



(12) 发明专利申请

(10) 申请公布号 CN 112822012 A

(43) 申请公布日 2021.05.18

(21) 申请号 202110276787.4

(22) 申请日 2021.03.15

(71) 申请人 合肥硅臻芯片技术有限公司

地址 230601 安徽省合肥市经济技术开发区宿松路以东、观海路以北智能装备科技园E栋10层东02室

(72) 发明人 丁禹阳 刘午

(74) 专利代理机构 北京集佳知识产权代理有限公司 11227

代理人 尹秀

(51) Int.Cl.

H04L 9/08 (2006.01)

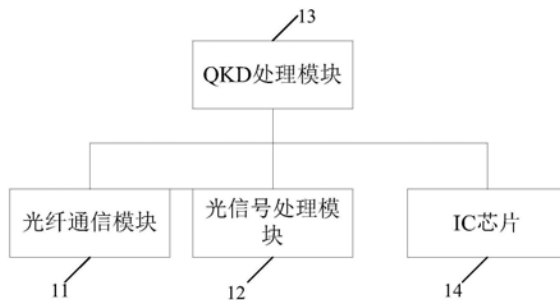
权利要求书2页 说明书8页 附图3页

(54) 发明名称

一种量子密钥分发设备及量子密钥分发方法

(57) 摘要

本发明提供了一种量子密钥分发设备及量子密钥分发方法,光信号处理模块生成并发送激光光束至QKD处理模块,QKD处理模块依据接收的IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至光纤通信模块,以使光纤通信模块输出光信号,IC芯片还将随机数通过连接器发送至外接控制设备,以使外接控制设备基于随机数进行QKD后处理操作。本发明中,采用QKD处理模块以及IC芯片,体积较小,相比与采用独立的光学元器件的方式,可以降低量子密钥分发设备的体积以及设备数量,进而提高量子密钥分发设备中的器件的稳定性和降低器件的功耗,提高量子密钥分发设备的可靠性。



1. 一种量子密钥分发设备,其特征在于,包括:

光纤通信模块、光信号处理模块、QKD处理模块以及IC芯片;所述光纤通信模块、所述光信号处理模块、所述IC芯片分别与所述QKD处理模块连接,所述IC芯片通过连接器与外接控制设备连接;

所述光信号处理模块用于:生成并发送激光光束至所述QKD处理模块;

所述QKD处理模块用于:依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号;

所述IC芯片用于:生成与第一随机数对应的第一电平驱动信号、将所述第一电平驱动信号发送至所述QKD处理模块,以及将所述第一随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作。

2. 根据权利要求1所述的量子密钥分发设备,其特征在于,所述QKD处理模块还用于:依据接收的所述IC芯片发送的第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

所述光信号处理模块还用于:对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块发送至所述IC芯片;

所述IC芯片还用于:生成与第二随机数对应的第二电平驱动信号、将所述第二电平驱动信号发送至所述QKD处理模块,以及将所述第二随机数和所述探测结果发送至所述外接控制设备。

3. 根据权利要求1所述的量子密钥分发设备,其特征在于,所述量子密钥分发设备还包括随机数处理模块;所述随机数处理模块与所述IC芯片连接;

所述随机数处理模块用于:生成第一随机数,并将所述第一随机数发送至所述IC芯片。

4. 根据权利要求1所述的量子密钥分发设备,其特征在于,所述QKD处理模块为QKD光芯片模块;所述QKD光芯片模块和所述IC芯片集成在同一PCB板上。

5. 根据权利要求1所述的量子密钥分发设备,其特征在于,所述光信号处理模块包括激光器、激光器驱动芯片,光学探测器以及探测器驱动芯片。

6. 根据权利要求1所述的量子密钥分发设备,其特征在于,所述连接器为金手指连接器。

7. 一种量子密钥分发方法,其特征在于,应用于如权利要求1所述的量子密钥分发设备,所述量子密钥分发方法包括:

所述IC芯片确定第一随机数,以及将所述第一随机数发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作,得到量子密钥;

所述IC芯片确定与第一随机数对应的第一电平驱动信号,并将所述第一电平驱动信号发送至所述QKD处理模块;

所述QKD处理模块基于所述第一电平驱动信号,对接收到的激光光束进行调制操作,得到光信号;所述激光光束由所述光信号处理模块生成;

所述QKD处理模块将所述光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号。

8. 根据权利要求7所述的量子密钥分发方法,其特征在于,还包括:

所述IC芯片确定第二随机数,以及将所述第二随机数发送至所述外接控制设备;

所述IC芯片确定与第二随机数对应的第二电平驱动信号,并将所述第二电平驱动信号发送至所述QKD处理模块;

