脚与 V_{EE} 电源连接,以增加约 10 mV 的滞后量。若 V_P 大于 V_N,则超快速电压比较器处于比较模式,此时 Q 为高电平,$\bar{Q}$ 为低电平。后连高达 10.7 Gbps 的高速光调制器,外部直流电压编程控制的集成控制

运算放大器从而起到调制电路的作用,边缘速度为 23 ps。带宽较高,为减少抖动累积,全差分信号路径设置在内部实现,当时钟信号可用时,选择集成的数据重新定时以抑制输入信号的抖动,其内部还包含一个可调脉宽控制电路,用于补偿不对称调制器特性。内部集成的脉宽控制电路可以用来补偿调制器引入的脉宽失真,8 和 9 引之间的差分电压调整脉冲宽度补偿,调整范围通常为 ±50 ps。当 22 引脚悬空时,调制输出使能,在 MODSET 引脚上施加一个高于 V_{EE}的电压即可。15 号引脚输出的 EML_RF 信号,实现了对激光器内部 EAM 的控制,调制激光器输出所需的诱骗态光脉冲。利用条纹分辨二次谐波相关法(FRSHG)对电吸收调制后产生的光脉冲进行测量,通过迭代计算,可知波长啁啾小,消光比高,光脉冲的半极大全宽窄,适合在长距离光通信中使用。

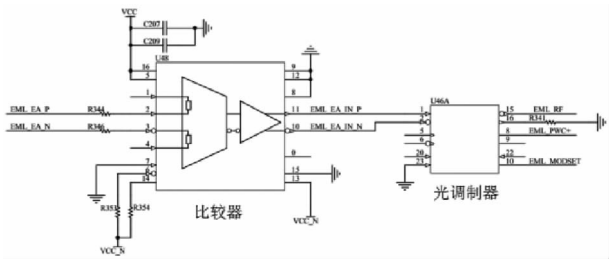


图 4 EA 驱动电路

Fig. 4 EA drive circuit

4.3 LD 驱动电路设计

驱动信号通过 1:2 差分扇出缓冲器,该芯片输入时钟频率最大可以达到 4 GHz,上升/下降时间较短。输出的四路差分信号经过快速双通道可编程时钟/数据延时芯片用以产生所需的窄脉冲,时序图如图 5 所示,该芯片可以去除时钟或数据偏移和时序调整,具有时钟频率高于 1.5 GHz,输入数据速率大于 2.5 Gb/s,延迟范围可控等优势,根据需要可选择 Dual Delay(双延时)或 Extended Delay(扩展延时)模式。所需的延迟是 FPGA 通过 3 引脚串行数据接口对每个延迟通道进行编程完成的,双延迟模式下每个通道的净可编程延迟范围为 0 ~ 6 ns,而在扩展模式下,范围为 0 ~ 11.2 ns。MSEL 位决定延迟模式(低电平为双延时,高电平为扩展延时)。

随后信号经过多功能差分逻辑门芯片输入到 EML 激光器的高速驱动芯片中,这是一款性能优良的高速激光器驱动芯片,数据传输速率可直接从 2 Gbps调制到 11.3 Gbps,具有集成的自动功率控制(APC)回路、可编程的输入均衡器和激光器保护功能。FPGA 控制模数转换器芯片对驱动芯片和温度控制芯片分别进行控制。激光器详细驱动电路原理图如图 6 所示,Q2 是一个开关三极管,控制驱动芯片的输出电流大小,由两个电阻上分压可控制三极管的导通与否。当三极管导通时,LD 处于截至状态,当三极管基极电流较小截止时,LD 正极对地有电压输入,处于工作状态。