所述QKD处理模块基于所述第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

所述光信号处理模块对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块以及所述IC芯片发送至所述外接控制设备,以使所述外接控制设备基于所述第二随机数和所述探测结果进行QKD后处理操作,得到量子密钥。

9. 根据权利要求7所述的量子密钥分发方法,其特征在于,所述量子密钥分发设备还包括随机数处理模块;所述随机数处理模块与所述IC芯片连接;在所述IC芯片确定第一随机数之前,还包括:

所述随机数处理模块生成第一随机数,并将所述第一随机数发送至所述IC芯片。

10. 根据权利要求7所述的量子密钥分发方法,其特征在于,所述QKD处理模块为QKD光芯片模块;所述QKD光芯片模块和所述IC芯片集成在同一PCB板上。

一种量子密钥分发设备及量子密钥分发方法

技术领域

[0001] 本发明涉及量子密钥领域,更具体的说,涉及一种量子密钥分发设备及量子密钥分发方法。

背景技术

[0002] 量子密钥分发(quantum key distribution,简称QKD),是利用量子力学特性来保证通信安全性。它使通信的双方能够产生并分享一个随机的、安全的密钥,来加密和解密消息。

[0003] 量子密钥分发设备能够实现上述的量子密钥分发功能,保证了通信的安全性。但是现有的量子密钥分发设备的功耗较高,稳定性较差,使得量子密钥分发设备的可靠性较差。

发明内容

[0004] 有鉴于此,本发明提供一种量子密钥分发设备及量子密钥分发方法,以解决现有的量子密钥分发设备的功耗较高,稳定性较差,使得量子密钥分发设备的可靠性较差的问题。

[0005] 为解决上述技术问题,本发明采用了如下技术方案:

[0006] 一种量子密钥分发设备,包括:

[0007] 光纤通信模块、光信号处理模块、QKD处理模块以及IC芯片;所述光纤通信模块、所述光信号处理模块、所述IC芯片分别与所述QKD处理模块连接,所述IC芯片通过连接器与外接控制设备连接;

[0008] 所述光信号处理模块用于:生成并发送激光光束至所述QKD处理模块;

[0009] 所述QKD处理模块用于:依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号;

[0010] 所述IC芯片用于:生成与第一随机数对应的第一电平驱动信号、将所述第一电平驱动信号发送至所述QKD处理模块,以及将所述第一随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作。

[0011] 可选地,所述QKD处理模块还用于:依据接收的所述IC芯片发送的第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

[0012] 所述光信号处理模块还用于:对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块发送至所述IC芯片;

[0013] 所述IC芯片还用于:生成与第二随机数对应的第二电平驱动信号、将所述第二电平驱动信号发送至所述QKD处理模块,以及将所述第二随机数和所述探测结果发送至所述外接控制设备。

[0014] 可选地,所述量子密钥分发设备还包括随机数处理模块;所述随机数处理模块与所述IC芯片连接;

[0015] 所述随机数处理模块用于:生成第一随机数,并将所述第一随机数发送至所述IC芯片。

[0016] 可选地,所述QKD处理模块为QKD光芯片模块;所述QKD光芯片模块和所述IC芯片集成在同一PCB板上。

[0017] 可选地,所述光信号处理模块包括激光器、激光器驱动芯片,光学探测器以及探测器驱动芯片。

[0018] 可选地,所述连接器为金手指连接器。

[0019] 一种量子密钥分发方法,应用于上述的量子密钥分发设备,所述量子密钥分发方法包括:

[0020] 所述IC芯片确定第一随机数,以及将所述第一随机数发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作,得到量子密钥;

[0021] 所述IC芯片确定与第一随机数对应的第一电平驱动信号,并将所述第一电平驱动信号发送至所述QKD处理模块;

[0022] 所述QKD处理模块基于所述第一电平驱动信号,对接收到的激光光束进行调制操作,得到光信号;所述激光光束由所述光信号处理模块生成;

[0023] 所述QKD处理模块将所述光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号。

[0024] 可选地,还包括:

[0025] 所述IC芯片确定第二随机数,以及将所述第二随机数发送至所述外接控制设备;

[0026] 所述IC芯片确定与第二随机数对应的第二电平驱动信号,并将所述第二电平驱动信号发送至所述QKD处理模块;

[0027] 所述QKD处理模块基于所述第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

[0028] 所述光信号处理模块对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块以及所述IC芯片发送至所述外接控制设备,以使所述外接控制设备基于所述第二随机数和所述探测结果进行QKD后处理操作,得到量子密钥。

[0029] 可选地,所述量子密钥分发设备还包括随机数处理模块;所述随机数处理模块与所述IC芯片连接;在所述IC芯片确定第一随机数之前,还包括:

[0030] 所述随机数处理模块生成第一随机数,并将所述第一随机数发送至所述IC芯片。

[0031] 可选地,所述QKD处理模块为QKD光芯片模块;所述QKD光芯片模块和所述IC芯片集成在同一PCB板上。

[0032] 相较于现有技术,本发明具有以下有益效果:

[0033] 本发明提供了一种量子密钥分发设备及量子密钥分发方法,量子密钥分发设备包括光纤通信模块、光信号处理模块、QKD处理模块以及IC芯片;所述光纤通信模块、所述光信号处理模块、所述IC芯片分别与所述QKD光芯片模块连接,所述IC芯片通过连接器与外接控制设备连接,所述光信号处理模块生成并发送激光光束至所述QKD处理模块,所述QKD处理模块依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得

到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号,所述IC芯片还将所述随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述随机数进行QKD后处理操作。本发明中,采用QKD处理模块以及IC芯片,体积较小,相比与采用独立的光学元器件的方式,可以降低量子密钥分发设备的体积以及设备数量,进而提高量子密钥分发设备中的器件的稳定性和降低器件的功耗,提高量子密钥分发设备的可靠性。

附图说明

[0034] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据提供的附图获得其他的附图。

[0035] 图1为本发明实施例提供的一种量子密钥分发设备的结构示意图;

[0036] 图2为本发明实施例提供的另一种量子密钥分发设备的结构示意图;

[0037] 图3为本发明实施例提供的一种QKD处理模块的结构示意图;

[0038] 图4为本发明实施例提供的一种量子密钥分发设备的外观图;

[0039] 图5为本发明实施例提供的一种QKD发射端和接收端的通信示意图;

[0040] 图6为本发明实施例提供的一种量子密钥分发方法的方法流程图。

具体实施方式

[0041] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0042] 量子密码通信结合了量子物理原理和现代通信技术。量子密码通信藉由物理原理保障异地密钥协商过程和结果的安全性,与“一次一密”加密技术结合,可以实现不依赖算法复杂度的保密通信。

[0043] 目前,量子密码技术主要用光量子作为实现载体,通过自由空间或光纤信道进行分发。经典随机比特通过偏振编码、相位编码等方式加载到光量子的偏振、相位等物理量之上。现今,QKD(量子密钥分发,quantum key distribution)系统主要分为离散变量QKD和连续变量QKD系统这两类,而由于光纤通信已经成为现代信息传输的基础架构和发展趋势,在光纤信道中进行量子密码通信具有非常重要的意义和应用前景,并且设备化的QKD系统已经逐渐部署在世界各地,为政府,大众提供量子密钥分发服务。

[0044] 现有的实用化QKD系统一般包含一个发射端和一个接收端,发射端用于将密钥编码在光量子上,而接收端用于光量子的解码以及测量。但现有QKD设备依然存在着一些问题,使得其不能大规模实用化,其中最主要的问题包括设备体积较大,对于GHz重复频率的商用QKD系统,其体积一般可以达到3U机箱的大小,设备体积较大,就会导致设备中的各个器件所处的环境不同,如湿度、温度等不同,进而使得不同的器件的稳定性不统一,进而使得QKD系统功耗较大,稳定性较差,进而使得QKD系统的可靠性较差。

[0045] 其次设备成本较高,一般GHz重复频率的QKD系统单个设备价格可以达到百万以上。而发明人经过研究发现,以上的问题主要是由于现有QKD系统的光学和电子学结构均是基于分立光学元器件以及PCB电路板来实现的,这种实现方式成本较高,体积较大。

[0046] 为了解决上述问题,发明人经过研究发现,QKD光集成芯片是现今全世界非常重要的研究方向,利用该技术,可以将原本基于各个独立光器件的QKD光学系统集成在一块体积非常小的芯片中,同时为了最终实现小体积实用化的QKD系统,还需要对现有设备中的电子学部分利用大规模集成电路技术变成一颗IC芯片。进而可以降低成本,缩小体积,增加稳定性,降低功耗,进而提高可靠性。

[0047] 综上所述,按照以上设计思路,本发明提供了一种量子密钥分发设备的整体结构,利用该结构最终可以实现实用化,通用化的QKD模块,同时由于体积缩小,光路和电子学部分芯片固化,使得各个器件的环境相同,系统稳定性变强,并且在可复制,大规模生产情况下,成本有可能可以降至现有QKD设备的百分之一。

[0048] 具体的,在上述内容的基础上,本发明实施例提供了一种量子密钥分发设备,参照图1,可以包括:

[0049] 光纤通信模块11、光信号处理模块12、QKD处理模块13以及IC芯片14。

[0050] 所述光纤通信模块11、所述光信号处理模块12、所述IC芯片14分别与所述QKD处理模块13连接,所述IC芯片14通过连接器与外接控制设备连接。

[0051] 在实际应用中,参照图2,光纤通信模块与量子密钥分发设备外部通信光纤进行连接,一般为标准商用光学光纤接口,在量子密钥分发设备内部,光纤通信模块也可以通过光纤与其他设备,如QKD处理模块连接。

[0052] 所述光信号处理模块为激光器/探测器模块,根据QKD芯片所执行的QKD协议的不同,该模块中可以包含激光器以及激光器驱动芯片,光学探测器以及探测器驱动芯片,或者两者皆有。其中激光器一般为1310nm或者1550nm等通信波长的DFB激光器,或者DBR激光器。

[0053] QKD处理模块,具体可以为QKD光芯片模块。在为QKD光芯片模块时,根据模块所要运行的QKD协议,设计的一片集成光芯片,光芯片可以基于光刻工艺或者激光直写等光芯片制作工艺,在Silicon on Insulator (SOI), SiN, InP等材料制备,该芯片主要功能是对进入光芯片中的光脉冲进行量子态调制,片上一般包括特定QKD协议所需要的调制器,衰减器,探测器等结构,对于InP等三五族材料光芯片,在片上还可能集成相应的激光器结构等。典型的QKD光芯片结构,如图3所示,这里以相位编码QKDBB84协议离散变量QKD发射端和接收端系统为例,其中调制解调部分主要片上器件包括片上强度调制器,偏振调制器,相位调制器等有源器件,以及多模干涉仪(MMI),片上偏振分束器等无源器件,注意对于某些QKD协议,接收端探测器可以使用零拍探测器结构,这种结构在现有工艺下是可以在片上实现的,所以此时图3中的接收端芯片光耦合模块2是不需要的,替换成所需要的探测器结构。而对于光芯片部分,一般为了保持系统稳定,还需要在芯片附近放置电控温度控制器(TEC)以及热敏电阻等结构。

[0054] IC芯片,也称为驱动控制IC芯片:该芯片是一颗IC电子学芯片,IC芯片可以通过标准CMOS大规模集成电路工艺实现。其中结构根据模块所运行的QKD协议,一般包括模拟前端部分(运算放大器等结构),QKD芯片驱动逻辑结构部分,后处理算法部分,密钥输出接口部分等辅助QKD光芯片模块运行的各种结构。同时,以上所述的这些功能模块也可以拆分成多

个IC芯片,与QKD处理模块配合完成量子密钥分发的功能。

[0055] PCB电路板:针对模块中QKD处理模块以及驱动控制IC芯片模块等结构对应的电极布线进行相应设计,连接各个分立模块,并通过金手指连接器与上位机设备连接。

[0056] 金手指连接器:一般为标准的PCB连接接口,可通过标准通信协议实现与上位机进行通讯,传递密钥的功能。

[0057] 此外,在实际应用中,量子密钥分发设备还可以设置有随机数处理模块,所述随机数处理模块与所述IC芯片连接。随机数处理模块用于产生随机数经典比特,用于量子态的随机调制过程,该模块基于QKD系统的安全等级,可以是量子随机数芯片,经典热噪声随机数芯片,或者该芯片也可省略,替代为由驱动控制IC芯片内部产生的物理类随机数,或者软件随机数等。

[0058] 上述为量子密钥分发设备内部结构表述,上述经过外壳封装后,形成一个完整的量子密钥分发设备,其可能的外观图之一如图4所示。该模块结构根据其中QKD处理模块以及IC芯片模块的不同,可以实现包括连续变量QKD,离散变量QKD等多种QKD协议。

[0059] 上述各个模块之间的连接,可以通过标准的wire-bonding工艺或者共晶焊工艺先将各个芯片所需要外部连接的电极,连接到PCB电路板上,而PCB电路板则通过合理布线的方式,对上述芯片进行连接,使其正常工作。

[0060] 在上述结构的基础上,所述光信号处理模块用于:生成并发送激光光束至所述QKD处理模块;

[0061] 所述QKD处理模块用于:依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号;

[0062] 所述IC芯片用于:生成与第一随机数对应的第一电平驱动信号、将所述第一电平驱动信号发送至所述QKD处理模块,以及将所述第一随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作。

[0063] 在实际应用中,QKD可以实现QKD发射端,QKD接收端两种方案,或者同时实现发射端和接收端这两种功能,即QKD收发一体模块,下文中以分立的QKD发射端模块以及QKD接收端模块为例,描述具体实施方法,收发一体模块实施方法类似。