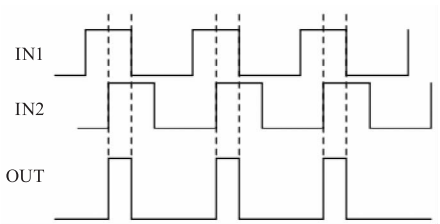


图 5 窄脉冲形成时序图

Fig. 5 Diagram of narrow pulse timing

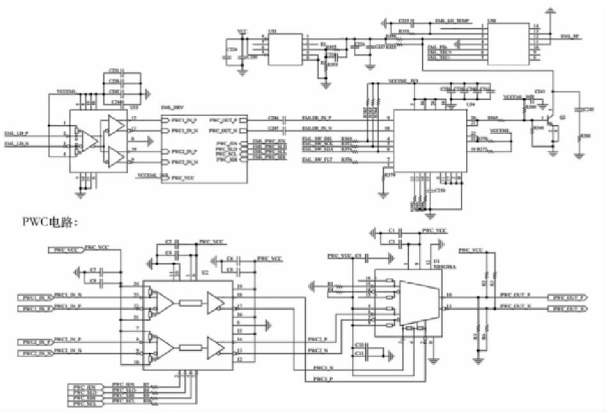


图 6 LD 驱动电路

Fig. 6 LD drive circuit

5 实验与分析

搭建实验测试平台,采用力科公司 6G 示波器和康冠公司 24G 光电转换探头,激光器中心谱线波长为 1550 nm,根据相关数据手册和实验要求,使用热电制冷控制芯片作为半导体制冷器的驱动芯片精确控制实验温度,随机产生比例为信号态:诱骗态:真空态 =6 :2 :1 的光脉冲,信号态和诱骗态光脉冲分别为 0.6 光子和 0.2 光子每脉冲,真空态为 0 光子每脉冲,在高速示波器中观察到的脉冲调制前后对比曲线如图 7 所示。

由实验结果可知,本方案成功制备了诱骗态光脉冲,符合预期目标,选用集成度高的 EML 激光

器,而且是用同一个 LD 制备三种状态的光脉冲,不仅实现了诱骗态光脉冲的制备,也避免了因使用多个 LD 可能导致的波长、脉宽等光学特征参数不一致导致时频上的安全漏洞。由于诱骗态光子的光谱与信号光子基本相同,在长距离通信中可忽略色散差异。

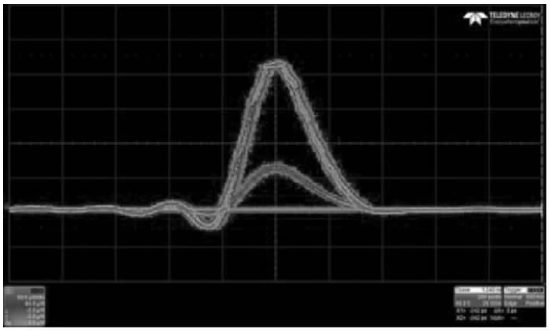


图 7 实验结果图

Fig. 7 Result of experiment

6 结 论

综上所述,针对 QKD 系统中诱骗态光脉冲的制备,提出了一种基于电吸收调制电路的内部调制制备方法。通过对 LD 驱动电路的设计,采用高速驱动芯片和简易的开关电路,LD 内部集成的热敏电阻和半导体制冷器以精确控制温度,在保证光源同一性的同时,使得产生的窄脉冲具有精确可控的优点。最后通过 EA 电路,实现了诱骗态光脉冲制备和强度控制。

参考文献:

[1] PAN Jianwei, CHEN Zengbing, PENG Chengzhi. Application of decoy quantum cryptography to establish practical application test of secure communication network [J]. China Basic Science, 2010, 12(2): 30 – 30. (in Chinese)
潘建伟,陈增兵,彭承志. 应用诱骗态量子密码技术建立安全通信网络的实际应用测试[J]. 中国基础科学, 2010, 12(2): 30 – 30.

[2] WU Hua, WANG Xiangbin, PAN Jianwei. Quantum communication: status and prospects [J]. Scientia Sinica: Informationis, 2014, 44(3): 296 – 311. (in Chinese)
吴华,王向斌,潘建伟. 量子通信现状与展望[J]. 中国科学:信息科学, 2014, 44(3): 296 – 311.

[3] Bennett C H, Brassard G. Quantum cryptography: public-key distribution and coin tossing [C]. Proceedings of the International Conference on Computers, Systems and Signal Processing. Bangalore, India. (IEEE, New York) 1984: 175 – 179.

[4] Zhang Y, Chen W, Wang S, et al. Practical non-Poissonian light source for passive decoy state quantum key distribution [J]. Optics Letters, 2010, 35(20): 3393 – 5.

[5] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441 – 444.

[6] Lo H K. Decoy state quantum key distribution [J]. International Journal of Quantam Information, 2008, 03 (supp01): 143.

[7] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography [J]. Physical Review Letters, 2005, 94(23): 230503.

[8] Yu Z W, Zhou Y H, Wang X B. Three-intensity decoy state method for device independent quantum key distribution [J]. Physical Review A, 2013, 88 (6): 3869 – 3876.

[9] WANG Chen. The study of clock recovery and demultiplexing module 160 Gbit/s OTDM [D]. Beijing: Beijing Jiaotong University, 2009. (in Chinese)
王晨. 160 Gbit/s 光时分复用系统中时钟提取与解复用器模块的研究[D]. 北京:北京交通大学, 2009.

[10] WANG Kaidi, HONG Zhanyong, DAI Yunqi. Adjustable bias driver for DFB laser in QKD system [J]. Laser & Infrared, 2017, 47(2): 164 – 168. (in Chinese)
王凯迪,洪占勇,代云启. QKD 系统中 DFB 激光器的可调偏置驱动 [J]. 激光与红外, 2017, 47 (2): 164 – 168.