[0064] QKD发射端,接收端模块典型工作模式如图3所示,通过光纤信道,将运行同一协议的QKD发射端模块和接收端模块进行连接,使其完成量子密钥分发过程,并且结合上位机通过经典信道运行包括对基,误码估计等后处理过程,从而完成完整的量子密钥分发过程。另外,接收端和发射端的通信过程具体参照图5。

[0065] 本实施例中,量子密钥分发设备作为发射端进行介绍。具体的,QKD既可以是独立的发射端,也可以是收发一体中的发射端。且本实施例中的QKD处理模块为QKD光芯片模块;所述QKD光芯片模块和所述IC芯片集成在同一PCB板上。QKD光芯片模块的材料为SOI材料,在该材料体系下,激光器等光源是在片外的。

[0066] 具体的,所述随机数处理模块生成第一随机数,并将所述第一随机数发送至所述IC芯片。IC芯片接收到第一随机数之后,会通过金手指连接器将第一随机数发送至外接控制设备,本实施例中的外接控制设备为上位机,上位机基于该第一随机数,通过经典通讯过程完成对基、误码估计等QKD后处理过程,完成与通讯对端,即接收端的密钥协商。

[0067] IC芯片接收到第一随机数之后,除了将第一随机数发送至上位机之外,还可以生成与第一随机数对应的第一电平驱动信号,具体的,IC芯片根据运行的QKD协议制备对应的电平驱动信号,本实施例中,称为第一电平驱动信号,并将第一电平驱动信号发送至QKD处理模块。

[0068] 上述的光信号处理模块,如激光器/探测器模块,会产生激光光束,激光光束进入QKD处理模块,经过斩波、相位随机化等处理后,在QKD处理模块内部,调制装置使用第一电平驱动信号对相位随机化等处理后的光束的对应状态进行调制,得到光信号,将光信号经过衰减后,通过光纤发送至光纤通信模块中的量子光纤通道,以使光纤通信模块输出所述光信号。

[0069] 上述实施例中,QKD作为发射端,此外,QKD还可以作为接收端,具体的,假定发射端模块材料是基于SOI体系,在这种情况下,一般对于连续变量QKD系统来说,其需要的零拍探测结构是可以在芯片中实现的,但是对于一般离散变量QKD系统来说,其接收端需求的单光子探测器结构是需要放置在SOI芯片片外的,以下实施方法结合这两种情况给与实施方案说明。

[0070] 所述QKD处理模块还用于:依据接收的所述IC芯片发送的第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

[0071] 所述光信号处理模块还用于:对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块发送至所述IC芯片;

[0072] 所述IC芯片还用于:生成与第二随机数对应的第二电平驱动信号、将所述第二电平驱动信号发送至所述QKD处理模块,以及将所述第二随机数和所述探测结果发送至所述外接控制设备。

[0073] 具体的,随机数处理模块生成第二随机数,并将第二随机数输入至IC芯片中,IC芯片生成与第二随机数对应的第二电平驱动信号,具体的,IC芯片根据运行的QKD协议制备与第二随机数对应的第二电平驱动信号。IC芯片将所述第二电平驱动信号发送至所述QKD处理模块。

[0074] 此外,IC芯片通过金手指连接器将第二随机数发送至外接控制设备,如上位机。

[0075] 携带量子信息的光信号,本实施例中称为待处理光信号,经过光纤通信模块中的量子信道进入QKD处理模块,经过QKD处理模块中的调制装置基于第二电平驱动信号对待处理光信号进行解调制操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块进行探测,如激光器/探测器模块,根据协议不同,该探测器可以是片上集成的零拍探测结构或者位于激光器/探测器模块中的单光子探测器结构。

[0076] 光信号处理模块对解调信号进行探测得到探测结果,并将所述探测结果通过所述QKD处理模块发送至所述IC芯片,IC芯片通过金手指连接器发送至外接控制设备,以使外接控制设备根据上述的第二随机数,以及探测结果,通过经典通讯过程完成对基、误码估计等QKD后处理过程,完成与通讯对端,即发射端的密钥协商。

[0077] 对于其他材料的QKD光芯片实现方案,发射端和接收端实现方法类似,同样,对于收发一体的QKD模块来说,除了QKD光芯片以及IC芯片的设计结构更改之外,实施方案是以上两种实施方法的结合。

[0078] 综上所述,我们提出了一种量子密钥分发设备,利用这种方法,可以实现小型化的QKD模块,以及经典量子集成的通信模块设备,大大提高了未来QKD技术的使用场景。

[0079] 本实施例中,量子密钥分发设备包括光纤通信模块、光信号处理模块、QKD处理模块以及IC芯片;所述光纤通信模块、所述光信号处理模块、所述IC芯片分别与所述QKD光芯片模块连接,所述IC芯片通过连接器与外接控制设备连接,所述光信号处理模块生成并发送激光光束至所述QKD处理模块,所述QKD处理模块依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号,所述IC芯片还将所述随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述随机数进行QKD后处理操作。本发明中,采用QKD处理模块以及IC芯片,体积较小,相比于用独立的光学元器件的方式,可以降低量子密钥分发设备的体积以及设备数量,进而提高量子密钥分发设备中的器件的稳定性和降低器件的功耗,提高量子密钥分发设备的可靠性。

[0080] 在上述内容的基础上,本发明实施例提供了一种量子密钥分发方法,应用于上述的量子密钥分发设备,参照图6,所述量子密钥分发方法包括:

[0081] S11、所述IC芯片确定第一随机数,以及将所述第一随机数发送至所述外接控制设备,以使所述外接控制设备基于所述第一随机数进行QKD后处理操作,得到量子密钥;

[0082] S12、所述IC芯片确定与第一随机数对应的第一电平驱动信号,并将所述第一电平驱动信号发送至所述QKD处理模块;

[0083] S13、所述QKD处理模块基于所述第一电平驱动信号,对接收到的激光光束进行调制操作,得到光信号;所述激光光束由所述光信号处理模块生成;

[0084] S14、所述QKD处理模块将所述光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号。

[0085] 进一步,上述实施例QKD作为发射端,此外,QKD还可以作为接收端,此时量子密钥分发方法还可以包括:

[0086] 所述IC芯片确定第二随机数,以及将所述第二随机数发送至所述外接控制设备;

[0087] 所述IC芯片确定与第二随机数对应的第二电平驱动信号,并将所述第二电平驱动信号发送至所述QKD处理模块;

[0088] 所述QKD处理模块基于所述第二电平驱动信号,对所述光纤通信模块接收的待处理光信号进行解调操作,得到解调信号,并将所述解调信号发送至所述光信号处理模块;

[0089] 所述光信号处理模块对所述解调信号进行探测,得到探测结果,并将所述探测结果通过所述QKD处理模块以及所述IC芯片发送至所述外接控制设备,以使所述外接控制设备基于所述随机数和所述探测结果进行QKD后处理操作,得到量子密钥。

[0090] 本实施例中,量子密钥分发设备包括光纤通信模块、光信号处理模块、QKD处理模块以及IC芯片;所述光纤通信模块、所述光信号处理模块、所述IC芯片分别与所述QKD光芯片模块连接,所述IC芯片通过连接器与外接控制设备连接,所述光信号处理模块生成并发送激光光束至所述QKD处理模块,所述QKD处理模块依据接收的所述IC芯片发送的第一电平驱动信号,对接收到的激光光束进行调制,得到光信号、并将光信号通过光纤发送至所述光纤通信模块,以使所述光纤通信模块输出所述光信号,所述IC芯片还将所述随机数通过所述连接器发送至所述外接控制设备,以使所述外接控制设备基于所述随机数进行QKD后处

理操作。本发明中,采用QKD处理模块以及IC芯片,体积较小,相比与采用独立的光学元器件的方式,可以降低量子密钥分发设备的体积以及设备数量,进而提高量子密钥分发设备中的器件的稳定性和降低器件的功耗,提高量子密钥分发设备的可靠性。

[0091] 对所公开的实施例的上述说明,使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的,本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下,在其它实施例中实现。因此,本发明将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

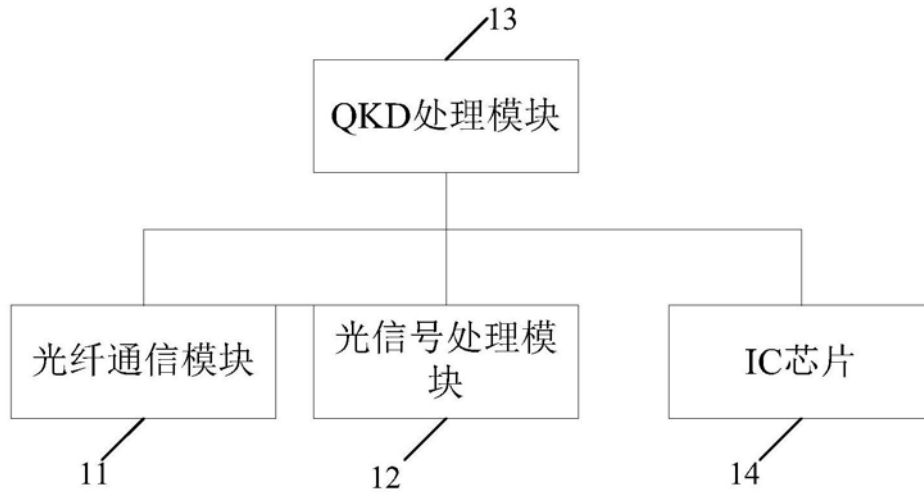


图1

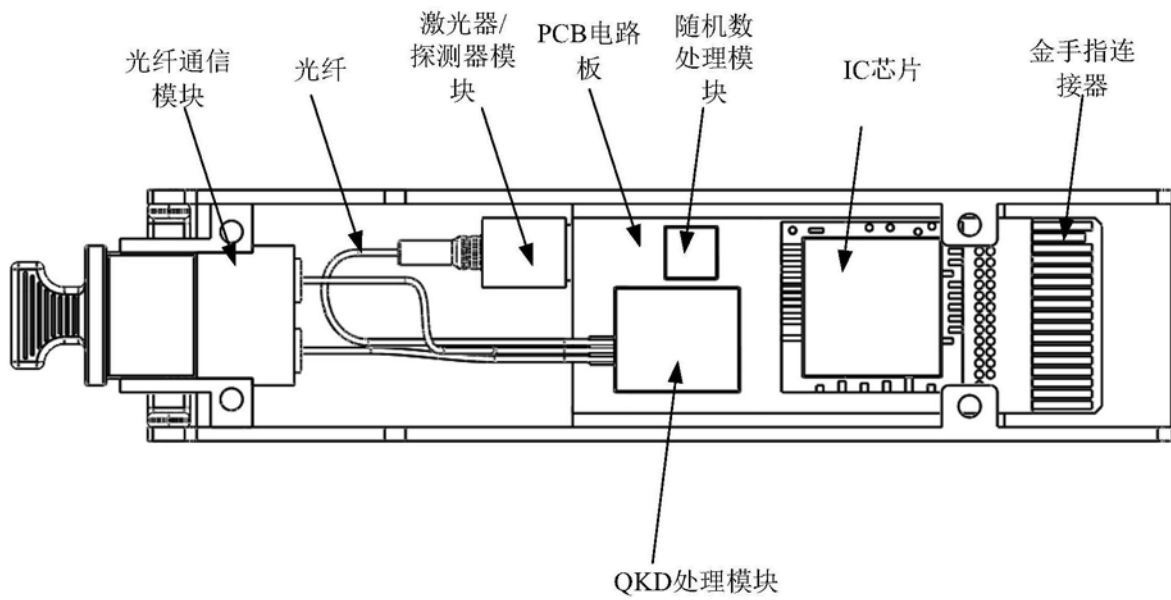


图2

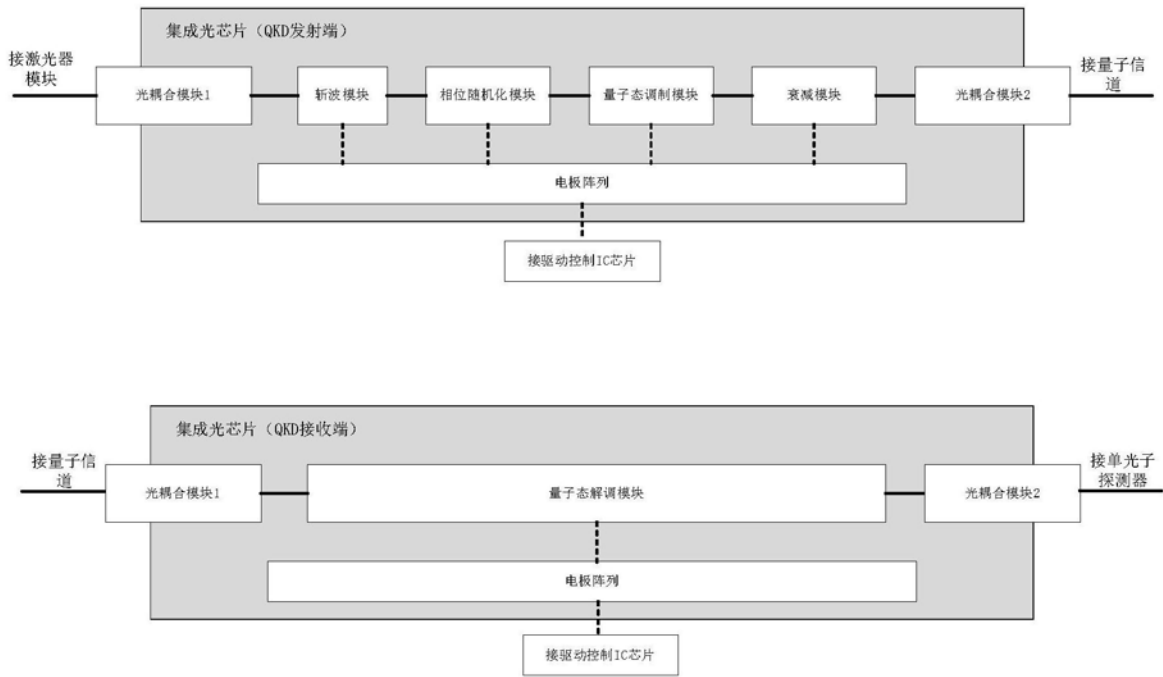


图3

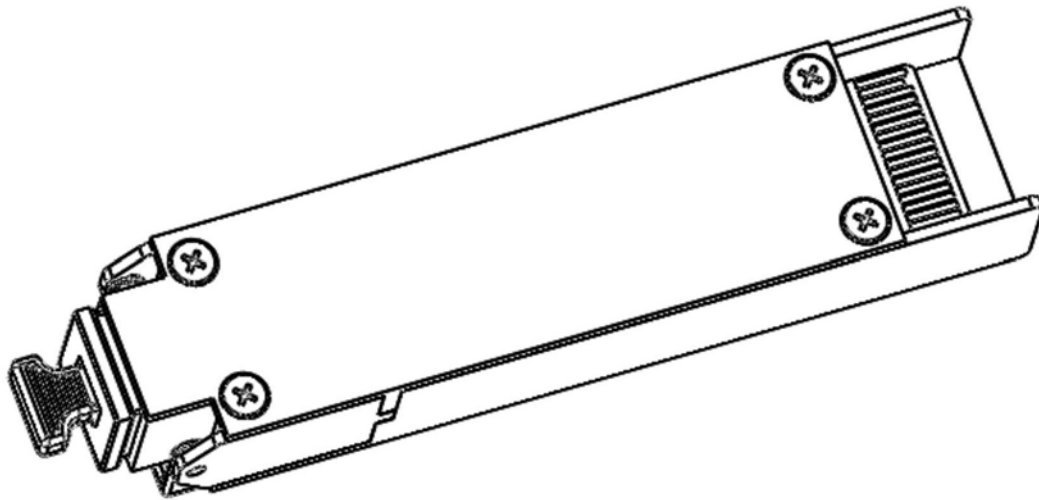


图4



图5

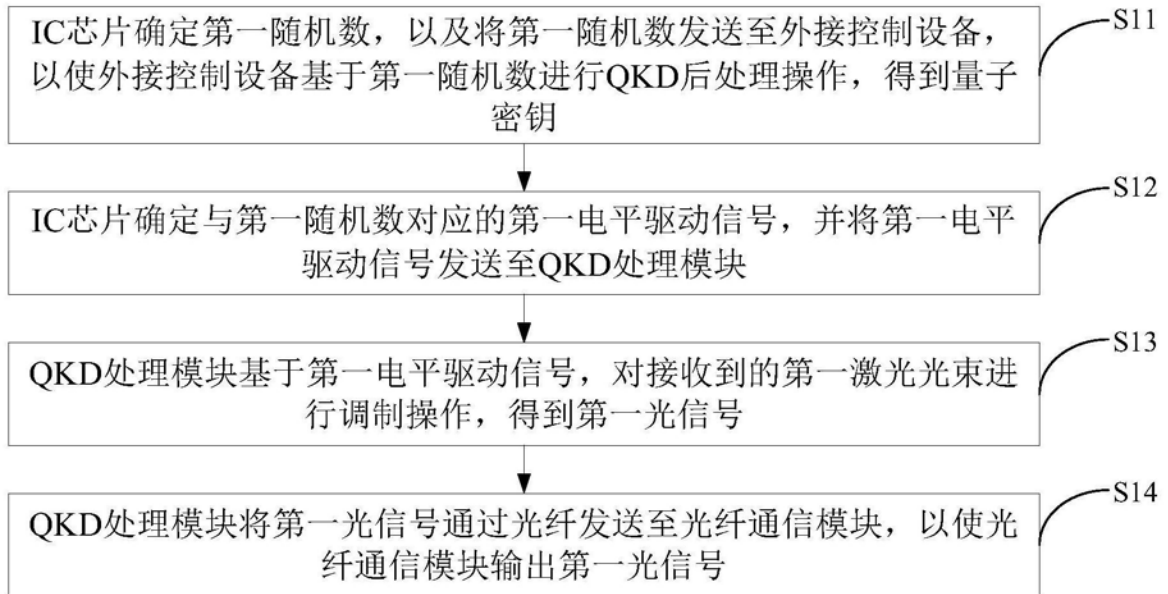


图6